AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ASIA: THE CYBER SECURITY BATTLEGROUND

HEARING

BEFORE THE

SUBCOMMITTEE ON ASIA AND THE PACIFIC

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JULY 23, 2013

Serial No. 113–42

Printed for the use of the Committee on Foreign Affairs

Available via the World Wide Web: http://www.foreignaffairs.house.gov/ or http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

82–145PDF 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

COMMITTEE ON FOREIGN AFFAIRS

EDWARD R. ROYCE, California, *Chairman*

CHRISTOPHER H. SMITH, New Jersey
ILEANA ROS-LEHTINEN, Florida
DANA ROHRABACHER, California
STEVE CHABOT, Ohio
JOE WILSON, South Carolina
MICHAEL T. MCCAUL, Texas
TED POE, Texas
MATT SALMON, Arizona
TOM MARINO, Pennsylvania
JEFF DUNCAN, South Carolina
ADAM KINZINGER, Illinois
MO BROOKS, Alabama
TOM COTTON, Arkansas
PAUL COOK, California
GEORGE HOLDING, North Carolina
RANDY K. WEBER SR., Texas
SCOTT PERRY, Pennsylvania
STEVE STOCKMAN, Texas
RON DESANTIS, Florida
TREY RADEL, Florida
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
TED S. YOHO, Florida
LUKE MESSER, Indiana

ELIOT L. ENGEL, New York
ENI F.H. FALEOMAVAEGA, American Samoa
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
THEODORE E. DEUTCH, Florida
BRIAN HIGGINS, New York
KAREN BASS, California
WILLIAM KEATING, Massachusetts
DAVID CICILLINE, Rhode Island
ALAN GRAYSON, Florida
JUAN VARGAS, California
BRADLEY S. SCHNEIDER, Illinois
JOSEPH P. KENNEDY III, Massachusetts
AMI BERA, California
ALAN S. LOWENTHAL, California
GRACE MENG, New York
LOIS FRANKEL, Florida
TULSI GABBARD, Hawaii
JOAQUIN CASTRO, Texas

AMY PORTER, *Chief of Staff* THOMAS SHEEHY, *Staff Director*
JASON STEINBAUM, *Democratic Staff Director*

SUBCOMMITTEE ON ASIA AND THE PACIFIC

STEVE CHABOT, Ohio, *Chairman*

DANA ROHRABACHER, California
MATT SALMON, Arizona
MO BROOKS, Alabama
GEORGE HOLDING, North Carolina
SCOTT PERRY, Pennsylvania
DOUG COLLINS, Georgia
LUKE MESSER, Indiana

ENI F.H. FALEOMAVAEGA, American Samoa
AMI BERA, California
TULSI GABBARD, Hawaii
BRAD SHERMAN, California
GERALD E. CONNOLLY, Virginia
WILLIAM KEATING, Massachusetts

CONTENTS

Page

WITNESSES

Phyllis Schneck, Ph.D., vice president and chief technology officer, Global Public Sector, McAfee, Inc. 6
Mr. James Lewis, director and senior fellow, Technology and Public Policy Program, Center for Strategic International Studies 15
Mr. Karl Frederick Rauscher, chief technology officer and distinguished fellow, EastWest Institute 23

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Phyllis Schneck, Ph.D.: Prepared statement 9
Mr. James Lewis: Prepared statement 17
Mr. Karl Frederick Rauscher: Prepared statement 25

APPENDIX

Hearing notice 56
Hearing minutes 57

ASIA: THE CYBER SECURITY BATTLEGROUND

TUESDAY, JULY 23, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ASIA AND THE PACIFIC,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:24 p.m., in room 2172, Rayburn House Office Building, Hon. Steve Chabot (chairman of the subcommittee) presiding.

Mr. CHABOT. The committee will come to order.

Good afternoon. I would like to welcome everyone, my colleagues and our distinguished witnesses, to the Subcommittee on Asia and the Pacific hearing this afternoon. The ranking member Mr. Faleomavaega and I will make opening statements, and then other members of the subcommittee will be recognized for making 1-minute statements should they wish to do so.

Over the course of the last few years, there has been growing acknowledgment of the need for an international cyber security policy. The growing interdependence of the world by way of the Internet and vast frequency and similarity of cyber attacks reported in nearly every corner of the Earth illustrates why.

As they say, cyberspace knows no borders. This implies that cyber security is only as good as its weakest link. In other words, we can work tirelessly to build up the defenses of our critical infrastructure systems and networks here in the U.S., but back doors could still be found in overseas routing points and links in the global supply chain, for example, through which adversaries can find ways to attack U.S. Government systems and private companies. This is why the U.S. must engage its allies around the world to promote the preservation of global network functionality, in addition to establishing confidence-building measures that foster trust and reliability with nations that have become Wild West havens for cyber criminals so that we can close these back doors.

As an effort to recognize cyber security's growing international attention and importance, the State Department established the Office of the Coordinator for Cyber Issues in 2011 to more effectively coordinate global diplomatic engagement on cyber issues. It was around the same time that the White House issued its International Strategy for Cyberspace.

While we are not here today to discuss the progress or effectiveness of this relatively new State Department office, I think at the very least it is an acknowledged step in the right direction, even if they could not somehow provide anyone to brief the sub-

committee on its activities before this afternoon. Even so, today's hearing is part of our efforts here in Congress to examine how to advance this strategy in such a critical region of the world as Asia.

Almost every day U.S. businesses are victims of cyber exploitation and theft by nation-state actors such as China. Theft of intellectual property not only takes away American jobs and hurts innovation and competitiveness, but it costs U.S. businesses anywhere between $200 billion and $400 billion a year. In order to engage American economic prosperity and security, the integrity and openness of our networks must be maintained. And as we discuss this afternoon the evolving threats and a growing number of cyber challenges facing our Nation, I recognize this will be no easy task.

Asia is a region beset by some of the world's most aggressive cyber actors. I think it is fitting that today's hearing calls the region the cyber security battleground, because as Asia has become the most economically dynamic region in the world, it has also become the hub of cyber conflict. Alternatively, while Asia is not an actual battleground as we know one to be or in the throes of a drawn-out war, this term symbolizes that the region is faced with many serious threats and actors that are unstable, uncertain and volatile.

It is unlikely for a real cyber war to start between Asian nations at this point, but it is critical to note how cyberspace has become a source of great economic and military rivalry, as well as the primary medium for political activism. As we know, in many Asian nations political dissent via the Internet is obstructed by ruling governments and considered a threat. An issue we discuss here frequently, this is a source of great internal conflict and human rights abuses.

Nevertheless it is the networked interconnection of our lives, information, financial systems and institutions that is enabling global business to expand and thrusting growing Asian economies forward, providing before-unavailable economic opportunities to people throughout the world. Competition is growing, and with the growth of competition has come the growth of malicious activities aimed at stealing economic and military secrets for groups and nations to get ahead. Nearly every military in Asia will eventually have some level of cyber capability, if they don't already, and because of cyberspace's lack of security or an established set of norms, the risk of miscalculation only grows. This is why regional engagement on cyber is imperative because building trust capacity and security is not going to be easy and it will take time.

The "cyber powers" in Asia include the U.S., China, Taiwan, South Korea, North Korea and Australia. Just like many other issues in Asia, the growth of cyber capabilities in these countries and other Asian nations revolves around China's strength and growing desire for influence. China has been called by numerous high-level officials in the Obama administration an advanced cyber actor and an aggressive practitioner of economic espionage against the U.S., and no doubt, our allies in Asia as well.

The instances in which China was behind cyber attacks or intrusions of U.S. Government systems and companies are endless. While I think that opening dialogue with the Chinese about cyber crime, theft and espionage is good, establishing some sort of norms

or principles to guide actions in cyberspace that the Chinese can agree to will be incredibly difficult. China will continue to deny accusations, and its behavior is unlikely to change.

Similarly, North Korea's behavior has shown its aversion to change; however, the Kim regime is not only unstable, irrational, and erratic, but it is also risk averse. North Korea's growing cyber capabilities present the greatest likelihood of a cyber conflict in Asia. Earlier this year it demonstrated its capabilities in South Korea, where it crippled the operations of banks and news agencies by wiping the hard drives of thousands of computers. While McAfee's report on what is now called Operation Troy does not attribute these attacks to North Korea, it could not be clearer who was responsible. North Korea is not only a nuclear threat, but it a serious cyber threat as well.

Lastly, we cannot forget the cyber threats emerging from Pakistan that challenge the national security of the U.S. and its neighbor, India. Mutual distrust dominates the relationship, which severely hampers opportunities for bilateral cooperation. As home to numerous terrorist groups, the cyber risks materializing from Pakistan are exceedingly multifarious. Just the other day the Director of the National Security Agency said, "Terrorists use our communications devices. They use our networks . . . they use Skype, they use Yahoo, they use Google . . . and they are trying to kill our people." Cyber terrorism is real.

I look forward to hearing the witnesses' testimonies today, and I thank each of you for making the time to be here. The private sector's role in building cyber collaboration and awareness in Asia is just as important as what our administration is doing, so I am glad we have a diverse panel here this afternoon.

I now yield to my good friend, the gentleman from American Samoa, the ranking member, Mr. Eni Faleomavaega.

Mr. FALEOMAVAEGA. Thank you, Mr. Chairman. And I do appreciate your leadership and especially for calling this hearing this afternoon.

I also want to welcome personally our distinguished guests and members of the panel, who are pretty capable experts in this area of cyberspace or cyber security.

Cyberspace is a global infrastructure that has become the backbone of the world economy, but as we know, it is badly secured and governed. Asia Pacific is a focal point for cyberspace, and the information technology industry is mostly Pacific-based with the U.S., India and other Asian countries creating the most digital products.

While this kind of technology is providing economic opportunity in the region, there is also a downside when it comes to cyber conflict. Cyber conflict involves the planning for military and strategic competition, and asymmetric warfare and engagement, and economic espionage to gain long-term economic and trade advantages. Cyber powers include the United States, China, Taiwan, South Korea, North Korea, and Australia, and New Zealand. And Japan and India are exploring military cyber capabilities as well.

China and the United States are engaged in the strategic competition: How do we plan ahead of establishing rules of the road in cyberspace? Interesting to note, Mr. Chairman, there are some 500 million people in China are Internet users, with some addi-

tional 300 million use Twitter, like our version of Twitter. So it is very interesting that the fact that out of the total population of some 7 billion people living on this planet, over 50 percent of the world's population reside in the Asia Pacific region, and I think it is quite obvious that this region is very important.

I recall a couple of years ago when the People's Republic of China had developed a missile that was capable of shooting the satellite, Chinese satellite, that was traveling some 18,000 miles per hour, and they were able to do it. Oh, there was a tremendous uproar about China violating whatever it was. The fact of the matter is the United States and Russia were about 20 years ahead of China as far as this kind of cyberspace security technology that we have developed.

I think it is important that in terms of what is happening in countries like China, I am a little more optimistic to the fact that because of this number of Internet users, despite the problems with security and the way the government controls this technology, the fact of the matter is I don't see how any government is going to be able to control public demand and the wanting to use the way it is done right now in China, and I think it is going to come out with better results in terms of greater freedom and greater access to the Chinese consumers and whatever it is that they want to do as far as developing and improving their economic well-being.

With that, Mr. Chairman, I look forward to hearing from our witnesses this afternoon. Thank you.

Mr. CHABOT. Thank you.

We will now recognize members in case they would like to make opening statements. We will do it in the order they arrived once we started.

The gentleman from Pennsylvania, Mr. Perry, is recognized.

Mr. PERRY. Thank you, Mr. Chairman.

Gentlemen, ladies, thank you for your time and testimonies today in advance.

Consumers in government, private companies have grown increasingly reliant on cyberspace to manage projects, reach potential clients, serve their constituents and disseminate mission-critical information. Unfortunately, as you know, cyber threats have more than kept pace, and, according to reports this year, will be an even more sophisticated assault on business, private citizens and government organizations.

Former Secretary of Defense Panetta warned government and business leaders to be prepared for an escalation of cyber attacks. Rather than simply being prepared for disruption in organizations' activities in cyberspace through denial-of-access regimes, leaders need to develop strategies to handle destructive behavior that cripple systems or corrupt data.

There has been no shortage of recommendations to address this concern because of the immense value of information shared on secured networks and systems. Private-sector companies have a financial and competitive incentive to safeguard their intellectual property and to ensure novel innovations are brought to market. Public-sector entities must safeguard sensitive information, including intelligence reports, citizens' personal information, and financial data, and national security information, to keep it secure and

protect it from those who wish to harm our people and our economy.

In light of our military and economic strategic shift to the Asian Pacific region, it is increasingly important that we put great focus on this area of the world when considering cyber security policy.

Thank you. I look forward to your testimony, and I yield back.

Mr. CHABOT. Thank you. The gentleman's time has expired.

The gentleman from California, Mr. Bera, is recognized.

Mr. BERA. Thank you, Mr. Chairman, and thank you, Ranking Member, and thank the witnesses.

We live in an interconnected world. We live increasingly in a world and an economy that is global and interconnected, and that does create more marketplaces. It does create more efficient opportunities for us to move information, for us to—a more efficient financial marketplace.

But with that interconnectiveness are real threats and vulnerabilities, and the opportunity for us to come together as democratic countries, as freedom-loving countries, you know, particularly countries like the U.S., India, Taiwan, South Korea, Japan, to really protect this interconnectedness and protect what the future looks like, but at the same time be very cognizant of the threats and vulnerabilities.

I look forward to hearing from the witnesses on how we allow this marketplace to grow, how we allow this interconnectedness to grow, but, again, being vigilant of the threats that they pose and how we protect us from those threats.

So thank you. I yield back.

Mr. CHABOT. Thank you. The gentleman yields back.

If there are no other members who wish to make opening statements, we will go ahead and introduce the panel at this time.

Our first witness will be Dr. Phyllis Schneck. Dr. Schneck is the chief technology officer for public sector at McAfee, Inc. In this role she is responsible for the technical vision for public-sector applications of security and global threat intelligence, cyber security technology, and policy strategies, leading McAfee security and intelligence initiatives in critical infrastructure protection and cross-sector cyber security.

She has served as a commissioner and a working group co-chair on public-private partnership, and co-chaired the Critical Infrastructure Protection Congress. She is also the chairman of the board of directors of the National Cyber Forensics and Training Alliance. Previously, Dr. Schneck served for 8 years as chairman of the national board of directors of the FBI's InfraGard program and founding president of InfraGard Atlanta.

Named one of the Information Security Magazine's top 25 women leaders in information security, she has briefed the Governments of Japan, Australia and Canada on information sharing and infrastructure protection. Dr. Schneck has also served as vice president of research integration for Secure Computing, vice president of Enterprise Services for eCommSecurity, vice president of Corporate Strategy for SecureWorks, Inc., and was founder and chief executive officer of Avalon Communications, among many others. She received her Ph.D. in computer science from Georgia Tech. We welcome her here this afternoon.

Next, I would like to introduce James Lewis, who is a senior fellow and program director at CSIS, where he writes on technology, security and international relations. Before joining CSIS, he worked at the Departments of State and Commerce. He has also served as the Rapporteur for the 2010, and the 2012–2013 United Nations Group of Governmental Experts on Information Security. His current research examines the political effects of the Internet, asymmetric warfare, strategic competition and technological innovation. Dr. Lewis received his Ph.D. from the University of Chicago. We welcome you here this afternoon.

Finally, we have Karl Frederick Rauscher, who is a distinguished fellow and the chief technology officer of the EastWest Institute. Leading the institute's Worldwide Cybersecurity Initiative, he oversees strategic track 2 bilaterals among the world's cyber superpowers—China, India, EU, Russia and the U.S.; pioneers—policy for norms of behavior for cyber conflict, advances emergency preparedness for crises in cyberspace, and helps foster innovative problem solving in the private sector. He recently led and authored reports for three major bilaterals between the U.S., China, and Russia.

He previously served as executive director of the Bell Labs Network Reliability and Security Office of Alcatel-Lucent. Mr. Rauscher has also served as an advisor for senior government and industry leaders on five continents, including as vice chair of the U.S. President's National Security Telecommunications Advisory Committee industry executive committee and as leader of the European Commission-sponsored study on the Availability and Robustness of Electronic Communications Infrastructures.

Mr. Rauscher is the founder and president of the nonprofit Wireless Emergency Response Team, which led search-and-rescue efforts using advanced wireless technology in the disaster sites of September 11th, 2001, and the 2005 Hurricane Katrina New Orleans flood.

We welcome all three of our witnesses here this afternoon. You will each be given 5 minutes to testify. There is a lighting system on the desk. The yellow light will let you know you have 1 minute to wrap up. The red light will let you know that your time has expired. We would ask you to wrap up by that time. Then we will have 5 minutes to ask questions.

Dr. Schneck, we will go to you first. You are recognized for 5 minutes.

STATEMENT OF PHYLLIS SCHNECK, PH.D., VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR, MCAFEE, INC.

Ms. SCHNECK. Thank you, and good afternoon, Chairman Chabot, Ranking Member Faleomavaega, and other members of the subcommittee. As said, I am Phyllis Schneck, VP and chief technology officer for global public sector for McAfee. We really appreciate the subcommittee's interest on these issues and the security threats as well as the solutions on certainly how we keep that economy going to the point before.

My testimony today will focus on three areas: The threat landscape; and, as the chairman mentioned, the attacks against South

Korea that McAfee investigated and named Operation Troy; and recommended security solutions. Again, how do we allow this economy to grow?

A little bit about McAfee. Our role in cyber security is to protect our customers worldwide from these cyber threats. We are headquartered in Santa Clara, California; Plano, Texas; and a wholly owned subsidiary of the Intel Corporation. And we are the largest dedicated security company in the world focused on protecting against those threats with products, services, and, as I will describe in a moment, deep investigations of that threat which help us understand how to go out and protect against an adversary that moves faster than we do, because they have no lawyers, they have no laws, and they have plenty of money. So we have to find ways to maintain our economies and execute even faster.

I am going to focus on a little bit different today. Instead of just the threat that we hear about from the Asia Pacific region, let us talk a little bit about the threat to the region as we saw in Operation Troy demonstrated against South Korea. As was mentioned, the Asia Pacific region has a large economy. It affects a lot of our global marketplace today, and so many of those businesses that are impactful there are based on Internet, Internet communications, which makes cyber security so important so that we build in resilience and keep those markets up for the rest of the globe.

We heard about on March 20th the attacks against South Korea against the banking and financial institutions. McAfee led an investigation we called Operation Troy. I do want to call out my colleagues, one for McAfee Labs, Ryan Sherstobitoff, for the record; and one from Office of the CTO with me was Jim Walter, who really led and dove into this investigation.

I also want to start out by defining "malware." Malware is an enemy's instruction or a malicious instruction that executes on someone else's machine, thus giving someone else control of your cyber. Their instruction is next to execute memory, and that is important, and I will get to that in a moment.

But on March 20th, in the end of an operation that we discovered was actually a covert operation of espionage spanning 4 years, Operation Dark Seoul landed instructions on machines in South Korea that erased the disk drives of many of those machines, and also you hear in the news it said it "wiped the master boot record." That means it disabled or erased the record that would have been used by that machine to even start up. So the industry term is it bricked them, it destroyed the machines. And what we discovered is that this had been going on about 4 years. This was the seventh variant. That is just sort of a different version of malware that had been used over those 4 years.

And here is how we actually investigated that. If you look at two things, one we call fingerprints, what it looks like. Actually we discovered the same file path, or directory, or names in malware going back all the way to December 2009 used by campaigns all the way, again, through 4 years, winding up in this attack. And the second thing we look at is called footprint. So, again, not what it looks, the fingerprint; the footprint is how the thing moves.

So over the past 4 years, the adversaries had used dedicated machines to send the instructions to the malware. So they were lit-

erally shipping instructions to malware that was embedded in machines in South Korea. And it is important to note this malware got to the machines in South Korea likely by a first victim clicking on a link in what they call a spear phish, or a custom-made email that looks like it is just for you. Then the instructions would be sent in from a dedicated machine, and we believe that the malicious code was propagated to the other machines from that; and then a second stage through a regular software update. So it looked like you were improving the security of your software when really you were downloading more enemy code. And, again, the footprint of this or how they did it for the first 4 years was having a dedicated machine to feed the malicious instructions.

The more modern, sophisticated version that they landed in Dark Seoul in South Korea was through the use of a botnet, a more dynamic system which made actually the adversary more resilient. You take out one machine, there are thousands of others you can use.

So on the more optimistic side, what can we do to keep economies up? At McAfee we believe very strongly in connected security systems. Every component of your network should be a producer and consumer of information. Don't let instructions execute that should not. Have networks run resilience, like the human body and immune system behaviorally attack viruses or disease or things that we know are bad without knowing their name. And all computer systems should learn from events from others, having them connected in real time. And we are active worldwide in these types of operations to ensure that we share information and, again, keep these economies alive.

So again, thank you very much for requesting McAfee's views on these issues, and happy to answer any questions.

Mr. CHABOT. Thank you very much.

[The prepared statement of Ms. Schneck follows:]

STATEMENT OF DR. PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR

McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON FOREIGN RELATIONS

SUBCOMMITTEE ON ASIA AND THE PACIFIC

"ASIA: THE CYBER SECURITY BATTLEGROUND"

JULY 23, 2013

Good morning, Chairman Chabot, Ranking Member Faleomavaega, and other members of the subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector for McAfee, Inc., a subsidiary of Intel Corporation. We appreciate the subcommittee's interest in cyber security threats and solutions as they affect Asia and the Pacific.

My testimony will focus on the following areas:

- The threat landscape in Asia Pacific
- Attacks against South Korea, as demonstrated by Operation Troy
- Recommended security solutions

I'm going to focus on something a little different, and that is the threats *to* the region rather than the threats *from* the region.

First I would like to provide some background on my experience and on McAfee.

I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to my role with McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 400 cyber criminals worldwide.

Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence. I am the Vice Chair of the Information Security and Privacy Advisory Board (ISPAB) and have

also served as a commissioner and working group co-chair on the public-private partnership for the Center for Strategic and International Studies (CSIS) Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Prior to joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

McAfee's Role in Cyber Security

McAfee protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combatting the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 160 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Threat Landscape for Asia and The Pacific

The APAC region consists of over half of the world's population and is made up of a diverse group of countries with different levels of technological expertise and capacity. Capacity building is of utmost importance for all regional organizations in order to maintain a safe and prosperous cyber industry. Businesses relying on the Internet or IT industries are responsible for much of the region's recent prosperity and are critical for the continuing growth and development of APAC populations. Gaps in expertise, however, expose vulnerabilities in the cyber infrastructure of the region. In other words, if a hacker can target the weakest link in the APAC cyber infrastructure, one attack can

potentially cause damage throughout the region and to global supply chains. Thus, capacity building, information sharing and cyber security are critically important to APAC nations. This is particularly relevant as it pertains to certain extremist sectors of the population of Southeast Asian nations, who may potentially exploit weaknesses in the region's security infrastructure to meet their economic/political/ideological ends.

I want to focus in on South Korea, which has recently experienced attacks on several of its official websites, including that of its president and its ruling conservative party. Earlier, experts at McAfee investigated the Dark Seoul attacks in March that affected the country's financial and media sectors. This operation, led by McAfee researchers Ryan Sherstobitoff and Jim Walter, is known as Operation Troy.

Operation Troy

When reports of the Dark Seoul attack on South Korean financial services and media firms emerged in the wake of the attack on March 20, 2013, most of the focus was on the Master Boot Record (MBR) wipe functionality, or the ability to destroy the MBR, which is necessary for a computer to "boot" or start up, as it finds the correct location on the disk for boot instructions. In Dark Seoul, PCs infected by the attack had all of the data on their hard drives erased. McAfee Labs, however, has discovered that the Dark Seoul attack includes a broad range of technology and tactics beyond the MBR functionality. Our analysis has revealed a covert espionage campaign. Typically this sort of advanced persistent threat (APT) campaign has targeted a number of sectors in various countries, but Operation Troy, as these attacks are now called, targets solely South Korea.

The forensic data indicates that Dark Seoul is actually just the latest attack to emerge from a malware development project that has been named Operation Troy. The name "Troy" actually comes from repeated citations of the ancient city found in the compile path strings of the malware. The primary suspect group in these attacks is the New Romanic Cyber Army Team that makes significant use of Roman terms in their code. The McAfee Labs investigation into the Dark Seoul incident uncovered a long term domestic spying operation operating against South Korean targets all based on the same code base.

Software developers (both legitimate and criminal) tend to leave fingerprints and sometimes even footprints in their code that forensic researchers can use to identify where and when the code was developed. It's rare that a researcher can trace a product back to an individual developer (unless they're unusually careless). But, frequently these artifacts can be used to determine the original source and development legacy of a new "product." Sometimes, as in the case of the New Romanic Cyber Army Team or the Poetry Group, the developers insert such fingerprints on purpose to establish "ownership" of a new threat. McAfee Labs uses sophisticated code analysis and forensic techniques to identify the sources of new threats, as such analysis frequently sheds light on how to best mitigate an attack or predicts how the threat might evolve in the future.

Operation Troy History

The history of Operation Troy extends back to 2010 with the appearance of the "NSTAR Trojan," the first piece of malware in Operation Troy, and one designed to gain privileged system access by disguising its true intent. Since the appearance of NSTAR, seven known variants, or new pieces of malware based on the original NSTAR, have been identified. Despite the rather rapid release cycle, the core functionality of Operation Troy really has not evolved all that much, and the main differences between NSTAR and several of its future variants had more to do with programming technique than functionality.

The first real functional improvements were seen in early 2013, when a variant called Concealment Troy changed the Command & Control architecture and did a better job of concealing its presence from standard security techniques. The variant Dark Seoul added the functionality that disrupted financial services and media companies in South Korea and was also the first variant used to conduct international espionage. All previous versions were simple domestic cybercrime/cyber espionage weapons.

Linking malware to its developers isn't always an easy task, as most attackers are careful enough to ensure they can't be traced. This is especially important in cases such as cyber espionage, in which the intent is to remain invisible. Yet in our analysis we observed a number of unique attributes in the components involved in these attacks; these markers allowed us to link specific samples to a specific group.

While two groups have taken credit for these attacks, we can tell that the variants that destroyed the systems link to the New Romanic Cyber Army Team.

Fingerprints

As interesting as the legacy of Operation Troy is, what's more enlightening are the fingerprints and footprints that allow McAfee Labs to trace its legacy. In the "fingerprint" category is what developers term the compile path – which is simply the path through the developer's computer file directory to the location at which the source code is stored.

By analyzing attributes such as the compile path, Labs researchers were able to, among other things, confirm that the attackers have been operating for over three years against South Korean targets.

Footprints

In the footprint category McAfee Labs documented the most significant functional change that occurred as the 2013 release of the Concealment Troy. Historically, the Operation Troy Command & Control (C&C) process involved routing of operating commands through concealed Internet Relay Chat (IRC) servers. The first three Troy variants were managed through a Korean manufacturing website in which the attackers installed an IRC server.

From the attacker's perspective there are two issues with this approach. The first is that if the operator of the infected server discovered the rogue IRC process, they would remove it and the attacker would lose control of the Troy infected client devices. The second is that the Troy developers actually hard coded the name of the IRC server into each Troy variant. This means that they had to first find a vulnerable server, install an IRC server, and then recompile the Troy source into a new variant controlled by that specific server. For this reason nearly all Troy variants needed to be controlled by a separate C&C server.

The Concealment Troy variant was the first to break this dependency on finding an IRC Command & Control server. Concealment Troy presumably gets its operating instructions from a more sophisticated (and likely more distributed) botnet that is also under the control of the Troy syndicate.

What Operation Troy Reveals

This investigation into the cyber-attacks on March 20th, 2013 revealed ongoing covert intelligence gathering operations. McAfee Labs concludes that the attacks on March 20th, 2013 were not an isolated event strictly tied to the destruction of systems, but rather the latest in a series of attacks dating to 2010. These operations remained hidden for years and evaded the technical defenses that the targeted organizations had in place. Much of the malware from a technical standpoint is rather old, with the exception of Concealment Troy, which was released early 2013.

McAfee Labs can connect the Dark Seoul and other government attacks to a secret, long-term campaign that reveals the true intention of the Dark Seoul adversaries: attempting to spy on and disrupt South Korea's military and government activities. The Troy-era malware is based on the same source code used to create these specialized variants and shares many commonalities that are found consistently throughout the families. The attackers have attempted since 2009 to install the capability to destroy their targets using an MBR wiper component, as seen in the Dark Seoul incident. From our analysis we have established that Operation Troy had a focus from the beginning to gather intelligence on South Korean military targets. We have also linked other high-profile public campaigns conducted over the years against South Korea to Operation Troy, suggesting that a single group is responsible.

What's The Solution?

What could have prevented Operation Troy and other attacks against South Korea? It's difficult to say for certain, of course, but at McAfee we believe in a connected, adaptable, open and dynamic security platform to guide security decisions made by machines and people. We emphasize the importance of every network component being both a producer and consumer of intelligence. This intelligence can then be shared within the network and externally (as policy allows) to enable an adaptive, learning ecosystem that gets smarter as it protects.

This ecosystem concept is well described in the white paper from the National Protection and Programs Directorate within the U.S. Department of Homeland Security. Done correctly, networks can detect behaviors over time and begin to recognize, almost biologically, threats before those threats can overtake network functionality. Maturity models have shown that for any size organization, a wise design up-front leads to increasing security and decreasing cost over time. This ecosystem model would work well for any sector of a nation's economy.

A key technology that informs this ecosystem is Global Threat Intelligence (GTI), which feeds each security component, enabling it to have continual situational awareness. GTI serves as a cyber immune system, protecting against attacks by electronically detecting and correlating, at machine speed, cyber behavioral data from worldwide sources that is identified as harmful. In milliseconds GTI can assess changes, assign risk levels, and distribute protection recommendations to every product in the ecosystem.

Another key technology, application whitelisting, turns the old signature-based approach on its head. Rather than having to list every known piece of harmful code – a process where you're always behind the curve – whitelisting allows only code that is known to be good into the ecosystem.

At McAfee we call this ecosystem approach Security Connected: an integrated platform of intelligent products that leverage threat intelligence. McAfee provides every necessary component of the ecosystem. However, Security Connected is also an open platform, allowing products from a host of vendor partners from our Security Innovation Alliance (SIA) to participate just as fully. Currently SIA is 160 partners strong and growing.

This ecosystem approach can be applied at every level of the computing continuum – from the application layer down to the silicon in the chip. This is what McAfee and parent Intel developed together – the technology known as "DeepSafe" (and the product is DeepDefender). When DeepSafe is loaded on a machine it loads below the operating system level, which is significant because malware often installs itself in the kernel of an operating system. With DeepSafe the security sits below that, right on the hardware, protecting the entire ecosystem.

McAfee is also working beyond our own borders on the ecosystem concepts. We're helping to lead the creation of global protocols to transport cyber event indicators at machine speed to and from all components of the network, enabling the best intelligence from all sources to be used throughout the greater Internet architecture. These initiatives can enable any entity, any product, any company and any government – small or large -- to become part of a greater ecosystem in which the detection of a threat on the Internet is used as protection going forward – at the speed of light. This is the kind of agility our adversaries cannot achieve.

Thank you for requesting McAfee's views on these important issues. I am happy to answer any questions.

Mr. CHABOT. Dr. Lewis, you are recognized for 5 minutes.

STATEMENT OF MR. JAMES LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC INTERNATIONAL STUDIES

Mr. LEWIS. Thank you, Mr. Chairman. I thank the committee for the opportunity to testify.

Weak cyber security creates the risk of conflict in Asia. In cyber security, as in so many other issues, China's behavior is the central strategic issue. North Korea's cyber actions are worrisome, but China's actions have a destabilizing regional and global affect.

The U.S. response to this should have four elements. One, we need to engage with China to reduce cyber espionage and the risk of a cyber incident escalating into armed conflict. Two, we need to modify existing alliances with Australia, Japan and Korea to make collective cyber defense a reality. Three, we have to expand formal cooperation with ASEAN countries and India on cyber security. And four, we need to make Asia a central part of the global effort to build common understandings on the secure cyberspace.

The most important thing we can do to increase stability is to reach agreement on norms for responsible state behavior, the rules, practices and obligations that states observe in their dealing with each other and with the citizens of other states.

In June of this year, a 15-nation group at the U.N., a group of government experts that included the U.S., China, India, Indonesia, Australia, Japan and Russia, agreed on rules for cyber security. They agreed that the U.N. Charter applies, that international law applies, the principle of state responsibility applies, and that national sovereignty is applicable in cyberspace, which means you can define borders.

This U.N. Agreement is a significant step forward. China agreed to this only reluctantly and after considerable pressure. Cyber security is a fundamental task of China's willingness to play by the rules and will determine if its rise will be peaceful. China can choose to play the game by the rules, or it can ignore them. This choice will influence future relations with China and the stability of Asia.

The U.S. can influence China's decision with persistence and the right strategy. We have done this before in the 1990s and later, and while China is now more powerful than it was then, we can again persuade it to change its behavior to save global norms.

Military competition between the U.S. And China is increasing, but there is no military solution for cyber security. No Asian country, including any of our allies, wants a cold war with China. Asian nations will consider both their relations with the U.S. And their relations with China. They want to find some way to balance both. China is too important as a market, and the U.S. is too important as a guarantor of regional stability. Asian nations would prefer not to have to choose between the two.

Political issues will complicate efforts to reach agreement on cyber security. Many Asian nations want to regulate content, citing pornography and online gambling as examples of Web services they would like to block. It is also too early to measure the affect of

Snowden revelations on U.S. efforts to build international agreement on cyber security.

Making sure that Asia does not become a cyber security battleground will require sustained engagement with China and cooperative arrangements with other Asian nations on cyber security. Reaching agreement will not be easy, nor will it be quick, but it is the best and probably the only way to advance U.S. interests.

I thank the committee and look forward to your questions.

Mr. CHABOT. Thank you very much.

[The prepared statement of Mr. Lewis follows:]

Testimony
Subcommittee on Asia and the Pacific
House Foreign affairs Committee
"Asia: The cybersecurity Battleground"
James A. Lewis
Center for Strategic and International Studies
July 23, 2013

I would like to thank the Committee of this opportunity to testify.

Cybersecurity is a volatile issue in Asia. The flashpoints are rampant Chinese cyber espionage and its destabilizing effect on relations with the US and other Asian nations, and the North Korean cyber attacks on the Republic of Korea. China and the U.S., the two major cyber actors in the region, have been careful to keep their activities below the threshold of armed conflict. Even the actions of North Korea against South Korean targets do not clearly rise to the level of the use of force that would justify a military response.

There is a military competition in cyberspace as nations build cyber capabilities, but both China and the U.S. only intend to use these capabilities only in the event of war. The primary problems are political and economic. Spying is not warfare and does not justify the use of force in response by the victim - the U.S. itself should be glad of this. It is not in our economic interest and certainly not in China's economic interest, given the steady weakening of their economy, to see the issue deteriorate into an armed clash. Cybersecurity as an issue for international security is best addressed using diplomatic and trade tools. Our goals should be to prevent escalation into armed conflict and build cooperation in cybersecurity.

There is a risk that we could find ourselves in a conflict, given the deep problems between the U.S. and China and the worsening public perceptions on both sides. Avoiding miscalculation and escalation, where one nation mistakenly assumes that espionage or political action is the precursor to an actual take is a problem for the U.S. and China and for the region. Adjusting to and managing China's rise is the fundamental security problem for the region, a problem with global implications as the Pacific regions displaces Europe as the world's economic engine.

For cybersecurity as with other Asian security and economic issues, the rise of China is the central problem. China's cyber actions are a threat to stability in Asia. Chinese espionage – political, military and economic is rampant. The U.S. is not the only victim. Australia, India, Japan, the Philippines, the Republic of Korea, Russia, Vietnam and perhaps others have been the victims of Chinese cyber espionage. The Chinese are "noisy" in their operations, making them relatively easy to detect. Chinese foreign policy is bumptious. They do not have the experience of the U.S. or Russia in managing security disputes. More importantly, China's cyber activities cannot be divorced for the larger security and political context in Asia, where Chinese actions have alienated many of its neighbors and have increased tensions by attempting to assert its regional authority.

The Chinese would portray things somewhat differently. They are still deeply marked by the "Century of Humiliation," where European powers and Japan carved their country into colonial

fiefdoms. The Chinese are suspicious of the United States, particularly in the PLA, which has not shed enough of its Maoist heritage. The Chinese are convinced that we have a "Grand Strategy" to preserve our global political, military and economic hegemony and that part of this strategy is to contain a rising China. They see the discussion of an "Air-Sea Battle and a "Pivot to Asia" as confirmation of U.S. hostile intentions. China's own cybersecurity efforts are hampered by the use of pirated software, which is almost unsecurable, making China one of the easiest countries in the world to hack. Chinese official know how vulnerable they are and this reinforces their suspicions and fears.

The Snowdon revelations, while embarrassing, have not had as much effect on Chinese policy as you might think (although we should not discount the effect on the larger U.S. multilateral effort). In discussions with China they U.S. has always been clear that espionage is a two way street, something that all great powers do, and that espionage against military and political targets is legitimate. What we object to is the economic espionage, the stealing of commercial secrets where there is no national security value. We also emphasize that rampant commercial cyber espionage creates a risk of misperception and miscalculation where a mistake could escalate into a much more damaging conflict. This frankness makes it hard, at least in private, for the Chinese to object too much, although they clearly enjoy our embarrassment wand will see how much diplomatic advantage they can get from the incident.

This month's meeting of the Security and Economic Dialogue and its Cyber Working Group are an important step that, if it succeeds, will make the situation in Asia more stable, but we are looking at a long effort and the S&ED process will need to be sustained and reinforced. One precedent can be found in the successful effort to engage China on nonproliferation in the 1990s. The U.S. and it allies created international norms that established that responsible states did not engage in proliferation. The U.S., supported by its allies, met regularly with Chinese officials to make this point and providing the Chinese with specific examples of objectionable behavior. Senior U.S. officials and leaders from European countries and Japan made the point that China's involvement in proliferation would harm China's relations with the rest of the world. This multilateral approach was important, as it demonstrated to the Chinese that nonproliferation was not solely an American concern. Finally, the U.S. used or threaten to use sanctions and measures to encourage a change in China's behavior.

The precedent is not perfect because the relationships of power and influence among key nations have changed. China is more powerful and Europe is weaker; China may believe it self to be less dependent, and it is certainly more confident. It is unlikely that many Asian countries will be willing to engage China on cyber espionage and even some major European allies, such as Germany, are unwilling to put business interests at risk even though it has suffered from cyber espionage. This will be a difficult process and cyber espionage has become a flashpoint in Asia and in the bilateral relationship. In this, the U.S. is the only interlocutor that can lead in effectively engaging China to bring its cyber actions in line with global practice.

China will find it difficult to bring cyber espionage under control even if it chooses to do so. Cyber espionage plays an important part in the growth of the Chinese economy and Chinese leaders will be reluctant to put this at risk at a time when their economy is slowing down. Cyber espionage is a moneymaking activity for the PLA and others and President Xi may need to find

some way to compensate them they are to get out of the cyber espionage business. There will be a domestic political price for Beijing to bring cyber espionage under control and little incentive for the party's leadership to pay this price absent external pressure and a changed view of what best serves China's own interests.

U.S. and Chinese interests for Asia have much in common when it comes to cybersecurity, are, but cooperation is increasingly blocked by mistrust and competition. U.S. and Chinese interests in cyberspace are symmetric in some areas – reducing the chance of miscalculation that could escalate into military conflict – but diverge widely in others, chiefly over political control of the internet. This is an area of divergence, but unlike political control of the internet, which Beijing sees as essential for regime survival, there is scope for progress in changing China's behavior.

To achieve this, the U.S. will need a long-term diplomatic strategy linked to our larger goals for cyberspace in Asia and the world. The U.S. must manage and reverse Chinese economic espionage while avoiding military or trade frictions. It must modify its existing alliances with Australia, Japan and Korea to make collective cyber defense more than a slogan. It must build a relationship with India on security challenges. All of this must be done as the U.S. helps to lead a global effort to develop norms for responsible state behavior in cyberspace to make it more stable and secure, an effort in which ASEAN nations play an important role.

This is a complex picture with many moving parts. The bilateral U.S.-Chinese relationship is at the heart of the issue, but other Asian nations will consider both their relations with the U.S. and their relations with China. They want to find some way to balance both. China is too important as a market and the U.S. is too important as a guarantor of regional stability. Asian nations would prefer not to have to choose between the two, although there is a growing discomfort with Chinese cyber activities that plays in the U.S.'s favor.

This is not a new Cold War. No Asian country, including any of our allies, is interested in a Cold War with China. Looking to a conflict that ended more than twenty years ago to explain the current situation is a sign of conceptual bankruptcy. China is at the center of Asian markets in a way that the Soviet Union never was. Asian economies are too interdependent for the bipolar separation of the Cold War. This lack of interest in a Cold War among Asian nations also means that China's fears of "containment" are a reflection of its own fears rather than an accurate assessment of the situation.

There are military tensions but this is not a problem where militaries can play a useful role. Each country has elements that define the bilateral relationships in terms of military competition, particularly in the PLA, and Chinese society can be prone to fits of hyper-nationalism, but if China wants to continue to grow and if the U.S. wants to remain a global leader, we have to find ways to cooperate in Asia. It is not in our interest to start a military conflict with China, nor is it in our interest to damage the Chinese economy. Similarly, a trade war between the U.S> and China would damage the global economy - something that could unleash another global recession.

If the problems for Asian cybersecurity are Chinese espionage and North Korean bellicosity, the answers lie in engagement with China, creating international commitments on cyberspace, and in

modifying existing U.S. collective defense agreements to apply to cybersecurity.

The U.S. has collective defense arrangements with Japan, Korea, and Australia. All are being modified to include cooperation on cybersecurity. One issue for collective defense comes from the differing capabilities of the partners. Another involves the difficulty of sharing sensitive information with partners whose ability to protect it may be less effective than we would wish. The U.S., in modernizing collective defense, must avoid the impression that it is building a regional alliance to contain China. The largest problem involves defining what collective cyber defense means and what actions would be required under our treaty commitments, particularly because most malicious cyber actions fall below the threshold of an armed attack that would clearly trigger collective defense.

The U.S. and Australia have a special relationship and they agreed to add cybersecurity cooperation to the existing defense treaty in 2011. Australia faces extensive Chinese espionage efforts and has made considerable progress in developing its national cybersecurity programs - in some areas, it is ahead of the U.S. The relationship with the U.S. makes an important contribution to Australia's national cybersecurity effort. Australia must take into account its close economic ties with Beijing as it strengthens security ties with the U.S., but in cybersecurity, there is a strong existing relationship between the U.S. and Australia and a large commonality of interests in defense cooperation and in the creation of a stable international order for cyberspace.

Japan, like Australia and the U.S., has suffered from extensive Chinese cyber espionage. Japan has in the last year undertaken a number of actions to improve cybersecurity. These include the publication of a new cybersecurity strategy, the creation of a cybersecurity unit in the JSDF, and plans to create a governmental coordination cybersecurity center by 2015 (which will be an expansion of the existing National Information Security Center in the Cabinet Secretariat). Japanese and U.S. share similar economic and security interests in cybersecurity, and while progress in defining collective defense has been slow as Japan works through constitutions issues related to the definition of self-defense in cyberspace, but discussion with the U.S. are underway and Japan has been an important partner in the efforts to build international agreements for cybersecurity.

The situation in Korea differs from that in Japan and Australia because, in addition to Chinese espionage, the ROK faces an erratic and active opponent in cyberspace. North Korea is a source of turbulence and an irritant to both the U.S. and China. So far, most North Korean activity seems to have been directed against the ROK. Since other witnesses will discuss North Korean capabilities, I will note that confirmable intelligence is sparse. There are also disputes about the role for China in the North Korean activities and the extent to which China is witting, supportive, or opposed to the North Korean activities.

North Korea's motives for cyber attack, to the extent they can be discerned are a complex and irrational mix of objective. The North has been developing cyber capabilities for many years and uses them not only for espionage but also for clumsy attempts to sway opinion in the South. Some South Korean analysts believe that the recent cyber attacker could have been a murky diplomatic signal from the North about direct negotiations. They could have been a

demonstration for the North's new leader by a cyber attack unit of their capabilities against a media target that had attracted his displeasure. The problem with this is the stability of North Korean decision-making and the ability of North Korea's leaders to accurately calculate the risk that a cyber attack could entail. This is a country that does not mind shelling villages or sinking patrol boats, but a miscalculation in the use of cyber weapons could have much broader and perhaps escalatory effects. The ROK, in response to the North's actions, has increased the amount of resources devoted to cyber security. As with Japan, the U.S. has begun discussion with the ROK on cybersecurity cooperation and collective defense.

North Korea will be an anomaly and an outlier in the efforts to make cyberspace more secure and stable in Asia. Progress, as with the nuclear issues, will be a captive of internal North Korean politics, but it would be helpful to embed the issue of North Korea's use of cyber attacks in a larger international framework, especially a framework that China accepts. This means that U.S. strategy must pursue three interconnected goals simultaneously. The first is sustained, high level dialogue with China. The second is close coordination with allies. The third is multilateral engagement to create international norms of responsible behavior in cyberspace.

In June 2013, the U.S., China, Australia, India, Japan and Indonesia, as part of a fifteen nation Group of Government Experts (GGE) on Information Security established by the UN endorsed the application to cyberspace of the UN Charter, international law, the principle of state responsibility, and national sovereignty. This included agreement that States would not use "proxies" for malicious cyber actions. We know that there are many steps between agreement and implementation when it comes to international practice, but at a recent Track II discussion in Beijing a Chinese official said in a reference to the GGE, "China's position was evolving in the light of international experience." The U.S. has been working with other nations to build on the success of the GGE to create norms and agreement on responsible state behavior in cyberspace. As this effort progresses and there is international consensus on responsible behavior in cyberspace, China's cyber espionage will be difficult to sustain.

The U.S. has been working with other nations to build on the success of the GGE, to create norms and agreement on responsible state behavior in cyberspace. Singapore, Vietnam, Thailand, New Zealand, the Philippines, and Indonesia, all have active cybersecurity efforts at varying levels of maturity. The most important venues for this in Asia are APEC, ASEAN and the ASEAN Regional Forum (ARF). APEC focuses on law enforcement and technical cooperation at the CERT level. The ARF, in its larger effort on terrorism and transnational crime, has begun work with the U.S. on cybersecurity confidence building measures.

The focus of the global effort to develop agreed norms of state behavior in cyberspace will take place this fall in Korea. Seoul will be the venue for a third meeting of a global process started by the UK's Foreign Minister William Hague, to be held in October of this year. Previous meetings have been held in London and Budapest. Korea, as the host, will build on the work done in the ARF and in the GGE. The content of any norms emerging from this meeting will resemble and build upon those agreed at the UN GGE.

The fundamental decision is whether to continue to pursue an effort to obtain universal agreement among all states on norms and responsibilities for states in cyberspace or whether to

move to seeking agreement first among like-minded states, as was the case with nonproliferation, while leaving the door open for other nations to join later.

Like-minded nations would almost certainly not include China. In part to forestall any criticism at the first meeting in London, Russia and China introduced their Code of Conduct to shift the terms of debate in their favor and provide an easy riposte to charges that they are not serious about state responsibilities for cybersecurity. The Code reflects their view of how international commitments developed in a bipolar era when they were largely "outside" should be restructured to increase the rights of the state vis-à-vis the rights of citizens. The Code would amend international law in this direction. It reflects a larger dispute over "universal" values. The Chinese position on the Code is more rigid than that of Russia, but it has become largely untenable after failing to win broad support.

Any like-minded effort cannot be a transatlantic initiative. Important "fence sitters" like India and Indonesia – both of which are at early stages in their work on cybersecurity - must be engaged from the start. While some ASEAN nations share to a degree Russia and Chinese concerns about the "U.S.-centric" nature of the internet, it should be possible to build a partnership with them, but building partnerships with the new powers may require flexibility and concessions on issues like internet governance. Several Asian nations, not just China, have expressed a desire to be able to regulate content consistent with the national laws (citing pornography and online gambling as examples of web services available from the U.S. that they would like to block).

This political issue may complicate efforts to reach agreement on cybersecurity norms. It is also too early to measure the effect of Snowdon revelation on US diplomatic efforts to build international agreement on cybersecurity. Making sure that Asia does not become a "cybersecurity battleground" will, however, require regional and perhaps global agreement on the norms, practices and obligations that states observe in their dealing with each other and their dealings with the citizens of other states. This is the essential requirement for making cyberspace stable and more secure.

The common element is the need to address the destabilizing effect of Chinese cyber espionage. Cybersecurity is a fundamental test of China's willingness to "play by the rules" and whether its integration into the international "system," will be peaceful. China can choose to amend rules that it believes do not serve its national interests or it can choose to ignore them, but the outcomes from these different choices will be very different for Asia, the U.S. and the world. Cybersecurity in Asia is not a problem that can be resolved by force or coercion, and our engagement with China will be reinforced if there is multilateral agreement on norms. Our goal should be sustained engagement on cybersecurity, globally, in Asia and with China, to build the cooperative agreements that will make cyberspace more secure for all nations. This will not be an easy process nor will it be quick, but it is the best way to advance U.S. interests.

I thank the Committee for the opportunity to testify and look forward to you questions.

Mr. CHABOT. Mr. Rauscher, you are recognized for 5 minutes.

STATEMENT OF MR. KARL FREDERICK RAUSCHER, CHIEF TECHNOLOGY OFFICER AND DISTINGUISHED FELLOW, EASTWEST INSTITUTE

Mr. RAUSCHER. Good afternoon, Mr. Chairman, members of the committee and fellow panelists. My name is Karl Frederick Rauscher, and I am the chief technology officer and a distinguished fellow of the EastWest Institute, where I lead the institute's Worldwide Cybersecurity Initiative and its new Cyber Policy Lab. I am pleased to be before the committee today to testify about cyber in Asia.

I submitted my full statement to the committee, which I ask to be made part of the hearing record.

Mr. CHABOT. Without objection, so ordered.

Mr. RAUSCHER. Thank you on that. I now move to give a brief opening statement.

I am an electrical engineer that has spent over 25 years in the Bell Labs environment. In the course of my career, I have provided guidance on ultra-high reliability and ultra-high security applications to senior governments on five continents.

As the primary challenges of reliability and security have shifted in recent years from technology to policy, my primary association is now with the EastWest Institute. EWI is a global think-and-do tank whose board of directors comes from highest levels of government, business and civil society, and has had bipartisan and international representation from the East and the West, allowing it to maintain its neutrality and fiercely guarded independence.

My recent publications include India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure; Fresh Tracks for Cybersecurity Policy Laterals—Updating the Track 1 and Track 2 Paradigm to Tracks Kappa, Epsilon and Phi; a Russia-U.S. Bilateral on Critical Infrastructure Protection: Rendering the Geneva and Hague Conventions in Cyberspace; and a China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust. Perhaps of interest to the committee, this last publication was recently singled out by the New York Times editorial board as recommended reading for Presidents Obama and Xi prior to their recent June 2013 California talks.

The point of my testimony today is that policy innovations that break through the East-West ideological gridlock are essential for the stability of cyberspace. I see solutions to the current predicament between the U.S. and China that are based on a major overhaul of ideological and political regimes as having a low probability of success. Thus my focus is on real, tangible steps to progress that will actually make cyberspace better for all of us.

There are four key aspects of navigating the solution space: First, recognizing that the U.S. and China have both shared and unshared, or simply different, interests. This is what makes the world interesting and also very dangerous.

Second, regarding the shared interests, there is potential for cooperation; however, the current environment of growing mistrust impedes straightforward understanding of each other's interests.

Third, the contour of cooperation can be optimized if we, (A) extend cooperation into new areas based on enlightened understanding of actual shared interest; and, (B) pull back cooperation where shared interests are not, after careful examination, in reality enjoyed.

And fourth, an optimized contour of cooperation of shared interest can reset the tone for discussions, giving both sides the confidence the relationship can improve as steps of new cooperation are taken. As we have found with the success of the fighting spam work, we can now move into arenas of higher complexity and higher consequence.

I offer some tangible evidence that demonstrates the doability of breaking through policy gridlocks with Asia and cyberspace by pointing out examples of recent successes. We are encouraged that to date we have forged 27 innovative recommendations that break through policy roadblocks. And most encouraging, we have seen within a short period of time an uptake of these recommendations by major companies and governments. In fact, over 50 percent of the innovative recommendations are being implemented, and over a quarter are now institutionalized for long-term sustainability.

The first examples I draw attention to are the 2 recommendations and 46 best practices of the Fighting Spam to Build Trust report, which was prepared jointly by a combined dream team of Chinese and U.S. subject-matter experts and stakeholders. Spam can make up as much as 95 percent of email messages sent and is often a vehicle for malicious code, as was referred to earlier.

The report's two recommendations have not only been implemented, but their continued, sustained implementation has been institutionalized by the highly recognized international Messaging, Malware and Mobile Anti-Abuse Working Group, also known as the M3AAWG.

I pivot now in my remarks to facing the future. What are we going to go do next? As we look at the U.S.-China relationship, I submit that we would do well to remember a lesson from our great American sport of baseball. Home runs are hard to come by and if there are many people swinging for the fence and striking out. In contrast, consistently hitting singles, and keeping a good batting average is still a great strategy for putting points on the board. I humbly submit that these examples are proof that striking out is not inevitable, and that we can get on base.

In conclusion, the top priority for engaging Asia and specifically China at this time is to make genuine, tangible progress. Policy breakthroughs with Asia are needed for the safety, stability and security of cyberspace. Policy breakthroughs have been shown to be possible, and more policy breakthroughs in key areas are also possible.

Thank you, Mr. Chairman and committee members, for the opportunity to appear before you today. I stand ready to answer any questions that you may have.

Mr. CHABOT. Thank you very much.

[The prepared statement of Mr. Rauscher follows:]

KARL FREDERICK RAUSCHER

CHIEF TECHNOLOGY OFFICER & DISTINGUISHED FELLOW
EASTWEST INSTITUTE

BELL LABS FELLOW

Written Statement for the

UNITED STATES CONGRESS

HOUSE COMMITTEE ON FOREIGN AFFAIRS

July 23, 2013 Hearing on

"Asia: The Cyber Security Battleground"

Introduction

Good afternoon, Mr. Chairman, and Members of the Committee, fellow panelists.

My name is Karl Frederick Rauscher.

As the Chief Technology Officer and a Distinguished Fellow of the EastWest Institute I am responsible for the Institute's Worldwide Cybersecurity Initiative, including its Cyber Policy Lab.

I am pleased to be before the committee today, testifying with regard to the subject of Asia and cybersecurity.

I have submitted my full statement to the committee, which I ask to be made part of the hearing record. I will now give a brief opening statement.

Career Summary

I am an electrical engineer that has spent over 25 years in the Bell Labs environment, including 10 years at Bell Communications Research. Throughout this time my primary focus has been on the reliability and security of information and communications infrastructures, networks, systems and services. I'll note that this is well before such a subject became popular.

In the course of my career, I have provided guidance on ultra-high reliability and ultra-high security applications to senior government and industry leaders on 5 continents. I have led the development of hundreds of industry consensus best practices for reliable and secure infrastructure, architected numerous quality improvement breakthroughs and led a Bell Labs team that achieved the first six "9's" performance for a system, meaning it operates continuously with long-term availability of 99.9999%.

As the primary challenges to reliability and security have shifted in recent years from technology to policy, my primary association for the past 4 years has been with the EastWest Institute. I also continue to conduct research across the full spectrum of concerns related to the reliability and security of cyberspace, and provide advice to business and government leaders around the world.

Publications

My recent publications include:

- *The Reliability of the Global Undersea Communications Cable Infrastructure*[1]
- *Priority International Communications Staying Connected in Times of Crisis*[2]

[1] *The Reliability of Global Undersea Communications Cable Infrastructures* (ROGUCCI), IEEE: 2010, www.ieee-rogucci-org .

- *India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure*[3]
- *Fresh Tracks for Cybersecurity Policy Laterals - Updating the Track 1 -Track 2 Paradigm to Tracks κ, ε and φ*[4]
- *Mutual Aid for Resilient Infrastructure in Europe*[5]
- Russia-U.S. Bilateral on Cybersecurity: *Critical Terminology Foundations*[6]
- Russia-U.S. Bilateral on Critical Infrastructure Protection: *Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*[7]
- China-U.S. Bilateral on Cybersecurity: *Fighting Spam to Build Trust*[8]

Perhaps of interest to the committee, this last publication was recently singled out by *The New York Times* editorial board as recommended reading for Presidents Obama and Xi prior to their June 2013 California talks.[9]

Leadership Roles

Here in the United States I have previously served in appointed leadership roles for Federal Advisory Committee Act (FACA) organizations, namely the President's National Security Telecommunications Advisory Committee (NSTAC) and the Federal Communications Commission Network Reliability and Interoperability Council (NRIC).

I have served in industry-elected leadership roles, including for the Network Reliability Steering Committee and the IEEE Technical Committee on Communications Quality and Reliability. I am also the Founder and President of the nonprofit Wireless Emergency Response Team, which led efforts to use advanced wireless technology to conduct search and rescue efforts in the aftermath of 9-11 and Hurricane Katrina disasters.

The EastWest Institute (EWI)

The EastWest Institute is a global 'think-and-do' tank that devises innovative solutions to pressing security concerns and mobilizes networks of individuals, institutions and nations to implement these solutions. EWI's mission is to provide an arena where key leaders, policy makers and groundbreaking innovators deliver a roadmap for achieving a safer and

---

[2] *Priority International Communications – Staying Connected in Times of Crisis*, EWI: 2012, www.ewi.info/pic .

[3] *India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure*, (India) Institute for Defence Studies and Analysis: 2012.

[4] *Fresh Tracks for Cybersecurity Policy Laterals - Updating the Track 1 -Track 2 Paradigm to Tracks κ, ε and φ*, Proceedings of the Third Worldwide Cybersecurity Summit, New Delhi, IEEE: 2012.

[5] *Mutual Aid for Resilient Infrastructure in Europe*, ENISA: 2011, www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance/mutual-aid-agreements .

[6] Russia-U.S. Bilateral on Cybersecurity: *Critical Terminology Foundations*, EWI: 2011, www.ewi.info/cybersecurity-terminology-foundations .

[7] Russia-U.S. Bilateral on Critical Infrastructure Protection: *Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*, EWI: 2011, www.ewi.info/working-towards-rules-governing-cyber-conflict .

[8] China-U.S. Bilateral on Cybersecurity: *Fighting Spam to Build Trust*, EWI: 2011, www.ewi.info/fighting-spam-build-trust .

[9] *Preventing a U.S.-China Cyberwar*, The Editorial Board, The New York Times, May 25, 2013.

more secure tomorrow. As EWI enters its fourth decade, its mission continues to be as relevant as it was at its founding. EWI's Board of Directors comes from the highest levels of government, business and civil society from around the world. Traditionally and consistently, EWI has had bi-partisan and international representation from the "East" and the "West," allowing it to maintain its neutrality and fiercely-guarded independence.

Consistent with the mission of the EastWest Institute to make the world a safer and better place, the mission of the Cyber Policy Lab is to make cyberspace safer, more stable and more secure. Our high level strategy has four goals:

I. **Build Trust** among the cyber super powers: China, India, EU, Russia, U.S.
II. **Pioneer 'Rules of the Road'** for cyber conflict
III. **Champion Emergency Preparedness** for international crises in cyberspace
IV. **Unleash Private Sector Leadership** for innovative problem solving

Policy Innovations that Breakthrough East-West Gridlock are Essential

The point of my testimony today is that policy innovations that breakthrough the East-West ideological gridlock are essential for the stability of cyberspace.

In my brief remarks today I will first outline the current situation and the need for policy breakthroughs.

Second, I will demonstrate the do-ability by pointing out examples of recent successes.

Third, I will then move onto some ripe opportunities awaiting action.

The Current Situation and the Need for Policy Breakthroughs in the East-West Ideological Gridlock

First, let's look at the need. From both a U.S. and world perspective, policy breakthroughs with Asia are essential for the safety, stability and security of cyberspace. Economic growth for both developed and developing countries is highly correlated with the use of information and communications technology. The United States is the leading innovator in cyberspace while China is the largest manufacturer of hardware systems, and India is a leading supplier of both software and networked services. Our mutual interdependence in cyberspace is profound.

Cyberspace has inherent vulnerabilities - susceptibilities that are intrinsic to the ingredients that make it up. These intrinsic vulnerabilities cannot be removed. So the first order problem we face is our reliance on imperfect technology platforms. Society, businesses and governments have enthusiastically embraced the efficiencies of the

applications we enjoy, and have been slow to accept the trade-offs. We are now facing the music.

The systems we use get their 'power' so to speak from their connectivity. Security is a *secondary* consideration. In other words, our systems, devices and applications are first *networked* to provide their value, and then *"un-networked"* to shield them from those we don't want to access our information.

Just as hardware, software and networks are essential technology ingredients of cyberspace, so too is policy an essential ingredient. Policy, or more completely, Agreements, Standards, Policies and Regulations (ASPR), are vital for the reliable and secure operation of cyberspace. When so intimately and pervasively connected, as in cyberspace, entities, whether they be machines, individuals, companies or governments, need to be able to anticipate the behavior of other entities. When this anticipation is not tightly coordinated, unintentional or intentional harm can result. In cyberspace, malicious agents exploit, in particular, the lack of international coordination of behaviors — more specifically, they exploit policies that should be there but are lacking, out-of-date, misinterpreted, unimplemented, mis-implemented, or otherwise failed. Thus, this is the situation for why, in my opinion, the policy category has risen to be the major cause behind unacceptable safety, stability and security in cyberspace.

Evolving Threats from Asia

In the invitation letter I received to this hearing, one of the questions the committee has posed regarded the evolving threats from Asia. My initial response to this query is that being aware of the trends of threat profiles is very useful and can help one react better. It is my observation that China's primary concern with hacking, unlike that of the U.S., is internal. Thus any growth in hacking activity in the region first presents a concern for China's government around insider attacks on its stability. However there has been a marked increase in attention dealing with the international concerns, and China is showing a heightened interest in cooperating internationally on the hacking issue. For example, China has new interest to cooperate on fighting crime in cyberspace. Thus the conditions are much improved for the newly commenced U.S.-China Security and Economic Dialogue.

But the most useful point I offer with regard to evolving threats is that we need to shift substantial resources from our primary mode of being reactive so we can invest in proactive measures. As a scientist, I am best grounded in the vulnerability side of the discussion. Threats can only have an impact if they are given a chance to exercise a vulnerability. Thus, our best investments are those that make us independent of the changing threat profiles; that is, investing in those countermeasures that prevent a vulnerability from being exercised, or ameliorate the impact if it is exercised.

In fact, if you removed Asia from the equation -- say the continent did not exist -- we must face it -- America -- our government, our businesses and our personal information -

- would still be as exposed as it is now. We are fundamentally at risk because of intrinsic vulnerabilities within the ingredients that make up cyberspace -- networks that connect, software that controls and hardware that obeys the commands given to it.

Our reliance on cyberspace is the first order problem. Malicious actors who take advantage of the vulnerabilities in cyberspace -- no matter where they come from -- are a second order problem.

The Right Direction

This last response also applies to another question posed by the committee. Specifically, "Is the U.S. Government cyber community headed in the right direction?"
We have a lot of smart people doing a lot of important things. But by and large the use of these resources is far too reactive. The threat vs. vulnerability focus is out of balance. By having a chief orientation around threats, we are chasing after the wind. Or to switch metaphors, we have too many people practiced in bailing water out of the boat and not enough capable of plugging holes. But when there is water in the boat, and you are getting wet, it is hard to focus on long-term solutions. We need leadership to shift the focus. Given its more intimate knowledge of technology design and development, this leadership will likely need to come from the private sector.

Navigating the Solution Space

Shifting back to the current situation with Asia, I see solutions to the current predicament that are based on a major overhaul of ideological or political regimes as having a low probability of success. Thus my focus is on real, tangible steps toward progress that will actually make cyberspace better for all of us. As an example, for interfacing with the Chinese, for example, I use Figure A to convey four key aspects of navigating the solution space:

- *First,* the U.S. and China have both *shared* and *unshared*, or simply, different interests. This is what makes the world so interesting and dangerous.

- *Second,* regarding the shared interests, there is *potential* for cooperation, however the current environment of growing mistrust impedes straightforward understanding of each other's interests.

- *Third,* the contour of cooperation can be optimized if we (a) extend cooperation into new areas based on enlightened understanding of actual shared interests, and (b) pull back cooperation where shared interests are not, after careful examination, in reality enjoyed.

- *Fourth*, an optimized contour of cooperation of shared interest can reset the tone for discussions, giving both sides the confidence that the relationship can improve

as steps of new cooperation are taken. As we have found with the success of the fighting spam work, we can now move into arenas of higher complexity and higher consequence.

Note that this process is not for the timid. Once on this path, one will find real opportunities where mutual benefit that protects the interests of both sides can be achieved, and thus will eventually require action, such as implementing the agreed to recommendations.

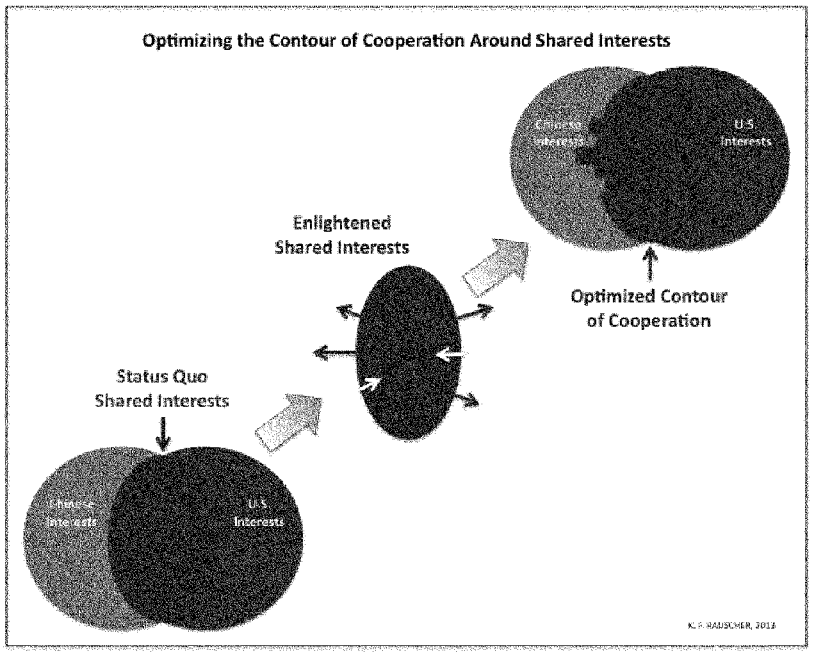

Figure A. Optimizing the Contour of Cooperation Around Shared Interests

Examples of Recent Successes

I now offer some tangible evidence that demonstrates the do-ability of breaking through policy gridlocks with Asia in cyberspace by pointing out examples of recent successes.

For the past three years, I have been primarily occupied with leading initiatives to address seemingly intractable problems whose unresolved disposition puts in jeopardy the safety,

stability and security of cyberspace. Stakeholders have deemed these as "impossible missions." Most of these issues are directly or otherwise highly correlated with Asia.

In this capacity, I have had the privilege of working with hundreds of the best minds in the United States and around the world, who individually, or through their organizations, volunteer to support these initiatives. These are individuals who also see these policy issues as major obstacles that threaten the potential of cyberspace and that therefore need to be overcome. They have a passion for solving hard problems that often takes them beyond the call of duty of their daily jobs.

We are encouraged that, to date, we have forged 27 innovative recommendations that break through policy roadblocks. And, most encouraging, we have seen within a short period of time, an uptake of these recommendations by major companies and governments. In fact, over 50% of these recommendations are being implemented, and over a quarter are already institutionalized for long-term sustainability. Keep in mind these are all recommendations for what were considered intractable problems, for which no solutions exist, so the comparative benchmark is 0%.

The first examples I draw your attention to are the 2 recommendations and 46 best practices of the *Fighting Spam to Build Trust* Report, which was prepared jointly by a combined "dream team" of Chinese and U.S. subject matter experts and stakeholders. Spam may make up as much as 95% of all email messages sent and is often a vehicle for malicious code. The report's two recommendations have not only been implemented, but their continued, sustained implementation has been institutionalized by the international Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG). Furthermore, 2 important commitments were made at the EWI-IEEE Third Worldwide Cybersecurity Summit in New Delhi this past October.

- *First*, leaders from the respective Indian and Chinese Computer Emergency Readiness Teams (CERTs) agreed to cooperate based on the guidance of this report. Those familiar with the China-India tensions know that this is a non-trivial step forward.

- *Second*, during the same Summit, the Indian industry agreed to establish an Indian M^3AAWG in Mumbai -- quite significant -- as India is now the top ranked producer of international spam traffic. Equally as important as the Indian government recently standing up a National Cyber Coordination Centre (NCCC) is the industry's active participation in fora such as this new MAAWG and existing ones like the Data Security Council of India (DSCI). India is a unique place where, from an American perspective, the relative independence of industry from regulation is even greater than our own experience. Coordination is the key for the Indian government. While the country has the third largest online population, its coordination is far behind that of China and the U.S., making it very open to exploitation by malicious actors. And this is likely to be the case for some time as online penetration is still at a low level, just around 10%. While it is

too early to tell if India's new coordination center is a model for other countries in Asia, private sector led fora like the MAAWG and high functioning Computer Emergency Readiness Teams (CERTs) are.

As we look at the China-US predicament, I submit that we do well to remember a lesson from our great American sport of baseball. Home runs are hard to come by. Yet there are many people swinging for the fence and striking out. In contrast, consistently hitting singles, keeping a good batting average, is still a great strategy for putting points on the board. I humbly submit that these examples are proof that striking out is not inevitable and that we can get on base.

Ripe Opportunities

I now pivot in my remarks to face the future.

What we are going to do next?

This is a critical step in the discussion, because there are many voices opining on the cybersecurity problems our country is experiencing with Asia, and particularly China. We cannot stay in this holding pattern forever without losing elevation. We we need to convert the problems into opportunities.

So 'what next?'

Based on mutual shared interests, cooperative action can be taken in several areas of high consequence to the safety, stability and security of cyberspace. I offer some very practical and specific opportunities that are ripe for picking.

Geographic Diversity for the Luzon Strait Chokepoint (ROGUCCI Recommendation No. 1)

The first opportunity concerns the stability of the global economy and I refer to it as the "Luzon Strait Chokepoint." Daily, international financial transactions on the order of ten trillion dollars pass through the GUCCI (the Global Undersea Communications Cable Infrastructure), which underpins global connectivity, carrying over 99% of international traffic.

Most of the undersea communications cables coming from North America into Asia's major financial center, Hong Kong, converge into a single point of failure in the Luzon Strait. With Hong Kong's dependence on international bandwidth doubling every 18 months, the criticality of this connectivity is dramatically increasing with time. As I point out in Recommendation No. 1 of the 2010 IEEE ROGUCCI Report, providing geographic diversity for GUCCI is vital for the stability of global connectivity, and specifically, the global economy. It is vital for the connectivity of the two largest economies that additional alternative routes with geographic diversity, such as a North-South route through the Taiwan Strait, be added. The next step is for China to open

access to investors and cable operators and clarify policies for these very sensitive and disputed waters. But the U.S. must be ready to support new cable landings on our West Coast.

Priority International Communications

The second opportunity deals with the robustness of our connectivity; that is, making sure the most important functions remain intact under stresses that are outside of design constraints. Today, when a major disaster strikes, like the 9-11 terrorist attacks or the Fukushima nuclear meltdown, communications networks become immediately congested, preventing critical communications from getting through unless a priority scheme is in place. At the international level, standards have existed for such a scheme since before the 9-11 attack, yet they remain largely unimplemented. So as the world becomes increasingly interdependent, we are becoming less prepared for emergencies. The *Priority International Communications* (PIC) Report explains how the existing international standards can be implemented at a very low cost using existing network equipment and end user devices. PIC is an international extension of the existing United States national priority schemes known as Government Emergency Telecommunications Services (GETS) and Wireless Priority Service (WPS), currently managed by the Office of Emergency Communications with in the Department of Homeland Security.

I ask the committee to consider the relative importance between a recent agreement with Russia relative to the value offered by PIC. I submit that if it was important enough for Presidents Obama and Putin to sign an agreement to utilize nuclear risk reduction centers, which allow communications between decision makers who happen to be in single physical locations in Moscow and Washington, D.C., then surely an agreement for PIC is even more important. It would ensure critical communications for government-authorized users getting through between any places covered by ubiquitous global public networks.

Implementing PIC is not controversial and is a natural confidence building step. It can be implemented at a very low relative cost, as its implementation is almost entirely software. It would be prudent for those in Congress charged with managing America's interests in foreign affairs to ensure that our national level priority schemes like GETS that were critical in the response to 9-11 are extended to international reach, and particularly with the key countries in Asia.

Cooperate in Measuring Cybersecurity Problem

The third opportunity is one largely for the private sector to lead, but encouragement from government stakeholders can make a critical difference in the speed of implementation. It concerns measuring the cybersecurity problem. The premise of the current discussion is that the frequency and impact of the aggravations in cyberspace are increasing, especially those associated with Asia. Measurement is essential to managing a problem. Yet no estimated to even an order of magnitude is widely accepted on a global basis. Lord Kelvin has underscored this point with the pithy statement "To measure is to

know." An EWI report to be released this quarter offers guidance on steps that can be taken to create a trusted entity and encourage private sector participation.

Protect Humanitarian Critical Infrastructure

The fourth opportunity squarely focuses on practical ways to move forward with establishing norms of behavior in cyberspace. I raise to your attention the opportunity to carry forward to cyberspace the principles of the Geneva and Hague Conventions that protect purely humanitarian interests. A joint analysis between Russian and U.S. experts, which EWI released coincident with the 2011 Munich Security Conference, outlines key observations around the entanglement in cyberspace of legitimate military targets and protected humanitarian infrastructure. Given the pervasive integration of medical infrastructure with information and communications technology, if deliberate steps are not taken, the precious humanitarian protections of international law that have been hard earned over the last century and a half in the physical world will not be carried into the future.

Tying into this humanitarian interest opportunity, and as a follow up from the joint China-U.S. cybersecurity effort on fighting spam, we have now moved onto addressing the unacceptable hacking situation. We continue to be supported by the top minds in these fields from both countries. Figure B depicts a framework that I use to understand the primary forces and assets at play in this landscape, namely humanitarian, commercial and national security. The three key "take aways" from this landscape are:

- *First*, there are opportunities for agreements in protecting purely humanitarian interests, based on existing principles coded in widely accepted international humanitarian law. This protection may be able to extend to the for-profit enterprises that support humanitarian interests. Both of these categories are well suited for protection agreements in cyberspace.

- *Second*, on the other side of the landscape of interests in cyberspace, there are national security interests, for which nation-states are expected to continue to operate and such interests have always expected, do now expect, and always should expect, to be the target of mischief. Likewise, the industrial complexes that support these industries should expect similar treatment.

- *Third*, in the middle of the landscape lies the commercial interests, where there are fewer rules in place and thus unacceptable behavior abounds. This is our sore point. The Chinese know it.

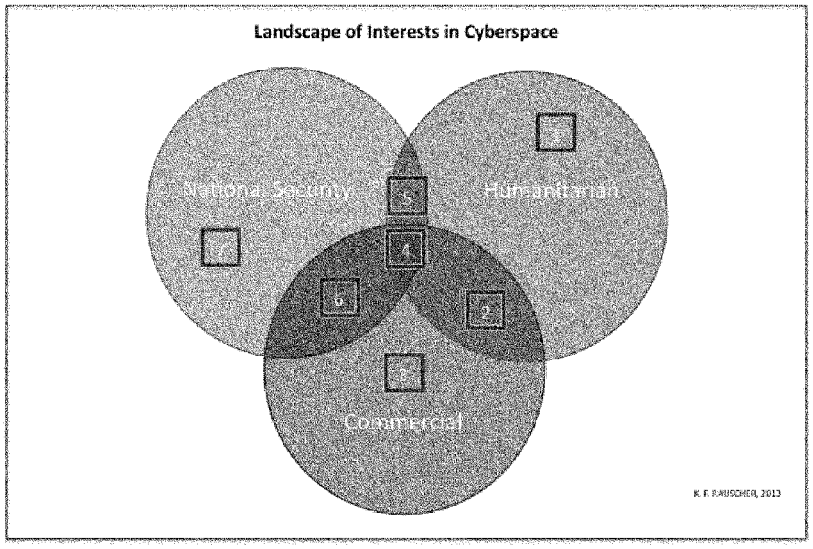

Figure B. Landscape of Interests in Cyberspace

Summary

In conclusion, the top priority for engaging Asia, and specifically China, at this time is to make genuine, tangible progress. Policy breakthroughs with Asia are needed for the safety, stability and security of cyberspace. Policy breakthroughs have been shown to be possible, and, more policy breakthroughs are possible in key areas, should the private sector and government have the will to act.

Yes, the United States government has an important role, but so does the private sector -- both the commercial and non-profit and philanthropic components. In fact, I submit that without the vision and talent of the latter, solutions to these problems will simply be unsatisfactory. Thus my remarks in the public record are also a call for the unleashing of bold new private sector leadership.

Thank you, Mr. Chairman and committee members, for the opportunity to appear before you today. I stand ready to answer any questions you might have.

Mr. CHABOT. Before we get into the 5-minute questioning by panel members, the Chair would like to call on the gentleman from Georgia to be recognized for a moment. Mr. Collins.

Mr. COLLINS. Mr. Chairman, I do appreciate it. And, Dr. Schneck, I just wanted to—from Georgia, so I could not let it pass by. Although I represent the University of, Georgia Tech is a wonderful institution. She would—for those in the audience don't know, Go, Dogs. But Tech is also my heart as well. But just your expertise in the way you have represented in your doctorate coming from Georgia Tech, and the instruments, and where you played in this field, and the expertise that you give give your alma mater a wonderful name, and I just wanted to say that for the record.

This a huge issue. It is the defining issue, I believe, for the next number of years, and not only in our warfare, but also in our relations between countries. And I could not let it go without recognizing your accomplishments and achievements from the fine institution of Georgia Tech.

Mr. CHABOT. Any response?

Ms. SCHNECK. I would love to say thank you. You know the response I need to give someone from Georgia. I cannot say that in this venue. But thank you so very much for your comments, and I did really love my time in Georgia.

Mr. COLLINS. Well, I am going to be having to leave, so I wanted to make sure I recognized that fact.

Ms. SCHNECK. Thank you so much.

Mr. CHABOT. Thank you.

I now recognize myself for 5 minutes.

I mentioned in my opening statement that establishing cyber confidence-building measures with our allies and friends in Asia is critically important. There has been much discussion, mostly negative, about creating a global treaty, and that this goal is impractical and unenforceable. The large number of actors and new and fast-changing technologies in cyberspace increases the complexity of collaborating to resolve issues domestically and internationally in a timely manner.

Because of the cross nature of cyber security, different countries in Asia have different interests concerning privacy, openness, and regulation of cyberspace—vastly different in some cases. As a result, what is the best way to go about establishing greater trust and confidence? While many efforts to enhance cooperation have taken a bilateral approach, what form would you see cyber cooperation in Asia taking in the future? How much influence does the U.S. have in actually building capacity and security in cyberspace? Lastly, how do you think broad security concerns about revealing intelligence sources and methods will prevent cooperation from advancing, especially considering China's growing presence and aggressiveness in the region?

I will go down the line and ask each of you to take a relatively brief shot at those questions. Dr. Schneck, we will begin with you.

Ms. SCHNECK. Thank you very much.

When it comes to how much influence the U.S. has in building that cooperation, I look at cyber security and cyber resilience: How do you keep our networks up while they are being attacked? They will always be attacked.

Right now we are setting, I think, a beautiful example in the U.S. with the work that is being done by NIST and with the Department of Homeland Security and across interagency in combining information in people time and in machine time. So building ways—and we need liability protections, of course, for companies to share information in good faith about cyber threat, but also building ways for people to get together across, transcending those boundaries between competition in companies as well as transcending private-sector and industry boundaries.

And in machine time the Department of Homeland Security is actually crafting protocols to build that Internet ecosystem that I mentioned, which would allow cyber threat indicators—if you see something behaviorally strange or off, computers could communicate to other computers around the Internet just as your body communicates and fights a disease without knowing its name, so that you build an ecosystem that is learning where an adversary is trying to attack before it propagates so much that it causes damage.

I think the U.S., between our academic institutions, our industry, and our government, is doing a very good example of taking the first couple of steps at building that framework to foster global innovation instead of regulation, which is always so many years behind.

And we are also setting a great example working with many in the Asia Pacific community, many in the EU to really build those protocols, because the competitor is not the adversary anymore in industry, government is not an adversary, other countries are not adversaries necessarily. It is all about how we keep these networks up to sustain our way of life. And to wrap that part of your question, I think the U.S. is doing a beautiful job in that way, and we have a lot of work to do globally on that.

Mr. CHABOT. Can I stop you there so I can include the others? I have about 1½ minutes left, so I will give you about 45 seconds, Dr. Lewis, and about 45 seconds to Mr. Rauscher.

Mr. LEWIS. Okay. I should note that for the last 3 years I have led semiformal talks with the Chinese Government, with the Ministry of State Security and the PLA. State was able to go to them along with DOD. And what we found in those talks is that a global treaty just isn't possible. One morning is the Russians are the guys proposing a global treaty. That alone should be enough to tell us it is a bad idea.

There is a meeting coming up in Korea this October that is part of a process begun by the U.K. To get agreement on norms and confidence-building measures. We are not going to get a treaty; we can get agreement on norms and confidence-building measures, and the U.S. is a leader in this.

Mr. CHABOT. Thank you.

Mr. Rauscher.

Mr. RAUSCHER. Yes, I think there are several opportunities that are ripe for the picking. The first deals with the underpinning of cyberspace, how we are connected between North America and the major financial center, Hong Kong, in China, and that is through undersea cables that all come together underneath in the Luzon Strait, and that is a choke point.

A recommendation in this ROGUCCI report suggests that we need geographic physical diversity and a route around the west side of Taiwan, very sensitive waters, that will land in North America would bring great stability to our two economies. This is really something that needs to be done. The Chinese need to take a step where they would give assurances to investors, but in North America we need to make it clear that the United States has places that cables could land.

Another great opportunity for a confidence-building measure is to implement priority international communications. This is a capability at a national level that was critical for us, but we do not have an extension of it internationally. We are increasingly dependent on each other, and yet we cannot communicate in a crisis like Fukushima or 9/11 because there is massive congestion that works particularly internationally. This is a great opportunity.

I think there are other opportunities in areas that we are exploring. Perhaps I will have a chance to address that later in the hearing. Thank you.

Mr. CHABOT. Thank you very much.

I will now recognize the ranking member, the gentleman from American Samoa, Mr. Eni Faleomavaega.

Mr. FALEOMAVAEGA. Thank you, Mr. Chairman.

I have become somewhat apprehensive about the idea that China is the new monster, you have to be very careful, you have to watch out for them. The fact is I think they are not that—I mean, it seems to me, in my opinion, they are not really up to the same capacity in terms of the advancements that we have made as far as cyber security is concerned, and technology has been primarily still between Russia and the United States. Correct me if I am wrong on that.

And, Dr. Schneck, you mentioned something about the activities that the McAfee Company has operated on this Operation Dark Seoul as well as Troy. I am not very good in your technical explanations that you gave. What exactly happened? Was it a virus, or how—and did it come from China? Where is the source of this virus that seemed to have gotten Seoul really upset in the month of March?

Ms. SCHNECK. In a nutshell, malicious instructions, computers were given direction to erase their hard drives. They were rendered useless. So that takes down systems of——

Mr. FALEOMAVAEGA. Who was doing this?

Ms. SCHNECK. When we focus these investigations, we don't like for attribution. We look for how to protect our customers. We leave the attributions, the corporate decision, to law enforcement, who are trained to get that right. Our investigation is about protecting the networks worldwide that are being bombarded with these literally instructions that say, erase now, which can cause damage.

Mr. FALEOMAVAEGA. So you were able to save it, but you don't know the source—who originated the virus and all of that. Am I correct on this? I am a little confused here.

Ms. SCHNECK. We don't know that definitively. I can go back and get the actual guides from the lab to see what else they know. Our corporate direction and our mission is to protect. So we focus on what is the damage being done, how is it being done, and how do

we make sure that no one else on the planet has to take it from this particular attack, and how do we learn it from that.

Mr. FALEOMAVAEGA. Dr. Lewis?

Mr. LEWIS. The Chinese are pretty good, and we don't want to underestimate them. They are not as good as the U.S. in offensive capabilities. And the big problem for China is that they use pirated software, and pirated software just can't be made safe. So they are in a weaker position, and they are a little afraid of us, but they are also not constrained in engaging in cyber espionage, and that is really the big problem.

So we don't want to paint them as a monster, but they are also not entirely innocent when it comes to this stuff.

Mr. FALEOMAVAEGA. No different than the Russians or any even of our allies.

Mr. LEWIS. The Russians are at the top of league, and one of the reasons you see China in the paper all the time and not Russia is just because the Russians are better at not being caught.

Mr. FALEOMAVAEGA. And the United States as well.

Mr. RAUSCHER. Cyberspace has inherent, intrinsic vulnerabilities in the ingredients that make it up. And so, in fact, if you removed Asia from the map, if Asia didn't exist, the fact is, we must face it, America, our government, our businesses, our personal information is still exposed just as it is now. And so we are fundamentally at risk because of the intrinsic vulnerabilities within the ingredients that make up cyberspace, the networks that connect us, the software that controls things, and hardware that obeys the commands that it is given.

So reliance on cyberspace is the first-order problem. The malicious actors who take advantage of vulnerabilities in cyberspace no matter where they come from are the second-order problem.

Mr. FALEOMAVAEGA. I mentioned earlier the fact some 500 million Chinese have access to the Internet. That is a pretty good number as far as potential marketing, business, consumer, and demands and all of that. If were you to do it in terms of proportions, how would any government be able to put any kind of controls on that number of people are currently using the Internet even alone here in the United States? I seem to look at this as a positive trend rather than saying that it is bad that people have access to the Internet is something that we should be careful about. I don't know, maybe you could help me on that.

I have 30 seconds left now.

Mr. RAUSCHER. My observations are that China's primary concern regarding hacking is unlike ours. They are concerned about the insider threat. They do have—they are very challenged about controlling their own citizens.

On the other hand, quickly, to contrast with India, they well are the third largest country in terms of online population, yet they have a very low penetration rate. Only 10 percent of them are online. And so malicious actors are able to exploit the relatively low maturity of their ICT (information communications technology) in their country.

Mr. FALEOMAVAEGA. I am sorry, my time is up.

Thank you, Mr. Chairman.

Mr. CHABOT. Thank you.

The gentleman's time has expired. The gentleman from Pennsylvania, Mr. Perry, is recognized for 5 minutes.

Mr. PERRY. Thank you, Mr. Chairman.

So since we know what China is interested in and what they are not interested in, they are not interested in having their population informed. They are interested in stealing intellectual property from various countries, including ours, and they have been pretty prolific as far as we know and expect and announce.

Should it be our policy to hit them where it hurts, to coin the phrase, I mean, to find a way? I imagine there is a way to open up the Internet to free information for the Chinese people. I mean, what would you say should be our plan from a national security standpoint regarding cyber security and diplomacy with China to avert? Because all the warnings, all the discussions, all the announcements seem futile; they do what they—they disavow it, and they continue to do it. So what should be our plan?

Mr. LEWIS. In private they are they aren't disavowing it anymore. So it is interesting to see that their public posture and their private posture has changed.

We went through something like this with China before regarding nonproliferation, and the steps we used there probably will work in this case. You need to engage the Chinese directly and tell them, this isn't what responsible nations do. You need some kind of agreement on what is responsible behavior, and the U.S. is helping to build that. You need your allies and partners to come in and say the same thing. That was very helpful before.

And it is going to be a long process. It is going to be hard. You will need to think of measures that will help encourage the Chinese to think the right way, and some of the things that do this could include putting people on Treasury lists to prevent them from banking in the U.S., putting them on no-fly lists, sanctioning Chinese companies.

I always found the Hill very helpful when I had to negotiate with them, because what I would say is, you have got to help me out here, you got to give me something, because I can't control those crazy people on the Hill. And that was a good tactic, because they know our system, and they know that the Congress is going to be a little more assertive.

And so putting together a package of engagement, allies, and possibly some kind of sanctions, including information or sanctions like were you talking about, I think that will get us there. It will take a number of years, but I don't see an alternate path.

Mr. RAUSCHER. I think the Internet is going to win. First, the power of the devices in the system that we have, so to speak, is their connectivity. And so if you limit the connectivity, you are not going to be as competitive in research or in business. So at the global level, countries are going to want to be connected to the Internet to be competitive. Once they do that, there is going to be the free flow of information.

No matter how good you are, its just simple mathematics, once you are connected, if you think of that as a 1, your filtering can only be something less than 1. Perfect filtering would be a 1. So if you are at 95 percent, and you are really good at filtering, that 5 percent of information on the Internet is a vast amount of infor-

mation, incomparable to anything that, you know, we dealt with like in the Cold War in the 1950s and such.

So I think with that amount of information that the Internet delivers, the Internet will win. And so if we are able to keep the Internet as it is now, as a robust place for the marketplace and for education and learning, it is going to be a powerful force, even more so in the future than it has been to date.

Mr. PERRY. So the Budapest agreement says that retaliation by, let us say, U.S. companies, retaliation against cyber crimes is disallowed, right?

Mr. LEWIS. Yes.

Mr. PERRY. What are United States companies supposed to do to proactively protect themselves as opposed—understanding they buy McAfee, right? That is a great line for you. But, you know, to me I feel like we are dealing with something on a higher level, and once all your information is gone, or your proprietary information or your employee information has been compromised, it is too late, and you can't unring the bell. So what proactively can they do? Is there some method of some type of retaliation that would be authorized?

Ms. SCHNECK. So I think—look, this is about making everybody more secure and more resilient and safer, because the Internet is a wonderful thing, and it is not going anywhere. It makes life better.

What we need to do is reduce the profit model. Right now the adversaries are doing very well, and we are not putting anything in between that. But yet we look at bank robbery, and that has pretty much stopped because it is not worth it, you know you are going to get caught. And I think what companies can do is work with government to make it harder for the adversaries to win this. We keep our Internet, but we also build in better controls.

It is not about products; it is about how you assess your risk, how you make boardroom-level decisions to make things safer whatever you buy and whatever you do. But that is a global private-to-government discussion that needs to be had very powerfully right now.

Mr. CHABOT. The gentleman's time has expired.

The gentleman from California Mr. Bera is recognized for 5 minutes.

Mr. BERA. Thank you, Mr. Chairman.

The problem with bank robbery, though, is the penalties are pretty stiff if you get caught. I think that goes to my colleague's concern.

I have got two questions, first for Dr. Schneck. McAfee's perspective is really one of protection, how do you protect your customers, how do you identify those vulnerabilities and threats and proactively protect as opposed to seek out who the person who is threatening you are.

What steps should this body take to strike that right balance of, you know, having a thriving, open marketplace where we are open for business, but at the same time knowing that we want to keep the Internet open, and we are seeing these threats? Are there some specific actions that you would like to see us discuss here in Congress?

Ms. SCHNECK. I think it is so important to, number one, as I mentioned before, have the protections for companies to be able to share information with each other about what we are learning and what we are seeing. We have seen before, worried about the threat of a lawsuit the next day, we were not able to share information about certain oil and gas companies and the fact they are being targeted. Our lawyers didn't let us because they worried we would get sued the next day if the stock prices of the energy sector went down. And there is legislation in Congress, or had been, that looked at how do you protect companies, all companies, in that situation.

I think the second is incentivizing the private sector to really look at how do you do a risk-based assessment of cyber security and consider your network as a critical asset, because the Internet is so important, and how do you invest in that from the boardroom? This is not necessarily a technology discussion. It doesn't even have to do with technology providers. This is about how does business protect themselves, and how does the government—what you can do is help incentivize that, and that will actually foster creative innovation for new and better and less expensive methods.

Mr. LEWIS. We did a report about 6 months ago that found that most corporate networks are tremendously insecure, and it actually doesn't take very much effort to break in. In fact, when we did the research, I was feeling sorry that I had gone into the wrong line of business.

Here is a good example we came up with this morning in our discussion with DOD. When you buy equipment, the password default is "password," and 90 percent of the time people remember to change the password. That is great, except the remaining 10 percent you are in. So finding a way to get companies to do more—and it is not rocket science—do more to secure their networks is crucial.

Mr. BERA. I have got a follow-up question, Dr. Lewis. If we use the example of the World Trade Organization, you know, with regards to trade, their norms of trade and their treaties that have been negotiated, and there is mechanisms if we feel someone is engaging in unfair trade practices where we can take a country and have a system of an arbiter.

Now, you have already commented that you don't think a treaty is doable at this juncture at the international level, but you talked in terms of creating norms and confidence builders. Can you talk about some of those norms and confidence builders and then a mechanism, though, still if bad actors or bad state actors act out of those norms and confidence builders, there does—you know, again, using the bank robber analogy, there has to be some system of penalty to incentivize good behavior.

Mr. LEWIS. True, that is a good question. And you might want to look at the Budapest Convention as an example of why a treaty won't work. About 80 nations, I think, have signed up to it. The pace of getting more signatories is slow.

But what you could do is think of ways to agree on what responsible behavior is, and one of them would be that the international commitments you have in the physical world also apply in cyberspace, and you exchange information on what you are doing, mili-

tary white papers, for example. And if people don't observe those norms, then we need to think about penalties. And an organization you might want to look at, it is called the Financial Action Task Force. That is an example. If you do money laundering and you are a country, guess what? It is going to be harder for you to change money. It is going to be a little harder for your central bank. We may have to think about measures like that, making it harder to do business on the Internet if you don't play by the rules.

Mr. RAUSCHER. The malicious actors are taking advantage of the lack of cooperation in this space. As an engineer I think of policy in this arena as the ability for entities to anticipate the behavior of other entities, whether they be machines, or governments, or individuals, or enterprises. And we just don't have the tight coordination that we need, and so there is a gap, and that is what is being taken advantage of.

What we have been doing at the institute is convening some 40 countries or more annually at an international summit. Our next one this year in November is hosted by Stanford, in Silicon Valley. We will be convening government and business leaders from 40 countries and going head on addressing these issues to try to tighten up that coordination.

Mr. CHABOT. Thank you.

The gentleman's time has expired.

The gentleman from Indiana, Mr. Messer, is recognized for 5 minutes.

Mr. MESSER. Thank you, Mr. Chairman. Thank you to members of the panel.

I think you are getting close to the end of your presentation. I think there is at least a question or two more, but obviously, this is a very important issue. The cost to the American economy is billions of dollars. The national security threats are large and growing. You—there is little doubt—there is no doubt that rogue nation states are participating in these attacks, and that it is a complex problem that is going to complex solutions that require a lot of cooperation.

You have talked a little bit, each of you in the panel, about the role of business and the role of government in solving this problem. Is it more business or more government?

Mr. RAUSCHER. Well, I guess I will start. You know, for traditional issues like security and trade, for military issues, that has to be the government, and part of the reason for that is that other countries expect it to be the government. The Chinese once told me there is really no such thing as the private sector, you know, it is all government. So for those issues, trade, security, armed conflict, it has got to be government.

For other issues it is not so clear. When we talk about innovation or technical standards or business relationships, that probably should be a private-sector lead.

Mr. MESSER. And as you answer, you cited the need for cooperation. Could you cite any examples of where cooperation has occurred, because I think some of those examples might be illustrative of the question.

Mr. RAUSCHER. I can cite an example. As I mentioned earlier in my testimony, we have a Track 2 bilateral that we have done with

the Chinese on fighting spam, and we have many individuals and corporations supporting this with their contributions of mind share, and very rigorous analysis in their actions with the Chinese on this. And this was able to be the result, I think, because of the trusted facilitation that a third party could do.

I actually did an analysis of how we were successful over the last couple of years. I mentioned earlier that we had 27 recommendations, and over half are implemented. And the comparative benchmark really is zero percent, because these are really hard issues that, if you look at what we have taken on, these are issues people aren't trying to address because they think they are impossible. And in the analysis, why these issues were stuck was governments have a difficulty at the international level because they are appropriately representing the national security interests that they have of their individual countries, and so every other country is a little suspect of what is happening. And then commercial entities are appropriately protecting the fiduciary responsibilities that they have toward their share owners, and so there is a little suspicion sometimes about the commercial interests they may have.

Now, both of these entities, governments and the private-sector, companies that are commercially oriented are capable, in many ways, of solving most of their problems. But there are niches where there are really intractable problems that you can't get into, and that is where a third-party entity that is philanthropic and internationally overseen is able to create the necessary trust to get over that hump. And so for the really difficult problems, I think using NGOs that are oriented toward action in trying to get breakthroughs is the right solution and approach.

Ms. SCHNECK. So to this point on the NGOs, I have been running these partnerships most of my adult life as a volunteer, and one of them that I chair now, the National Cyber-Forensics and Training Alliance, brings in the top-flight analysts from banks, pharmaceutical companies, telecoms, et cetera, and teams with other governments, and is anchored by our U.S. Federal Bureau of Investigation.

So with all the legal agreements finally worked out over 10 years, it helped arrest over 400 cyber criminals worldwide, and I think that is an example of how when you get the right partnership, you get the expertise that each side brings, and you maintain the swim lanes, from the points earlier. There are things that government is better trained and better able to do, and there are a lot of things, such as innovation, that are going to survive quickly in the private sector.

Mr. MESSER. One other question, a bit of a hot potato, but I am going to go ahead and throw it out, which is just to what extent, if any, do you think the recent revelations on the NSA online surveillance activities have impacted and complicated negotiations on these topics?

Mr. LEWIS. With the bilateral negotiations with China, they haven't had that much effect, largely because the U.S. has previously told the Chinese, espionage is a two-way street, all big countries do it; what we object to is the commercial espionage. So the Chinese weren't particularly surprised or didn't learn much from Snowden.

We don't know how it will play out internationally. It has gotten a considerable reaction in Europe, less of a reaction in Asia. One thing to bear in mind is most countries do things like this, so it is not—it is a little—some of our European friends are a bit hypocritical, and I hope they will calm down a little bit and think about what their own agencies do.

So far not that much effect.

Mr. CHABOT. The gentleman's time is expired.

The gentleman from Virginia, Mr. Connolly, is recognized for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Thank you to our panelists for being here.

I happen to believe cyber security probably is one of the most important challenges, maybe the biggest threat, we face, tied in with terrorism and superseding it.

Let me ask, Mr. Lewis, I read your testimony, and you said in your testimony, cyber security as an issue for international security is best addressed using diplomatic and trade tools. It shouldn't be an item that leads to armed clash. And I think in an ideal world, that is true. But it seems to me, dealing both with the Russians and with the Chinese, there have to be some understandings about red lines.

Red lines are dangerous things because sometimes they get crossed, and we still don't react. But take the Cold War as a parallel. I mean, during the Cold War both sides tested each other as to the limits. So when the Soviets blocked surface transportation to and from West Berlin, President Truman launched the Berlin airlift and outlasted the Soviets. Now, what the Soviets understood was they could buzz, they could try to jam aircraft flying into Berlin, but they could not attempt to shoot them down. That would be casus belli. So with respect of that, back when we had planes that crashed, they even returned the bodies of our airmen in the midst of this clash between the two powers. So, there were unwritten rules, there was always testing, but there was respect for something even ill-defined that was a red line.

Clearly I think you would agree that if, for example, organized cyber security attacks by a foreign government or agents of a foreign government were to detonate a nuclear weapon here in the United States by manipulating technology, that would be a cause of war. That is not okay, and that is not going to be solved by diplomatic means.

If you shut down—now, so where is that line? What are the examples—we don't want to be too specific by implying that everything else is okay, but I guess I am worried that maybe the Chinese and, for that matter, the Russians, in testing us and in exploiting the vulnerability of technology, they are perhaps underestimating the backlash that can occur here that can most certainly lead to armed conflict, and, by the way, in some cases will.

I wonder if you would comment on that, because I know you didn't mean forever, no matter what, and under all circumstances.

Mr. LEWIS. Three quick points. We do have red lines. Then-Secretary Panetta laid them out in a speech last October. If a cyber attack looks like it will cause the death of American citizens or do significant economic harm to the U.S., we will use military force

preemptively. So those are our red lines: Death, significant economic harm. Everybody knows that.

China, Russia, and others have been very, very careful not to cross that line, not to use force, and we have the best cyber offensive capability in the world. It has zero ability to deter espionage or crime, zero. We are—zero to deter espionage or crime, right. So we can keep people from attacking the U.S. in a military sense, but we can't keep them from doing other things.

The country that is testing us, and this is the worrisome—this is the part I worry about. The country that is testing us is Iran, and so Secretary Panetta's speech was aimed at Iran. They backed down. And it was funny because the Iranian activities went down for a couple of weeks, and they went right back up, and they continue to this day. So we are being tested, but it is by a country that is not as stable in its decisionmaking as Russia and China. They know the rules. They are not going to do anything that——

Mr. CONNOLLY. One quick question, any of you. Do we need some kind of international regime comparable to the WTO on trade or the International Court of Justice in the Hague to help govern the rules of engagement with respect to this subject and—or not? Would that help or not?

Mr. Rauscher?

Mr. RAUSCHER. I see three spheres. I see humanitarian, national security, and commercial. I think that the first two have rules that can pretty much be aligned, and I think the commercial one does need more cooperation. I am not sure if—the type of entity, what it should look like, whether it is intergovernmental or otherwise.

Mr. CONNOLLY. Mr. Chairman, would you allow the other two panelists to be able to respond, and I am done?

Mr. CHABOT. Yes. Without objection, we will give them an additional minute.

Mr. CONNOLLY. I thank the chair.

Mr. LEWIS. Well, the official U.S. position is that we don't need a new institution, and it is already the case that we use some of the existing institutions, the ASEAN Regional Forum, the Organization for Security and Co-operation in Europe, the U.N., as a way to address this. But one of the things you see from other countries, including a lot of countries in Asia is, yeah, maybe we will need some kind of institution to deal with this, probably anchored in the U.N.

So it is sort of an open question. I think the U.S. approach is right. First, let us agree on the rules, the general rules, and then let us figure out how we want to enforce them.

Ms. SCHNECK. So, we believe in global conversation. We think there needs to be more conversation and commend some of the recent efforts like those in the U.N. But these four, like that mentioned by Dr. Rauscher and others, these are good starts to that global forum, and we are committed to the opportunity to participate in those and think that there is a place for government and industry across the world, and this is a conversation that is just beginning and really needs to happen.

Mr. CONNOLLY. Thank you.

Thank you, Mr. Chairman.

Mr. CHABOT. Okay. Thank you. And the gentleman's time has expired.

We will go into a second round of questions. I will recognize myself for 5 minutes.

We spend a great deal of time talking about cyber threats in East Asia, but as we are all aware, South Asia plays an important role. In some cases it is not very positive. Pakistan has joined with China and Turkey and Malaysia to counter cyber threats posed by Western nations. The terrorism angle adds a different perspective to this cooperation. My question is, should we be worried about these nations, Pakistan, China, and Turkey, for example, coordinating their cyber policies with each other? Anyone may answer the question.

Mr. LEWIS. Well, if the—the Malaysian effort you are referring to is an organization called IMPACT. That hasn't developed quite as much as you—they might have hoped, so I don't think we have to worry about that.

It is interesting to ask whether the Pakistanis, the Turks, the Chinese will come up with some competitive model that will compete with the U.S. and its allies in how we should order cyberspace. That is unlikely, but it is something certainly that the Chinese are interested in.

The Indians are more likely to end up on our side. They are a democracy, they like free speech, we have close commercial ties.

So very complex diplomatic landscape, but I think that when you look at places like Turkey, Pakistan, India, these are countries whose views we do have to take into account now, that we do have to find an arrangement with.

Mr. CHABOT. Let me focus on India. They have been quite active of late establishing its National Cyber Coordination Center last month and releasing its National Cyber Security Policy earlier this month. It calls the U.S. one of its biggest threats, next to China, after the information revealed by Mr. Snowden. However, India maintains a wide-ranging surveillance program of its own that monitors its citizens' emails, phone calls, social media activity, and Web searches without judicial oversight.

Cooperation with India is an important aspect of U.S. efforts to rebalance toward Asia, especially in regards to trade and military cooperation. How do you think disagreements on cyber will affect the overall U.S.-India relationship? What is your opinion of the way India is handling cyber security? Do you think these recent initiatives or policies could possibly negatively affect its already hostile bilateral relationship with Pakistan?

Yes, Mr. Rauscher.

Mr. RAUSCHER. I have some insights that might be useful on some of this. We held our annual summit last year in New Delhi, so I spent a lot of time in New Delhi working with government leaders and the industry there, and certainly the step you cite, this National Cyber Coordination Center, is in the right direction.

A key word there is "coordination." There is a lot of coordinating to do, but there are also limitations in the capacity. As I mentioned earlier, the penetration rate, it is still fairly early in that country, about 10 percent, and so there is a lot of capacity to be built to coordinate both in the government and in the private sector.

Whether or not this is a role model for other countries in the region is unclear yet, but what is a role model is a highly functioning CERT, the Computer Emergency Readiness Team, that is a model that works consistently effectively, and also the MAAWG.

There is a private-sector organization being set up in Mumbai to deal proactively with botnets that are being set up there by external actors of the country. Spam is identified as the leading producer of international spam. India is recognized as the leading producer of international spam. And, again, as I mentioned earlier, it is a vehicle for malicious code, and their coordination with external experts to root out these botnets and sources of spam is really critical not only for India, but the rest of the world, particularly in English-speaking countries.

Mr. CHABOT. Thank you.

I have about 1 minute left if either of the other panel members want to weigh in on either issue.

Mr. LEWIS. Sure.

Mr. CHABOT. Mr. Lewis?

Mr. LEWIS. The Indians' primary concern in cyber security is with Pakistan and Pakistani nonstate actors or state-sponsored actors launching some kind of attack against India.

Their second concern is Chinese espionage, and one of the things that works in our favor is they aren't particularly friends with the Chinese all the time, and they worry a lot about it, so we have an opportunity to work with India. The thing we have to avoid in doing that is giving the impression that we are trying to contain China. The Chinese worry about this a lot. We do need to build a partnership with India, but we have to do it in a way that doesn't appear to be deliberately trying to contain China.

Mr. CHABOT. Thank you very much.

The gentleman from American Samoa, Mr. Faleomavaega, is recognized for 5 minutes.

Mr. FALEOMAVAEGA. Thank you, Mr. Chairman.

We are in a dilemma here, and maybe I am not on the right track, and somewhat of an irony here that we are concerned about our national security. At the same time how do we go about making sure that government does not intrude into fundamental, basic constitutional rights and freedom?

And I guess you know where I am headed at. Right now before us is a situation where an American citizen has decided that total violation of the right of the American people to know what is going on. I am talking about Mr. Snowden. How do we put Snowden's situation here with what we are talking about as far as cyber security, intelligence, the spying, the espionage, and all that is going on? And by the way, it seems that it is not just toward China, but our own allies. And, of course, our own allies spy on us, too. So, where do we—where do we measure the sense of balance in what was raised earlier when we talk about cyber security in that regard? Please.

Mr. RAUSCHER. Well, I think it has been humbling for us as Americans who travel abroad and talk about these issues—what is happening in our own country. And I am proud when I go anywhere in the world to talk about our ideals. I think we have the best country that has been set up in history. And I think if we look

back to our Founding Fathers and the challenges they have given us in the Constitution, we could get some direction to answer your question.

I know when we look at this issue, we are often looking at the Fourth Amendment. But this is a bit bold, and pardon me a little bit, I am an electrical engineer here, but I actually think that information is power, and when I look at the Second Amendment, that is the place where our Founding Fathers boldly, you know, set up this power balance with the people. And I think that we should look for the analogy from the Second Amendment to say, as the government seeks to use technology to enhance its ability to protect national security legitimately, that it needs to look at how it affects the balance with the power that the people have—not independent courts that are kind of private, but actual people, the public—have in terms of information regarding what the government's activities are.

So I think there is some insight. It is not a completely traced proposal, but I think that there is something—a principle there in our Bill of Rights that gives us some insight about how we should handle that.

I think it is important for us to continue to carry the mantle of freedom. We have done that for generations now in our country, and we need to continue to do that for the rest of the world.

Mr. FALEOMAVAEGA. The only thing that disturbs me about Mr. Snowden's situation is the fact that when you are in this kind of a relationship in terms of your employment with the national government, and you are given an oath to swear as far as security interests of the country, and especially putting the lives of our men and women at risk in terms of when you get into the intelligence, when you get into espionage, when you get into the kind of activity the National Security Agency is involved—and by the way, this administration simply followed what the PATRIOT Act provisions provide, allowing the President to do what he is doing, and there is nothing illegal in what the President in this administration has done as far as putting out these feelers, if you want to call it, whether it be in our European Union country allies or any other country in the world.

But what—again, it goes back again, does Mr. Snowden really believe that what our Government has done is beyond the rights that have been given under the Constitution of our country as far as the freedom to know?

Mr. LEWIS. Mr. Snowden is kind of a naive child. I mean, if he had a brain, he would have gone to Brazil, right, where they don't have an extradition treaty. But he did bring us to a debate that maybe we should have had, and it has to be an open debate over the balance between surveillance and privacy.

It would hurt—it wouldn't hurt to have greater transparency, you know, where you could publish FISA findings with things blacked out, but we have to recognize—and this is getting lost—there is a trade-off between privacy and security. And what I worry is that we will overreact to Snowden's foolish revelations and constrain our ability to protect American citizens. We need that debate, greater transparency would be good, but let us not forget this is what it is protecting us.

Mr. FALEOMAVAEGA. Dr. Schneck.

Ms. SCHNECK. Yes. There is nothing more important than that balance of privacy and security for our national security and for our country. All the other stuff aside, information protects information, and we need security and privacy to protect each other. That is what we are here to protect is our way of life and our way of life as global citizens and as Americans, and that takes data, and it takes data to protect data, and we need to find the right way to make sure that we maintain that in an electronic world.

Mr. FALEOMAVAEGA. Again, Mr. Chairman, I truly want to thank our panel of experts here this afternoon. They have been a most entertaining and educational experience for me in understanding more about cyber security. Thank you, Mr. Chairman, and I want to thank the panel as well.

Mr. CHABOT. Thank you very much.

We will conclude with the gentleman from Virginia for 5 minutes.

Mr. CONNOLLY. Hello again.

Mr. Lewis, let me pick up on something you said and play devil's advocate, and I do genuinely mean devil's advocate.

You said that, yeah, we need to work with India, but we have to be very careful that the perception is not that we are somehow tilting against the Chinese or ganging up on them. Chinese are very sensitive about that. Devil's advocate question: Why should we care?

I mean, here is a country that is cheating. They are cheating on intellectual content, they are cheating on protections of intellectual property, I mean, from Starbucks coffee to software. It is breathtaking. Rather than invent their own, they just steal it from us, let us do the R&D investment. They are stealing military secrets using cyber security hacking attacks. It is systematic. It is not rogue elements running around in China who can control them. This is actually headquartered in the military compound, run by elements of the Chinese People's Liberation Army.

It is wholesale, state-supported theft, and a direct threat to the national security of this country as well as some others. So why wouldn't we openly cooperate with India to send a message that we are prepared to protect our interests and work with those who want to work with us, and, yeah, it is at your expense. You have been engaged in all kinds of things at our expense. Why should we be so sensitive to China?

Mr. LEWIS. No, that is a good point, and the Chinese would probably say—I am starting to play devil's advocate—is you guys don't care about our feelings, and you are trampling over them anyhow, and you are trying to contain us.

I think I look at it from the perspective of, you know, we are in the phase now where we need to persuade the Chinese to change their behavior. We cannot coerce them. They are too big a country. The only way you are going to coerce them is if we go to a war. That is in no one's interest.

So we need to persuade them, we need to avoid conflict. And the Chinese are paranoid. One of the things, I think, that would be useful is if the Chinese, especially the PLA, moved away from the

sort of Maoist heritage of everyone is trying to get out—everyone is trying to get us.

So in thinking about how to shape the Chinese internal politics, I think that, you know, this open approach, we have just started to try it, we have just started engagement, let us see how it works. There are factions in China that want to work with the U.S., that want to move in the right direction. Let us encourage them. Three years from now, 4 years from now, if it hasn't worked, then we can think about stronger measures.

Mr. CONNOLLY. I guess I would suggest to you that my own observation over four decades is the Chinese respect power and sometimes little else, so the "there, there, now, now, let's try to work this out, and my, my, try not to do that again" approach is not one that is very efficacious, and not one that is respected in Beijing. And at some point, it seems to me, we have to protect our own interests, economic, political, military.

I am not arguing for a forceful, you know, armed conflict, but I am arguing for much tougher enforcement and teeth with it than has occurred heretofore.

Mr. LEWIS. No, I think that is right. I think we will get to the point where we will need to use punitive measures to encourage the Chinese, but we want to do it in a careful fashion. They are afraid of us, right? They look at us, and they know we are infinitely more capable than them.

We are all over their networks, right? Their networks can't be defended. So we are ready. We don't have to send the message, we are mad at you, and we could overpower you. They already know it. So I want to find a way to work with them. If that doesn't pan out, you know, give it a few years, and if we get into a harder place, sure, think of harder measures. But we don't have to scare them; they are already afraid.

Mr. CONNOLLY. Final question: What is your assessment of the talks between the new President of China and President Obama on this subject?

Mr. LEWIS. Well, the State Department says the talks went very well, so I know that comes as a news flash. And I think actually they did. In some of the preparatory meetings, Chinese officials told us that China is reconsidering its position in light of the changes in the international environment. The Chinese know they have a problem; they know they have to change. How much they will change will depend on how consistently and persistently we press them.

Overall I am confident if we can maintain this effort for 3 or 4 years, we will be in a different place. If we back off, you are right, the Chinese will just revert to their normal behavior. But they are interested in saying, how do we get to a deal with U.S., what does a deal mean? It is true that their first thing was, okay, we agreed to a working group, doesn't that make you happy, right? And I think that Americans thought it was good in saying, no, it is nice that we have a working group, but we need to do more. And they agreed to more talks, they agreed to work on norms. So we are on the right path.

It is a big country. It is going to take a while to talk them out of it. When we did this in proliferation, it took 4 or 5 years to get them to change.

Mr. CONNOLLY. You know, Mr. Chairman, Mr. Lewis' answer to me at the beginning, the State Department said the talks went very well, reminded me of that famous incident with Ronald Reagan when he was President. He was on the White House lawn, and a scrum of reporters were shouting out questions. He either couldn't or feigned he couldn't hear, and he was with Nancy Reagan at one point, and so she says in his ear, but it gets picked up, "We are doing the best we can," and he goes, "We are doing the best we can."

Mr. CHABOT. I remember that.

Mr. CONNOLLY. The talks went very well.

Thank you very much.

Mr. CHABOT. God bless Ronald Reagan.

I want to thank the panel for their testimonies this afternoon. It has been very helpful to the committee. Without objection, members will have 5 days to submit questions or revise remarks.

If there is no further business to come before the subcommittee, we are adjourned. Thank you.

[Whereupon, at 3:45 p.m., the subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

SUBCOMMITTEE HEARING NOTICE
COMMITTEE ON FOREIGN AFFAIRS

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515-6128

Subcommittee on Asia and the Pacific
Steve Chabot (R-OH), Chairman

July 18, 2013

TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS

You are respectfully requested to attend an OPEN hearing of the Committee on Foreign Affairs, to be held by the Subcommittee on Asia and the Pacific in Room 2172 of the Rayburn House Office Building (and available live on the Committee website at www.foreignaffairs.house.gov):

DATE: Tuesday, July 23, 2013

TIME: 2:00 p.m.

SUBJECT: Asia: The Cyber Security Battleground

WITNESSES: Phyllis Schneck, Ph.D.
Vice President and Chief Technology Officer
Global Public Sector
McAfee, Inc.

Mr. James Lewis
Director and Senior Fellow
Technology and Public Policy Program
Center for Strategic International Studies

Mr. Karl Frederick Rauscher
Chief Technology Officer and Distinguished Fellow
EastWest Institute

By Direction of the Chairman

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF SUBCOMMITTEE ON *Asia & the Pacific* HEARING

Day *Tuesday* **Date** *7.23.13* **Room** *2172*

Starting Time *2:22pm* **Ending Time** *3:46pm*

Recesses [ ] (____to ____) (____to ____) (____to ____) (____to ____) (____to ____) (____to ____)

Presiding Member(s)

Chairman Steve Chabot (R-OH), Ranking Member Eni Faleomavaega (D-AS)

Check all of the following that apply:

Open Session [✓]
Executive (closed) Session [ ]
Televised [✓]
Electronically Recorded (taped) [✓]
Stenographic Record [✓]

TITLE OF HEARING:

Asia: The Cyber Security Battleground

SUBCOMMITTEE MEMBERS PRESENT:

Rep. Matt Salmon (R-AZ), Rep. Scott Perry (R-PA), Rep. Doug Collins (R-GA), Rep. Luke Messer (R-IN), Rep. Mo Brooks (R-AL), Rep. Ami Bera (D-CA), Rep. Gerald Connolly (D-VA)

NON-SUBCOMMITTEE MEMBERS PRESENT: *(Mark with an * if they are not members of full committee.)*

HEARING WITNESSES: Same as meeting notice attached? Yes [✓] **No** [ ]
(If "no", please list below and include title, agency, department, or organization.)

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*

TIME SCHEDULED TO RECONVENE _____
or
TIME ADJOURNED *3:46pm*

Priscilla Koob
~~**Subcommittee Staff Director**~~ Professional Staff Member