

EXECUTIVE SUMMARY
prepared for #cybersummit2013



CHINA-U.S. TRACK 2 BILATERAL ON CYBERSECURITY

FRANK COMMUNICATION AND SENSIBLE COOPERATION TO **STEM HARMFUL HACKING**



EASTWEST INSTITUTE

Forging Collective Action for a Safer and Better World



中国互联网协会
Internet Society of China

READ MORE

Learn more about EWI's cybersecurity work and read all our reports at www.ewi.info/cyber

Measuring the Cybersecurity Problem

Building Trust in Cyberspace

Cyber Detente Between the United States and China

Priority International Communications

The Internet Health Model for Cybersecurity

Mobilizing for International Action

Fighting Spam to Build Trust

Critical Terminology Foundations

Working Towards Rules for Governing Cyber Conflict

Protecting the Digital Economy

SILICON VALLEY 2013

World Cyberspace Cooperation Summit IV

cybersummit.info
[#cybersummit2013](https://twitter.com/cybersummit2013)

ORGANIZED BY:

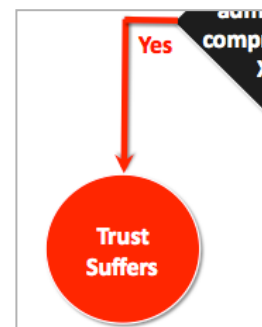


PARTNERS:



EXECUTIVE SUMMARY

By KARL FREDERICK RAUSCHER & ZHOU YONGLIN [周勇林]



The 'hacking' issue is a *serious challenge* for the future friendship and the prosperity of China and the United States. *Unlike* superpowers before, history's two largest economies are intimately intertwined and mutually reliant in cyberspace. Information and communications technology (ICT) is pervasively applied to medical care and social life, industry and trade, research and education, and law enforcement and national security, to name a few. The technologies that China and the United States are now so reliant upon are rapidly advancing in both the power they wield and the complexity they bring, thus making us more and more vulnerable. China and the United States are mutually reliant upon ICT products that are made by each other. While the U.S. has a unique grasp of the technology supply chain with its research and development leadership in core software and hardware platforms, China is catching up. They are so close in their integrated reliance on each other, that each can easily do harm to the other – *devastating* harm. Unfortunately, in the past years, China and the U.S. have seen the trust in their relationship suffer. The current situation is thus one of growing instability for China and the U.S. with regard to cybersecurity.

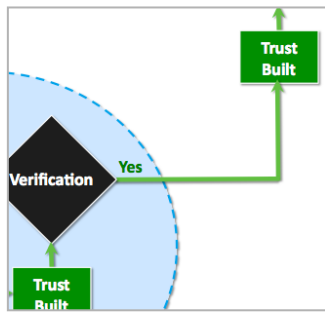
Arising from a variety of motivations, including crime, politics and curiosity, a growing number of harmful activities are conducted in the cyberspace we are so much relying upon. Such harmful hacking threatens the safety and prosperity of the world. From a pure numbers perspective, the networks of China and the U.S. have many Internet Protocol (IP) addresses, and thus have many potential sources of malicious activity, as well as many potential targets. Among all written and spoken words on the subject, the suspicions and blames have taken on the strongest voice for the relationship of China and the U.S. Yet we know that such an approach can never solve such difficult problems. On the contrary, such accusations and arguments have fueled escalations so that the relationship is now strained, making even routine dialogue apprehensive, rather than comfortable and confident.

Presidents Obama and Xi have placed cybersecurity on their bilateral agenda, and front and center is damaging hacking.¹ The problems include the exfiltration of commercially sensitive data, access into operations of critical infrastructure and national security assets, the militarization of cyberspace, unequal scrutiny of behaviors in cyberspace and the dependence on the other's systems in its critical infrastructures. The joint problem statement was agreed as:²

For China and the United States, the following are unacceptable: (i) the **perceived core beliefs** of each other for what is permissible behavior in cyberspace, (ii) the **proliferation of compromises** being made to each other's assets in cyberspace, and (iii) the **unsettled dispositions of identified incidents** of compromises that have affected each other's assets.

¹ Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting, Sunnylands Retreat, Rancho Mirage, California, 8 June 2013.

² Section 2.2, *Problem Description*.



What is common is that neither side is comfortable with the policies and practices of the other. Both sides also recognize that harmful hacking is not a China-U.S. issue, as it is an issue now for the world.

This report was prepared to help these two countries get out of this predicament. This report was prepared through the agility of a track 2 bilateral approach, with the insights of over 150 volunteer subject matter experts with profound experience and knowledge of policy, technology, business and law, as relevant to cybersecurity. Facilitated by the Internet Society of China (ISC) and the EastWest Institute (EWI) this research report answers two questions:

1. *How do we build trust between China and the U.S. in cyberspace?*
2. *What practical countermeasures can we take to improve the safety of cyberspace?*

This report submits ten immediately actionable Recommendations, which if implemented, will establish practical conversations and relationships that can slow the rate of destabilization around this subject, and, with continued application then reverse the trend's direction to one that is favorable (Section 4).

Together, the first four recommendations support a Total Trust Management (TTM) system that assures a reliable assessment (Figure 1). With this system in place, genuine trust can thrive and each party can have confidence in their assessment. This system will also detect when either party is demonstrating behavior that is *not* trustworthy, and likewise enable a party to have confidence in its judgment that there is insufficient evidence that their interests are being protected.

The TTM system is equally applicable for a wide range of topics, including international cooperation in fighting crime, international cooperation in tracking down malicious hackers, protection of humanitarian interests, protection of commercial intellectual property and norms of behavior in cyberspace. The first set of recommendations can be summarized as:

■ **Recommendation No. 1 *Stated Policy***

The first step to building trust is setting expectations. This first recommendation calls on governments, businesses and other organizations to state clearly their interests and practices in cyberspace.

■ **Recommendation No. 2 *Policy Deployment***

Once policy is stated, the second step in building trust can begin: moving from words to actions. This recommendation calls on governments, businesses and other organizations to deploy the policies they espouse.

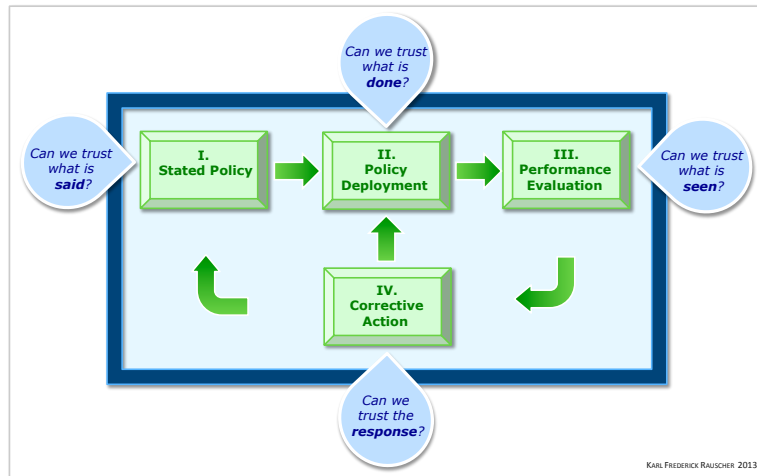


Figure 1. Total Trust Management Model, with Trust Questions.

■ Recommendation No. 3 *Performance Measurement*

Once policy is stated and deployed, then the third step in building trust can begin: engaging stakeholders who perceive an apparent failure in policy or its deployment. This recommendation calls for cooperation in analyzing incidents of failed policy or its deployment.

■ Recommendation No. 4 *Corrective Action*

The response to failures in stated policy or its deployment are a key indicator of an organization's trustworthiness, whether it be a government agency, a business, or otherwise. Corrective actions are tangible ways that show serious commitment to stated policy.³

Each party is evaluated based on adherence to its stated policy and plan of action.⁴ If implemented, these recommendations will clear the air. Stakeholders will have confidence in each other based on their observations from a pattern of what is said, done and seen. This cycle of meaningful dialogue and engagement will in turn produce tangible progress at various levels in confidence building and risk reduction, with the aim of producing an upward spiral of reinforcing cooperation and trust.

The simple truth is that the essential 'asks' in these first four recommendations are actually quite *basic*. Yet the present day China-U.S. crisis over hacking is evidence of how these *basics* have been neglected. In the unfortunate case where either one or both sides is unwilling to commit to these basics, discussions on more advanced subjects can be delusional; giving a false sense of safety for which there is no foundation. Thus the TTM system can help inform both parties and stakeholders of a status of good health, improving health, deteriorating health or bad health. The TTM system is an alternative to brinkmanship, i.e. deterioration of confidence that is reinforced by the negative cycle of non-cooperation and misinformation.

An element of the analysis was the Landscape of Interests in Cyberspace framework, which enabled focused analysis of three primary interests, and their interactions (Figure 2, Section 2.4.1, *Landscape of Interests*). By examining the interests, we categorize the information systems into 7 groups. Different groups have different involvement with cybersecurity. One major conclusion from this analysis is agreement that humanitarian assets in cyberspace deserve special protection. A second major conclusion is that governments, businesses, and other entities with national security missions should acknowledge the higher risk created when conducting international espionage.

³ i.e., Recommendation No. 4, *Corrective Action*, anticipates regular needs to adjust Stated Policy and Policy Deployment plans.

⁴ At its core, the TTM system described above is an empirical method of arriving at the truth, but one that allows for human imperfections along the way.

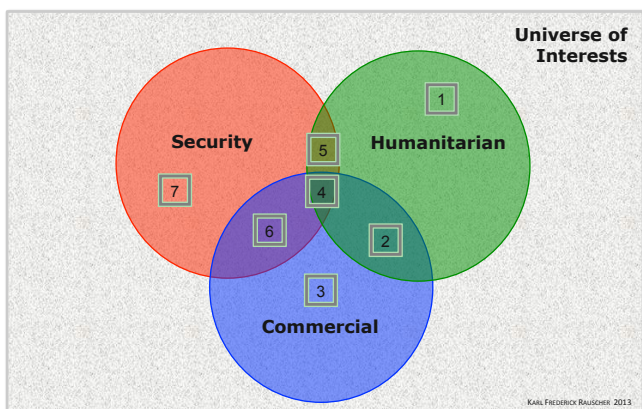


Figure 2. Landscape of Interests in Cyberspace.⁵

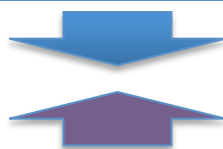
Another element of the analysis was the Model of Harmful Hacking and Defense (see Figure 3, page 5), which suggests the kinds of countermeasures that can address attacks and improve security.

Based on the above analysis, another six recommendations were developed to provide additional guidance that compliments the first set of recommendations by emphasizing specific critical areas requiring special attention:

- **Recommendation No. 5** *Separate Critical Humanitarian Assets*
This recommendation calls for qualified humanitarian entities to articulate their interests and to seek separation of their assets in cyberspace.
- **Recommendation No. 6** *De-Clutter Espionage Expectations*
This recommendation acknowledges the expectation that national security-oriented assets, because of their potential for hostility, are elevated as targets for espionage by foreign interests. This factor suggests a differentiation between incidents experienced by national security interests and other entities.
- **Recommendation No. 7** *Summon a Roundtable of Subject Matter Experts*
This recommendation calls on world-class subject matter experts from both countries to create a new mode of collaboration, and as a resource for objective analysis and assessment.
- **Recommendation No. 8** *Continuous Approach Status Indicator*
This recommendation calls for a provisional capability to monitor, assess and report on the status of each of these crucial components. It will provide a reliable, independent assessment of the health of the dialogue and cooperation.
- **Recommendation No. 9** *Prepare Sufficiently, React Quickly and Summarize Seriously.*
This recommendation calls for transformation of the harmful hacking responses from one that is primarily reactive to one that is pro-active, and includes setting goals that define sufficient preparation and response.

⁵ Rauscher, Karl Frederick, *Written Statement for the United States Congress House Committee on Foreign Affairs, Hearing on "Asia: The Cyber Security Battleground"*, 23 July 2013.

Defense	Phase	Preparation	Responding	Follow-up
	Task	Make policy to encourage good and punish bad actions; Deploy resources to build defense capability; Remove the possibility for abuse of internal resources and functions	Continuously remove resources that can be used by hackers; Monitor attacks and abnormal behaviors; Send warnings and alerts and stop the attacks quickly.	First, recover normal business operations; Investigate and punish the bad actors; Learn from each incident to improve preparation and response.



Hacking	Task	Make the [im]moral choice to hack; Prepare the attack techniques; Evaluate benefits and risks.	Carry out the attacks to take down the target, steal data, commit fraud, etc.	Use multiple network and server hops; Erase hacking tracks.
	Phase	Preparation	Implementation	Escape

Figure 3. Model of Harmful Hacking and Defense.

■ **Recommendation No. 10 Launch Parallel Bilateral Collaboration on Government and Industry Levels**

This recommendation calls for industry level collaboration to supplement the new cooperation undertaken at the governmental level. Industry technical expertise and business insights are required to combat the harmful hacking that is out of control.

This report also presents voluntary Best Practices, which provide complimentary support to the Recommendations (Section 5). The Best Practices development was informed by the Eight Ingredient Framework and intrinsic vulnerability analysis (Section 2.5.2) and the Lifecycle of a Hack (Section 2.5.3). Best Practice examples include the following:

This bilateral report can be summarized statistically as follows:

1	Common purpose to reverse the hacking that is harming our countries
2	The number in a series of bilateral reports ⁶
10	Recommendations
>50	Key Observations from analyses
>50	Voluntary Best Practices
>150	Contributing subject matter experts and stakeholders
>2,000	Years of combined experience of contributing experts and stakeholders
>100,000	Analysis points with determinations made

⁶ Rauscher, Karl Frederick, Zhou, Yonglin, *China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust*, EastWest Institute and Internet Society of China: 2011.

This report is *not* a typical policy paper, nor are its ideas ‘in the sky’. Rather, it is a document that includes the practical, ‘down to earth’ guidance essential for solving the harmful hacking problem. The character of this report may be more likened to that of a musical score for a symphony orchestra, where distinct contributions are called for from a diverse range of talents; if each performs in harmony with the other, the results are awesome. Those who care about the cyber relationship, and those who care about the security and prosperity of the cyber space, are encouraged to read and reference this report.

Note from the Authors

We are deeply appreciative of the many subject matter experts who have contributed to this report. Please see their names in the full report, to be published at www.isc.org.cn & www.ewi.info.

World
**Cyberspace
Cooperation
Summit IV**

**SILICON
VALLEY
2013**

cybersummit.info
#cybersummit2013

"This report indicates that China and the U.S. can make joint efforts for a safe and secure cyber space. I support concrete actions like this."

蔡名照
CAI Mingzhao

"While the U.S and China may approach cyberspace from different political and cultural vantage points, both nations have a fundamental stake in an Internet that is secure and trustworthy. This report frames a way forward that builds trust in a deliberate and verifiable manner."

Michael Chertoff