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.

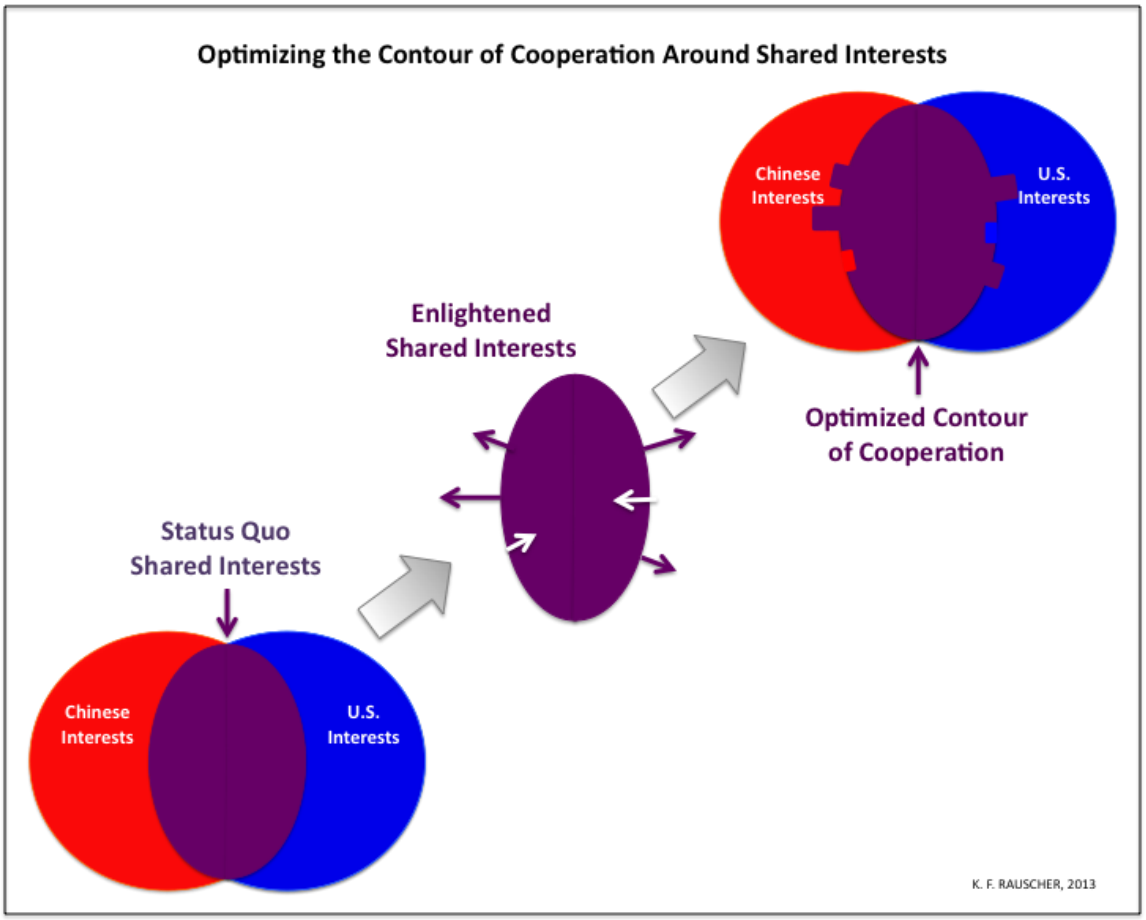

Figure A. Optimizing the Contour of Cooperation Around Shared Interests

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.

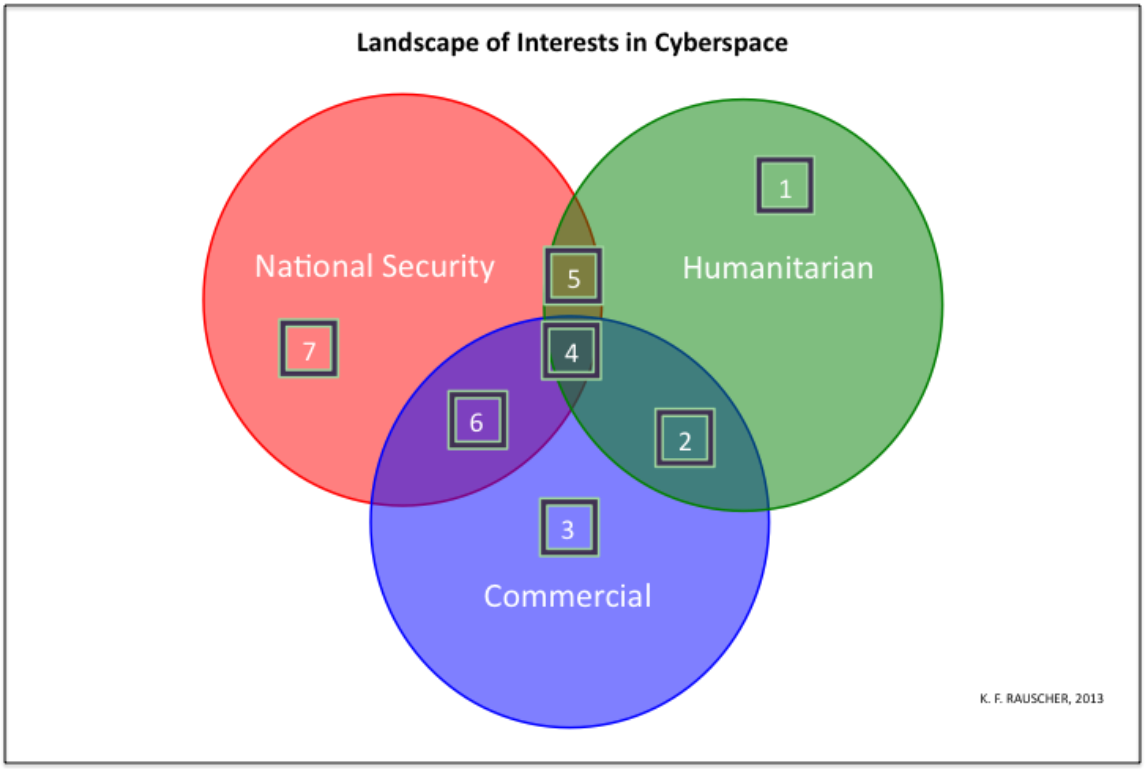

Figure B. Landscape of Interests in Cyberspace

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.

One Hundred Thirteenth Congress
U.S. House of Representatives
Committee on Foreign Affairs
2170 Rayburn House Office Building
Washington, DC 20515
www.foreignaffairs.house.gov

July 18, 2013

Mr. Karl Rauscher
Chief Technology Officer and Distinguished Fellow
EastWest Institute
1069 Thomas Jefferson Street, N.W.
Washington, DC 20007

Dear Mr. Rauscher:

I am writing to invite you to testify at a hearing entitled, "Asia: The Cyber Security Battleground" to be held before the Subcommittee on Asia and the Pacific at 2:00 p.m. on Tuesday, July 23, 2013, in Room 2172 of the Rayburn House Office Building.

Asia is a region beset by some of the world's most aggressive cyber actors, which makes regional engagement imperative for promoting the preservation of global network functionality, and for establishing confidence building measures that foster trust and reliability. The purpose of this hearing is to discuss the growing cyber threats emerging from Asia, and ways in which international cooperation can build cyber security capacity and ensure innovation flourishes alongside efforts to safeguard U.S. national security. Please address the following questions:

- What are the priorities for cyber security engagement efforts with China? How do you think cooperation will develop following the first Cyber Working Group held at last week's U.S.-China Security & Economic Dialogue?
- How are cyber threats from China evolving? How can the U.S. pressure China to take more accountability of and deter the growing number of attacks emerging from within its borders?
- What are the broader implications of India creating its first cyber security coordination center? Are India's efforts a model for other Asian nations?
- How is the growing hacker industry impacting the region? Would it be possible to institute a set of international norms? Is the U.S. Government's cyber community headed in the right direction?

Enclosed are the Subcommittee's instructions for hearing witnesses, as well as the required truth-in-testimony disclosure form. I ask that a biography, completed form, and written testimony be sent electronically to priscilla.koepke@mail.house.gov as soon as possible. Should you need any additional information for this hearing, please contact Priscilla Koepke at (202) 225-0358.

Sincerely,

EDWARD R. ROYCE
Chairman

Enclosures