AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CHINESE HACKING: IMPACT ON HUMAN RIGHTS AND COMMERCIAL RULE OF LAW

HEARING

BEFORE THE

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JUNE 25, 2013

Printed for the use of the Congressional-Executive Commission on China

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

U.S. GOVERNMENT PRINTING OFFICE

81–855 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

LEGISLATIVE BRANCH COMMISSIONERS

Senate

SHERROD BROWN, Ohio, *Chairman*
MAX BAUCUS, Montana
CARL LEVIN, Michigan
DIANNE FEINSTEIN, California
JEFF MERKLEY, Oregon

House

CHRIS SMITH, New Jersey, *Cochairman*
FRANK WOLF, Virginia
MARK MEADOWS, North Carolina
ROBERT PITTENGER, North Carolina
TIM WALZ, Minnesota
MARCY KAPTUR, Ohio
MICHAEL HONDA, California

EXECUTIVE BRANCH COMMISSIONERS

SETH D. HARRIS, Department of Labor
FRANCISCO J. SÁNCHEZ, Department of Commerce
NISHA DESAI BISWAL, U.S. Agency for International Development

LAWRENCE T. LIU, *Staff Director*
PAUL B. PROTIC, *Deputy Staff Director*

CONTENTS

STATEMENTS

	Page
Opening Statement of Hon. Sherrod Brown, a U.S. Senator from Ohio; Chairman, Congressional-Executive Commission on China	1
Smith, Hon. Christopher H., a U.S. Representative from New Jersey; Cochairman, Congressional-Executive Commission on China	3
Levin, Hon. Carl, a U.S. Senator from Michigan; Member, Congressional-Executive Commission on China	5
Pittenger, Hon. Robert, a U.S. Representative from North Carolina; Member, Congressional-Executive Commission on China	6
Meadows, Hon. Mark, a U.S. Representative from North Carolina; Member, Congressional-Executive Commission on China	1
Gorton, Hon. Slade, former U.S. Senator from Washington State; Member, Commission on the Theft of American Intellectual Property	7
Mulvenon, James, Vice-President, Intelligence Division, Director, Center for Intelligence Research and Analysis, Defense Group, Inc.	9
Wen, Yunchao (Online Alias "Bei Feng"), Independent Journalist and Blogger, Visiting Scholar, Institute for the Study of Human Rights, Columbia University	19
Greve, Louisa, Vice President for Asia, Middle East, and North Africa, and Global Programs, National Endowment for Democracy	21

APPENDIX

PREPARED STATEMENTS

Gorton, Hon. Slade	28
Mulvenon, James	29
Wen, Yunchao	38
Greve, Louisa	49
Brown, Hon. Sherrod	52
Smith, Hon. Christopher H.	53

CHINESE HACKING: IMPACT ON HUMAN RIGHTS AND COMMERCIAL RULE OF LAW

TUESDAY, JUNE 25, 2013

CONGRESSIONAL-EXECUTIVE
COMMISSION ON CHINA,
Washington, DC.

The hearing was convened, pursuant to notice, at 2:41 p.m., in room 538, Dirksen Senate Office Building, Senator Sherrod Brown, Chairman, presiding.

Also present: Senator Carl Levin; Senator Jeff Merkley; Representative Christopher Smith; Representative Robert Pittenger; and Representative Mark Meadows.

OPENING STATEMENT OF HON. SHERROD BROWN, A U.S. SENATOR FROM OHIO; CHAIRMAN, CONGRESSIONAL–EXECUTIVE COMMISSION ON CHINA

Chairman BROWN. The hearing will come to order. Thank you very much, Senator Gorton, for joining us, Cochairman Congressman Smith, and Senator Levin. I appreciate your being here, and especially your work on these issues and your legislation, which I know you will be talking about to hold China accountable for cyber theft. I thank the staff again for its tireless efforts and the work that they do on human rights and rule of law in this Commission. Congressman Smith and I have cochaired this Commission for a number of years now and appreciate the good working relationship there and with staff.

We know—and Senator Gorton and I just spoke about this—how the public is not paying a lot of attention, and we here are not paying enough attention either, with the exception of Senator Levin and a few others, to the serious threat that China poses in terms of cyber attacks and how that threatens U.S.-China relations in some ways, so much so that President Obama raised the issue during his recent summit with Chinese President Xi Jinping. It will be a key topic, we know, at the U.S.-China Strategic and Economic Dialogue to be held in Washington in a few weeks.

Today's hearing will focus on the aspects of cyber that fall within the Commission's mandate, notably the impact on the rule of law and on human rights. Recent headlines have revived the debate over the appropriate balance between security and freedom, but we cannot overlook the enormous impact that cyber attacks from China have had, and continue to have, on American jobs and American companies. They seriously call into question the Chinese commitment to the rule of law.

We are talking about massive theft of valuable technology, commercial secrets from American companies. General Alexander, Director of the NSA, calls it the greatest transfer of wealth in history. The scale and scope are staggering.

The Commission on the Theft of American Intellectual Property, which is represented here today by former colleague Senator Gorton, released a comprehensive report identifying the People's Republic of China as the world's biggest violator of intellectual property [IP] rights.

It estimates that China accounts for 50 to 80 percent of the IP theft in the United States and around the globe. It found that IP theft, including from China, costs the U.S. economy hundreds of billions of dollars a year and literally millions of jobs, dragging down our GDP and undermining our ability to innovate and to prosper.

The IP Commission noted that a 2011 study by the U.S. International Trade Commission estimated that if China's IP protection improved to a level comparable to ours it would add 2.1 million jobs to our economy, yet, the IP Commission acknowledges this figure underestimated the real cost to jobs in this country.

The victims of IP theft include companies in my home State of Ohio, in Michigan, and in New Jersey. Those affected are hardworking Americans trying to make an honest living and trying to spur innovation, only to see their products, their services, and their technology stolen and handed over to state-owned enterprises and other businesses in China.

With a growing prevalence of computer networks in America's heavily wired economy, cyber attacks represent an increasingly growing threat alongside more traditional forms of intellectual property theft. China simply does not play by the same rules as we do. The Chinese Government denies these attacks, even though there is mounting evidence of Chinese state involvement.

This evidence includes a February 2013 report by the cyber security firm Mandiant that linked attacks on 141 companies, including 115 based in the United States, to a unit of the People's Liberation Army, working from a building in Shanghai.

The increase of attacks has coincided with the Chinese Government's push for indigenous innovation and development of key industries, creating an environment where it is perfectly acceptable to cheat and steal your way to the top.

As we have seen in the last few years, it is not only American companies that are the targets, it is media and it is human rights organizations, something particularly important to Congressman Smith and me.

Journalists writing about corruption in China find their computer systems hacked and their passwords stolen.

For human rights organizations and activists, dealing with hacking attacks from China is almost a daily fact of life.

We cannot sit idly by. That is why I support a comprehensive, common sense, bipartisan approach to hold China accountable.

I urge Congress and this administration to do everything it can to combat unfair trading practices, including another topic, the important bipartisan Currency Exchange Rate Oversight Reform Act of 2013, which passed the Senate two years ago and has not yet

gone to the House. We hope to reschedule it for a vote soon. I commend Senator Levin for his recent proposed legislation to hold China accountable for cyber theft.

I will turn it over to Cochairman Smith. I have a vote at 2:45, as does Carl, but I think we will be able to keep this going.

STATEMENT OF HON. CHRISTOPHER SMITH, A U.S. REPRESENTATIVE FROM NEW JERSEY; COCHAIRMAN, CONGRESSIONAL–EXECUTIVE COMMISSION ON CHINA

Representative SMITH. Thank you very much, Chairman Brown. Thank you for calling this extraordinarily important hearing.

In December 2006, and then again in March 2007, my Human Rights Subcommittee, the committee that I chaired, as well as the personal computers in my office, that of my chief of staff and myself, were attacked by a virus that, in the U.S. House Information Resource Office's words, "intended to take control of our computers."

At that time the IT professionals cleaned the computers and informed my staff that the attacks seemed to come from the People's Republic of China. They said it came through, or from, a Chinese IP address. The attackers hacked into files related to China. They contain legislative proposals directly related to Beijing, including a major bill that I was in the process of authoring called the Global Online Freedom Act.

Also hacked were emails with human rights groups regarding strategy, information on hearings that I intended to chair on China, and the names of Chinese dissidents. While this absolutely does not prove that Beijing was behind the attack, it raises very serious concerns that it was. Certainly Chinese agents have not only attempted to target me or my offices, but many other Members of the House and Senate have also been the victim of that kind of attack.

Cyber attacks on Congress are only a small, but not insignificant, part of a much larger pattern of attacks that have targeted the executive branch, the Pentagon, and American businesses.

How do we know this? In recent months we have seen in-depth reports come out detailing this massive intrusion into our cyberspace and massive theft of our cyber data. Chinese agents have stolen our designs for helicopters, ships, fighter jets, and several missile defense systems.

They have stolen our innovative technologies, from solar panel designs to biotech research. These thefts appear to have paid off for China. In recent years, the Chinese Government has made tremendous jumps in its military capabilities, while boosting the competitiveness of China's "national champions."

While cyber thefts have existed for years, increasingly we can prove that many of these outrageous thefts deemed "the greatest transfer of wealth in history" originate in the People's Republic of China, and these attacks are not random. We now know with some certainty that some thefts are being organized by the Chinese Government agencies.

As we learn about the sources of these attacks and we are learning about their motivations, talented Chinese Internet users are working day and night to infiltrate our networks and to steal se-

crets. Chinese actions are part of the larger coordinated state-sanctioned effort to increase China's competitiveness militarily as well as commercially.

Today we will hear about how the commercial rule of law system in China allows these types of attacks to occur and how these attacks disadvantage American businesses, innovators, contractors, and government agencies. We will hear about the size and scope of the attacks and we will hear how the U.S. Government remains largely unprepared for many of these challenges.

We will also, however, hear about another side of this important topic, one that is often overlooked during recent discussions about China's cyber attacks. The Chinese Government is not only targeting American businesses and military organizations, but it is also targeting ordinary Chinese citizens seeking to advance their most fundamental freedoms.

Chinese hackers do not simply look beyond their borders to steal secrets. As we will hear today, Chinese citizens, including those advocating freedom and rights, free speech, and food safety, are also targeted by state-sponsored hackers.

These courageous citizens are also monitored, their private information stolen. The brave pastors seeking to organize a service, the father seeking to raise awareness about toxic foods, the wife of an imprisoned activist, the mother who was made to undergo a forced abortion, all of these citizens realize that in any instance the government may, and probably is, watching. China, of course, also targets those outside of China who similarly wish and promote human rights and political reform.

Today we know the system of surveillance and theft occurs. We know that China is organizing these cyber attacks, or at the very least is complicit in their existence. The question we must ask ourselves is why. Clearly China's rise as a military power requires technology. China's economy will no doubt benefit from the latest innovations from abroad.

But why is China so obsessed, so concerned about its domestic citizenry, especially those who advocate peacefully for legal and political reforms? Why is China so worried about international NGOs [non-governmental organizations] that seek to highlight official abuses and wrongful imprisonments?

Why is China so reluctant to provide a fair regulatory environment in China where commercial laws and regulations will eventually protect all businesses, domestic and foreign, seeking to provide the best services for these Chinese consumers?

These may be difficult questions, but thankfully today we are fortunate to have four guests, four witnesses who are well versed on these issues. They are expert on how China is monitoring our cyber actions and how China is attacking targets globally.

I do want to point out that I will have to leave, but I will read their testimonies. I am chairing a hearing at 3 o'clock over on the House side on the attack and the slaughter of Christians in Syria. It begins at 3 o'clock so I will have to leave, but I want to convey to our witnesses my sincere gratitude for your testimonies. I look forward to reading them and for the insight you provide.

I yield back, and yield to Senator Levin.

STATEMENT OF HON. CARL LEVIN, A U.S. SENATOR FROM MICHIGAN; MEMBER, CONGRESSIONAL–EXECUTIVE COMMISSION ON CHINA

Senator LEVIN. Thank you very much, Congressman Smith. First of all, I want to thank you and Senator Brown for organizing this very important hearing on Chinese hacking and its impact on human rights and on commercial rule of law.

The hearing is timely. It is timely for many reasons. There have been many recent reports and indisputable evidence of large-scale cyber intrusions by the Government of China on a vast number of private, government, and nonprofit entities for the purpose of stealing valuable intellectual property or proprietary information. This is in addition to what is also well known, that China hacks the accounts of human rights activists in order to suppress human rights in China.

American companies invest hundreds of billions of dollars every year in research and development. That innovation results from those investments. The innovation drives investments and drives, in turn, the growth of American companies and the U.S. economy.

Unfortunately, our companies are having their intellectual property stolen and it is stolen right out from underneath them through cyberspace. Such theft threatens to undermine America's global competitiveness.

Both U.S. Government and private reports point to China as by far the worst offender. As far back as 2011, the National Counter Intelligence Executive said in its annual report to Congress that "Chinese actors are the world's most active and persistent perpetrators of economic espionage."

This May, the U.S. Trade Representative stated in its Special 301 report that "obtaining effective enforcement of IPR in China remains a central challenge, as it has been for many years." The report continued that "this situation has been made worse by cyber theft, as information suggests that actors located in China have been engaged in sophisticated, targeted efforts to steal intellectual property from U.S. corporate systems."

Today we will be hearing from Senator Slade Gorton, an old friend of mine, who is on the Commission on the Theft of American Intellectual Property. That report is just further powerful evidence of what the problem is. So, it is long overdue that we equip the American Government with the tools that it needs to fight back.

I recently introduced Senate bill 884, the Detect Cyber Theft Act, with Senators McCain, Rockefeller, and Coburn. S. 884 requires the Director of National Intelligence to produce a report that includes a watchlist, and a priority watchlist, of foreign countries that engage in economic or industrial espionage against the United States in cyberspace.

The bill also requires the President—and this is the action forcing mechanism and the remedy—if he determines that such action is warranted for the enforcement of intellectual property rights or to protect the Department of Defense supply chain, to block imports of goods in three categories: First, goods made with U.S. technology or proprietary information stolen in cyberspace; second, goods made by companies that engage in or benefit from such theft;

and third, goods produced by state-owned enterprises in countries designated as the worst cyber thieves.

This is a powerful remedy. It is hitting countries that engage in cyber theft in the pocketbook and it is time that we fight back to protect American businesses and American innovation. We have to call out those who are responsible for cyber theft and empower the President to hit the thieves where it hurts most, in their wallets.

Dennis Blair, former Director of National Intelligence and Co-Chair of the IP Commission report said recently, "Jaw-boning alone won't work. Something has to change China's calculus." Well, we think our bill will do exactly that. Blocking imports of products that either incorporate intellectual property stolen from U.S. companies or are from companies otherwise that benefit from cyber theft will send the message that we have had enough.

If foreign governments like the Chinese Government want to continue to deny their involvement in cyber theft despite the overwhelming proof that is one thing. We cannot stop Chinese denials. But we are not without remedies. We can prevent the companies that benefit from the theft, including state-owned companies, from getting away with it.

Maybe once they understand that complicity will cost them access to the U.S. market, they are going to press their governments to end it. We have sent our bill to the administration. We await word from the White House and from the administration.

Hopefully the word will be one of support. We have stood by for far too long while our intellectual property and proprietary information is plundered in cyberspace and used to undercut the very companies that developed it. In other words, it is time to act.

I want to thank everybody who is a part of the effort to stop cyber theft for their efforts, many of whom are going to be testifying here today. Again, I want to thank our commission and our staff for all the great work that they are doing on this subject.

Thank you. I have to leave for a vote too, so I will yield to whoever is next in line.

STATEMENT OF HON. ROBERT PITTENGER, A U.S. REPRESENTATIVE FROM NORTH CAROLINA; MEMBER, CONGRESSIONAL–EXECUTIVE COMMISSION ON CHINA

Representative PITTENGER. Thank you, Senator Levin. It is a privilege to serve with you on this important commission. I am Congressman Robert Pittenger. I am a new commissioner on this important effort. I do want to thank Chairman Brown and Cochairman Smith for leading this commission.

The issue of human rights and the rule of law in China have been of great importance to me my entire adult life. These are issues I have been dedicated to since I graduated from college and spent 10 years in service with Campus Crusade for Christ.

Chinese hacking is hurting the attempts by the people of China to advance their own human rights. Dedicated heroes are being subjected to relentless cyber attacks as they try to use the Internet to break the silence on continued persecutions of Chinese citizens.

Allowing for freedom of expression via the Internet will be critical to advancing human rights in China. This will only happen if the cyber attacks cease to exist. Ironically, in light of the reported

issues related to corruption within China, individuals who are people of faith provide the best resources and assets for the continuation and the strength of the Chinese economy.

Cyber attacks by the Chinese Government have a significant impact, both here at home as well as on the citizens of China. American businesses have been affected by these cyber attacks to the tune of hundreds of billions of dollars.

As the Chinese Government is propping up national companies, it is doing so on the backs of American companies playing by the rules. The Chinese Government is responsible for 50 to 80 percent of global theft of intellectual property, hurting American businesses and costing American jobs.

The United States must remain committed to monitoring the continued violation of the rule of law by the Chinese Government, not just to protect American jobs but to help stand with those committed to ending the persecution of Chinese citizens for practicing their religious beliefs.

I yield to my fellow Congressman.

STATEMENT OF HON. MARK MEADOWS, A U.S. REPRESENTATIVE FROM NORTH CAROLINA; MEMBER, CONGRESSIONAL–EXECUTIVE COMMISSION ON CHINA

Representative MEADOWS. Thank you, Mr. Pittenger. Thank you both for coming today and for your willingness to testify. I will keep this real brief so you can go ahead and share what you have for us. Most of what I have come to know has already been mentioned a number of times, but obviously in a global economy what we have to look at is the rule of law and the impacts that it has, either the respect for that or the lack of respect in what it does.

So I have been fortunate enough to meet with a number of different people, both from the Chinese Government and also those that trade with our largest trading partner. In doing that, I think coming to real grips with a substantive way to address this problem is what we are all looking for. We cannot tolerate what we would not stand in our own backyard, and we have got to make sure that we address that, both from a policy standpoint and from a legislative standpoint.

So with that I will yield to you, Mr. Gorton, and let you start off. Thank you.

STATEMENT OF HON. SLADE GORTON, FORMER U.S. SENATOR FROM WASHINGTON STATE; MEMBER, COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY

Senator GORTON. Chairman Brown not only summarized the report, but he summarized my opening statement which simply adds to the fact that when I was on your side of the bench I always wondered about people reading written statements that I already had, whether they were implying that I was illiterate. I will not insult you by any means in that fashion. I want to make only two or three of the major points of this commission report, which we have given copies to your staff and have more if you wish it.

The first, is we have found ourselves sailing in uncharted seas. There were no other former commissions that had looked into this problem in the past. I think we did a good deal of fairly original

research to try to bring together both the scope and the breadth of intellectual property theft around the world.

I think our conclusions are pretty cautious. We use a figure of over $300 billion a year. Personally, I think it is higher than that. That is what we could absolutely all be totally comfortable with. Fifty to eighty percent of it coming out of China is also a statement. We are quite confident, but we hope this will lead to more study, particularly on your part, of an important way in which our economy is being harmed.

One example is on page 12. A software company, that we will not name, sold a single program in China for, say, roughly a hundred bucks. When there was an update on it, they got 30 million calls. One to 30 million. This may be the single most dramatic example we have but it is far from the only one.

So what we have done is to try to gather together the nature of the problem, where it comes from, and set up policy responses that the Congress and the administration can come up with that, to a certain extent, cures it.

Senator Levin's bill is totally consistent with the recommendations that we make here because he gets to the central point, we will not really get command over this kind of intellectual theft in China until we have created internal incentives within China for abiding by rules with respect to intellectual property.

At this point it is free theft. There are no consequences of doing so. The way to create that internal desire to do something better is to punish Chinese businesses and our government, which are making money out of doing it today.

We have a large number of recommendations, some for Congress and some for the administration itself. Bluntly, I would say that if you did every one of them we would have started down the road but we would not have gotten all the way down the road to an honest and straightforward relationship.

So on the very last page of the Commission report there are three subjects that came up during our deliberations which are not our formal recommendations but which are nevertheless ideas that we think you ought to consider. Each of them, I can say, is more radical than the formal recommendations of the Commission itself. But one is to allow cyber counter-attacks on the part of American interests that are hit by cyber attacks at the present time, something prohibited by the law at the present time.

A second one has to do with requiring the United Nations World Health Organization to certify that when we give them things they are not going to be immediately stolen from them. Those two came from outside the Commission.

The third was one on which I testified before a different Commission some time ago, and that is simply to say that every year the Secretary of Commerce will determine the losses we have talked about in here from all forms of intellectual property theft and that we there, for the next year, impose a tariff on all goods coming from China designed to produce 150 percent of that figure.

I do not think we would get very much money from that but I think we would get action for the protection of our intellectual properties. In fact, it would violate the WTO [World Trade Organization] rules, but China cannot win a trade war against the United

States because of the huge amount of its trade surplus with us. It will also create within China itself a view that they ought to abide by the same rules that the rest of the world abides by.

I will make only one final comment. When I look back on 18 years in this body I think the single vote I most regret is permanent MFN [most-favored-nation status] for China. We gave up an ability to affect their policies by doing so and I wish I had that vote back over again.

Chairman BROWN. Thank you, Senator Gorton, very much.

Thank you, Congressman Pittenger for being here, Congressman Meadows, thank you. I know how, during the PNTR [permanent normal trade relations] with China, I was in the House and I remember working with the North Carolina delegation especially.

Let me just properly introduce both, then Dr. Mulvenon, we will turn to you. Senator Gorton served 18 years in the Senate, a distinguished member of the Appropriations Committee when it was a different sort of committee than now, I would editorialize, and he was on the 9/11 Commission after leaving the Senate. He is here representing the Commission on the Theft of American Intellectual Property and has been a real leader on the bipartisan initiative chaired by Governor Huntsman and Admiral Blair. So, thank you for your testimony.

Dr. Mulvenon is vice president of Defense Group, Inc.'s Intelligence Division, director of DGI's Center for Intelligence Research and Analysis. He runs teams of nearly 40 cleared Chinese, Russian, Arabic, Pashto, Erdu, and Farsi linguist-analysts performing open-source research for the U.S. Government. Thank you for joining us. He is also the author of "Chinese Industrial Espionage" and knows this issue very well.

Dr. Mulvenon, thank you.

[The prepared statement of Senator Gorton appears in the appendix.]

STATEMENT OF JAMES MULVENON, VICE PRESIDENT, INTELLIGENCE DIVISION, DIRECTOR, CENTER FOR INTELLIGENCE RESEARCH AND ANALYSIS, DEFENSE GROUP, INC.

Mr. MULVENON. Thank you, sir. I would like to thank the Commission and I would also like to thank its excellent staff with whom I have worked for many years on some important and tractable problems, particularly on this issue.

I bring a lot of perspectives to this issue, one being a Chinese linguist. As you said, 20 years of building teams of cleared linguist analysts doing open-source research for the U.S. Government, particularly on cyber issues, as early as the late 1990s, working on Chinese Internet censorship issues with this commission, and then finally the perspective of being a victim of these attacks given my own profile and my own writings and trying to expel Chinese attackers from the ramparts of my own corporate networks on a daily basis.

We talked a lot in the last six or nine months about Chinese cyber espionage. I would say that it is a multi-faceted issue and there is not a one-size-fits-all answer to it. I would just like to highlight quickly five different areas of cyber espionage which are different in form and require slightly different strategies, and I

think it is important for us to not treat it as a monolith but to break it down into pieces.

The first category, frankly, is the traditional government/military classified defense contractor espionage. We have very few options in this case. Countries will always spy on one another. We cannot legislate against espionage, we cannot impose treaties against espionage, but it is important to note that at least since 1996 I personally have watched Chinese intelligence preparation of the battlefield with regard to a Taiwan contingency, monitoring U.S. military asset movements, getting into unclassified Pentagon networks to be able to get into logistics databases, providing, now, strategic near real-time intelligence to Chinese leaders about our dialogues with them, stealing the talking points of our various meetings, and frankly getting into a lot of classified defense contractor companies, stealing critical classified technology about our newest weapons systems and then using that information to fine tune their own defensive systems and their offensive systems.

In each of those three cases, they have almost immediate benefit from stealing that information, being able to immediately operationalize it.

On the commercial espionage side it is a little bit more complicated. On the one hand, we have what we call sensitive business information. So you break into the sea suite of a major Western oil company, you steal the dollar number of what they are going to bid on a tract in the South China Sea, you hand it to your national offshore oil company, they bid $100 over that and they win the bid. So there is an immediate benefit. But the one that has been thorny to us, analytically at least within the system, has been this issue of intellectual property rights.

One, a lot of companies do not self-report the intrusions so we do not really have as much data as we would like, particularly data that shows us intrusions that steal intellectual property, that has been exfiltrated back to China, that is then given to a national champion in that sector who then is successfully able to reverse engineer it, who can then productize it, marketize it, and then show a demonstrable, quantifiable loss of U.S. company market share in China and then when they compete with them globally.

There are actually very few cases where we have enough data to make that change. It primarily is because there are not really the guidelines for many of these companies to self-report those problems.

The Securities and Exchange Commission has tightened up some of their guidelines about reporting loss of shareholder value, but many of the companies I deal with feel that they are not properly indemnified from reporting that so in many ways many of them are looking to Congress for legislation that will provide them with the indemnification that they need to share information with the government without antitrust problems, or to even collude with one another and share intrusion data with one another so they can engage in collective defense without legal jeopardy.

Now, we have begun to talk to the Chinese in a much more serious fashion about these issues, particularly in the last six months. I think the President at Sunnylands struck the right top-level tone with President Xi by pointing out the following fact, not to educate

them about whether this is happening, we are not going to insult their intelligence about that, but to point out that the real strong pillar in favor of cooperative Sino-U.S. relations, particularly past the PNTR era, has been the business and trade community.

Yet, that is the community that you hear now the most complaining about how they cannot make money in China, how the Chinese Government has its thumb on the regulatory scale favoring national champions, and how the rampant cyber espionage is actually reducing their competitiveness and stealing their core technologies.

And so to emphasize to President Xi as we are to senior Chinese leaders that this fundamentally threatens the bilateral trade relationship, which fundamentally threatens China's overall economic development, which therefore threatens their social stability, which is the number-one priority of the Chinese Government.

That is the message that is getting through to the top leadership and hopefully will incentivize them, along with a whole range of other measures that we are contemplating—naming and shaming, denied entities list, and all sorts of other measures we have—against Chinese companies and universities engaged in this behavior, that I think together could possibly stem the tide on this behavior which is, frankly, draining the American innovation economy.

[The prepared statement of Mr. Mulvenon appears in the appendix.]

Chairman BROWN. Thank you very much, Dr. Mulvenon. Those companies you mentioned that are now complaining are the same companies that really did the heavy lifting to push PNTR through the U.S. Senate and the U.S. House of Representatives and have sort of played this bangle a lot of ways. But more on that later, perhaps.

Let me start with Dr. Mulvenon on this question. I spend a lot of my time—my State makes more things, more products in terms of net worth than any State but California and Texas, States much larger, from aerospace, to autos, to food processing, to chemicals, to all kinds of things, wind turbines, solar panels. I spend a lot of time on shop floors. What you notice is that in terms of innovation, product innovation and process innovation so often take place on the shop floor.

So when U.S. companies do the innovation in California, as Apple brags about often, or in Ohio, or anywhere else, or North Carolina, and then the production is done overseas, automatically that innovation is happening on those shop floors in terms of process and product both.

How did this theft work beyond that? Talk that through, how that sort of exacerbates or enhances the opportunities these companies have for that kind of intellectual property theft when they do it from cyber attacks here, when they do it when our companies are actually overseas, producing overseas, if you would discuss that.

Mr. MULVENON. I think first it is important to note why this is happening. For the first 25 years of Chinese economic modernization, in my view, China was content. We have all seen the dramatic numbers, the covers of the magazines, everything that emphasizes the tremendous gains that they have made.

But it was a very shallow modernization because there were enclaves in China, we would send our components over there, they would get reassembled and then re-exported out.

In roughly the early 2000s, the Chinese Government looked at this issue and they said this is not the kind of deep economic modernization we want. We do not really feel that it is developing the national champions.

We are not innovating within China, we are simply assembling other people's stuff and re-exporting it. So in roughly the 2005–2006 time frame, they came up with this idea of indigenous innovation that was mentioned earlier and they put out a large number of state policies, the 2006–2020 Medium- to Long-Range S&T Plan, and they tried to emphasize that this was going to be a large-scale government effort, multi-billions of dollars.

What they discovered, however, was state-driven R&D is an oxymoron, akin to jumbo shrimp and military intelligence. That is not how innovation happens and so they were failing in some key sectors to be able to do that. The only place they could turn, if they could not squeeze it out of the multinationals by forcing them to build R&D labs in China, if they could not squeeze the tech transfer out of the companies that were competing for market share and being increasingly forced by regulatory ministries who were partnered with those national champion companies to squeeze that technology transfer out, the remaining option that they had, frankly, was to steal it.

Unlike 20 years earlier where you would have had to physically steal it from a plant, you would have had to smuggle the blueprints out of the shop, you would have had to take the part and run out the door with it, unfortunately our move toward connectivity and putting all this information online allowed them to steal that at great distances.

So that would not have been true in a pre-Internet era, but unfortunately now many companies, for a lot of reasonable reasons, have been putting all that information online and unfortunately that made it all that much easier for people to steal it from them, particularly China.

Chairman BROWN. Thank you. That was very helpful.

Senator Gorton, talk about your experience and your report and give us thoughts on, including Senator Levin's legislation, what you think we should do in this body and in the House of Representatives.

Senator GORTON. Well, Dr. Mulvenon put it quite correctly when he said we are half-blind at least in determining how much it really is and what is going on because lots of companies either see no point in saying that they have been stolen from or think that it would make it worse, or that they would lose what markets they have in China.

So I would say one of the first things that you want to do is to see to it that there is one department, one office in the United States that is in charge of finding out the total scope of the problem, all of the various elements that the doctor has spoken about, so that you as the policymakers know how big the problem is.

As I say, we have given you a conservative estimate. I think that estimate is low. But to a certain extent, I am just guessing on that.

We need to know what is going on and no one is really in charge of this at the present time. But from the point of view of the cure, the cure is, again, as I think Senator Levin has at the heart of his bill, the cure is in creating internal lobbyists in China for obeying the law.

There has got to be a group there that will say, "We will be better off if we follow a fair set of rules than we are now." There is no one there who says that now because it simply is not true. Stealing our intellectual property is very largely risk free.

But tying up the U.S. market, which is so important to them in one respect or another, will be very important in creating a group in China that will say yes rather than simply smile and nod their heads and go ahead down the same road.

This is not a new problem. We were concerned about this a decade ago, and even more than a decade ago, but the Chinese economy has changed, its desires have changed and it is becoming worse, not better.

Chairman BROWN. Senator Gorton, is Chinese cyber theft a greater threat to our national security or to our economic security?

Senator GORTON. Well, I really will defer to Dr. Mulvenon on that. It is a major threat to our national security. Even the solutions that I have suggested and that Senator Levin has suggested only indirectly get at that. How you value in dollars the loss of intellectual property that is important to our national defense is not easy to determine and the degree to which you can punish them directly for that is hard to determine.

But at one level, at least, that is the most important challenge, the challenge to our national security. But the challenge that may have cost us 2 million jobs or more is a major challenge and something that we should be attempting to cure right now.

Chairman BROWN. Thank you.

Dr. Mulvenon, would you like to comment?

Mr. MULVENON. I do not think you can dissemble the two. They are inextricably linked. The Chinese see them as inextricably linked and we should as well. In other words, any decline in our economic security, any decline in our technological competitiveness has an automatic implication for a decline in our national security.

Similarly, a decline in our national security with respect to the Chinese impacts our ability to enforce fairness on the Chinese side with regard to economic competitiveness, so for me they are pieces of a part.

The Chinese themselves write about their own comprehensive national power in a way that does not even make the distinction between the two, so again, talking to senior Chinese leaders about their impact on economic development, they will automatically see the connection to their own national security and the defense of their own country, as we should as well.

So I do not think anything is to be gained by separating the issues. In fact, I think we have a greater power to influence them by connecting them together and not allowing them to be treated separately.

Chairman BROWN. Congressman Pittenger?

Representative PITTENGER. Thank you, Mr. Chairman.

Dr. Mulvenon, as we look at the collaborative efforts among government agencies to address cyber, how are we doing, with DHS, the FBI, the U.S. Trade Representative and others? Are we working well together? Is there anything we could do to improve that?

Mr. MULVENON. Well, we have some very important and difficult seams, if you will, in the system that continue to bedevil the way we do things. In other countries that do not have our particular legal and bureaucratic system frankly have us at an advantage.

But the struggle between, for instance, domestic cyber security under DHS and where that boundary line is between that and foreign cyber security with respect to cyber at NSA, continues to be a point of friction. I will tell you, I have read multiple internal Chinese military sources in which they talk about exploiting those seams, exploiting those jurisdictional issues for their own advantage.

I will give you one example. As early as 1996, internal Chinese military sources were talking about how they wanted to delay or disrupt our logistics deployment to a Taiwan contingency by disrupting the Pentagon's unclassified logistics computer systems.

But they said quite pointedly that they would initiate that attack from within the continental United States, knowing that that would activate a different bureaucracy, namely the FBI, and not the NSA and other people who would see it as a foreign intelligence operation, and in that window of us frankly being screwed up and not knowing what was going on, they would be able to seize that strategic advantage. So I do not think we are doing well on that front in particular, and I think even our adversaries are well aware of it.

Representative PITTENGER. Given that understanding, I am not trying to get you out of your box in terms of your focus, but how would you remedy that?

Mr. MULVENON. Well, to be honest, at many levels it is an indemnification issue because there are a lot of companies around the world that believe that there is sovereignty in cyberspace.

In other words, that nations have boundaries and that those boundaries can be protected. We alone have been arguing for sort of an Internet freedom model that is sort of boundary-less.

For the Chinese, the Russians, the Iranians, all they talk about is sovereignty. They are frankly more Westphalian than we are in many of these issues with regard to cyberspace.

At the end of the day, we have to recognize that in fact our best assets for defending the country on the cyber side are the ones that are precluded from operating within the domestic United States.

I realize that this may not be the best time to raise that issue given the news of the day, but ultimately we want to have our best capabilities in terms of defending the Nation and those capabilities often reside with organizations within the U.S. system that are not currently authorized to fully exercise those within the United States. So the only way that is going to get solved is to give people top cover at the Title 10, Title 50 level that does not currently exist.

Representative PITTENGER. Thank you.

Senator Gorton, thank you again for your tremendous perception on this issue. You believe as I do in free and fair markets, other

realistic market leverages that we have remaining today to try to stop the Chinese from the continued, what we believe is cheating, and continued theft of intellectual property.

Senator GORTON. The leverage we have is our market, the fact that we have purchased far more from Chinese sources than they purchased for us. That is a tremendous leverage and in my view it is the highest leverage we have. By threatening that market in a straightforward fashion, we will at least get them to begin to hear about what our concerns are and have to respond to them.

Representative PITTENGER. You said that American companies do not want to be public as much in coming out that they have been the recipient of cyber, what role still do they have in protecting themselves?

Senator GORTON. Well, they have a tremendous role in protecting themselves. But I think one of the reasons that many of them are reluctant to talk publicly about it or to come to the government about it is they do not think anything is going to get done in any event. If we show the government that we are serious about the question I think we will get more cooperation from the private sector.

Representative PITTENGER. Do you see a public/private partnership then?

Senator GORTON. Of course it is. The fundamental defense of the United States is a public responsibility.

Representative PITTENGER. Yes. Sure.

Senator GORTON. But obviously every company wants to protect its own intellectual property and its markets.

Representative PITTENGER. Sure. Thank you.

Chairman BROWN. Mr. Meadows? Thank you, Mr. Pittenger.

Representative MEADOWS. Thank you, Mr. Chairman. I can see, Doctor, you wanted to go ahead and make a comment on that last question, so go ahead.

Mr. MULVENON. Well, I think, frankly, this body has an important role to play because in the absence of strong government intervention on this issue I am sure many of you have seen the rise of certain companies that are now advertising as part of their services that they themselves will engage in aggressive defensive measures, shall we say, or even hack back on behalf of companies in the absence of the perception that the U.S. Government is going to do anything to help them.

When I testified before the Huntsman-Blair Commission, we had a lengthy discussion about some of the outdated features of the 1986 Computer Fraud and Abuse Act and the fact that, frankly, many companies right now are looking to Congress for clarification, and frankly the Department of Justice, as to where the legal boundaries are on this issue about hack back and being able to aggressively go after your own intellectual property.

That act is 27 years old. I believe that many features of it are outdated and have been rendered obsolete by technology, and I think it really needs to be revisited. That was certainly one of the most interesting debates we had in the Commission hearing that I testified at.

Representative MEADOWS. So as we look at the Commission, I think, Senator, your comments were that this will get us down the

road but it will not get us all the way. Again, I may be paraphrasing there, but how far down the road does it get us? I mean, is this a marathon of which we have gone one mile, are we doing a half marathon? I need to realize how far down the road we are going.

Senator GORTON. Well, I think it is a marathon at which we are still at the starting line.

Representative MEADOWS. But you were talking about, if all your recommendations are implemented.

Senator GORTON. I do not think I can quantify that, except that I think it would be significant. It will be significant to exactly the extent that we have begun to create, within China itself, an interest group that is in favor of the protection of intellectual property rights.

Representative MEADOWS. So how do we do that? How do we create within China this interest or this respect for the rule of law, because we see that in so many areas where there is not that? So how do we do that?

Senator GORTON. By threatening the profitability of those Chinese companies, both public and private, that sell large amounts of their goods and products in the United States.

Representative MEADOWS. All right. So you used the word "threat." I do not ever bluff, so let me ask you this. When does threaten and when does consequences to actions—because too many times we threaten without resolve. I guess what I am asking——

Senator GORTON. Congressman, I agree with you. Do not threaten unless you are willing to carry it out.

Representative MEADOWS. Exactly. So what you are saying is to have real consequences that we are committed to, regardless of the circumstances of implementing.

Senator GORTON. Yes.

Representative MEADOWS. All right.

Would you agree with that, Doctor?

Mr. MULVENON. Well, first of all I would say, as a matter of principle, China and the Chinese economy and the Chinese Government will respect intellectual property when they have their own intellectual property to defend.

Representative MEADOWS. I agree.

Mr. MULVENON. I mean, one of the real dilemmas we have is I know that talking about patent trolling is very popular these days.

Representative MEADOWS. Right.

Mr. MULVENON. I see a tremendous upswing in patent trolling in China. In other words, Chinese doing patents of things that are registered with their own Patent and Trademark Office and then attempting to sue or coerce American companies that are in China by claiming that they have the Chinese patent for something that clearly is one of our patents.

Now, the trends are going in the right direction, they are just not going there quickly enough in terms of China's own intellectual property development and therefore its own desire for protections.

In my view, on the cyber side in particular, what I have been pushing for internally is a focus on identifying a specific number of companies and, frankly, a number of civilian universities, very

large universities in China, that are known to have been engaged in this activity, have been supplying tools, have been supplying personnel, have been engaged in this activity and putting them on the denied entities list from the Commerce Department.

That will deny them visas to the United States, professors will not get fellowships, graduate students will not be able to get fellowships over here. There will be a constituency, as Senator Gorton said, that all of a sudden is now feeling the pain of actions that they are not profiting from and it will create basically a constituency within China that will begin to say, "All right, this is no longer a consequence-free activity for us anymore."

Senator GORTON. I would just go on to say that I agree almost totally. What bothers me about at least a part of that statement is that when the Chinese have so much intellectual property that they have more to defend then they have to attack, we will have already lost the struggle.

Representative MEADOWS. It would be too late, yes. When they become the consumer of their own products, it is game over. So when we look at this—and let us go on a little bit further if the Chairman will indulge—it used to be that investing in China, American companies or foreign companies got a better deal from a regulatory standpoint, from an incentives standpoint.

My understanding is that that is no longer the case, that those regulations are being beefed up. So the regulations that companies fleeing from America to produce in a foreign country are not as, I guess, lucrative anymore. Would you concur with that, agree with that, or disagree?

Senator GORTON. I think maybe it is slightly too broad a statement because I do not think every kind of company or every kind of investment in China is exactly the same. Some may not have much in the way of intellectual property, some obviously still find it profitable to do business there. Many others have found that it costs far more than it is worth.

Representative MEADOWS. Doctor?

Mr. MULVENON. I would probably disagree with the characterization that there was some sepia-toned better past where we actually were successful making money in China. My father did business in China for 20 years selling nuclear radiation detectors and always felt the deck was stacked against him.

We used to watch people who came to China believing in the whole "if everyone bought one shoe we would sell a half a billion shoes" kind of philosophy repeatedly getting used. But I think the hope was always that the Chinese economy would mature to the point where it became a more level playing field and that there was more predictability in the regulatory system.

In fact, what we are finding now is that the regulatory system is becoming even more predatory and more capricious as they are trying to force this indigenous innovation. They are no longer content to allow Western multinationals to have pride of place, but instead are trying to replace them with these national champions. That has created a very uneven playing field and a lot of, frankly, unfair activity that is in violation of their WTO commitments.

Representative MEADOWS. And my last question is, how big does the problem need to get before there is a demand from the Amer-

ican people to deal with it? We are estimating today a low estimate of $300 billion that could be $400 or $500 billion in terms of economic impact. How big does it have to get before you see a concerted effort on all parts to come together and to address it?

Senator GORTON. It is big enough right now, and the fact of this hearing is an illustration of that fact.

Representative MEADOWS. All right. Thank you. I yield back. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Mr. Meadows.

I would even argue that a decade and a half ago, when some of these issues were decided in the House and Senate, that the public was kind of always a bit ahead of these two institutions, perhaps.

I wanted to just—and then I will close for the next panel, but I appreciate very much Mr. Pittenger and Mr. Meadows's comments. I have watched this over from my House days during PNTR and just watched the way that—American corporations and the relationships in China.

At the time of the PNTR vote in the House of Representatives, I remember a friend of mine that worked at National Airport told me there were more corporate jets there that week leading up to the vote than at any time in his memory.

At that point I am not sure that our companies, our large companies' interests in China matched up with our national interests as a nation. I think perhaps it is more that way, but just a note of caution.

As an increasing number of American companies come to the government and say we need help here because of cyber attacks, that we keep in mind—and we should be there for them—that it is important that our national interests match these companies' interests there, because I remember being lobbied by one company in particular in my district who said this makes so much sense to pass PNTR, and then two years later he moved a lot of his production to China. He said I had to move because all my competitors are there because of this new set of rules through PNTR. That song was sung far too many times in North Carolina, in Ohio, and across the country.

So thanks very much, Dr. Mulvenon, for your work, and Senator Gorton, for your lifetime and continued work and service for our country.

I would call up the next panel, beginning with Wen Yunchao, known more commonly by his online alias, Bei Feng. He has launched a series of online campaigns in support of human rights and against Internet censorship. He was awarded the French Republic's Human Rights Prize 2010 by the French National Consultative Commission on Human Rights in recognition of his efforts and contributions to promoting China's human rights movement through social media. He is a graduate of Harbin Institute of Technology and is currently a visiting scholar at Columbia's Institute for the Study of Human Rights in New York City.

Louisa Greve is vice president for Asia, Middle East and North Africa, and Global Programs at the National Endowment for Democracy, where she served as director for East Asia. She has studied, worked, and traveled in Asia since 1980. She was a member of the AEI/Armitage International Taiwan Policy Working Group,

the Council of Foreign Relations Term Member Roundtable on U.S. National Security—New Threats in a Changing World. She served as a member of the board of directors of Amnesty International for five years and was a volunteer China and Mongolian specialist from 1990 to 1999. She served two terms as a member of the Virginia State Advisory Committee of the U.S. Commission on Civil Rights. If the two of you would join us, and thank you very much.

Cao Yaxue will translate for Mr. Wen. Mr. Wen, please proceed. Thank you.

STATEMENT OF WEN YUNCHAO (ONLINE ALIAS "BEI FENG"), INDEPENDENT JOURNALIST AND BLOGGER, VISITING SCHOLAR, INSTITUTE FOR THE STUDY OF HUMAN RIGHTS, COLUMBIA UNIVERSITY

Mr. WEN. Thank you, dear Senator Brown and Congressman Pittenger and Congressman Meadows. My name is Wen Yunchao. I am here to testify about the cyber attacks against me that occurred over the last few years.

In September 2009, I discovered that my Gmail account was set up for forwarding and that it would forward all my emails I received to another email account not under my control. This was the first time I realized that my email was attacked.

In February 2011, the so-called Jasmine Revolution broke in China. It refers to anonymous online calls for mass gatherings in public venues in major cities across China.

At the time I was working and living in Hong Kong. Starting at that time, all my electronic communications, including telephone and Internet products and services were under severe attack.

On June 2, 2011, I discovered that rather sophisticated hacking was being used against my Gmail account. That day I received an email with the subject "Li Chengpeng Invites You to Participate in Voting." The email provided a disguised link. On clicking it, a flash document opened up and the account would authorize other users to visit. When I reported this to Google, they responded that they were not even aware of such attacks.

The content of the email had to do with well-known Chinese author Li Chengpeng's campaign for election to the local Congress of the People's Representatives and was sent two days before the anniversary of the Tiananmen massacre on June 4. I believe the hacking was politically motivated and most likely an act of the government. I reported the hacking process and published it on You Tube.

In June 2011, I was attending the U.N. Human Rights Council's meeting in Geneva as part of the Internet Freedom Fellows Program. I gave a speech to call for support for Chinese citizens who have been persecuted because of the Jasmine Revolution. On June 8, the day before the speech, I received a text message warning.

After I gave the speech and before I left Geneva, my phone began to receive a large volume of incoming calls. My phone was attacked in such a manner between June and August 2011. At its heaviest on July 31, I received 311 calls in one day. All the calls hung up after the ring.

I did a statistic study of the calls between late July and early August and I found that attackers had a very regular time when

they start working and when they went off work. It was not a random person acting alone.

In July 2011, personal information of my wife, my son, and other relatives were published online, including the numbers of my wife and my son's Hong Kong/Macao travel permits. This is not information average people can easily access unless they are the police or authorities.

For about a year starting April 2011, unidentified persons bombed me on Twitter with trash information. Using software called Twin to filter the trash, I found the heaviest attack took place on April 25, 2012; a staggering 590,000 spam posts within 24 hours. Unidentified persons also posted viciously defaming information about me online at the rate of over 10,000 times per day. As far as I know, the artist Ai Wei Wei has also been similarly attacked.

Starting August 24, 2011, my Gmail account was spammed with an astonishing number of messages. At its peak in mid-March 2012, that flow was as high as five gigabytes per hour. If this were a personal attack it would take more than 20 users to attack my account simultaneously to reach that kind of volume. Therefore, I believe it was an organized attack.

The attackers also put my name in garbage messages to make it harder for me to filter them. I reported the attacks to Google through a third party. A Google official contacted me subsequently and Google made specific efforts to deal with the attack on me, but the results were not that great.

Around the same time, unidentified persons also published hundreds of articles online to denigrate me and I believe it was an organized campaign to destroy my personal reputation.

At 4 p.m. on May 28, 2012, attacks on Twitter and Gmail stopped simultaneously. This also shows these were organized behaviors.

Chairman BROWN. Ms. Cao, if you can try to wrap up in the next minute or two.

Mr. WEN. We are just about done. Yes. Thanks. From April 2009 to the present time I have received an untold number of phishing emails and Trojan emails from the one email attack system that I successfully broke into myself. I found 192 people who were the objects of attack and they included Chinese dissidents, rights lawyers, and foreign journalists reporting on China.

From the sources of the pack, I was able to identify, and also from the Mandarin I heard in the background in the earlier stage of the telephone harassment, I believe all the attacks came from mainland China.

I hope that the U.S. Congress and the government will recognize such cyber attacks against human rights defenders as human rights persecution and impose sanctions and visa restrictions on organizations, companies, and their employees who engage in such malicious activities.

Thank you.

Chairman BROWN. Thank you very much, Ms. Cao, and thank you, Mr. Wen.

Ms. Greve, thank you for joining us.

STATEMENT OF LOUISA GREVE, VICE PRESIDENT FOR ASIA, MIDDLE EAST, AND NORTH AFRICA, AND GLOBAL PROGRAMS, NATIONAL ENDOWMENT FOR DEMOCRACY

Ms. GREVE. Thank you so much. For Chinese, Tibetan, and Uyghur human rights activists working from exile, cyber hacking is a form of repression that reaches across state boundaries to undermine their ability to exercise the fundamental political freedoms they should be enjoying in democratic countries.

Being under sustained cyber attack means these groups are not, in practice, able to routinely access free communications media in the public square. The hackers' success in hampering the ability of these groups to do their work normally results from a combination of specific targeting and the use of up-to-the-minute hacking skills.

Some examples. First, the activists have to contend with real-time and preemptive interference with their communications. Increasingly, hackers are no longer having the misspelled emails we have all experienced; you know, when somebody sends you something and they misspell their own name it is a little bit of a giveaway.

Now, the hackers are obtaining genuine emails and then sending them on within a malicious email within hours, which greatly increases their plausibility, especially when they are related to an ongoing conversation, upcoming event, or conference. I have an example from the Uyghur American Association. There was at least one incident when a staff member received an immediate reply from a colleague, which turned out to be the work of a hacker.

Second, there is all-device harassment. Mr. Wen has talked about the jamming of his telephone. This happened in 2011 in a number of places. The World Uyghur Congress experienced, for a full week, continuous jamming of the land lines in Munich of the personal apartment and office telephone lines for a week. During the same time, which was the sensitive political anniversary of the July 5 riots in Urumchi, the Web site was down and there was the massive spam attack, 15,000 emails in one week.

Then the third example has to do with the innovation. There is some innovation having to do with software for cyber attacking. This was the first-ever documented attack against Android devices. Now, this is getting to the Smartphones and the tablets.

In fact, Kaspersky Lab, a research company, has issued a report saying that in March they discovered the first-ever use of spear-phishing email that attacked and succeeded in damaging Android users' equipment. The vehicle for this attack did have to do with the Uyghur, the World Uyghur Congress, having sent an email to speakers who had attended a conference.

The sender of this copied text was purportedly a high-level Tibetan activist. The malware that was attached extracted data about the phone itself: the phone number, the OS version, the phone model, and the contacts stored both on the phone and on the sim card, and call logs, and their SMS messages, and their GO location.

Now, the frequency and sophistication of all these attacks reveal a significant investment of resources. In fact, activists note an upgrading of the resources devoted to this campaign, including in-

creased knowledge of the social networks that they are trying to attack, language proficiency, and the technical means.

We should note another example, another piece of evidence of the nature of the political targeting, the attacks always surge before sensitive political anniversaries, June 4, July 5, and others.

As we look at this kind of deliberate targeted hacking, why is it such a potent tactic for impeding the work of human rights activists? It is because of its numerous practical effects. It silences activists' ability to communicate with the wider public when their Web sites are down for weeks at a time when they have something to say; it compromises the ability of research groups to keep information confidential, which is essential when doing human rights work and helping refugees.

It diverts the energies of the activists because they have to deal with recovering from the cyber attacks and double-checking all their communications to ensure their authenticity. It raises the cost, the financial cost, by requiring expensive back-up systems, very expensive technical assistance, and so on.

It undermines cooperation with the wider world. International organizations, the journalists, the media experts are also frustrated with these fake and malicious emails and other hacking interference. Finally, hacking, frankly, increases fear, again, even for those who are outside of China, even for those living in free countries. This is a great deterrent effect, making people afraid to be in touch with each other, to have solidarity.

Again, while they are outside of China they do not want to compromise their strategies, as Congressman Smith mentioned, or their confidential information, and certainly in communicating with people inside China, given the potential for harassment and arrest. So this portfolio of effects, silencing critical voices, undermining credibility, undermining trust, increasing isolation, raising costs and inducing fear, this is the panoply of tactics of repression perfected by authoritarian regimes and it is now being globalized. It deserves our unqualified condemnation.

Thank you.

Chairman BROWN. Thank you very much, Ms. Greve.

Mr. Wen, first of all, thank you for your courage in speaking out. I know that you are in New York, at least for a while. I also know you have a wife and a son. If your speaking out does endanger you in any way or expose you to any issues or problems, please let us know and we will help you in any way we can. I think that I can speak for all the members of this commission, and institutionally, too, if you would keep us informed about any potential retribution. So, thank you for that.

My question is, why didn't they just shut you down?

Mr. WEN. In 2011, I was awarded a human rights award in France. Since then, I have not been able to return to China. I was working and living in Hong Kong until recently. That is why, today, I am able to sit here to tell you my story. Late last year, they refused to renew my Hong Kong Exit-and-Entry permit, so I could not stay in Hong Kong anymore. That is why I came to New York.

Chairman BROWN. Thank you.

Ms. Greve, thank you for particularly your last comments about the draining resources, increasing costs, and instilling fear. It seems that a number of U.S. companies are reluctant to speak out because of fear of economic retribution that the Chinese Government or state-owned enterprises or others could levy against them.

Do human rights and civil society organizations, both inside and outside China, feel—you talked about fear. Explore that a little more, the fear they may feel in speaking out or pointing fingers, or whatever they might want to do in response.

Ms. GREVE. A number of groups report that it is very hard to even do the basic documentation because victims and witnesses are afraid to speak. This can be true before the cyber age, but it is true in spades now, as James Mulvenon said about stealing intellectual property.

Once you reveal information about yourself it becomes known that you have spoken out and your family can suffer back home in China. So there is an effect of fear. It silences individual victims to speak up and it certainly makes it very hard for journalists and human rights groups to provide the data and the documentation so the world can know the extent of the problem.

Chairman BROWN. So what do U.S. lawmakers do to help protect these civil organizations, civil society organizations and human rights groups and all?

Ms. GREVE. I certainly believe that the work of the National Endowment for Democracy, my organization which is supported by an annual appropriation from the Congress, is one lifeline. We give grants to human rights groups outside China who are doing their best. Then they have money for server space and the ability to travel to meet each other.

So some kind of offsetting of the financial cost is the very least that can be done and that is certainly being done through my organization. There are a number of programs that the State Department has done to help human rights defenders, and these are all worth doing even though they are at a very micro level.

Then certainly the voices of those in China who are still in China and subject not only to harassment and impeding of their normal work, but of course under the thumb of the security apparatus of the state when they raise their voices, it is very gratifying for them to hear Members of the Congress echo their concerns and recognize the justice of their cause.

Chairman BROWN. Does it always matter when—we sort of sometimes walk this line of judging others, of speaking out—does that sometimes jeopardize people whom we defend as American elected officials speaking out individually in support of a Chinese citizen? Does that cut both ways? Is that something we should always do? Does that always help them?

Ms. GREVE. It is a good idea to ask the individual or advisors, but most of the time activists tell us that when they are ready to stand up and be counted it can only help them to have solidarity around the world based on universal values after all.

Chairman BROWN. All right. Thank you.

Mr. Pittenger?

Representative PITTENGER. Thank you, Mr. Chairman.

Mr. Feng, thank you for your testimony. I would like to just get some idea of the penalties that are enforced against the Chinese citizens in their efforts to expose human rights and how they are targeted in China.

Mr. WEN. Internet hacking and cyber security is only one problem they face. In real life, their security, their physical security is an issue. They could be disappeared, their Internet ability could be invaded and their telephones monitored, and so on and so forth.

Representative PITTENGER. Thank you.

Are these penalties pervasive throughout the country or are they different in different provinces? Does it matter where in China?

Mr. WEN. The Internet attacks, the more prominent dissidents and activists are suffering more. But emails, like phishing, it is very common, very widespread. As for disappearance and detention, there might be little difference. In some provinces, like in Guangdong, it might be a little bit better than elsewhere, but it is also very common.

Representative PITTENGER. Thank you.

As it relates to religious freedoms and religious practices, do you see that there is greater openness and freedom in some provinces given than there are in others, and does the official church—is it demanded in some provinces—is the underground church able to live in greater freedom in some areas than in other areas?

Mr. WEN. As far as I know, in the northeastern or the greater northern area in China, religious persecution is very serious. We all know, of course, about what's happening in Xinjiang and Tibet. In the southern provinces, religious persecution might be a little milder but it depends on what is your standard. If your standard is universal values, the persecution, even in what we consider the milder provinces, are still very severe.

Representative PITTENGER. Thank you for that.

Ms. Greve, thank you also for your testimony. As it relates to these organizations, you said that you appreciated the support from our government. I find myself in a predicament sometimes when I am addressing, for example, the Chinese Chamber that I have spoken to and others, and how direct I am. I know Chairman Brown brought this up some, but I would like to get a better feel how you could counsel me on addressing the human rights issues and concerns that I could have the greatest impact.

My challenge has been not to be overbearing, but to be real and understanding. I have 25 years of experience in terms of working with the underground church in that country and their deep appreciation for what they have gone through. I want to be as direct as I can without losing them in the discussion.

My argument has been that people of faith are the most dependable, moral, ethical people, that they could be constructive inside their own government, given all the reports of pervasive problems with crime and other issues inside the government. So I just think I would like a bit more input in how you would help us as legislators bring better focus and light to this issue that could put pressure on the Chinese Government.

Ms. GREVE. Even the work of this Commission proves that there is extensive, detailed, undeniable documentation—the annual re-

port is just full—and yet merely the naming and shaming, merely the exposure does not bring the facts always to the forefront.

When there are face-to-face encounters, there is always an opportunity. Sometimes people who are coming from China are not aware or sometimes believe active government propaganda about hostile forces outside China who want to needlessly smear the good name of China. I think the calm repetition of facts has to have a place in all of this.

I think the investment in the work of documentation has a role, and there is also the question of the long term versus the short term. You may not get an immediate response but you have to stand for what is right for the long term. Maybe you are planting seeds.

Representative PITTENGER. Thank you so much.

Chairman BROWN. Thank you.

Mr. Meadows?

Representative MEADOWS. Thank you, Mr. Chairman. The time is late so I will be very brief, but I have one question as a follow-up. I have been in a number of hearings where we have heard about human rights abuses in China and as it continues. Ms. Greve, if you could comment on this.

We understand when Congress takes an active role, when under the guidance of the Chairman or others when we say we will not tolerate human rights abuses it does not necessarily change it, but those that are suffering suffer less when we highlight it.

So is there a time coming where, instead of a threat, where we truly mean what we say and that we will not tolerate the human rights abuses that have become so really commonplace, is what I understand. But when we highlight it, does it become, indeed, less in China?

Ms. GREVE. Numerous former prisoners report how important it was that political leaders and the people in charge of their detention institutions knew that other people were speaking up on their behalf, improved treatment, health, and so on. And of course the real hope has to come, as with the question of commercial rule of law, an internal transformation in Chinese society. This is where the long-term change will come.

The American institutions and love for liberty and universal values cannot by itself change the situation on the ground in China. It has to come from within China. I believe the point should be to invest as much as possible in strengthening those who have the right principles, who are in a position to shape the institutions in the right direction and to have the greatest, strongest friendship for those kinds of people for the sake of the future of China.

Representative MEADOWS. And with that, I will yield back. Let the message be one that we will not yield until this is dealt with. So I yield back, and I thank the Chairman.

Chairman BROWN. All right. Thank you very much, Mr. Meadows.

Thank you all. The record will stay open for one week. If any of the three panelists, Ms. Cao, Mr. Wen, Ms. Greve, would have anything you would like to submit, and it is possible any of us may have questions for you, written questions, if you would answer

those as quickly as possible. Thank you for speaking out. Thanks for being here. Thank you.

The hearing is adjourned.

[Whereupon, at 4 p.m. the hearing was concluded.]

A P P E N D I X

PREPARED STATEMENTS

PREPARED STATEMENT OF HON. SLADE GORTON, A FORMER U.S. SENATOR FROM WASHINGTON

JUNE 25, 2013

Over the past year, I have served as a member on the Commission on the Theft of American Intellectual Property. The Commission, co-chaired by Governor Jon Huntsman, the former U.S. Ambassador to China, and Admiral Dennis Blair, the former Director of National Intelligence, is an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics. The three purposes of the Commission are to: (1) document and assess the causes, scale, and other major dimensions of international intellectual property theft as they affect the United States; (2) document and assess the role of China in international intellectual property theft; and (3) propose appropriate U.S. policy responses that would mitigate ongoing and future damage and obtain greater enforcement of intellectual property rights by China and other infringers.

What we found during our research and due diligence was quite alarming but not all that surprising. Our findings suggest that the value of the total loss of American IP overseas to be over $300 billion per year, comparable to the current annual level of U.S. exports to Asia. Furthermore, we estimate that China is roughly 50–80 percent of the problem. Most tangibly, one study suggests that if China had the same level of IP protection as the U.S. or the U.K., there would be an increase of 2.2 million new jobs within the United States. Intellectual property rights are violated in a number of ways including violating copyright and trademark protections, infringing on patents, and stealing trade secrets. Trade secrets are stolen primarily through cyber espionage, or through traditional industrial and economic espionage.

Cyber theft is one of the main avenues by which these ideas are stolen. While hackers stealing trade secrets, money, and personal information are a worldwide problem, quantitatively, China stands out in regard to attacks for IP. A confluence of factors, from government priorities to an underdeveloped legal system, causes China to be a massive source of cyber-enabled IP theft. Much of this theft stems from the undirected, uncoordinated actions of Chinese citizens and entities who see within a permissive domestic legal environment an opportunity to advance their own commercial interests. With rare penalties for offenders and large profits to be gained, Chinese businesses thrive on stolen technology.

While our topic today is Chinese hackers and commercial rule of law, it is important to remember that cyber espionage is only part of the problem. The stories that most people hear or imagine when thinking about IP theft, economic espionage, or trade-secret theft are the grist of high-tech espionage thrillers. The mention of global IP thieves often conjures up images of a foreign enemy based somewhere on the other side of a vast ocean. State-sponsored efforts immediately leap to mind—for example, Shanghai-based PLA Unit 61398, which has been

identified as the source of many recent cyber attacks. However, while it is true that the rise of personal computing has added a new dynamic to protecting intellectual property, it is important to remember that nearly all IP loss, no matter how high-tech, still requires a human component. Much of today's IP theft still utilizes traditional economic espionage tactics. This is the apparent situation in the recent NYU case, where a Chinese government institution bribed researchers to disclose their valuable findings.

Industrial espionage is nothing new. It is a classic business tactic used by less than reputable organizations to try and obtain a competitor's secrets in order to gain an economic advantage in the marketplace. So, while members of Congress continue to work on solving the issue of cyber theft and Chinese hacking, we would encourage them to consider expanding policy proposals beyond cyber theft to international IP theft, generally.

Policy responses to the problem of IP theft must start with defensive measures here at home, to protect what we have, but this is not nearly enough. I believe that until there is a change in the internal incentive structure within China, or until there exists in China an interest group in favor of eliminating IP theft, we will likely see little progress. This is perhaps the only road to long term success. Purely defensive measures will likely just create better, more sophisticated thieves.

Along with my testimony today, I am submitting a copy of the IP Commission's report that was released May 22, 2013. The final chapters lay out a series of policy

recommendations, organized as short, medium, and long-term recommendations. The recommendations vary and would likely fall under the jurisdiction of a number of Congressional committees including the Senate Banking and House Foreign Affairs Committees. The short-term recommendations suggest changing the way the U.S. government is internally organized to address IP theft and suggest new tools to create incentives overseas. These include allowing for targeted financial sanctions and quick response measures for seizing IP infringing goods at the border. The medium-term solutions suggest, among other things, amending the Economic Espionage Act and shifting the diplomatic priorities of our overseas attachés. Our long term solutions focus largely on continuing to work on establishing stronger rule of law in China and other IP infringing countries. Additionally, we offer a set of cyber recommendations that this commission will likely find interesting given the topic of today.

It is our hope that this report will help to inform and strengthen the policy changes that come from Congress and the Administration. Thank you.

PREPARED STATEMENT OF JAMES C. MULVENON

JUNE 25, 2013

"CHINESE CYBER ESPIONAGE"

Introduction

Thank you, Mr. Chairman and the other members of the Congressional-Executive Commission on China for the opportunity to take part in the hearings you are holding today on the topic of "Chinese Hacking: Impact on Human Rights and Commercial Rule of Law." My remarks will focus on Chinese cyber espionage.

Chinese cyber espionage has emerged as a top issue in Sino-US relations, primarily because of concerns about theft of intellectual property. As I discuss in Chapter 9 of my book, *Chinese Industrial Espionage,* there are many different features of Chinese cyber activity towards the United States and there is no "one size fits all" approach for all of them.

THE SCALE OF THE PROBLEM

Cyber espionage is the latest and perhaps most devastating form of Chinese espionage, striking at the heart of American military advantage and technological competitiveness. Without mentioning China, General Keith Alexander, NSA Director and Commander, USCYBERCOM, told an audience at the Aspen Security Forum on 26 July 2012 that cyber espionage represents the "greatest transfer of wealth in history." Other government agencies are less circumspect about calling out Beijing for its cyber theft.[1] The Office of the National Counterintelligence Executive's 2011 report *Foreign Spies Stealing US Economic Secrets in Cyberspace* boldly asserts "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[2] While the media began reporting rumors of large-scale intrusions in 2005,[3] U.S officials did not publicly acknowledge exfiltrations of data until August 2006, when the Pentagon asserted that hostile civilian cyber units operating inside China had launched attacks against the NIPRNET and downloaded up to 20 terabytes of data.[4] In March 2007, then Vice-Chairman of the Joint Chiefs General Cartwright told the US-China Economic and Security Review Commission that China was engaged in cyber-reconnaissance, probing computer networks of US agencies and corporations.[5] This view was seconded in the 2007 *China Military Power Report,* an annual Pentagon assessment mandated by the National Defense Authorization Act, which claimed "numerous computer networks around the world, including those owned by the US government, were subject to intrusions that appear to have originated within" the People's Republic of China.[6] Former White House and DHS cyber official Paul Kurtz told Business Week that the Chinese activity was "espionage on a massive scale"[7] A 2009 study by Northrup Grumman for the US-China Economic and Security Review Commission concluded "Chinese espionage in the United States now comprises the single greatest threat to US technology . . . and has the potential to erode the United States' long-term position as a world leader in S&T [science and technology] innovation and competitiveness."[8] And the problem appeared to be getting worse over time. Robert Jamison, the top cyber-security official at DHS, told reporters at a March 2008 briefing, "We're concerned that the intrusions are more frequent, and they're more targeted, and they're more sophisticated."[9] After the Operation Aurora intrusions against Google and other Silicon Valley companies in 2009 and 2010, officials worried that China was escalating its in-

trusions. Whereas before the activities were targeted at government and military networks, threatening US military advantage and government policies, the new intrusions went beyond state-on-state espionage to threaten American technological competitiveness and economic prosperity.

Because the underlying evidence was classified, government and military officials could not provide detailed evidence of these allegations against the Chinese government and military, which naturally led to scrutiny of the specific attribution to China. In his confirmation testimony questions, current CYBERCOM Commander General Alexander agreed that "attribution can be very difficult."[10] Former senior DHS cybersecurity official Greg Garcia told the New York Times in March 2009 that "attribution is a hall of mirrors."[11] With respect to China, Amit Yoran, the first director of DHS's National Cyber Security Division cautioned, "I think it's a little bit naive to suggest that everything that says it comes from China comes from China."[12] Yet other officials were more confident in the assessment of Chinese responsibility. Then Director of the DNI National Counterintelligence Executive, Joel Brenner, told the *National Journal* in 2008:

> Some [attacks], we have high confidence, are coming from government-sponsored sites . . . The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It's a kind of cyber-militia . . . It's coming in volumes that are just staggering.[13]

Other reports by non-governmental actors reach varying levels of confidence in their determination of Chinese government involvement.[14] Given the technical challenges of attribution, however, a more fruitful approach might be to first understand the strategic context of Chinese cyber espionage, and then ask the question "who benefits?" from the activities attributed to Chinese actors, specifically the possible means, motives and opportunities.

STRATEGIC CONTEXT OF CHINESE CYBER ESPIONAGE: CHINA AND CYBER AS AN OVERT TOOL OF STATE POWER

As a rising power, Chinese national interests have logically expanded with the growth in its economic, political, diplomatic and military power. Yet its rise has occurred within a world system still dominated by American unilateral authority. Because of these imbalances, China has naturally sought to find asymmetrical advantages, and cyberspace at first glance appears to be a dimension of national power in which the United States is asymmetrically vulnerable because of its greater dependence on information systems. Moreover, China seems much more comfortable with cyber power as an legitimate, overt tool of state power, especially compared with the United States, which still treats cyber operations as a highly classified, compartmented capability. What do we mean by overt? Countries like China and Russia seems more comfortable with the overt use of cyber conflict, even by non-state proxies acting on their behalf, as we saw in numerous Chinese "patriotic hacker" events in the late 1990s and the Russian cyber conflicts in Estonia in 2007 and Georgia in 2008. When confronted with their potential involvement in these incidents, both Beijing and Moscow appeared to believe that the plausible deniability of the network was a sufficient fig leaf to cover their barely veiled affiliations and common cause with the attacks. By contrast, Washington does not even have a vocabulary for discussing these capabilities in public, as seen in the incoherence of official US comments about possible computer network exploit activities against Milosevic during ALLIED FORCE and the Stuxnet industrial control systems hack in 2011.

WHY CYBER ESPIONAGE?

Within the rubric of the Chinese government's view of cyber as a tool of national power, it is clear that this new dimension offers Beijing certain key strategic advantages, particularly with respect to intelligence collection, technological competitiveness, intelligence preparation of the battlefield, and strategic intelligence to policymakers.

Intelligence Collection Advantages

Cyber espionage is now a favored mode of tradecraft for China, principally because of its logistical advantages and the promise of plausible deniability. On the first issue, Joel Brenner highlights the relative ease of cyber versus other traditional forms of espionage: "Cyber-networks are the new frontier of counterintelligence . . . If you can steal information or disrupt an organization by attacking its networks remotely, why go to the trouble of running a spy?"[15] Take the case of Greg Dongfan

Chung, discussed in Chapter 8, as an example. Managing Chung required significant institutional resources, including case officers, covert communications, money transfers, and travel arrangements. In the end, Chung was caught, and his "perp walk" and public trial proved to be an embarrassment to the Chinese government. Now imagine a scenario in which the same volume of information can be exfiltrated out of Boeing or Rockwell's computer networks in a single evening via an exquisite computer network exploitation operation, covered by the plausible deniability of network intrusions. Given the choice between the two modes, it is only natural that intelligence services would increasingly pick the less risky, cheaper, and faster way of doing business.

Technological Competitiveness Advantages

After more than thirty years of serving as the world's assembly point and export processing zone, the Beijing government has clearly made the decision to transform Chinese economic development by encouraging "indigenous innovation."[16] Since 2006, James McGregor and others have highlighted "Chinese policies and initiatives aimed at building 'national champion' companies through subsidies and preferential policies while using China's market power to appropriate foreign technology, tweak it and create Chinese 'indigenous innovations' that will come back at us globally."[17] In the information technology sector, McGregor notes "Chinese government mandate to replace core foreign technology in critical infrastructure—such as chips, software and communications hardware—with Chinese technology within a decade." Among the tools being actively used to achieve these goals are:

> A foreign-focused anti-monopoly law, mandatory technology transfers, compulsory technology licensing, rigged Chinese standards and testing rules, local content requirements, mandates to reveal encryption codes, excessive disclosure for scientific permits and technology patents, discriminatory government procurement policies, and the continued failure to adequately protect intellectual property rights.[18]

Missing from this excellent list, however, are traditional technical espionage and technical cyber espionage, which many companies believe are already eroding their technical advantage. The logic for these latter approaches is clearly outlined by David Szady, former head of the FBI's counterintelligence unit: "If they can steal it and do it in five years, why [take longer] to develop it?"[19] Rather than destroying US competitiveness through "cyberwar," former DNI McConnell argues that Chinese entities "are exploiting our systems for information advantage—looking for the characteristics of a weapons system by a defense contractor or academic research on plasma physics, for example—not in order to destroy data and do damage."[20]

Examples of Chinese cyber espionage to obtain science and technology can be divided into two broad categories: external and insider. The 2011 NCIX report offers three illustrative examples of insider cyber threats:

- David Yen Lee, a chemist with Valspar Corporation, used his access to internal computer networks between 2008 and 2009 to download approximately 160 secret formulas for paints and coatings to removable storage media. He intended to parlay this proprietary information to obtain a new job with Nippon Paint in Shanghai, China. Lee was arrested in March 2009, pleaded guilty to one count of theft of trade secrets, and was sentenced in December 2010 to 15 months in prison.
- Meng Hong, a DuPont research chemist, downloaded proprietary information on organic light-emitting diodes (OLED) in mid-2009 to his personal email account and thumb drive. He intended to transfer this information to Peking University, where he had accepted a faculty position, and sought Chinese government funding to commercialize OLED research. Hong was arrested in October 2009, pleaded guilty to one count of theft of trade secrets, and was sentenced in October 2010 to 14 months in prison.
- Xiangdong Yu (aka Mike Yu), a product engineer with Ford Motor Company, copied approximately 4,000 For documents onto an external hard drive to help obtain a job with a Chinese automotive company. He was arrested in October 2009, pleaded guilty to two counts of theft of trade secrets, and sentenced in April 2011 to 70 months in prison.[21]

External cyber threats to scientific and industrial data, believed to originate in China, have been well-documented in reports by outside vendors. Some examples include:

- In its *Night Dragon* report, McAfee documented "coordinated covert and targeted cyberattacks have been conducted against global oil, energy, and petrochemical companies," "targeting and harvesting sensitive competitive propri-

etary operations and project-financing information with regard to oil and gas field bids and operations."[22]

- In his *Shady Rat* report, McAfee's Dmitry Alperovitch identified 71 compromised organizations in one set of intrusions, including 13 defense contractors, 13 information technology companies, and 6 manufacturing companies.[23]
- In January 2010, Google reported a "highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property," including source code.[24] Google claimed that the intrusion also targeted "at least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media and chemical sectors," and was corroborated in separate admissions by Adobe.[25]
- In its *GhostNet* report, researchers at Information Warfare Monitor found 1,295 infected computers in 103 countries, including a range of political, diplomatic and economic target organizations such as Deloitte and Touche's New York office.[26] The follow-on report, *Shadows in the Cloud,* identified additional targets, including Honeywell.[27]

Each of these reported intrusions were traced to IP addresses in China, and almost certainly represent only a fraction of the known hacks, given the reluctance of companies to report data breaches.

Intelligence Preparation of the Battlefield (IPB)

It is also important to contextualize China's interest in cyber espionage within Beijing's threat perceptions of potential scenarios for military conflict. In the minds of the Chinese leadership, the available evidence suggests that the most important political-military challenges and the most likely flashpoints for Sino-US conflict involve Taiwan or the South China Sea. Should the late 1990s, the PLA has been hard at work bolstering the hedging options of the leadership, developing advanced campaign doctrines, testing the concepts in increasingly complex training and exercises, and integrating new indigenous and imported weapons systems.

Yet cyber operations are also expected to play an important role in these scenarios, necessitating intelligence preparation of the cyber battlefield. At the strategic level, the writings of Chinese military authors suggest that there are two main centers of gravity in a Taiwan scenario, both of which can be attacked with computer network operations in concert with other kinetic and non-kinetic capabilities. The first of these is the will of the Taiwanese people, which they hope to undermine through exercises, cyber attacks against critical infrastructure, missile attacks, SOF operations, and other operations that have a psyop focus. Based on assessments from the 1995–1996 exercises, as well as public opinion polling in Taiwan, China appears to have concluded that the Taiwanese people do not have the stomach for conflict and will therefore sue for peace after suffering only a small amount of pain. The second center of gravity is the will and capability of the United States to intervene decisively in a cross-strait conflict. In a strategic sense, China has traditionally believed that its ICBM inventory, which is capable of striking CONUS, will serve as a deterrent to US intervention or at least a brake on escalation.[28]

Closer to its borders, the PLA has been engaged in an active program of equipment modernization, purchasing niche "counter-intervention" capabilities such as anti-ship ballistic missiles, long-range cruise missiles and submarines to shape the operational calculus of the American carrier strike group commander on station.[29] According to the predictable cadre of "true believers," both of the centers of gravity identified above can be attacked using computer network operations. In the first case, the Chinese IO community believes that CNO will play a useful psychological role in undermining the will of the Taiwanese people by attacking infrastructure and economic vitality. In the second case, the Chinese IO community envisions computer network attacks against unclassified NIPRNET and its automated logistics systems as an effective way to deter or delay US intervention into a military contingency and thereby permit Beijing to achieve its political objectives with a minimum of fighting. *In both cases, China must conduct substantial computer network exploitation (the military term for cyber espionage) for intelligence preparation of this battlefield, and the alleged intrusion set into NIPRNET computer systems would appear to fulfill this military requirement.*

Why does the Chinese military believe that the deployment phase of US military operations, particularly the use of the unclassified NIPRNET for logistics deployments, is the primary focus of vulnerability? Since DESERT STORM in the early 1990s, the PLA has expended significant resources analyzing the operations of what it often and euphemistically terms "the high-tech enemy."[30] When Chinese strategists contemplate how to affect US deployments, they confront the limitations of their current conventional force, which does not have range sufficient to interdict US facilities or assets beyond the Japanese home islands.[31] Nuclear options, while

theoretically available, are nonetheless far too escalatory to be used so early in the conflict.[32] Theater missile systems, which are possibly moving to a mixture of conventional and nuclear warheads, could be used against Japan or Guam, but uncertainties about the nature of a given warhead would likely generate responses similar to the nuclear scenario.[33] Instead, PLA analysts of US military operations presciently concluded that the key vulnerability was the mechanics of deployment itself. Specifically, Chinese authors highlight DoD's need to use civilian backbone and unclassified computer networks (known as the NIPRNET), which is a function of the requirements of global power projection, as an "Achilles Heel." There is also recognition of the fact that operations in the Pacific are especially reliant on precisely coordinated transportation, communications, and logistics networks, given what PACOM calls the "tyranny of distance"[34] in the theater. PLA strategists believe that a disruptive computer network attack against these systems or affiliated civilian systems could potentially delay or degrade US force deployment to the region while allowing the PRC to maintain a degree of plausible deniability.

The Chinese are right to highlight the NIPRNET as an attractive *and* accessible target, unlike its classified counterparts. It is attractive because it contains and transmits critical deployment information in the all-important time-phased force deployment list (known as the "tip-fiddle"), which is valuable for both intelligence-gathering about US military operations but also a lucrative target for disruptive attacks. In terms of accessibility, it was relatively easy to gather data about the NIRPNET from open sources, at least before 9/11. Moreover, the very nature of the system is the source of its vulnerabilities, since the needs of global power project mandate that it has to be unclassified and connected to the greater global network, albeit through protected gateways.[35]

DoD's classified networks, on the other hand, are an attractive but less accessible target for the Chinese. On the one hand, these networks would be an intelligence gold mine, and is likely a priority computer network exploit target. On the other hand, they are less attractive as a computer network attack target, thanks to the difficulty of penetrating its high defenses. Any overall Chinese military strategy predicated on a high degree of success in penetrating these networks during crisis or war is a high-risk venture, and increases the chances of failure of the overall effort to an unacceptable level.

Chinese CNE or CNA operations against logistics networks could have a detrimental impact on US logistics support to operations. PRC computer network exploit activities directed against US military logistics networks could reveal force deployment information, such as the names of ships deployed, readiness status of various units, timing and destination of deployments, and rendezvous schedules. This is especially important for the Chinese in times of crisis, since the PRC in peacetime utilizes US military web sites and newspapers as a principal source for deployment information. An article in October 2001 in *People's Daily,* for example, explicitly cited US Navy web sites for information about the origins, destination and purpose of two carrier battle groups exercising in the South China Sea.[36] Since the quantity and quality of deployment information on open websites has been dramatically reduced after 9/11, the intelligence benefits (necessity?) of exploiting the NIPRNET have become even more paramount.[37] Computer network attack could also delay re-supply to the theater by misdirecting stores, fuel, and munitions, corrupting or deleting inventory files, and thereby hindering mission capability.

The advantages to this strategy are numerous: (1) it is available to the PLA in the near-term; (2) it does not require the PLA to be able to attack/invade Taiwan with air/sea assets; (3) it has a reasonable level of deniability, provided that the attack is sophisticated enough to prevent tracing; (4) it exploits perceived US casualty aversion, over-attention to force protection, the tyranny of distance in the Pacific, and US dependence on information systems; and (5) it could achieve the desired operational and psychological effects: deterrence of US response or degrading of deployments. *Looking back over more than ten years of China-origin intrusions into the very NIPRNET systems identified by PLA analysts as a high-priority network attack target as early as 1995, the logic of the intrusion sets becomes much clearer.*

Strategic Intelligence

An additional motivation for cyber espionage is strategic intelligence about the policies and intentions of civilian and military officials as well as the internals of debates within the US government and political parties:

1. In June 2006, the State Department was victimized by a series of intrusions at its foreign posts and headquarters in Washington. According to the *Associated Press,* "hackers stole sensitive information and passwords, and implanted 'back doors' in unclassified computers to allow them to return." Employees told the *AP* that State's East Asian and Pacific Affairs Bureau was particularly hard

hit by the intrusion, suggesting that the intruders had a special interest in Asia-related information.[38] Two reporters from *Business Week* relate the story of what happened:

"The attack began in May, 2006, when an unwitting employee in the State Dept.'s East Asia Pacific region clicked on an attachment in a seemingly authentic e-mail. Malicious code was embedded in the Word document, a congressional speech, and opened a Trojan "back door" for the code's creators to peer inside the State Dept.'s innermost networks. Soon, cyber security engineers began spotting more intrusions in State Dept. computers across the globe. The malware took advantage of previously unknown vulnerabilities in the Microsoft operating system. Unable to develop a patch quickly enough, engineers watched helplessly as streams of State Dept. data slipped through the back door and into the Internet ether. Although they were unable to fix the vulnerability, specialists came up with a temporary scheme to block further infections. They also yanked connections to the Internet. One member of the emergency team summoned to the scene recalls that each time cyber security professionals thought they had eliminated the source of a "beacon" reporting back to its master, another popped up. He compared the effort to the arcade game Whack-A-Mole. The State Dept. says it eradicated the infection, but only after sanitizing scores of infected computers and servers and changing passwords."[39]

2. In 2007, intruders broke into the e-mail system for Defense Secretary Robert Gates's office, and the Pentagon shut down about 1,500 computers for more than a week while the attacks continued. Officials told the *Financial Times* "an internal investigation has revealed that the incursion came from the People's Liberation Army. One senior US official said the Pentagon had pinpointed the exact origins of the attack. Another person familiar with the event said there was a 'very high level of confidence . . . trending towards total certainty' that the PLA was responsible."[40]

3. In the summer of 2008, the FBI informed both the Obama and McCain presidential campaigns that their computer systems had been infiltrated. *Newsweek* quoted an FBI agent as telling both teams: "You have a problem way bigger than what you understand . . . You have been compromised, and a serious amount of files have been loaded off your system."[41] The Financial Times later cited investigators "had determined that the attacks originated from China, but cautioned that they had not ascertained whether they were government-sponsored, or just unaffiliated hackers."[42] In a cybersecurity policy speech early in his Presidency, Obama referred to the incident: "I know how it feels to have privacy violated because it has happened to me and the people around me. It's no secret that my presidential campaign harnessed the Internet and technology to transform our politics. What isn't widely known is that during the general election hackers managed to penetrate our computer systems. To all of you who donated to our campaign, I want you to all rest assured, our fundraising website was untouched. So your confidential personal and financial information was protected. But between August and October, hackers gained access to emails and a range of campaign files, from policy position papers to travel plans. And we worked closely with the CIA—with the FBI and the Secret Service and hired security consultants to restore the security of our systems."[43]

These three sample cases show that Beijing clearly views cyber as a collection modality for obtaining strategic intelligence at the highest levels of the US Government.

CHINESE GOVERNMENT DENIALS

"The lady doth protest too much, methinks"—Shakespeare, *Macbeth*

In counterintelligence offices in Washington, one often sees the following sign: "Admit Nothing, Deny Everything, Make Vigorous Counter-Accusations". This philosophy is also a deeply held conviction of the Chinese side when it comes to discussing their possible role in cyber intrusions. First, they admit nothing and deny everything. When asked about the China-origin intrusions into German Chancellor Angela Merkel's office network, for example, "the Chinese Embassy in Berlin describing the accusation of state-controlled hacking as "irresponsible speculation without a shred of evidence."[44] Chinese officials also point to Chinese laws as an ironclad defense of its own lack of involvement. Reacting to accusations from that Chinese hackers were responsible for the intrusions revealed by Google in January 2010, Foreign Ministry spokeswoman Jiang Yu countered that "Chinese law proscribes any form of hacking activity."[45] After the release of the Office of the National Counterintelligence Executive's 2011 "Report to Congress on Foreign Economic Collection and Industrial Espionage," Chinese officials denigrated the quality

of the analysis, asserting that "identifying the attackers without carrying out a comprehensive investigation and making inferences about the attackers is both unprofessional and irresponsible."[46] Then, the Chinese government impugns the motives of the accusers, making its own counter-accusations. In his response to questions about GhostNet, Foreign Ministry spokesman Qin Gang accused foreigners of having a "Cold War mentality":

> The problem now is that some people abroad are keen to fabricate the rumor of the so-called 'Chinese cyber spy network.' The allegation is utterly groundless...There is a ghost called Cold War and a virus called China's threat theory overseas. Some people, possessed by this ghost and infected with this virus, fall ill from time to time. Their attempts of using rumors to disgrace China will never succeed. We should rightly expose these ghosts and viruses.[47]

Wang Baodong, a spokesman for the Chinese government at its embassy in Washington, darkly hinted that "anti-China forces" are behind the allegations.[48] After the US-China Economic and Security Review Commission's release of a Northrup-Grumman report on Chinese cyber espionage, Qin Gang railed:

> The report takes no regard of the true situation. It is full of prejudice, and out of ulterior motive. We urge the so-called commission not to see China through colored lens and not to do things that interfere with China's internal affairs and undermine China-US relations.[49]

Finally, the Chinese government describes itself as the victim of cyber intrusions. After a detailed expose of Chinese cyber espionage appeared in *Business Week,* Wang Baodong emailed the magazine's editors, claiming that China is "frequently intruded and attacked by hackers from certain countries."[50] When asked in early 2010 about Google's complaint that it had been hacked from China, Foreign Ministry spokesman Ma Zhaoxu said Chinese companies have also been hacked, adding that China resolutely opposes the practice.[51] Other officials have cited the fact that most of the world's botnets are controlled from servers in the United States, insinuating that Washington needed to get its own cybersecurity in order before accusing other countries of hacking. Finally, the Chinese government tries to paint itself as the patron of global cybersecurity, in contrast to the "militarized" US approach to cyber: "China is ready to build, together with other countries, a peaceful, secure and open cyberspace order."[52] While Beijing's style of strategic communications is not limited to cyber espionage, as seen in its rhetoric during crises (Belgrade Embassy bombing in 1999, EP–3A hostage crisis in 2001, etc.), the reaction of its officials has the unintended consequence of increasing suspicion.

HOW GOOD ARE THEY? OR DOES IT MATTER?

Measuring Chinese cyber espionage capability also involves the assessment of a group or country's ability to generate new attack tools or exploits. Outside analysts, many of whom are programmers themselves, tend to reify countries like Russia that abound with highly talented programmers, and look down upon countries or individuals that simply use off-the-shelf "script kiddie" tools or exploit known vulnerabilities, preferring to admire more advanced cyber operators who can discover their own "zero-day" vulnerabilities.[53] Indeed, analysts who have examined Chinese intrusions in detail often comment on their relative lack of sophistication and especially their sloppy tradecraft,[54] leaving behind clear evidence of the intrusion and sometimes even attribution-related information. For example, analysts who examined possible Chinese intrusions into energy companies concluded that Chinese hackers were "incredibly sloppy," "very unsophisticated," "made mistakes and left lots of evidence."[55] Perhaps the Chinese cyber operators are so convinced of the plausible deniability afforded by the current global network architecture that they do not see the need to hide more effectively, or perhaps they believe that their communications are secure because they are using Chinese language. Both are true to some extent, especially the latter, as many Chinese correctly perceive that their difficult language is actually the country's first line of defense, its first layer of cryptography, and there actually few foreigners with the skills or bandwidth to penetrate the veil. Most important, however, the Chinese probably perceive that they do not need to "up their game" because their relatively primitive and sloppy efforts have thus far been wildly successful and therefore see no need to change. In fact, one could argue that China's cyber espionage successes to date are more a function of the vulnerability of US systems than any inherent capability on the Chinese side. As time passes, however, one would expect Chinese capability to improve, particularly as information about China-origin intrusions becomes more widespread and victims begin to take concrete measures to protect themselves. This view is endorsed

by former counterintelligence chief Joel Brenner, who told the National Journal in 2008 that Chinese hackers are "very good and getting better all the time."[56]

* * * * * * *

[1] "General Warns of Dramatic Increase of Cyber-Attacks on US Firms," *Los Angeles Times,* 27 July 2012.

[2] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011,* October 2011, http://www.dni.gov/reports/20111103_report_fecie.pdf

[3] Tom Espiner, "Chinese Hackers US Military Defenses," *Silicon.com,* November 2005; and Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post,* August 2005.

[4] Dawn Onley, Dawn and Patience Wait, "Red Storm Rising: DoD's Efforts to Stave Off Nation- State Cyber Attacks Begin with China," *Government Computer News,* August 2006.

[5] See General James E. Cartwright, in hearing, *China's Military Modernization and Its Impact on the United States and the Asia-Pacific,* US-China Economic and Security Review Commission, 110th Cong, 1st Sess., March 29–30, 2007, p. 90, at www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf.

[6] Shane Harris, "China's Cyber Militia," *National Journal,* 31 May 2008.

[7] Brian Grow, Keith Epstein and Chi-Chu Tschang, "The New E-spionage Threat," *Business Week,* 21 April 2008, pp.32–41.

[8] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* published by the US-China Economic and Security Review Commission, 9 October 2009.

[9] Harris, "China's Cyber Militia."

[10] "Advance Questions for Lieutenant General Keith Alexander USA, Nominee for Commander, United States Cyber Command," published by Senate Armed Services Committee, accessed at: http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004–15–10.pdf

[11] Shaun Waterman, "Chinese Cyberspy Network Pervasive," *Washington Times,* 30 March 2009.

[12] Harris "China's Cyber Militia."

[13] Ibid.

[14] For a range of views on the attribution issue, see Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation;* McAfee® Foundstone® Professional Services and McAfee Labs™, *Global Energy Cyberattacks: 'Night Dragon',* 10 February 2011; Shishir Nagaraja and Ross Anderson, "The Snooping Dragon: Social-Malware Surveillance of the Tibetan Movement," UCAM–CL–TR–746, University of Cambridge Computer Laboratory Technical Report 746, March 2009; Dmitri Alperovitch, *Revealed: Operation Shady RAT,* McAfee, August 2011; and Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network,* Toronto: SecDev and Citizen Lab, 29 March 2009.

[15] Harris, "China's Cyber Militia."

[16] James McGregor, "China's Drive for 'Indigenous Innovation': A Web of Industrial Policies," Washington, DC: US Chamber of Commerce, July 2010.

[17] James McGregor, "Time to rethink US-China trade relations," *Washington Post,* 19 May 2010. See also McGregor, "China's Drive for 'Indigenous Innovation.'"

[18] Ibid.

[19] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)," *Time,* 29 August 2005.

[20] Nathan Gardels, "China is Aiming at America's Soft Underbelly: The Internet," *The Christian Science Monitor,* 5 February 2010, accessed at: http://www.csmonitor.com/Commentary/Global-Viewpoint/2010/0205/China-is-aiming-at-America-s-soft-underbelly-the-Internet

[21] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace.*

[22] McAfee, *Night Dragon.*

[23] Alperovitch, *Operation Shady RAT.*

[24] http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[25] http://blogs.adobe.com/conversations/2010/01/adobe—investigates—corporate—n.html

[26] Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network,* Toronto: SecDev and Citizen Lab, 29 March 2009, accessed at: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[27] Information Warfare Monitor and Shadowserver, *Shadows in the Cloud: Investigating Cyber Espionage 2.0,* Toronto: SecDec and Citizen Lab, 6 April 2010, found at www.shadows-in-the-cloud.net

[28] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011,* p.3.

[29] Ibid., pp.2–4, 28–29.

[30] Ibid., p.22.

[31] Ibid., p.31.

[32] Ibid., p.34.

[33] Ibid., pp.29,78.

[34] For a PACOM/J4 perspective on the issue, see http://www.navsup.navy.mil/scnewsletter/2009/jan-feb/cover1

[35] For an unclassified summary, see http://www.disa.mil/Services/Network-Services/Data/SBU–IP.

[36] "Whom, If Not China, Is US Aircraft Carriers' Moving onto South China Sea Directed Against?" *Renmin Ribao,* 24 August 2001.

[37] The Department of Defense's revised web site administration guidance, which can be found here (http://www.defenselink.mil/webmasters/policy/dod__web__policy__12071998__with__amendments__and__corrections.html), specifically prohibits the following: "3.5.3.2. Reference to unclassified information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of a military plan or program."

[38] "Computer Hackers Attack State Dept.," *Associated Press,* 12 July 2006.

[39] Grow, Epstein and Tschang, "The New E-spionage Threat."

[40] Sevastopluo, Demetri, "Chinese Hacked into Pentagon," *FT.com,* 3 September 2007.

[41] Evan Thomas, "Center Stage," Newsweek, 6 November 2008; David Byers, Tom Baldwin and Tim Reid, "Obama computers 'hacked during election campaign,'" *Times Online,* 7 November 2008.

[42] *Financial Times,* November 2008.

[43] "Remarks by the President on Securing our Nation's Cyber Infrastructure," Office of the Press Secretary, The White House, 29 May 2009.

[44] "Merkel's China Visit Marred by Hacking Allegations," *Spiegel Online International,* 27 August 2007.

[45] Helft, Miguel, and John Markoff, "Google Alerted Activists of Attacks," *New York Times,* 15 January 2010.

[46] "China Rebuts US Accusation of Hacker Attacks," *China Daily,* 31 October 2011.

[47] "China Denies Allegations on 'Cyber Spy Network'."

[48] Grow, Epstein and Tschang, "The New E-spionage Threat."

[49] Clayton, Mark, "Google cyber attack: the evidence against China," *Christian Science Monitor,* 13 January 2010.

[50] Grow, Epstein and Tschang, "The New E-spionage Threat."

[51] "China Says Google, Foreign Firms Must Respect Laws," *CIOL,* 19 January 2010.

[52] "China Rebuts US Accusation of Hacker Attacks," *China Daily,* 31 October 2011.

[53] http://en.wikipedia.org/wiki/Zero-day__attack

[54] Keizer, Gregg, "Chinese Hackers Called Sloppy but Persistent," *Computerworld,* 12 February 2011.

[55] Ibid.

[56] Harris, "China's Cyber Militia."

Cyber Attacks against Me

By Wen Yunchao

My name is Wen Yunchao. I'm here to testify about the cyber attacks against me that occurred over the last few years.

In September, 2009, I discovered that my Gmail account was set up for forwarding and that it would forward all the emails I received to another email account not under my control. This was the first time I realized my email was hacked.

In February, 2011, the so-called "Jasmine revolution" broke in China. The "Jasmine revolution" referred to anonymous online calls for mass gatherings in public venues in major cities across China. At the time, I was working and living in Hong Kong. Starting at that time, all of my electronic communications, including telephone and Internet services were under severe attack.

On June 2, 2011, I discovered that these rather sophisticated hacking attacks were targeting my Gmail account. That day I received an email with the subject "Li Chengpeng Invites You to Participate in Voting." The email contained a hidden link: On clicking it, a Flash document opened up, which authorized other users to visit. When I reported this to Google, they responded that they weren't even aware of such attacks. The content of the email had to do with well-known Chinese author Li Chengpeng's campaign for election to the local congress of the people's representatives, and was sent two days before the anniversary of the Tian'anmen Massacre on June 4th. I believe the hacking was politically motivated and most likely an act of the government. I recorded the hacking process and published it on You Tube (see Appendix 1).

In June 2011, I was attending the UN Human Rights Council's meeting in Geneva as part of the Internet Freedom Fellows program. I gave a speech to call for support for Chinese citizens who had been persecuted because of the "Jasmine Revolution." On June 8, the day before the speech, I received a text message warning me: ".....A wise person takes action after thorough thinking; do not let ignorance have the upper hand and leave you in sadness. Whereas life can be splendid, why obsess with one thing? Put it down, put it down" (see Appendix 2).

After I gave the speech and before I left Geneva, my phone began to receive a large volume of incoming calls. At first, I could connect, and I could hear loud ringing in the background. My impression was that I was not the only one being harassed. In the background, I also heard dialogue in Mandarin, but it

was inaudible. The telecommunications company told me that they had no way to know the sources of these calls. My phone was attacked in such a manner between June and August, 2011. At its heaviest on July 31, I received 311 calls in one day. All the calls hung up after it rang. I did a statistical study of the calls between late July and early August, and I found the attackers had a very regular time when they started working and when they went off work. It was not a random person acting alone (see Appendix 3).

In July, 2011, personal information about my wife, my son and other relatives was published online, including the numbers of my wife and my son's Hong Kong/Macao travel permits. This is not information average people can easily find unless they are police authorities (see Appendix 4).

For about a year starting April, 2011, unidentified persons "tweet bombed" me on Twitter with trash information. Using a software called Tween to filter the trash, I found the heaviest attack took place on April 25, 2012 – with a staggering 590,000 spam posts within 24 hours. Unidentified persons also posted viciously defaming information about me online at the rate of over 10,000 times per day. As far as I know, artist Ai Weiwei has been similarly attacked (see Appendix 5 and 6).

Starting August 24, 2011, my Gmail account was spammed with an astronomical number of messages. At its peak in mid-March, 2012, the data flow was as high as 5G per hour, and all the IPs came from Beijing. Given that the most common network access is ADSL, if this were a personal act, it would take more than 20 users to attack my account simultaneously to reach that kind of data volume. Therefore I believe it was an organized act. The attackers also put my name in garbage messages to make it harder for me to filter them. I reported the attacks to Google through a third party. A Google official contacted me subsequently, and Google made specific efforts to deal with the attack on me, but the results were not that great (see Appendix 7).

Around the same time, unidentified persons also published hundreds of articles to denigrate me, and I believe it was an organized campaign to destroy my reputation (see Appendix 8).

At 4 pm, on May 28, 2012, attacks on Twitter and Gmail stopped simultaneously. This also shows these were organized behaviors.

From April, 2009 to the present time, I have received an untold number of phishing emails and Trojan emails. From the one email attack system that I successfully broke into, I found 192 people who were objects of attack, and they included Chinese dissidents, rights lawyers and foreign journalists reporting on China. From the sources of attack I was able to identify, and also

from the Mandarin I heard in the background in the earliest stage of the telephone harassment, I believe all the attacks came from mainland China.

I hope that the US Congress and government will recognize such cyber attacks against human rights defenders as human rights persecution, and impose sanctions and visa restriction on organizations, companies and their employees who engage in such malicious activities.

Appendix 1: Video display of how my Gmail was hacked

Link: https://www.youtube.com/watch?v=CCq52MnnC4U

* * * * * * *

本人受到网络骚扰和攻击情况

我，温云超，谨在此陈述我过去几年来受到的网络攻击。

2009 年 9 月，我发现我的 Gmail 邮箱被人设置了转发，也就是我所有接收的邮件都会被转发到另一个不是我控制的邮箱。这是我第一次发现邮箱被入侵。

2011 年 2 月，中国爆发“茉莉花革命”，我当时在香港工作，从那时开始，所使用的电话、网络产品或服务受到严重的攻击。

2011 年 6 月 2 日，我发现有人针对 Gmail 设计了非常高水平的入侵，当天我收到了一封标题为“李承鹏邀您参加投票”的邮件，信件中提供了一个伪装的链接，点击之后，会打开一个 Flash 文件，账户即会被授权给其他的用户访问。我把这个发报告给 Google 公司时，他们都还没有发现这个攻击行为。信件内容有关中国着名作者李承鹏参加中国人大代表选举事项，信件在天安门事件纪念日前两日寄送，我认为攻击方含有政治目的，攻击水平非常高，极有可能是来自于政府背景的行为。我把被攻击过程作了记录并发布到了 Youtube 上。（参见附件： 1 ）

我于 2011 年 6 月参与“Internet freedom fellows”计划，在日内瓦出席联合国人权理事会的会议，并发表演讲声援中国因“茉莉花革命”受迫害的人士。6 月 8 日，在发表演讲的前一天，我即收到电话短信警告内容中包括：“智者三思而后行，莫让无知钻了空，空

悲切。人生可以更精彩，何苦一处穷纠结，罢罢罢。”（参见附件：2 ）

在发表完演讲之后，我还没有离开日内瓦，我的电话便开始受到海量呼入骚扰，在最开始的骚扰中，我能接通电话，听到背景中有不断的电话铃声，我估计不止骚扰我一个人；背景中还有人用普通话对话，但听不清对话内容。电讯公司称无法追查来源。2011 年 6、7、8 月间，本人的电话受骚扰攻击，7 月 31 日最高曾达 311 次，都是响铃之后挂断。我曾对当年 7 月底 8 月初的电话骚扰作了统计，可以看出攻击者有严格的上班和下班时间，并非个人行为。（参见附件： 3）

2011 年 7 月，我太太刘阳、儿子温嘉元及其他一些亲人的个人资料被发布到网络上，包括我太太及儿子的港澳通行证号码，除了中国警方，别人很难获得这些资料。（参见附件：4 ）

不明身份人士 2011 年 4 月起的一年中，不断在 Twitter 用垃圾信息轰炸我，我使用 tween 这个软件对这些信息进行过滤，在 2012 年 4 月 25 日的 24 小时中，我监测到最高的攻击曾达 59 万次。不明身份人士在网路上还发布造谣污蔑攻击本人的资讯，每天也过万次。就我所知，这种攻击，也曾发生在艾未未先生身上。（参见附件： 5 及 6 ）

2011 年 8 月 24 日开始，我的 Gmail 电子邮箱也受到饱和垃圾攻击，2012 年 3 月中旬时高达 1 小时 5G 的数据流量，攻击我的 IP 都来自于中国北京，以中国最常见的 ADSL 网络接入服务来看，如果是个人行为，需要 20 个用户以上同时发起攻击才能达到这个流量，我个人认为我所遭受的攻击来自于有组织的行为。攻击者还在垃圾邮件里面放进我的名字，还干扰我对这些邮件的过滤。我通过中间人将此事向 Google 公司报告，Google 公司的一名官员和我取得了联系，Google 公司为我受到攻击的情况专门进行了处理，但效果并不明显。（参见附件： 7）

在同一时间，不明身份的人士还在网上发布造谣污蔑后置攻击本人的文章数百篇，个人认为，这是有组织的污蔑和抹黑行为。（参见附件：8 ）

北京时间 2012 年 5 月 28 日下午 4 时，对我 Twitter 及 Gmail 的攻击同时停止了，这也说明，对我的攻击来自于有组织的行为。

从 2009 年起的 4 年来，我收到的钓鱼攻击邮件及木马邮件不计其数，从我破解的对方一个邮件攻击系统来看，在 192 人的攻击对象当中，主要包括了中国的异见人士、维权律师及外国报道中国问题的记者。从我监测到的攻击来源及最开始电话骚扰背景中听到的普通话，我认为攻击来自于中国大陆。

我希望美国国会和政府，能将这种针对人权捍卫者（human rights defender）的攻击行为认定为人权迫害，对所有从事相关攻击行为的机构、公司及人员实施经济制裁及签证制裁。

附件 1 ：Gmail 受入侵的过程演示

网址：https://www.youtube.com/watch?v=CCq52MnnC4U

附件 2 ：电话短信警告内容

附件 3：电话受骚扰攻击截图及统计：

7 月 29 日，47 次，9:07-23:58

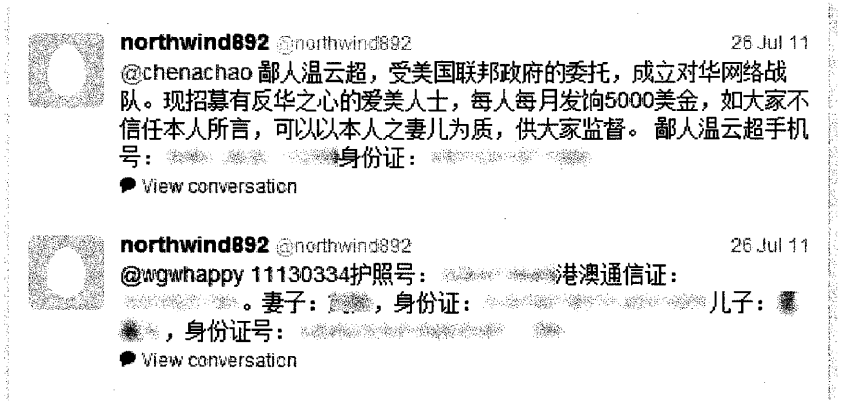
7 月 30 日，71 次，9:31-23:53

7 月 31 日，311 次，12:01-21:03

8 月 1 日，277 次，9:34-23:54

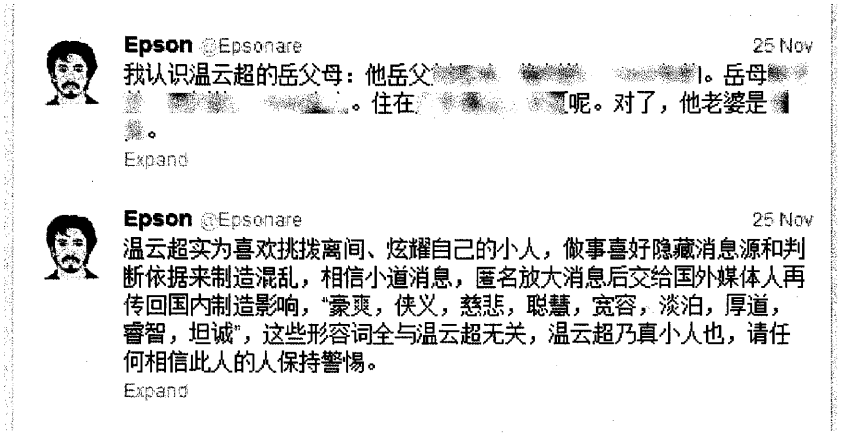
8 月 2 日，107 次，12:32-21:11

附件 4：太太及儿子的信息被发布上网



（来源：https://twitter.com/northwind892）

亲人的信息被发布上网



（来源：https://twitter.com/Epsonare/status/1398897663584624 64）

附件 5 ：Twitter 垃圾资讯轰炸

附件 6 ：（Twitter 污蔑）

输入 @用户名或全名

wrwerw @oiugy548 回复 转推 收藏 打开
温云超的丑恶嘴脸网上皆有真实写照。#北风猪 @wenyunchao #wenyunchao #温云超

QWE56 @btwe5321 2分
温云超的丑恶嘴脸网上皆有真实写照。#北风猪 @wenyunchao #wenyunchao #温云超

wrwerw @oiugy548 2分
这个人的嘴脸竟是如此险恶，我们极力争取的钓鱼岛领土，他竟然说是日本的，不知大家有何感想？#北风猪 @wenyunchao #wenyunchao #温云超

QWE56 @btwe5321 2分
这个人的嘴脸竟是如此险恶，我们极力争取的钓鱼岛领土，他竟然说是日本的，不知大家有何感想？#北风猪 @wenyunchao #wenyunchao #温云超

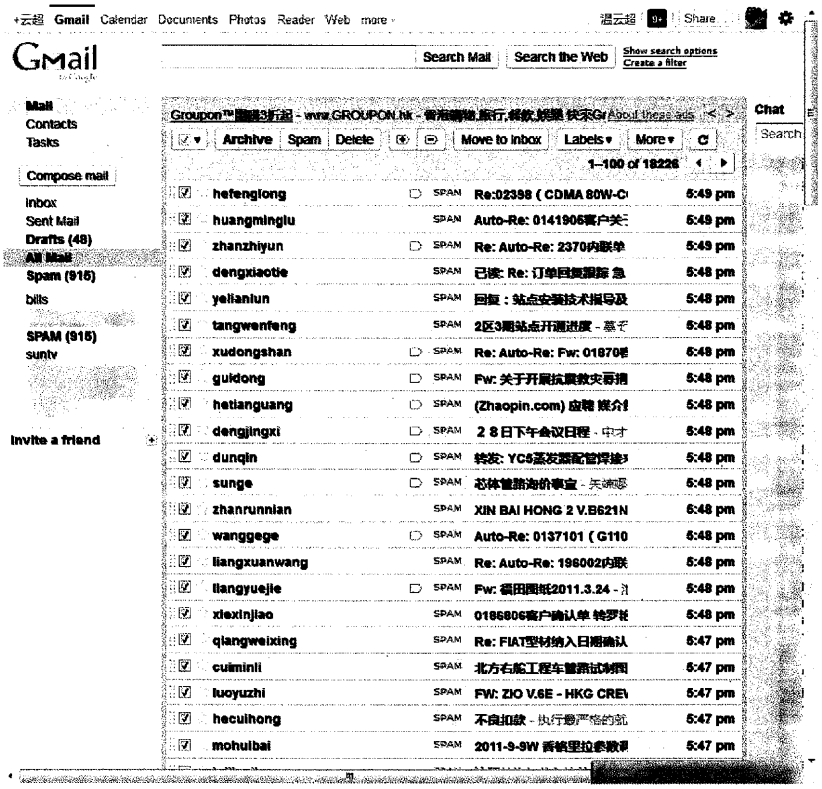
wrwerw @oiugy548 2分
梦想发财温云超， 美国绿卡来洗脑。 人性良知全泯灭， 不做国人做宵小。 境外狼狈同为奸， 专把亲眷朋友骗。#北风猪 @wenyunchao #wenyunch

QWE56 @btwe5321 2分
梦想发财温云超， 美国绿卡来洗脑。 人性良知全泯灭， 不做国人做宵小。 境外狼狈同为奸， 专把亲眷朋友骗。#北风猪 @wenyunchao #wenyunch

wrwerw @oiugy548 3分
温云超自称代表的民意，我们觉得他更象是意淫人民。他种种的反常说明什么其实他的一切言行都是唯西方洋人的意旨行事。#北风猪 @wenyunchao

QWE56 @btwe5321 3分
温云超自称代表的民意，我们觉得他更象是意淫人民。他种种的反常说明什么其实他的一切言行都是唯西方洋人的意旨行事。#北风猪 @wenyunchao

附件 7 ： Gmail 邮箱受到攻击



附件 8 ：网上污蔑我的文章

无耻小人温云超 - Chariweb.com :: 中国
chinese.chariweb.com/ - 轉為繁體網頁
Chariweb.com於 2012年9月4日發表
关于近期李旺阳先生的死，我首先也对"被自杀"深信不疑，而在李死后温云超四处发呼吁搞签名要为李旺阳讨回公道的做法，也让我从未想到李的死会与温云超有关系。然而联想到温云超曾资助过李旺阳，而李并没有提供他所需要的东西，根据温云超 ...

陈然: 我眼中的温云超
chengran911.blogspot.com/ - 轉為繁體網頁
陈然於 2012年9月3日發表
关于近期李旺阳先生的死，我首先也对"被自杀"深信不疑，而在李死后温云超四处发呼吁搞签名要为李旺阳讨回公道的做法，也让我从未想到李的死会与温云超有关系。然而联想到温云超曾资助过李旺阳，而李并没有提供他所需要的东西，根据温云超 ...

龌龊小人——温云超| 天山之子
xaiofa18.blogspot.com/ - 轉為繁體網頁
天山之子於 2012年8月30日發表
逝者长已矣，小人求利时，李旺阳死后，唯恐中国不乱的温云超之流纷纷跳了出来对李旺阳自杀做颠三倒四的评论，呼吁签名要求调查李旺阳自杀"真相"。基于良 心的求知欲，人肉搜索，真是不搜不知道，一搜惊天动地，看到一帖《[惊！！]温云超说钓鱼岛 ...
天山之子 的其他相關資訊

风中的花香: 温云超到底想干什么
jiangwenwen2.blogspot.com/ - 轉為繁體網頁
将文於 2012年7月20日發表
最近网上吵的沸沸扬扬的"李旺阳自杀"事件，各路神仙都有，发表了各种各样的文章。不过旺阳先生已去了，不管他生前做过什么，为人怎么样，但是他毕竟已去了。然而有人却拿起李旺阳的事件不放手，大肆渲染造谣污蔑各党派，比如像温云超之流，台 ...

搜索结果参见：http://is.gd/SaHFFP

Congressional-Executive Commission on China
Hearing
Chinese Hacking: Impact on Human Rights and Commercial Rule of Law
June 25, 2013

Testimony of Louisa Greve
Vice President for Asia, Middle East and North Africa, and Global Programs
National Endowment for Democracy

The Congressional-Executive Commission on China is to be heartily commended for bringing much-needed attention to the extremely important issue of today's intensified, globalized harassment of human rights activists working to bring about the rule of law and human rights in China.

Since 1949, Chinese citizens who dare to speak freely have faced a blanket of harsh repression – there is no freedom of speech in China. Since the dawn of the global Internet, even Chinese who dare to speak freely in any other place on earth have faced a continually renewed campaign of cyberhacking that acts as a virtual blanket of repression of their freedom of speech on human rights in China. Freedom of speech and action is now impeded even outside China.

For Chinese, Tibetan, Uyghur and Southern Mongolian democracy advocates and human rights activists working from exile in democratic countries, cyberhacking has the direct effect of reaching across the boundaries of state sovereignty to directly and severely undermine activists' ability to exercise the fundamental political freedoms they should enjoy in democratic countries. Being under sustained cyber-attack means these groups are not, in practice, able to routinely avail themselves of ordinary access to free communications media and the public square because they cannot count on being able to use normal modern means of communication. Victimized by widespread and gross human rights violations at home, after leaving their homelands, they still contend with cyberhacking – concerted, strategic, and targeted disruptive tactics administered from afar via the Internet.

Numerous human-rights groups concerned with China experience routine and persistent denial-of-service attacks and implanting of malicious code on their websites. Organizations and news sites that have gone public about hackers' success in embedding malware, or closing their websites for days or weeks, include the Human Rights in China, Asia Catalyst, China Aid, the Independent Chinese PEN Center, Canyu, the Office of the Dalai Lama, Aboluowang, Boxun, China Human Rights Defenders, New Century, Livelihood Watch, the World Uyghur Congress, the Uyghur American Association and the Uyghur Human Rights Project.

Activists working on China have contended for at least the past 8-10 years with fake emails spoofing their addresses going out to numerous recipients, purporting to be emails from them, and spear-phishing methods targeting addresses in their own contact lists designed to install surveillance and extraction software on victims' computers, some as early as 2005. The "GhostNet" report by researchers at Information Warfare Monitor made headlines in March 2009 by documenting extensive cyberspying software installed on computers used by Tibetan activists (and dozens of embassies) all over the world, from India to Europe to the U.S., through which hackers could turn on webcams and microphones at will.

Hackers' efforts to shut down the ability of groups to function normally, however, involves much more than DoS attacks and spoofing, spear-phishing and malware, and remote surveillance via keystroke monitors and webcams. Activists report evidence in the past year or two of new, even more Orwellian features of some of the targeted hacking: round-the-clock, real-time, non-machine (human) interference; all-device tracking; and software innovation to attack previously untouched systems, including, most

recently, android systems for mobile phones and tablets. The World Uyghur Congress (WUC) has prepared detailed documentation of its experience in this regard.

Real-time and pre-emptive interference with communication: Spear-phishing attacks are routinely sent among and from Uyghur, Chinese and Tibetan activist circles. In the past, these messages, with attachments containing malware, could often be spotted because the content of the email was strange and poorly written, to the point of misspelling information in the purported senders' address block. Increasingly, hackers obtain genuine messages and re-send them – often within hours, which is a significant factor in increasing their plausibility – for example when they purport to give information about an upcoming conference or event. On May 9 this year, the World Uyghur Congress prepared a written statement on behalf of an ECOSOC-accredited NGO about the Maralbeshi incident in Xinjiang (East Turkestan). On the same day that the writer sent the draft statement for review, the text of the original email asking for comments, and a malware-infected attachment, were sent from a spoofed email address to hundreds of people, not only to addresses in the original sender's contact list, but also to people with whom the sender had never had previous contact. The malware in the attachment was designed to enable the hacker to retrieve the recipients' usernames, passwords, and credit card details. The Uyghur American Association reports at least one incident in which a staff member received a reply to a message to a colleague within an hour, giving a plausible response on an issue that they had been working together on, that turned out to be the work of a hacker. Many of the hackers' fake emails received by Uyghur activists are written in fluent Uyghur (Latin script).

All-device harassment:
--The office and private telephone land-line numbers of several World Uyghur Congress staff in Munich were taken out of commission for a full week around July 5, 2011 due to continuous calls that blocked any use of the phones.
--At the same time, the WUC staff and general email accounts were subject to a massive spam attack. Between July 2 and July 7, a total of 15,000 spam emails were sent to the general account.
--The website was also disabled during this time.

Innovation for attacks via new platforms:
On March 26, 2013, Kapersky Labs[1] documented the first-ever use of a spear-phishing email used specifically to attack android users. The content of the spear-phishing email was extracted from a message sent by the WUC to speakers and participants in its just-concluded conference in Geneva. The email was purportedly sent by a high-profile Tibetan activist who had been at the conference. The malware was designed such that when the victim reads the email, the malware reports the infection to a command-and-control server and then begins to harvest information stored on the device. The copied data includes data about the phone itself (phone number, OS version, phone model, SDK version); contacts stored both on the phone and the SIM card; call logs; SMS messages; and geo-location.

The deliberate, directed characteristics of this campaign deserve emphasis.

Many overseas groups experience interference that is extremely sophisticated and conducted in real time. Hackers are creating fake emails, often of a spear-phishing nature or with malicious code attached, using content that had been sent between colleagues, within an hour or two after initially being sent. Often, the hacker uses the same errors in syntax, spelling, and grammar that the purported sender makes when using a second or third language on a day-to-day basis.

The attacks over the past few years reveal a significant upgrading of resources devoted to the attacks, in terms of increasing technical skills, language proficiency, and technical means. Activists report, for

[1] http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf, June 5, 2013

example, that the English-language proficiency and Uyghur-language proficiency of the hackers is much better than it was only a year ago. Hackers are using the most up-to-date code available – often same-day code -- to evade commercially available defenses. The extent of new and innovative software used in the hacking is an indicator of massive resources being devoted to the effort.

And we should note that the political targeting is explicit: attacks surge before sensitive political anniversaries in China -- June 4 every year, and since 2009, on and around July 5, the date of the deadly street violence in Urumqi that escalated from a peaceful protest to deadly ethnic rioting and lethal riot-suppression.

Hacking is a potent tactic for hampering and impeding the work of human rights advocates because of its numerous practical effects:

It silences activist groups' ability to communicate with the wider public or, in the case of independent media, disseminate news, when sites are shut down for extended periods.

It degrades their ability to conduct professional human-rights documentation by compromising groups' ability to keep information confidential. This can be devastating, and extends to assistance to refugees, as for example cases when Uyghurs are in deportation proceedings in Europe; alternative, manual means of communicating and documenting abuses take enormous time or make documentation impossible when researchers and witnesses are dispersed across different continents.

It distracts and diverts the energies of activists, by forcing them to deal with recovery from cyber-attacks and to double-check the authenticity of all the communications they receive.

It raises the monetary cost of the work by requiring multiple data backup systems, expensive specialized technical assistance, and often extensive and time-consuming searches for alternative server space .

It sows distrust and wastes time, as activists routinely cannot trust incoming communications.

It undermines cooperation in the wider world, as international organizations, experts, and media experience the frustration of fake and malicious emails purportedly from the targeted NGOs.

Hacking also increases fear, even among those who live in free countries. The real-time, all-device surveillance and tracking achieves a potent deterrent effect by making people afraid to be in contact with each other, whether outside of China (for fear of compromising strategies or confidential information, such as the identities of witnesses or victims) or inside China (for fear of instigating harassment or arrest of contacts).

The repressive effects of cyberhacking – bringing about conditions that silence critical voices, undermine the credibility of independent actors, undermine trust among dissidents, increase isolation, raise costs, and induce fear – is a remarkable extraterritorial extension of the tactics of repression practiced by authoritarian states. It deserves the outraged condemnation of all responsible institutions and defenders of universal human rights.

DETAILS OF SAMPLE DENIAL-OF-SERVICE CASES

June 14, 2013 - The Independent Chinese PEN Center (ICPC) and Canyu, the human rights documentation site maintained by China Free Press, publisher of the widely read citizen-journalism site Boxun, came under malicious attacks for 24 hours on June 14.

September 2012 – One of a series of regular DoS attacks on the website of the Uyghur American Association, designed to embed malicious code to infect website visitors' computers, succeeded. This series of attacks was identified as originating from IP addresses in China.

The websites of both the Uyghur American Association and the Uyghur Human Rights Project are blocked inside China. Yet these sites report that they experience regular flooding-style DDoS attacks (overwhelming numbers of data requests) that originate in part from IP addresses in China, which suggests that the attacking Chinese IP servers have unrestricted access to the Internet beyond the Chinese firewall.

February 2011 - Aboluowang, a news site run by Falun Gong volunteers, was attacked for two weeks, forcing even readers outside China to use proxies to visit the site.

Nov-Dec 2010 and Jan-April 2011 - The Independent Chinese PEN Center website was taken down for extended periods during the period when Liu Xiaobo's Nobel Peace Prize was in the news and the first few months of the Arab Spring.

October 2010 – Canyu and Chinese Human Rights Defenders, sites dedicated to documentation of human rights abuse, had their data deleted.

January 2010 – ICPC, Canyu, Chinese Human Rights Defenders, New Century, Livelihood Watch issued a joint statement condemning the series of DDoS attacks on their sites and numerous others in the period after the sentencing of Liu Xiaobo and the Google pullout. The scale and sophistication of the attack prompted a commercial server-space vendor based in the US to cancel its contract with a NED-supported US-based NGO that was providing hosting services for several of these sites. The NGO was forced to turn to inadequate temporary solutions using Twitter and disseminating information from blogspot pages for a number of weeks. For more details:

五中文网站关于网站受到恶意攻击的联合声明
http://peacehall.com/news/gb/china/2010/01/201001241220.shtml
关于《参与》网站近期被持续攻击的声明
http://peacehall.com/news/gb/china/2010/10/201010160141.shtml
"维权网"关于网站受到攻击的声明
http://peacehall.com/news/gb/china/2010/01/201001241233.shtml
博讯、参与等网站关于网站受到恶意攻击的联合声明
http://boxun.com/news/gb/intl/2012/04/201204282215.shtml#.UbNJFS2DE5s

---

PREPARED STATEMENT OF HON. SHERROD BROWN, A U.S. SENATOR FROM OHIO; CHAIRMAN, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

JUNE 25, 2013

I thank Cochairman Chris Smith, the other Commissioners, and our esteemed panel for attending this important hearing.

I also thank the staff for their tireless efforts in supporting the work of this bipartisan Commission and its important task of monitoring human rights and rule of law developments in China.

Cyber attacks from China pose a serious threat to U.S.-China relations.

So much so that President Obama raised the issue during his recent summit with President Xi Jinping. It will be a key topic at the U.S.-China Strategic and Economic Dialogue to be held in Washington in a few weeks.

Today's hearing will focus on the aspects of cyber that fall within the Commission's mandate, namely the impact on the rule of law and human rights in China.

While recent headlines have revived the debate over the appropriate balance between security and freedom, we must not overlook the enormous impact cyber attacks from China have had and continue to have on American jobs and companies. Indeed, they seriously call into question China's commitment to the rule of law.

We are talking about the massive theft of valuable technology and commercial secrets from American companies—what General Keith Alexander, director of the National Security Agency and head of U.S. Cyber Command, calls the "greatest transfer of wealth in history."

The scale and scope is staggering. The Commission on the Theft of American Intellectual Property, which is represented here today by our former colleague Senator Slade Gorton, released a comprehensive, report identifying China as the world's biggest violator of intellectual property rights.

It estimates that China accounts for some 50 to 80 percent of IP theft in the United States and around the globe. It found that international IP theft, including from China, costs the U.S. economy hundreds of billions of dollars per year and millions of jobs, dragging down our GDP and undermining our ability to innovate and prosper.

The IP Commission noted that a 2011 study by the U.S. International Trade Commission estimated that if China's IP protection improved to a level comparable to ours, it would add 2.1 million jobs to our economy. Yet, the IP Commission acknowledged this figure underestimated the real cost to American jobs.

The victims of IP theft include companies in my state of Ohio and across the nation. Those affected are hard-working Americans trying to make an honest living and trying to spur innovation, only to see their products, services, and technology stolen and handed over to state-owned enterprises and businesses in China.

And with the growing prevalence of computer networks and America's heavily-wired economy, cyber attacks represent an increasingly growing threat alongside more traditional forms of IP theft.

China simply doesn't play by the same rules as we do. The Chinese government has denied these attacks, even though there is mounting evidence of Chinese state involvement. This evidence includes a February 2013 report by the cyber security firm Mandiant that linked attacks on 141 companies, including 115 based in the United States, to a unit of the People's Liberation Army working from a building in Shanghai. The increase in attacks has coincided with the Chinese government's push for indigenous innovation and development of key industries, creating an environment where it's perfectly acceptable to cheat and steal your way to the top.

And as we've seen in the last few years, it's not only American companies that are the target of cyber attacks. It's also media and human rights organizations. Journalists writing about corruption in China find their computer systems hacked and passwords stolen. For human rights organizations and activists, dealing with hacking attacks from China is almost a daily fact of life.

We can't sit idly by while the Chinese government, either through active measures or by turning a blind eye, continues to perpetuate theft on a grand scale and to threaten the advance of human rights for the Chinese people, Tibetans, Uyghurs, democracy advocates, religious followers, and Falun Gong practitioners.

That's why I support a comprehensive, common sense, bipartisan approach that utilizes every tool in our arsenal to hold China accountable and to level the playing field. I urge Congress and this Administration to do everything it can—from leveraging access to our markets, trade negotiations, and WTO cases—to combat China's unfair trading practices. That includes taking up the bipartisan Currency Exchange Rate Oversight Reform Act of 2013 which I introduced earlier this month.

And I commend Senator Levin for his recent proposed legislation to hold China accountable for cyber theft. I look forward to hearing from our witnesses on what more we can do to address this most pressing issue.

PREPARED STATEMENT OF HON. CHRISTOPHER H. SMITH, A U.S. REPRESENTATIVE FROM NEW JERSEY; COCHAIRMAN, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

JUNE 25, 2013

In December of 2006 and then again in March of 2007, my Human Rights Subcommittee's computers were attacked by a virus that, in The U.S. House Information Resources Office's words, "intended to take control of the computers." At that time, the IT professionals cleaned the computers and informed my staff that the attacks seemed to come from the People's Republic of China. They said it came through or from a Chinese IP address. The attackers hacked into files related to China. These contained legislative proposals directly related to Beijing, including a major bill I authored, the Global Online Freedom Act. Also hacked were e-mails with human rights groups regarding strategy, information on hearings on China

and the names of Chinese dissidents. While this absolutely doesn't prove that Beijing was behind the attack, it raises very serious concern that it was.

Certainly, Chinese agents have not only attempted to target me or my offices. Cyber attacks on Congress are only a small, but not insignificant, part of a much larger pattern of attacks that has targeted the executive branch, the Pentagon, and American businesses.

How do we know this? In recent months, we have seen in-depth reports come out detailing this massive intrusion into our cyber space and massive theft of our cyber data. Chinese agents have stolen our designs for helicopters, ships, fighter jets, and several missile defense systems. They have stolen our innovative technologies, from solar panel designs to biotech research. These thefts appear to have paid off for China. In recent years, the Chinese government has made tremendous jumps in its military capabilities, while boosting the competitiveness of China's "national champions."

While cyber thefts have existed for years, increasingly, we can prove that many of these outrageous thefts—deemed "the greatest transfer of wealth in history"—originate in the People's Republic of China. And these attacks are not random. We now know, with some certainty, that some thefts are being organized by Chinese government agencies.

As we learn about the source of these attacks, we are also learning about the motivations. Talented Chinese Internet users are working day and night to infiltrate our networks and to steal secrets. China's actions are part of a larger and coordinated state-sanctioned effort to increase China's competitiveness, militarily and commercially.

Today, we will hear more about how the commercial rule of law system in China allows these types of attacks to occur and how these attacks disadvantage American business, innovators, contractors, and government agencies. We will hear about the size and scope of the attacks. And, we will hear how the U.S. government remains unprepared for far too many of these challenges.

We will, also, however, hear about another side of this important topic—one often overlooked during the recent discussions about China's cyber attacks. The Chinese government is not only targeting American business and military organizations, but also targeting ordinary Chinese citizens seeking to advance their most fundamental freedoms. Chinese hackers do not simply look beyond their borders to steal secrets. As we will hear today, Chinese citizens—including those advocating for human rights, free speech and food safety—are also targeted by state-sponsored hackers.

These courageous citizens are also monitored; their private information stolen. The brave pastor seeking to organize a service, the father seeking to raise awareness about toxic foods, the wife of an imprisoned activist, the mother who is made to undergo a forced abortion—all of these citizens realize that, in any instant, the government may be watching. China, of course, also targets those outside of China who similarly wish for human rights and political reform.

Today, we know this system of surveillance and theft occurs. We know that China is organizing these cyber attacks—or is, in the very least, complicit to their existence.

The question we must ask ourselves is why? Clearly, China's rise as a military power requires technology, and China's economy will, no doubt, benefit from the latest innovations from abroad.

But, why is China so concerned about its domestic citizenry—especially those who advocate peacefully for legal and political reforms? Why is China so worried about international NGOs that seek to highlight official abuses and wrongful imprisonments? Why is China so reluctant to provide a fair regulatory environment in China, when commercial laws and regulations will eventually protect all businesses—domestic and foreign—seeking to provide the best services for Chinese consumers?

These may be difficult questions. Thankfully, today we are fortunate to have four guests who are well versed in these issues. They are experts on how China is monitoring our cyber actions and how China is attacking targets globally. I would like to thank them for their participation here today, and I look forward to hearing their insights on these critical issues.

○