



CHINA-U.S. BILATERAL ON CYBERSECURITY

# FIGHTING SPAM TO BUILD TRUST



**EASTWEST INSTITUTE**  
*Forging Collective Action for a Safer and Better World*



**中国互联网协会**  
Internet Society of China

The China-U.S. Bilateral Against Spam Report, Issue 1

Copyright © 2011 EastWest Institute and the Internet Society of China

This document was prepared by principal authors:

Karl Frederick Rauscher  
Chief Technology Officer & Distinguished Fellow, EastWest Institute  
&  
ZHOU Yonglin  
Director, Network and Information Security Committee, Internet Society of China

Cover photo: Dragan Stojanovski

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused solely on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, and Moscow.

For more information about EWI or this paper, please contact:

The EastWest Institute  
11 East 26th Street, 20th Floor  
New York, NY 10010 U.S.A.

+1 212 824 4100

[communications@ewi.info](mailto:communications@ewi.info)

The Internet Society of China was inaugurated in 2001 with a main mission to promote the development of the Internet in China and make efforts to construct an advanced information society. ISC is expected to be a link among the community, to make efforts benefiting the whole industry, to protect Internet user's interests, to push forward industry self-discipline, to strengthen communication and cooperation between its members, to assist and provide support for policy making, and to promote Internet application and public awareness.

For more information about the ISC, please contact:

Tower A East, Tianyin Plaza  
No.2-B South Fuxingmen Ave  
Beijing, China 100031

+ 86 10 66035712

[isc@isc.org.cn](mailto:isc@isc.org.cn)

CHINA-U.S. BILATERAL ON CYBERSECURITY

# FIGHTING SPAM TO BUILD TRUST

BY KARL FREDERICK RAUSCHER & ZHOU YONGLIN

June 2011



## 献词

这份报告献给：

所有默默耕耘的网络创造者和运行工程师，

他们提供了我们今日如此依赖的可靠的信息服务。

如果没有他们努力防止垃圾邮件，电子信息服务将无法生存。

## DEDICATION

This report is dedicated to:

The unsung network creators and operations engineers

who provide the reliable messaging services we so depend on today.

Without their spam fighting efforts, electronic messaging services would not be viable.

## Foreword

The meeting of our two presidents in January 2011 demonstrated an ongoing mutual commitment to “a positive, cooperative, and comprehensive U.S.-China relationship for the 21st century, which serves the interests of the American and Chinese peoples and of the global community,” as the U.S.-China joint statement emanating from the meetings put it. The statement went on to proclaim a mutual agreement to “advance cooperation to ... address cyber-security.”

*Fighting Spam to Build Trust* is a perfect example of how this vision can be realized. This timely Track 2 bilateral initiative delivers specific and actionable recommendations that, if implemented, will have immediate benefits not only for America and China, but also for the rest of the online world. This work reflects a keen awareness of the structure needed for effective solutions. Implementing the guidance provided herein will require properly balancing industry leadership as it partners with government to reduce the pollution in cyberspace.

Spam is a persistent nuisance with a vastly underappreciated economic impact and far-reaching consequences. Since it is often the vehicle for malicious code and online fraud, it is a perilous threat to every one of the billions of computers and netizens in cyberspace. For that reason, it is an area of highly correlated common interest, which accounts for the cautious cooperation described in this report.

The road ahead for cyberspace cooperation is strewn with hurdles, but let us take time together to pause, appreciate and applaud this world-class team’s successful clearing of the first hurdle.



**HUANG Chengqing**  
Vice President  
Internet Society of China



**John Edwin Mroz**  
Founder, President and  
Chief Executive Officer,  
EastWest Institute



## Preface

*If you are holding this report in your hands or viewing it on your computer screen, you have come upon something unusual. In a time when heated verbal and written exchanges between our two countries are the norm for most topics related to cyberspace, the tone of this report is an exception. In a time of escalating mistrust, this report reflects some measure of cooperation, teamwork and a commitment to a shared goal. In a time when most can only see a grim, downward spiral of recrimination when it comes to all things cyber, this report is the product of cooperation and offers some hope for an improved relationship between China and the U.S.*

*Neither of us, nor any of our team members, is naive concerning the existing concerns that our two countries have about each other in cyberspace. Both of us recognize that the Internet is an evolving vehicle that has brought – and continues to bring – great benefit for the development of China, the U.S. and the world. It also brings with it many new societal challenges. In this first engagement, we managed to achieve trust and cooperate on a common, concrete problem.*

*Both of us want to thank the subject matter experts, whose names are listed on the next page. These individuals devoted significant time and expertise to this process, and this important step toward international cooperation in cyberspace would not have been possible without them.*



**KARL FREDERICK RAUSCHER**

Leader, U.S. Experts Group  
Chief Technology Officer  
& Distinguished Fellow  
EastWest Institute

Bell Labs Fellow  
New York City



**ZHOU YONGLIN**

Leader, China Experts Group  
Director  
Network & Information Security Committee  
Internet Society of China

Head, CNERT/CC Operations Department  
Beijing



Rauscher and Yonglin at  
EWI Worldwide Security Conference  
Brussels, February 2010

## **Contributors**

### **People's Republic of China**

CHANG Fugang, HiChina  
HAN Song, HiChina  
HU Anting, Internet Society of China  
JIN Xuan, Tencent  
LI Hong, Internet Society of China  
LI Hongyu, 263  
LIANG You, China Unicom  
LIN Jin, Tencent  
LIU Deliang, Asia-Pacific Institute for Cyberlaw Studies  
MA Xiaowen, HiChina  
SU Zhisheng, China Telecom  
TIAN Fei, 263  
WANG Mingda, Netease  
WANG Shuo, Internet Society of China  
XU Yuan, Internet Society China  
ZENG Mingfa, Internet Society of China  
ZHANG Lu, Sina  
ZHAO Liang, NSFfocus  
ZHU Yunqian, Internet Society of China

### **United States of America**

Jeff Ames, Switch NAP (ret.)  
Monica Chew, Google  
Gib Godwin, Northrop Grumman  
Stuart Goldman, Bell Labs Fellow (ret.)  
Ramses Martinez, VeriSign  
Patrick McDaniel, Pennsylvania State University  
Jack Oslund, George Washington University (ret.)  
Dominic Ruffolo, Comcast Cable  
Greg Shannon, CERT at CMU Software Engineering Institute  
Fred Stringer, AT&T  
Jody Westby, Global Cyber Risk  
Weider Yu, Professor, San Jose State University  
Jason Zabek, Cox Communications



## Acknowledgements

Special recognition and sincere appreciation is here expressed

to the Institute's financial contributors  
*whose devotion to making the world a safer and better place makes this work possible.*

**C.H. Tung and Joel Cowan,**  
*for their personal interest and invaluable insights into the Sino-American relationship.*

to **Anneleen Roggeman,**  
*for her dedication and project management support throughout the process.*

to **Michael O'Reirdan, Jerry Upton and Linda Marcus,**  
*for their contributions in the planning of worldwide outreach for the recommendations herein.*

to **XU Yuan, Andrew Nagorski, Abigail Rabinowitz and Dragan Stojanovski,**  
*for their quality control of this publication and for leading the communications processes.*

to **Greg Austin, Terry Morgan and Vartan Sarkissian,**  
*for their continuous support and encouragement of the China-U.S. bilateral program.*

to **ZHAO Liang (Richard),**  
*for his special role in helping out when needs arose and his support for the outreach phase.*

to **Piin Fen-Kok, David Firestein, Alison Kung and Euhwa Tran,**  
*for their experience, insights and dedication regarding the China-U.S. relationship.*

to **CAI Mingzhao, Qian Xiaoqian, HUANG Chengqing,, WEI Zhengxin, LIU Zhengrong,**  
**James L. Jones and John Edwin Mroz,**  
*for their vision that opened the door for this opportunity.*

and finally, to our wider community of respective stakeholder confidants in Beijing and Washington, D.C.  
*whose appreciation for Track 2 innovation confirms the value of accomplishments like this.*

# Contents

DEDICATION.....	4
FOREWORD.....	5
PREFACE.....	7
CONTRIBUTORS .....	8
ACKNOWLEDGEMENTS .....	9
CONTENTS .....	10
1. EXECUTIVE SUMMARY .....	12
2. INTRODUCTION .....	18
2.1 BACKGROUND .....	18
2.2 IMPORTANCE.....	19
2.3 OBJECTIVES.....	19
2.4 SCOPE.....	20
2.5 HISTORY AND GROWTH OF SPAM .....	22
2.6 THE IMPACT OF SPAM .....	23
2.7 OBSTACLES TO REDUCING SPAM .....	24
2.8 EXPECTATIONS FOR REDUCING SPAM .....	25
2.9 APPROACH.....	26
<i>Eight-Step Process</i> .....	26
<i>Methodologies</i> .....	26
2.10 PRINCIPLES .....	29
3. DEEPER UNDERSTANDING .....	30
3.1 INSIGHTS GLEANED BY U.S. EXPERTS ABOUT THE U.S. ....	30
3.2 INSIGHTS GLEANED BY U.S. EXPERTS ABOUT CHINA.....	31
3.3 INSIGHTS GLEANED BY CHINESE EXPERTS ABOUT CHINA .....	33
3.4 INSIGHTS GLEANED BY CHINESE EXPERTS ABOUT THE U.S. ....	34
4. JOINT RECOMMENDATIONS.....	36
4.1 IMPROVED INDUSTRY COOPERATION.....	37
4.2 VOLUNTARY IMPLEMENTATION OF EXPERT BEST PRACTICES .....	40
4.3 THE CONSENSUS BEST PRACTICES.....	42
<i>Reducing the Motivation</i> .....	46
<i>Reducing Volume</i> .....	47
<i>Detecting Transmission</i> .....	49
<i>Sharing Data</i> .....	50
<i>Filtering Messages</i> .....	53
<i>Reporting Abuse</i> .....	54
5. CONCLUSION.....	56
BIOGRAPHIES.....	57
ACRONYMS .....	64
REFERENCES.....	67
APPENDIX A. U.S.-CHINA JOINT STATEMENT, 19 JANUARY 2011.....	69
APPENDIX B. SAMPLE ISP LETTER TO CUSTOMERS .....	75

## **List of Figures**

Figure 1. Shannon’s Schematic Diagram of a General Communications System.....	27
Figure 2. The 8i Framework of ICT Infrastructure .....	27
Figure 3. Fighting Spam Parameter Adjustment Analysis Summary .....	28
Figure 4. An International Quality Management Framework for Spam.....	42
Figure 5. Presentation of China-US Consensus Best practices .....	43

## **List of Tables**

Table 1. Summary Statistics.....	17
Table 2. Top Spamming Sources [Countries / Regions].....	22
Table 3. Consensus Best Practices with Implementation Responsibilities.....	45

## 1. Executive Summary

Early in 2011, U.S. President Barack Obama and President Hu Jintao of the People's Republic of China committed to improving the U.S.-China bilateral relationship. In a joint statement, they specifically agreed to “advance cooperation to ... address cybersecurity.”<sup>1</sup> In anticipation of this commitment, over a year earlier the EastWest Institute and the Internet Society of China convened a team of China-U.S. experts for an ongoing bilateral dialogue on cybersecurity issues. *Fighting Spam to Build Trust*, the team's first report, represents the first effort by Chinese and U.S. experts to work together on a major cyberspace challenge.

To be clear, spam is a huge problem. Cyberspace is polluted with junk mail. Several hundred billion spam messages are originated and transported across networks every day, and account for about 90% of all email messages. And there are much more serious problems with spam. Spam is often the carrier of malicious code, like viruses, and is also a vehicle for fraud. Spam funds much of the malicious behavior on the Internet, infecting hosts via web browsers and viruses, and is often used to set up botnets – a host of infected computers taken over by hackers and used to perform malicious tasks. Botnet operators make money by sending spam via black markets, and the proceeds fund identify theft and fraud.

Still, spam is largely underestimated as a problem, perhaps because it is not an attractive topic. Neither network operators nor service providers are eager to focus on spam in their interaction with their subscribers because it is mostly a negative story. While the network operators and Internet service providers have made tremendous strides in minimizing the amount of spam that subscribers actually see, these messages are still transported and processed in networks, inflicting costly damage in a variety of ways. These messages consume energy in data centers, compete for computer processor cycles, delay the transmission of important messages and elicit customer complaints. Indeed, spam is a cost driver and a hidden tax on the Internet for these reasons. Spam indirectly inhibits growth and innovation as resources are diverted to manage it.

Email is an indispensable instrument of the modern world – a primary tool of daily business. Yet electronic messaging as we know it would be utterly impractical if not for very advanced countermeasures and constant vigilance on the part of network operators, Internet service providers (ISPs), email service providers (ESPs) and security application developers. Without their efforts to fight abusive messaging, spam could easily comprise more than 99% of all email messages. The burden on users to sift through one hundred or one thousand messages to find a legitimate message would create an intolerable situation. Yet these unsung heroes are few and need assistance breaking through the current barriers that block their countermeasures. This report describes the way forward to

---

<sup>1</sup> U.S.-China Joint Statement, *Addressing Regional and Global Challenges*, White House, Office of the Press Secretary, 19 January 2011. *Addressing Regional and Global Challenges* Article 16. This statement is provided in Appendix A. [www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement](http://www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement)

remove some of the most previously insurmountable barriers – those that block international cooperation.

The three foremost objectives of this initiative were to (1) open *genuine dialogue* between China and the U.S. on cybersecurity (2) acquire a *deeper understanding* of both countries' cybersecurity environment, and (3) provide *consensus guidance* for reducing spam both between and beyond the two countries. Each of these objectives has been achieved.

### **Genuine Dialogue**

34 subject matter experts formed the combined team that produced this report. Conversations were held over the course of 50 meetings, which took place in China, the United States and neutral sites. The interactions were in a wide variety of formats, including small and large group face-to-face discussions, live virtual meetings over the Internet, and extensive electronic correspondence. Throughout the process, team members had ample opportunity to engage their counterparts on both the general policy and technical aspects of the discussion.

### **Deeper Understanding**

The interaction of the joint team included consideration of well over 500 analysis points. These discussions covered a broad array of subjects, ranging from spammer motivations to ISP business models, social phenomenon to government interests, freedom of netizen expression to legal restrictions, failures of existing policies to world-class best practices, technical challenges to technology opportunities, local community outreach to international collaboration. The team considered practical next steps, as well as the theoretical limits asserted by the mathematical model of communications. Here are four examples of how mutual understanding was deepened during the process:

#### *Insights Gleaned by U.S. Experts About China (Section 3.2)*

**2. Cultural Transformation.** The Internet is transforming societies all around the world. But the transformation in China is particularly dramatic. This is because there has not been such readily available technology, communications and international exposure before. In China, both the rate and scale of online growth are impressive. Recognizing the great advantages of convenience and low cost, a large number of netizens with enterprising interests have opened businesses on the Internet. Such a phenomenon was not only unknown to a previous generation, but also just a few years ago to the current generation. Because spam is such an inexpensive way to advertise, there is constant pressure to make use of it. This presents understandable challenges for China regarding Internet management.

**9. Key Role for Industry Leadership.** The fact that the Chinese experts did not advocate government intervention as the primary path to solving spam problems was a surprise to many of the U.S. experts. The mindset and approach of the Chinese team members was quite sophisticated in understanding the advantages of industry leadership in promoting some spam-fighting measures. Like their U.S. counterparts, they see the industry as sometimes faster than governments, which is important to keep in mind with fast developing technologies. However, they did express the concern that, without punitive measures, the voluntary measures of potential spammers may be ineffective. The relative immaturity of Chinese policies to fight spam has prompted Chinese experts

to be action-oriented in implementing industry solutions, while considering legislative policy options in parallel.

### *Insights Gleaned by Chinese Experts About the United States (Section 3.4)*

**8. U.S. Spam Legislation Not Getting Job Done.** The most visible policy approach to fighting spam in the U.S. is a legislative measure.<sup>2</sup> This gave the Chinese experts the view that Americans believed that government intervention would produce a unified response and punitive measures to stop spam. Although the anti-spam bill was not nearly as effective as hoped, the U.S. experts were less critical of it than they could have been. The Chinese experts thought it is indeed important to launch effective punitive measures by the government, but that industry is best positioned to find and implement real solutions.

**9. Less Knowledge about China Internet Industry.** The U.S. experts had relatively less knowledge about the Internet industry in China than the Chinese experts' had of the U.S. Internet industry. This is considered part of the reason that some anti-spam organizations based in the U.S. treat IP addresses in China with bias, without adequate transparency to Chinese practitioners.

The complete discussion of how the teams' mutual understanding deepened is provided in Section 3.

### **Joint Recommendations**

This report presents two recommendations that, if implemented, will reduce the spam originated by China, the U.S., and other countries. The recommendations are presented in Section 4, and summarized here:

#### **RECOMMENDATION 1.**

#### **Improved Industry Cooperation**

Spammers have exploited weaknesses in international coordination in order to make their identities more difficult to uncover, their spam messages more difficult to recognize and anti-spam countermeasures more difficult to apply. Thus, international cooperation on policy and tactics is crucial to effectively countering spam.

Both countries have recognized international collaboration on fighting spam as a priority for several years. A natural next step is for the U.S. and China to cooperate on fighting spam. The reasons for the current lack in cooperation include both simple and complex factors, from time zones and languages to the intricate interactions of network message analysis and handling (Section 4.1). Until these issues are addressed, spammers will

---

<sup>2</sup> Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 (15 U.S.C. 7701).

continue to be able to effectively exploit this environment. Therefore, the joint team recommends that:

**The Network Operators, Internet Service Providers and Email Service Providers of China and the United States, along with peers in other nation-states, should establish a forum where regular cooperation can be fostered with the aim of reducing spam in cyberspace.**

This recommendation presents immediately actionable guidance for addressing the current lack of cooperation between China and the U.S. on spam. Industry experts from both countries have already expressed interest in swiftly moving forward with this recommendation. To create such a forum, existing international forums in the United States and China should proactively contact each other, and their country's respective network operators and service providers. Specifically, these organizations should adjust their charters, expand their membership and plan their meeting locations to accommodate members from the other country.

*Required Commitments:* To effectively implement this recommendation, industry companies in both China and the U.S. must cooperate with each other, Chinese and U.S. government agencies must encourage cooperative efforts focused on the reduction of spam, and an international spam-fighting industry organization to engage both Chinese and U.S. experts must be established.

## **RECOMMENDATION 2.**

## **Voluntary Implementation of Expert Best Practices**

Existing spam-fighting best practices have been vital for the continued viability of electronic messaging. Best practices are also the hope for improvements in our current situation.

Best practices are best developed when experts come together and share insights. This can be done within a company or agency, across an industry or country, and among international parties. It is the last level that has not yet been fully developed.

International cooperation to develop best practices has been underway for several years. However, cooperation between the West and China and, more specifically, the U.S. and China, has been insufficient. This recommendation seeks to fill the void by pointing to the 46 Best Practices developed jointly by the China-U.S. team. If implemented, these best practices would help reduce the origination, propagation and unintentional opening of spam messages. Further, the dynamic nature of some of these practices would continue to be effective as spammers continuously adapt to defeat existing anti-spam countermeasures.

**The Email Service Provider, Internet Service Providers, Network Operators and Government Policy Makers of China and the United States, along with peers in other nation-states, should cooperate to develop, maintain, and**

**voluntarily implement consensus Best Practices as appropriate, with consideration of network configurations, business models and other feasibility factors.**

*Required Commitments:* To effectively implement this recommendation, industry companies must implement best practices where appropriate, and contribute expertise to best practice development collaboration. Chinese and U.S. government agencies must implement best practices where appropriate, and respect the need for industry expertise and experience to guide best practice development and application.

### **Consensus Best Practices**

The combined team developed and agreed on 46 Best Practices. Each of these best practices is intended to be voluntary, with the understanding that the intended parties will have the local knowledge and expertise to determine if their implementation is appropriate and feasible. Four examples are provided immediately below. The explanation for how to interpret the format is provided in Section 4.3. Each of these best practices is already in use, demonstrating their effectiveness and operational feasibility.<sup>3</sup>

**CN-US 11-007**

#### **Identification of Intense Messaging Business**

ISPs  
NZNs

Email Service Providers and Internet Service Providers should utilize acceptable use policies (AUPs) that require businesses that intentionally originate messages to register as such a user and clearly disclose their business category to recipients in their messages.

**CN-US 11-015**

#### **Sooner is Better**

NOS  
ISPs

Network Operators, Internet Service Providers and Email Service Providers should prioritize anti-spam strategies that detect and remove spam messages as early as possible in their intended transmission path. This reduces inefficiency and the cost of transporting such messages across the Internet.

**CN-US 11-023**

#### **Utilize FBL Mechanisms Across Borders**

NOS  
ISPs

Network Operators, Internet Service Providers and Email Service Providers should make use of available Feedback Loop (FBL) mechanisms with the countries with which they interface in order to increase the information available to them to manage spam.

<sup>3</sup> See *Best Practice Principles* of Section 4.3.



GPMs  
NOs  
ISPs


 Government Policy Makers and the Industry should consider voluntary agreements across nation-state borders that would be beneficial in reducing spam (e.g., closing down sources).

Table 1 summarizes the China-U.S. *Fighting Spam to Build Trust* effort in seven numbers. The first and last speak to the importance of this subject matter, and the five in between demonstrate that the objectives of dialogue, understanding and consensus guidance were achieved.

**Table 1. Summary Statistics**

<b>2</b>	<b>Cyber superpowers</b>
<b>2</b>	<b>Joint recommendations</b>
<b>29</b>	<b>Facets of Deeper Understanding</b>
<b>32</b>	<b>Subject matter experts engaged</b>
<b>46</b>	<b>Consensus Best Practices</b>
<b>500+</b>	<b>Parameter evaluations considered</b>
<b>X00,000,000,000</b>	<b>Spam messages filtered every day</b>

### **Next Steps**

The suggested next steps for each recommendation are specified in detail later in the report (Section 4, “Next Steps” heading). At the time of this report’s publication, the team members are encouraged by the new opportunities for future collaboration defined by these recommendations.

Next steps also include engaging relevant parties and organizations in these discussions. At the program level, the EastWest Institute’s priorities include continuing to serve as a strategic convener for China-U.S. trust-building in cybersecurity. In addition, the institute’s priorities include its Worldwide Cybersecurity Initiative (WCI), in which it partners with the world’s leading thinkers, companies, non-government organizations (NGOs) and the Cyber40 governments in fashioning breakthroughs for international agreements, standards, policies and regulations (ASPR).

## 2. Introduction

This section provides background on the initiative, reviewing the importance of the undertaking, outlining its objectives, defining its scope, and describing its approach.

### 2.1 Background

Throughout 2008, senior government and industry stakeholders engaged with the EastWest Institute expressed their grave concerns about our increasing exposure to and reliance upon cyberspace. Top military leaders equated the new dangers posed by this realm to the threat posed by nuclear weapons. Top political leaders spoke of the uncertainty introduced by all things cyber. Both pointedly observed that international policy will play a vital role in the future of securing cyberspace. After careful review of the challenge in light of the institute's mission, EWI's international board of directors put in motion the EWI Worldwide Cybersecurity Initiative (WCI).

The WCI's structure and priorities emerged in the year that followed.<sup>4</sup> The WCI placed a high priority on the relationships among the five most influential cyber powers, namely China, the European Union (EU), India, Russia and the United States.<sup>5</sup> The WCI leaders drafted a broad framework that encompassed a range of subjects, with significance attributed to public safety, economic stability and national security. On one end of the framework's spectrum were strategic trust-building measures and on the other, advanced cyber conflict policies. In between lay areas such as critical infrastructure protection and economic stability. With this frame of reference, the institute began to facilitate Track 2 bilateral processes.

The most immediate focus was the China-U.S. relationship. After consultation with the appropriate stakeholders in both governments, EWI launched a cooperative dialogue on cybersecurity. The Internet Society of China (ISC) was designated as the counterpart for EWI for the initial cooperation.

This bilateral process partially fulfills objectives set out in policy statements by China and the United States. In the Chinese government's 2010 publication, *China and the Internet*<sup>6</sup>, the sixth principle, "Active International Exchanges and Cooperation," underscores China's active promotion of "bilateral dialogue" on topics related to the Internet. Participants in this process can attest to the support and commitment made by the Chinese government, companies and experts to support this effort. For the United States, the *2009 White House Cyberspace Policy Review* made international cooperation the seventh priority of a "Near Term Action Plan." Specifically, the objective calls for Americans to "strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity."<sup>7</sup>

This importance of this bilateral process is underscored by the January 2011 meetings between U.S. President Barack Obama and Chinese President Hu Jintao. In a joint statement, the

---

<sup>4</sup> The initiative commenced with an April 2009 meeting hosted at the U.S. Federal Reserve Board, in Washington, D.C.

<sup>5</sup> The "Cyber5"; The WCI has also formed the Cyber40, consisting of the G20 plus net most critical countries influencing cyberspace.

<sup>6</sup> *The Internet in China*, Information Office of the State Council of the People's Republic of China, June, 2010, Beijing, p. 28.

<sup>7</sup> *White House Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Table 1: Near Term Action Plan, Washington, D.C., 2009, p. vi.

presidents made a mutual commitment to “a positive, cooperative, and comprehensive U.S.-China relationship for the 21st century.” And they specifically called for both countries to “advance cooperation to ... address cyber-security.”<sup>8</sup>

*Fighting Spam to Build Trust* was conceived as a careful step forward for the bilateral relationship, which is undeniably complicated. On the one hand, China and the U.S. are profoundly interdependent, sharing economic and other ties. On the other hand, they often view each other as competitors and potential adversaries, particularly in cyberspace. The team who wrote this report did so with the hope that competition in cyberspace can be replaced by collaboration.

The choice of spam for a topic was not arbitrary. As *Fighting Spam to Build Trust* reveals, spam is a big problem that is too often neglected. The jointly developed guidance presented in this report, if implemented, will have significant impact on making cyberspace more efficient and more secure.

The team views collaboration on reducing spam as a first step for Chinese-U.S. collaboration on cybersecurity and plans to consider increasingly significant subjects in subsequent reports.

## 2.2 Importance

This China-U.S. Track 2 bilateral on *Fighting Spam to Build Trust* is significant for five reasons. First, it is engaging the world’s **two cyber superpowers** on the crucial subject of cybersecurity. Second, it addresses a **big, underreported and underappreciated problem** in cyberspace.<sup>9</sup> Third, it has accomplished **breakthroughs in cooperation** between these two countries in a landscape of considerable mutual distrust. Fourth, the progress **reveals new potential** for future cooperation in the cybersecurity arena. Finally, the report illustrates the unique and essential **effectiveness of industry-led initiative**.<sup>10</sup>

## 2.3 Objectives

Three objectives were set for this bilateral engagement. The first objective was to **open genuine dialogue** between subject matter experts, business and other stakeholders from China and the U.S. The team was successful at this first step, as demonstrated by in-person meetings and web conference meetings that added up to hundreds of person-hours in interactive dialogue.<sup>11</sup>

The second objective, building on the first, was to **develop a deeper understanding** of each other’s perspectives. The team was successful with this objective, as demonstrated by the fact that team members gained an advanced understanding of each other’s views. This was accomplished in part by the systematic review of over one hundred possible parameters that could influence spam. For each parameter, both sides shared their views of its theoretical, effectiveness, desirability and practical considerations of possible adjustments. Team members

---

<sup>8</sup> U.S.-China Joint Statement.

<sup>9</sup> Network operators and ISPs are certainly aware of the spam problem. However, because of the improvements they have made in dealing with the issue, we now have a situation where the general public is not aware of the amount of spam that is filtered.

<sup>10</sup> The Institute has introduced *Private*-Public Partnership (PPP), as opposed to Public-Private Partnership (PPP), which assumes a government leadership role.

<sup>11</sup> Meeting locations between China and U.S. team members included Beijing, Brussels, Dallas, the Lehigh Valley, New York City and Orlando.

had the opportunity to discuss each of these possible parameter adjustments with their counterparts and to understand why a net assessment of benefit or harm was rendered.<sup>12</sup>

Given the current state of China-U.S. relations when it comes to cybersecurity, both sides recognized that success with the first two objectives alone represented substantial progress. Still, the team included a third objective, built on the previous two: to **come to agreements** on international policy for reducing spam in cyberspace. “Section 3, Joint Recommendations,” provides guidance along these lines in the form of two joint recommendations and 46 voluntary best practices.

## 2.4 Scope

There are four parameters that best define the boundaries of this initiative. These are i) the parties involved, ii) the definition of spam, iii) the spam reduction efforts, and iv) trust-building. The first two are presented in this section. The third and fourth are described in Sections 4 and 1, respectively.

### Parties Involved

This analysis was conducted by subject matter experts and other stakeholders from China and the U.S. All experts are citizens of their respective countries and have been engaged in some critical aspect of ICT related to the interests of network security, network operations, public safety or national security.<sup>13</sup>

As a Track 2 collaborative effort, these individuals were not official government authorities. However, the leaders of both expert groups provided periodic briefings to their respective stakeholders in Beijing and Washington, D.C. The collective experience of these experts adds up to over five hundred years and includes the broad range of expertise needed for an examination of the subject matter. Many of the individuals involved were responsible for network security and countering messaging abuse for the largest ISPs in the United States and China.

As the final step of the process is to conduct outreach, additional parties engaged at the final stage have included, and will continue to include, network security specialists and other stakeholders.

### Definition of Spam

After considerable discussion and analysis of existing definitions, the team agreed that there are four essential attributes of a message that define spam.<sup>14</sup> When all the attributes are present, the message is spam. When any one of them is missing, it is not spam. These four attributes are:<sup>15</sup>

- being **uninvited** by the recipient<sup>16</sup>
- being **high in volume**<sup>17</sup>

---

<sup>12</sup> See Section 2.9, Approach, for more details.

<sup>13</sup> Additional background for each team member is provided in the biography section.

<sup>14</sup> Email spam is often referred to as “junk email.” A common synonym is unsolicited bulk email (UBE). The team is aware of other definitions of spam. As the term itself, like many in the cyber world, is not semantically derived, it is understandable why different definitions are offered. The attributes here embraced are arrived at based on both careful analysis of existing definitions and consideration of the optimum utilitarian function of the word given the problems it represents.

<sup>15</sup> Some published definitions assume the form is electronic. Others neglect to specify being wide in distribution, perhaps assuming that the high-volume (or “bulk”) nature accounts for this. However, many messages sent to the same person would be a form of annoyance, but not spam.

<sup>16</sup> Optional terms here include unwanted and unsolicited.

<sup>17</sup> i.e. a single unwanted message to a few people is **not** spam

- being **distributed widely**<sup>18</sup>
- being an **electronic message in any form**

Forms of electronic messaging include email, instant messaging, web search engine, fax, Internet site postings, mobile texting, SMS and tweeting as well as others.

While other forms of spam are evolving and growing more problematic, most spam is currently in the form of email. Extensive experience with email spam allows us to provide additional insights for this type of spam. First, the source of spam messages is often hidden. The message header information is often falsified so that the sender's identity or the email transmission route cannot be confirmed. The problem of spam is exacerbated by the use of botnets, which send messages from an infected computer without the system or device owner's authorization.<sup>19</sup> Spam message senders are often motivated by one of four primary ambitions: (i) commercial gain, via advertising, e-publications, and other promotional material, (ii) to commit crime, such as deliberate fraud, theft and other illegal activities,<sup>20</sup> (iii) to cause harm by spreading malware, or launching attacks towards communications network or computer systems (iv) circulation, that is, disseminating information that might otherwise be more difficult to spread such as pornography, unwanted advertisements, ideological promotion, terrorism propaganda and ethnic discrimination. This description provides better understanding of the intent and objectives of those responsible for sending spam. Such insights are helpful when considering possible countermeasures.

In addition to email, other spam includes unwanted, high-volume, widely distributed messages in the form of Short Message Service (SMS) messages, SPIT (Spam over Internet Telephony), web site postings and faxes.

The mobile world is experiencing a dramatic increase in types of malware. Types of malware can include secretly charging unsuspecting people by subscribing them to an unwanted service, or sending SMS or Multimedia Message Service (MMS), remote control through the Internet, privacy theft, corruption of data and fraud. Mobile phone malware even has more propagation channels than personal computers. These include connectivity to the Internet and transfer application software from PCs, MMS, Bluetooth and memory cards. Mobile services seem to be experiencing more spam in China than in the U.S. This may be related to the relatively higher utilization and lower cost of SMS and MMS in China: sending an SMS message costs ten cents in U.S., which is about six times the cost in China. Such a cost is an impediment to sending bulk messages.

There are reasonable expectations that subscriber mobile devices will be overtaken in a similar way, as botnets themselves are becoming a source of spam messages in the U.S. Actually, this has already happened in China. Recent developments suggest that such compromises are beginning to appear "in the wild" in greater numbers and some experts predict a significant upsurge in such incidents will occur in the next two years.

---

<sup>18</sup> i.e. many unwanted emails sent to the same person is **not** spam

<sup>19</sup> Botnets are collections of software programs that run automatically and are often networked to work together over multiple computer systems.

<sup>20</sup> Illegal activity may be defined by the sending country, receiving country or any country in between.

## 2.5 History and Growth of Spam

The essence of “spam” is not new. Before the Internet, “junk mail” was a common problem – and still is. The motivation for using junk mail and spam is similar, in that these are the most economically attractive options for reaching many people with a message.

The first email spam is believed to have been a marketing message sent on May 3, 1978 to all of the users at that time who were on the Advanced Research Projects Agency Network (ARPANET).<sup>21</sup> The number of addresses was about 600. Since the turn of the century, the volume of spam has exploded. Current measurements put the number of spam messages originating *every day* in the order of magnitude of hundreds of billions (X00,000,000,000). Many estimates suggest that email messages make up as much as 85 or 90% of all emails. Some estimates are higher.

**Table 2. Top Spamming Sources [Countries / Regions]**

Source	A	B	C	D	E	Most Common Rank
Argentina	-	17	-	-	-	Below Top 10
<b>Brazil</b>	3	3	5	4	3	<b>Top 5</b>
China	-		-	-	10	Below Top 10
Columbia	7	12	-	16	-	Below Top 10
France	9	11	9	6	-	Top 10
Germany	-	5	-	3	6	<i>Data too variable</i>
<b>India</b>	1	1	2	2	2	<b>Top 5</b>
Italy	10	8	-	8	-	Top 10
Korea	4	10	8	9	9	Top 10
The Netherlands	-	18	3	13	-	Below Top 10
Poland	-	14	-	10	-	Below Top 10
Romania	8	13	-	11	-	Below Top 10
<b>Russia</b>	2	4	4	12	4	<b>Top 5</b>
Saudi Arabia	-	15	-	18	-	Below Top 10
Spain	9	16	-	14	-	Below Top 10
Taiwan	-	-	7	17	-	Below Top 10
Ukraine	-	9	-	15	7	<i>Data too variable</i>
United Kingdom	-	6	10	5	8	Top 10
<b>United States</b>	6	2	1	1	1	<b>Top 5</b>
Uruguay	-	-	6	-	-	Below Top 10
Vietnam	5	7	-	7	5	Top 10

An actual accurate count of spam emails is not possible. For this reason, spam estimates are made on an order of magnitude – e.g., as presented in Table 1. There are numerous sources that offer statistics on spam. However a simple comparison among these numbers shows inconsistencies. This is understandable because the methods of measuring spam are different.<sup>22</sup> Differences include the number and locations of deployed equipment, the decision made about what is actually considered a spam message and conclusions drawn about the actual source of the message. Even with this variation, there are still some consistencies that can be drawn from this

<sup>21</sup> Waters, Darren, *Spam Blights Email 15 Years On*, BBC News, 31 March 2008.

<sup>22</sup> It is unfortunate that coverage and other limitations are not forthcoming with the provide statistics, as this would assist in the compilation of the available statistics in the aggregate.

analysis. For example, Table 2 below provides a summary of spam statistics from five industry sources.

A worthy observation of the data in the above table is that, all other conditions being equal, larger countries will tend to be proportionally larger contributors of spam. For the most part this holds true. However, the striking exception is China. With the world's largest online population, it has a disproportionately low contribution to sending spam outside its borders.<sup>23 24</sup>

## 2.6 The Impact of Spam

Spam is a global problem, as it pollutes our shared cyberspace with quadrillions of junk bits each day.<sup>25</sup> The impacts of spam are nontrivial and can be observed in terms of security, social well-being, economics, environment, performance, enablement and quality of experience.

A recipient's *quality of experience* is degraded due to the diligence required in screening for spam and in the time required to manually evaluate and delete spam.<sup>26</sup> Further, a user's experience may be degraded in that some network or local filters will have "false positive" identification of non-spam, and thereby block good messages. Spam brings a bad experience to email users, as well as subscribers to other services like SMS.

Spam has also become an *enabler* in that it can serve as the vehicle for malicious code introduction or other crime such as phishing.<sup>27 28</sup> Spam often spreads malware and launches attacks towards computer and network security. Spam is also an enabler in another sense, in that it creates the revenue stream that funds other malicious activities.

Spam impedes network *performance* as it congests network resources, queues and processor time, thus causing delays of legitimate messages throughout cyberspace. Several studies suggest that spam makes up as much as 90% of all email traffic globally.<sup>29</sup>

The *environmental* impact of spam has been projected in terms of global annual energy consumption on the order of tens of terawatt hours.<sup>30</sup>

The *economic* impact of spam has been estimated as on the order of 10€ billion annually to users through connection fees.<sup>31</sup> In addition, network operators must incur the cost of transporting, filtering and managing these messages.<sup>32</sup> Both network operators and end users must bear the

---

<sup>23</sup> Reported as over 450 million as of the end of 2010. This is twice that of the U.S. China Internet Network Information Center (CNNIC), [www.cnnic.net.cn](http://www.cnnic.net.cn).

<sup>24</sup> With additional online users and online computers there is an assumed potential for additional abuse of messaging services. Factors that may contribute to China's spam environment include the natural language barrier and the existing government role in managing aspects of the Internet.

<sup>25</sup> Calculations based on survey of published estimates for average number of daily emails (500 billion taken), percentage of email that is spam (85% taken), and average spam email size (5KB taken).

<sup>26</sup> The time required for an average recipient to determine that a message is spam and then delete it is estimated to be approximately 5 seconds. *Spam, time, and you: An educational video from Gmail*, 26 October 2007.

<sup>27</sup> Phishing is the illegal attempt to gain sensitive information (e.g., passwords, credit card numbers) through electronic messaging by deceptive means such as appearing to be a trustworthy entity.

<sup>28</sup> Per Symantec MessageLabs 3Q2009 Report, "1 in every 437 emails is a phishing attack"

<sup>29</sup> Symantec MessageLabs 3Q2009 Report. This same report calculated the US and Canadian spam level as over 91%.

<sup>30</sup> "... equivalent to the electricity used in 2.4 million homes, with the same [greenhouse gas] emissions as 3.1 million passenger cars using 2 billion gallons of gasoline." McAfee's Global Footprint of Spam, 2009.

<sup>31</sup> Commission of the European Communities *Unsolicited Commercial Communications and Data Protection* January 2001.

<sup>32</sup> There is a genuine point to be made that spam can have a positive economic benefit in enabling start-ups to establish momentum and for generating sales of advertised items. However, this is a costly trade-off, given the inefficiencies introduced.

cost of storing these messages in mailboxes. From a business standpoint, spam harms the ESP, ISP or Internet Content Provider (ICP)'s reputation for competence. Spam can be thought of as "an economic black hole" for the industry because it creates an imperative to build out networks to handle this traffic. Costs are therefore introduced by the need to build oversized networks, operate these networks, purchase and update hardware and software, pay technical staff, handle customer complaints, and cover many additional direct and indirect expenses.

The *social impact* of spam is felt in the unwelcome exposure of youth and others to objectionable content, such as pornography, terrorist propaganda and materials promoting ethnic discrimination. Unlike other media, spam does not require the sender's identity to be disclosed. Spam senders take advantage of the anonymity of the Internet, and this absence of accountability emboldens negative human behaviors. Many corporate policies against sexual harassment are routinely violated as sexually explicit language and images are regularly routed to employee inboxes.

Finally, the impact of spam on *security* spans electronic infrastructures at enterprise, network and nation-state levels, as critical operational systems can be impaired as they strain under the presented workload or become exposed to malicious code threats.

## **2.7 Obstacles to Reducing Spam**

Ridding cyberspace of spam would yield enormous benefits. However, there are formidable reasons why the spam problem has not yet been solved.

First, *spam works* for many businesses. It is simply the most economically efficient way of reaching many people. For a very low cost, a very large number of messages can be sent, so that even with a very low hit rate, the return on investment (ROI) can be attractive.<sup>33</sup> Another factor is the uncertainty surrounding the *legitimacy of advertising*, with varying degrees of legality for commercial electronic messaging found in different countries.<sup>34</sup> It is more acceptable in some countries than others to do whatever you can to deliver messages to potential customers.

While not as central, it's also important to consider the business motivation of the providers who sell services to spammers. These service providers make revenue from their business relationships with spammers. If a user's traffic volume does not violate the provider's acceptable use policy (AUP), then it is likely that the provider has a net financial benefit from the relationship. Like any business, service providers want to keep their customers. However, recent trends suggest that they are less willing to accommodate spammers.

Second, *spam works* for disseminating messages to large numbers of people.<sup>35</sup> Even for non-businesses, it is the most economically efficient way of reaching many people. Political, philosophical or other advocacy messages can be widely distributed instantly, and often from the cover of a far away location and disguised identity.

Third, *spam thrives* by exploiting the technical environment. There are four attributes of spam that make for its potency. Spam is:

---

<sup>33</sup> Most spam is generated automatically by groups of connected "software robots" or botnets.

<sup>34</sup> A difficult special case is where broadcasting wide distribution electronic messages may be an illegal practice in some jurisdictions, but the messages being sent may have a humanitarian interest (i.e. are not economically motivated).

<sup>35</sup> The Best Practices presented in Section 4.3 have a significant impact in reducing this effectiveness.



- ***Potentially viral***, as there is little impedance to proliferation;<sup>36</sup>
- ***Untraceable***, as it is very difficult to identify the true originator;
- ***Automated***, as computers can be controlled without their owners' authorization;
- ***Mutable***, and preventative measures against spam are primarily reactive.

Fourth, *spam takes advantage* of legal shortfalls including the un-harmonized international legal framework, lack of an attribution scheme for global networks and limited international cooperation. Spammers exploit the lack of cooperation across international borders, targeting foreign fields to avoid prosecution from governments at either network end.

Fifth, the problem of spam remains unsolved because of *asymmetry*. That is, spam is possible because the cost on the sender is very small and the cost on the infrastructure and recipient is much higher. This is known as a resource asymmetry and is at the root of all scalable denial or degradation of service attacks. Our inability to alter that imbalance is one of the main challenges posed by spam. Some have tried to address this (e.g., a minimum charge per email), but have met rejection by the market.

Sixth, *spam remains unresolved* because of several fundamental differences that stem from social values and politics priorities. These present serious policy challenges, and can only be resolved through both national and international cooperation. At the heart of such issues are questions like:

- *Should personal freedom enable us to send messages to other parts of the world where there are different laws?*
- *How is privacy to be protected when measures are being considered that can monitor netizens' use of the Internet, such as messaging?*
- *If something is annoying, is it wrong?*

At a global level, there is disagreement or moral ambiguity on these and related issues.

## **2.8 Expectations for Reducing Spam**

Given the reasonable use of electronic messaging for commercial interests, ridding cyberspace of all high-volume, wide distribution messaging is not a goal of this effort. Indeed, there would be much resistance from legitimate business interests to doing so. Rather, the objective is to reduce messages that are illegal in the jurisdictions in which they originate or are delivered.

---

<sup>36</sup> Viral is a term created by new social media networking to describe something (e.g., website, video, message, application) that has spread to a huge number (millions) of users in a very short interval of time (e.g., a day). The term has transitioned from slang to commercial use where software that counts views of content is now called viral metrics or viral measurements.

## 2.9 Approach

### Eight-Step Process

A custom process was created to meet the needs of this special bilateral engagement. The process design was aligned with the objectives, scope, methodologies and principles outlined throughout this document. The process was developed using engineering problem-solving principles, the Eight Ingredient (8i) Framework and extensive international consensus development experience.<sup>37</sup>

As team members were aware of the pioneering nature of this endeavor, they gave great care to the accuracy of the communications that took place throughout the process. In addition, they gave considerable care to the certainty of the consensus as it was being established.

The team's final step is to advance from bilateral to a multilateral process. This will be accomplished via outreach, as team members elicit input from respective stakeholders. With joint planning, the team agreed on appropriate venues for presenting jointly developed recommendations.<sup>38</sup>

### Methodologies

The team used four methods to make the process of considering possible parameters rigorous. This rigor significantly increased the workload, but provided rich insights. These four distinct methods were:

- Business motivation analysis
- Study of the model of communications theory
- Application of the Eight Ingredient (8i) Framework
- Review of existing agreements, standards, policies and regulations (ASPR)

For the first, the team reviewed the current dominant commercial motivations for sending spam. They also discussed how spam has evolved and is likely to evolve. The underlying motivation factors were then considered in the development of countermeasures to fight spam.

The Mathematical Theory of Communication was consulted to ground the analysis in a trustworthy and fundamental model of the communications process.<sup>39</sup> This enhanced the analysis of the sequential progression of the spam message from source to target. Another useful benefit of this structure was that it offered a different take on the fact that spam messages are often cloaked with deception to disguise their source or their real intent. This is a noticeable abnormality in that, unlike a typical communication scenario in which noise reduction is optimized, here noise is intentionally introduced by the sender. This noise makes it harder for the communication system to properly understand and handle the message, and it makes it more difficult for the receiver to interpret the message accurately.

---

<sup>37</sup> Notable success was achieved with this approach as has been seen with the EC ARECI and IEEE ROGUCCI Reports. See [http://ec.europa.eu/information\\_society/policy/nis/docs/studies/areci\\_study/areci\\_report\\_fin.pdf](http://ec.europa.eu/information_society/policy/nis/docs/studies/areci_study/areci_report_fin.pdf) and [www.ieee-rogucci.org](http://www.ieee-rogucci.org).

<sup>38</sup> e.g., The Message Anti-Abuse Working Group, the EWI-IEEE Worldwide Cybersecurity Summit, etc.

<sup>39</sup> Shannon, Claude E., A Mathematical Theory of Communication, Bell System Technical Journal, 1948.

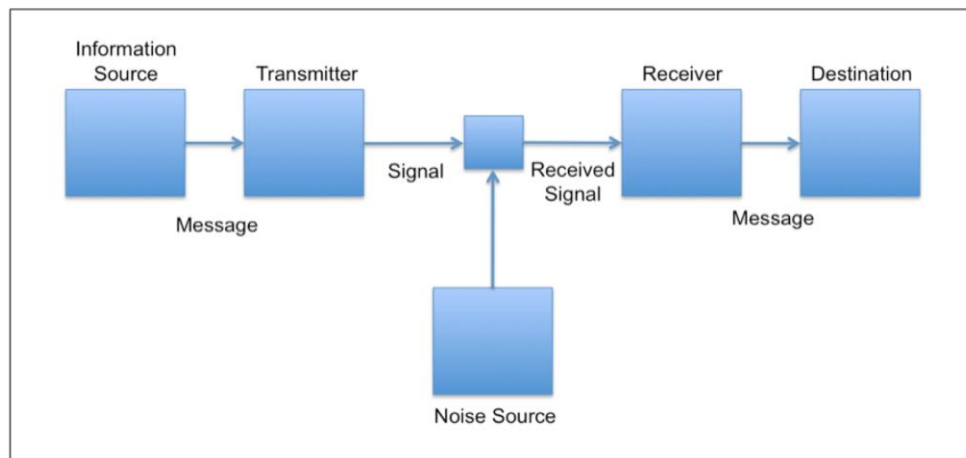


Figure 1. Shannon's Schematic Diagram of a General Communications System

The 8i Framework played a critical role in prompting the systematic analysis of the possible parameters that could be adjusted (Figure 2). As most of the parameters considered were identified by this method, it proved to be the most prolific source for the generated best practices.

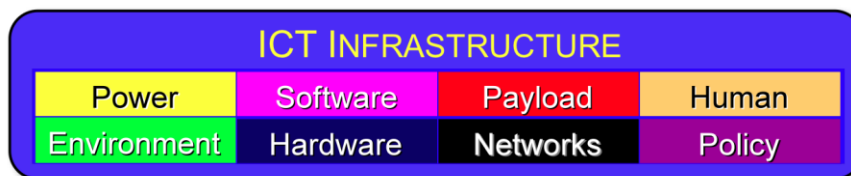


Figure 2. The 8i Framework of ICT Infrastructure<sup>40</sup>

A fourth method used to identify parameters that could be adjusted was a consideration of existing ASPR, including policies from China and the U.S., as well as other countries. In addition, the team reviewed the practices of the companies involved in the bilateral study. As a result of his analysis, the team identified existing best practices deemed useful by experts outside of the source country or company.

Figure 3 provides a summary of the assessments made by each country regarding the possible spam parameter adjustments. The original plan was for both groups to independently arrive at a single evaluation score for each parameter. However, both sides decided to make use of two

<sup>40</sup> ATIS Telecom Glossary; *Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop*, Rancho Bernardo; Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004; *The President's National Security Telecommunications Advisory Committee Next Generation Networks Task Force Report*, March 28, 2006, Background and Charge; ATIS Network Reliability Steering Committee (NRSC) 2002 Annual Report; Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003; NRIC VII Wireless Network Reliability Focus Group Final Report, Issue 3, October 2005; NRIC VII Public Data Network Reliability Focus Group Final Report, Issue 3, October 2005 ([www.nric.org](http://www.nric.org)).

parameters to enhance the ability to express analysis conclusions. The Chinese rated each parameter based on “in theory” and “in practice” considerations and used a scale that ranged from 0 (low) to 9 (high) to indicate relative correlation. Likewise, the Americans rated each parameter based on “desirability” and “effectiveness” and used a scale that ranged from 1 (low) to 10 (high). While the respective first terms are quite similar and likewise the latter, the team decided that leaving them as is was appropriate. Only those parameter adjustments that received a score above the midline for all four parameters were accepted as a consensus position of favorable and pursued.

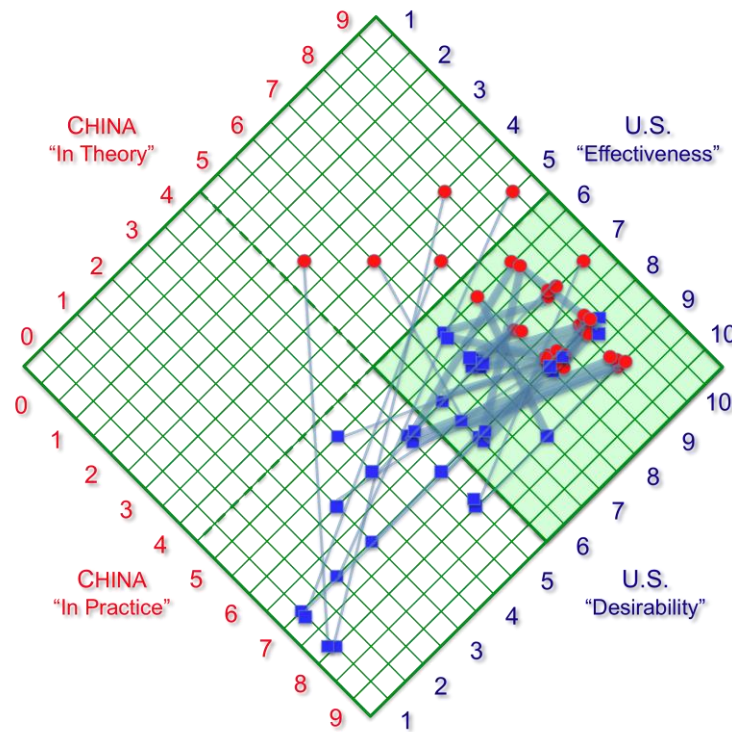


Figure 3. Fighting Spam Parameter Adjustment Analysis Summary

## **2.10 Principles**

### **One Team**

Unlike the Olympic Games, where the best Chinese and U.S. athletes compete against each other, participants of this bilateral initiative participated on one combined team against the common opponent of the spam in cyberspace. Participants included subject matter experts from equipment suppliers, infrastructure operators, network operators, ISPs, and ESPs, as well as researchers and other stakeholders. The expertise and experience of these individuals spanned science and engineering, business and law, and academia and the military. Team members demonstrated a commitment to the process, as was demonstrated by a degree of intellectual engagement, patience in seeking to understand each other, and genuine desire to achieve objectives for the mutual benefit of China and the U.S., as well as other countries.



### **Track 2**

This cooperative dialogue is led and supported by non-government organizations. Most experts are primarily affiliated with a company or academic institution. Both sides provided periodic briefings to their respective government stakeholders in Beijing and Washington, D.C.

### **Rigor**

While arriving at a level of consensus, the team interacted rigorously on various points throughout the process. Team members were even comfortable having this rigorous discussion among themselves when their foreign counterparts were present, observing disagreements and challenges. Participants saw this unfettered discussion as the best way to arrive at strong conclusions.

### 3. Deeper Understanding

The second primary objective of the bilateral engagement was to facilitate each party's understanding of the other. This section captures important insights that American and Chinese experts gleaned about the other country's respective challenges and priorities regarding spam.

Dialogue alone does not guarantee that participants grasp expressed ideas, intended messages and concerns. Rather, participants need to be diligent in clarifying statements and confirming the accuracy of perceptions. The team did this well. At times, the conversation may have seemed slow and overly cautious. However, the team did manage to cover a comprehensive array of parameters and angles regarding spam. The diligence and patience invested in this process yielded a tremendous reward. Both sides penetrated predominant superficial understandings to gain in-depth insights that will enable future cooperation.

#### ***3.1 Insights Gleaned by U.S. Experts About the U.S.***

The following are six key observations made by the U.S. experts about the spam situation in the United States:

1. **Statistics reveal ineffective policy to date:** U.S. policies intended to limit spam have been insufficiently effective per the statistical evidence.<sup>41</sup> The existing policies have neither sufficiently prevented the growth of spam in U.S. networks nor the U.S. contribution to spam in international cyberspace.<sup>42</sup>
2. **Reactive posture prevails:** There is a sense that spam-fighting is predominantly a game of catching up and reacting. Rather than anticipating where spam will show up next, we are too often reacting to it when it emerges in new contexts.<sup>43</sup> More proactive planning is needed.
3. **Relationship investment required:** U.S. network security engineers have *not* previously prioritized nurturing personal relationships with their Chinese counterparts. Such trusted relationships are a prerequisite for collaboration on fighting spam.<sup>44</sup> Trusted relationships exist along a spectrum, beginning with extremely cautious interactions.
4. **Consumers have varied experience regarding email spam:** The reasons are complex and stem primarily from the interaction of three factors: the complexity of the Internet, the business model implementation of the company managing the email account and the company messaging abuse practices. For example, popular free email services are designed to exploit the account holder's message content and sell advertisements. These services typically have no customer care support. On the other hand, network operators that provide email services for a revenue stream have both customer care concerns and an economic interest that complicates their practices. In fact, electronic message advertising is a business model for some of their users.

---

<sup>41</sup> Table 2.

<sup>42</sup> Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 (15 U.S.C. 7701).

<sup>43</sup> This is not only true in the U.S. but internationally.

<sup>44</sup> Rauscher, Karl, F., ARECI Report, European Commission, Brussels, 2007.

5. **Abuse of the economic landscape:** The hierarchy of the Internet played a key role in enabling it to grow and be cost-effective for everyone. However, the same hierarchy makes spam control complex and creates ineffective cost for use algorithms. The best control measures for spam tend to be at the sending source or at the target destination. However, network operators, who must bear the cost of carrying the messages, are only getting paid for carrying the bits.<sup>45 46</sup> This creates the situation where network operators are carrying bits with no connection to revenue, and yet can be asked by the destination to stop delivering messages that must be blocked.<sup>47</sup>
6. **Resigned to live with spam:** There are many highly skilled individuals and teams working on reducing spam and they are making continued progress in their efforts. Advanced technologies have been developed and introduced. On the other hand, spam seems to be something that many companies have accepted as a necessary annoyance and cost of doing business. There are currently no aggressive efforts that are likely to completely eliminate spam from cyberspace.

### ***3.2 Insights Gleaned by U.S. Experts About China***

This section details nine key observations that enabled the U.S. experts to better understand the Chinese business environment, their Chinese counterparts and their experience in fighting spam in China.

1. **The proportions of China present scalability challenges:** Well over one billion citizens, nearly one half billion netizens, and a steep growth rate of online accounts and company subscriber-bases in the hundred-million order of magnitude are profound statistics.<sup>48 49</sup> Chinese ISPs make even the largest U.S. companies reflect on whether their processes and practices could scale to such an “extreme” extent.
2. **Cultural transformation:** The Internet is transforming societies all around the world. But the transformation in China is even more dramatic. This is because China has never before had such readily available technology, communications and international exposure. In China, the rate of online growth and the scale are impressive. Knowing the great advantages of convenience and low cost, a great number of netizens with enterprising interests have opened business on the Internet. Such a phenomenon was unknown to not only the previous generation, but also to the current generation until just a few years ago. Because spam is such an inexpensive way to advertise, there is constant pressure to make use of it. This presents understandable challenges for China regarding Internet management.
3. **China is being a good neighbor when it comes to spam:** China is on a successful trajectory in its fight against spam. Spam statistics from both Chinese companies and independent sources confirm that the Chinese have made remarkable progress in reducing

---

<sup>45</sup> i.e. they do not inspect the message content.

<sup>46</sup> This is a fundamental difference with traditional postal email, where the sender bore the cost of postage.

<sup>47</sup> Again, this observation is applicably beyond the U.S.

<sup>48</sup> The population in China is over 1,338,000,000.

<sup>49</sup> Tencent and Netease each have over 300 million email users.

their outgoing spam to the rest of the world.<sup>50</sup> In particular, the level of spam being sent to the U.S. has decreased sequentially over each of the last three years.

4. **Sensitivity to content:** During the conversations about what makes up spam, the initial conversations included much discussion about the dangers of spam. The Chinese experts pointed out the harms of spam, including the idea that spam serves as a carrier for malicious code as well as content that may cause social instability, materials propagating ethnic discrimination, pornography and other illegal material.<sup>51</sup>
5. **Information sharing:** In order to describe the status of spam in China comprehensively, the Chinese experts shared statistical data with U.S. experts, which was important to making various points on spam trends. They offered the data willingly in a collegial spirit because it would help support the project.
6. **Focus on the practical.** The Chinese experts had a tendency to focus their attention on the hands-on aspects of the conversation. They had a higher interest in topics where implementation was tangible. There seemed to be a tendency to give a lower rating to ideas where the implementation was not already being practiced.<sup>52</sup> This pragmatic bent included a calculation of the efficiency associated with options discussed. However, the focus on the practical did not impede acceptance of more creative recommendations.
7. **Professional humility:** The Chinese experts seemed quite modest in their representation of their skills and knowledge. They were quite complimentary of the U.S. However, it was clear that they were very knowledgeable and experienced in operating networks, understanding business models and reducing spam.
8. **Asymmetric awareness:** The Chinese were more aware of U.S. companies than were the U.S. experts of the Chinese companies. This is likely because of the global presence of many U.S. companies (e.g., Google, Yahoo!, Microsoft, etc.).
9. **Key role for industry leadership:** Many of the U.S. experts were surprised that the Chinese experts did not advocate government intervention as the primary path to solving spam problems. The Chinese team members' mindset and approach was quite sophisticated when it came to understanding the advantages of industry leadership for some spam-fighting measures. Like their U.S. counterparts, they see industry as sometimes faster than the government, which is important to keep in mind with fast developing technologies. However, they did express concern that, without punitive measures, the voluntary measures of potential spammers may be ineffective.<sup>53</sup> The relative immaturity of Chinese policies to fight spam has encouraged the Chinese experts to be action-oriented in implementing industry solutions, while considering legislative policy options in parallel.<sup>54</sup>

---

<sup>50</sup> Table 2.

<sup>51</sup> Section 2.4 Scope.

<sup>52</sup> Figure 4 provides evidence for this observations. When an opportunity was rated low, for the Americans it tended to be for desirability reasons, whereas for the Chinese, it tended to be for practical reasons.

<sup>53</sup> The U.S. expert team notes that this observation is not limited to China, as it is in fact an element of discussions that applies to the U.S. and Europe.

<sup>54</sup> The Chinese team members referred to industry-led, or voluntary measures as "self-discipline."



### 3.3 Insights Gleaned by Chinese Experts About China

The following are five key observations made by the Chinese experts about the situation regarding spam in China:

1. **Spam is like a mouse on the street:** Everyone hates it. From the end user to the Internet operation level to the government level, everyone is clearly opposed to spam. End users hate spam because it can directly damage their computers. ISPs hate it because many IP addresses used to spread spam are thrown into blacklists and blocked. The government hates spam because of public press to strengthen anti-spam work.
2. **Lack of anti-spam legislation:** Besides the *Regulation on Internet Email Service Management*, there is no law on or regulation of spam. So far, the regulations mostly forbid ESPs' bad behaviors, rather than regulating the behavior of email users who might send out spam on purpose.
3. **Great achievements made by industry based on the principle of self-discipline:** Many countermeasures have been adopted by the industrial sector. Examples include fixing up default open relay email servers, training email server administrators, establishing reporting and handling mechanisms, publishing a spam blacklist and cleaning up zombie networks.<sup>55</sup>
4. **International cooperation and promotion should be enhanced:** Although ISC has established relations with the International Telecommunications Union (ITU), Organization for Economic Co-operation and Development (OECD), Asia Pacific Organization on Anti-spam (APCAUSE), and other international organizations, direct cooperation between China's ISPs and ESPs with those from other countries is inadequate. Without direct and effective collaboration, Chinese ISPs and ESPs cannot work with international counterparts in a timely manner. A lot of spam sources cannot be stopped and finally get blacklisted. China should further strengthen international cooperation through various channels in order to promote China's achievements and experiences, and cooperate with other interested parties to promote global anti-spam work.
5. **Improve ASPR:** China also needs to further develop and modify the anti-spam technical standards and the terms of agreement for industry-led initiatives. These are important steps for coping with new emerging problems, such as the difference between legitimate commercial email and spam and making it easier for end users to understand anti-spam email services.

---

<sup>55</sup> Zombie networks refer to botnets.

### **3.4 Insights Gleaned by Chinese Experts About the U.S.**

This section details nine key observations that enabled the Chinese experts to better understand the U.S. business environment, their American counterparts and their experiences fighting spam in the U.S. They include:

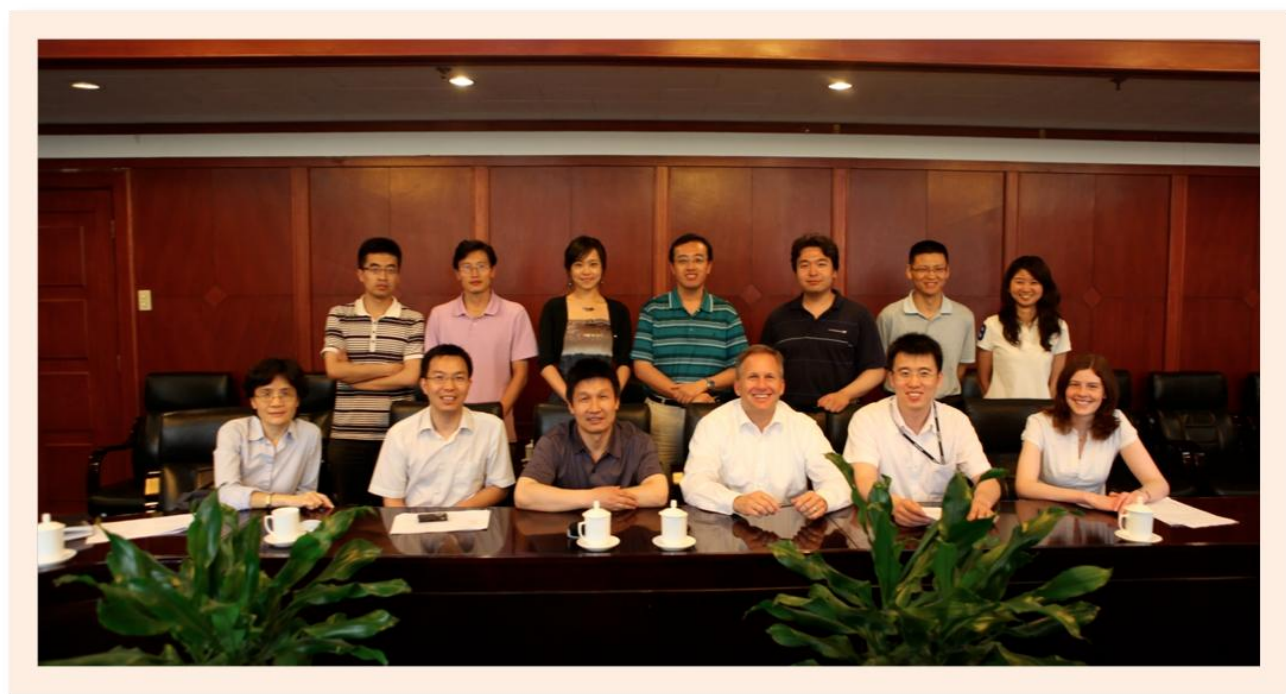
- 1. Framework and methodology:** The U.S. experts invested time early in the process to develop the proper framework and methodology before delving into the issues. Generally this approach would lead to a more comprehensive output and creative ideas. In contrast to the U.S. experts' attention to theory and policy, the Chinese experts focused more on engineering and technical approaches to solve the problems.
- 2. Maturity and experience:** The U.S. team had a range of expertise that included technical and engineering as well as legal and policy backgrounds. Even those with technical expertise had interest in the policy aspects of the discussions. This may be attributed to the U.S. experts' average experience being longer and their age higher than that of the Chinese experts. This is because the ICT industry developed much earlier in the U.S. than in China.
- 3. Remote collaboration:** Virtual meetings over the Internet are much more acceptable to the U.S. groups than to the Chinese groups. The virtual meetings were managed effectively to enable collaborative interactive work by the team, despite the disparate geographical locations. The U.S. experts were more comfortable working remotely because they were familiar with this format.
- 4. Spam statistics and coordination:** There seemed to be less of an industry-coordinated nationwide effort on anti-spam collaboration in the U.S. than in China. There did not appear to be an American equivalent to the Anti-Spam Center of the ISC. The statistical data on spam to be shared by the U.S. experts was often from the third party security service companies. Many companies were trying different measures to block spam, but there seemed to be no specific, unified rules in this field.<sup>56</sup>
- 5. Time horizon:** There was a feeling that the implementation of ideas that interested the Americans was based on a long-term effort, which seemed a little different from the thinking of the Chinese experts, who expected immediate practice or testing before the fast-developing technology progressed too far.
- 6. Respectful discussion:** Both the U.S. and Chinese experts overcame barriers in language, culture and ideology to make the dialogue very successful. In the conversation, the U.S. experts always double-checked the Chinese experts' ideas to make sure they understood correctly before the two parties went in different directions. The U.S. experts also allowed enough time for the Chinese experts to explain their ideas.
- 7. Professional research and tool utilization:** It was very clear that the U.S. experts were using a professional approach and making good use of research tools. They had systematic procedures that led the team to achieve their goals.

---

<sup>56</sup> Many U.S. messaging experts are actively engaged in industry collaboration taking place under the auspices of the Message Anti-Abuse Working Group (MAAWG), which is an international organization. The level of coordination taking place at the national level in this or any other forum is less extensive than what is coordinated by the Internet Society of China in China.

**8. U.S. Spam legislation not getting job done:** The most visible policy approach to fighting spam in the U.S. is a legislative measure.<sup>57</sup> This gave the Chinese experts the view that Americans believed that government intervention would give unified provision for stopping and punitive measures to stop spam. Although the effectiveness of the anti-spam bill was unsatisfying, the U.S. experts were less critical of it than they could have been, given its results. The Chinese experts thought it is indeed important to launch effective punitive measures by the government, but industry is best conditioned to find and implement real solutions.

**9. Less knowledge about China's Internet industry:** The U.S. experts had relatively less knowledge about the Internet industry in China compared to the Chinese experts understanding of the U.S. Internet industry. This is considered part of the reason that some anti-spam organizations based in the U.S. treat IP addresses in China with bias, without adequate transparency to Chinese practitioners.



The team meets in Beijing

---

<sup>57</sup> The CAN-SPAM Act.

## 4. Joint Recommendations

The previous sections demonstrated the team's success in achieving the first two goals of the bilateral, *opening genuine dialogue* and *developing deeper understanding*. This section is devoted to the third objective, *coming to agreement* on international ASPR to reduce spam in cyberspace and its negative impact on recipients. With this focus on international policy, it is here noted that the focus of the guidance provided is on ASPR.<sup>58</sup>

This report submits two joint recommendations and 46 Best Practices. Each recommendation is actionable and, if implemented, can be effective in reducing spam. The experts from both sides urge timely consideration and action for each of these recommendations.

### Industry Leadership

The implementation of these recommendations will require both leadership and support from governments, industry and NGOs. However, both the Chinese and U.S. experts acknowledged that industry must play a leading role in analyzing the problem, discovering effective solutions and implementing these solutions. This joint conclusion was derived from the simple fact that the primary technical expertise and operational knowledge resides with the individuals within companies who build, operate and own networks or otherwise provide services upon them.<sup>59</sup> This is an example of industry-led *private-public* partnership.<sup>60</sup>

### Voluntary Measures

Further to the above point, most of the provided guidance takes the form of voluntary best practices. As such, it is important to appreciate that the applicability of each best practice for a given circumstance depends on many factors that need to be evaluated by individuals with appropriate experience and expertise in the same area addressed by the best practice.

While the best practices are voluntary, network operators, ISPs and ESPs should be aware of the consequences of not performing due diligence. Aside from possibly losing subscribers frustrated by poor customer service and being behind the curve in best practice deployment, they may very soon unintentionally cultivate a colossal amount of spam.

### Recommendation Presentation

Each recommendation is presented in a concise manner in order to support critical decision-making, to maintain the momentum from the report development and to mobilize resources toward action. The outline of the recommendation presentation is as follows:

- **Title** - for identification and a summary.
- **Background** - to provide the essential elements of the context of the issue being addressed.
- **Recommendation** - to identify who should do what.
- **Required Commitments** - crisply outlines the requirements from critical parties for success.
- **Benefits** - encapsulates the value proposition for implementing the recommendation.
- **Alternatives and Their Consequences** - outlines the other options and likely outcomes.
- **Next Steps** - offers suggestions for keeping momentum and focus.
- **Measures of Success** - provides means to objectively evaluate performance.

---

<sup>58</sup> i.e. those purely technical are excluded. Some policy or cooperation aspect is associated with the guidance included.

<sup>59</sup> Table 3 provides a detailed outline of the best practices with the primary implementation roles.

<sup>60</sup> PPP, to emphasize the role of the private sector leadership; a phrase coined by the author in keynote speech prepared for the *European Union Ministerial Conference on Critical Information Infrastructure Protection*, Tallinn, 27-28 April 2009 ; Also, *A Conversation on Information and Communications Infrastructure Dependability*, IEEE, 2009.

## 4.1 Improved Industry Cooperation

### Background

Spam messages often traverse long distances across multiple networks. The passage between multiple networks can make it more difficult for network operators and service providers to trace the path of a message. This difficulty can be even more pronounced when the interface is between two countries. Indeed, spam generators have exploited weaknesses in international coordination in order to make their identities more difficult to uncover, their spam messages more difficult to recognize and countermeasures more difficult to apply. Thus, international ASPR is essential to effectively fighting spam.

International collaboration on fighting spam has been recognized as a priority by both the U.S. and China for several years.<sup>61 62</sup> A natural next step is for the U.S. and China to cooperate with each other on spam. Currently, there is a gap in cooperation for both simple and complex factors. One simple reason is the language barrier. A spam countermeasure discussion among network security engineers involves advanced concepts and terms that make a conversation quite involved, thus a high level of language skills is required. Other simple reasons include the time zone challenge and the general lack of awareness of the other country's network environment.<sup>63</sup> In addition to these factors, there are other, less simple reasons for the current stunted level of cooperation on fighting spam. One more complex reason is that there is insufficient relationship-development between network security engineers from both countries.<sup>64</sup> Another factor is the general context of mistrust that dominates ICT discussions between the two countries. Until these issues are addressed, spammers will continue to be able to effectively exploit this environment.

This recommendation addresses this gap head on by presenting immediately actionable guidance. In addition, industry experts from both China and the United States are interested in swiftly moving forward with this recommendation.<sup>65</sup> This recommendation calls on existing international forums serving each country to proactively connect with each other, and with network operators and service providers. Specifically, these organizations should adjust their charters, expand their membership and plan their meeting locations to accommodate members from the other country. The new forum may be used to exchange ideas about countermeasures, anti-spam technology and incidents of special interest.

---

<sup>61</sup> The 2005 Seoul-Melbourne Anti-Spam Agreement: This Memorandum of Understanding (MoU) was signed by Australia, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, the Philippines, Thailand and Taiwan.

<sup>62</sup> U.S. network operators and service providers are actively engaged in private sector-led international initiatives such as the Message Anti-Abuse Working Group (MAAWG).

<sup>63</sup> *Asymmetric Awareness*, Insights Gleaned by U.S. Experts About China, Section 3.1.

<sup>64</sup> People ultimately trust other people, making personal relationships vital to improvements. See Key Finding 98, *Availability and Robustness of Electronic Communications Infrastructures (ARECI) Final Report*, European Commission, March 2007.

<sup>65</sup> At the time of this report's publication, several interested parties on both sides have expressed an enthusiastic willingness to engage their counterparts on fighting spam.

## RECOMMENDATION 1

The Network Operators, Internet Service Providers and Email Service Providers of China and the United States, along with peers in other nation-states, should establish a forum where regular cooperation can be fostered with the aim of reducing spam in cyberspace.

### Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Industry companies in China must be committed to cooperating with their peers in the U.S.
- ☐ Industry companies in the U.S. must be committed to cooperating with their peers in China.
- ☐ Chinese and U.S. government agencies must be committed to encouraging cooperation that will focus on the reduction of spam.
- ☐ An international spam-fighting industry organization must be established anew, or from an existing forum, that will be committed to extending participation to include both China and the U.S.

### Alternatives and Their Consequences

Alternatives to this approach include the following:

- Do nothing . . . *resulting in increased spam between the two countries, and to the world.*
- Limit spam-fighting cooperation to existing collaborative efforts . . . *resulting in lost opportunity from open dialogue and deeper understanding.*
- Government agencies seek to manage the industry interaction . . . *resulting in cumbersome engagements with unnecessary political complications.*

### Benefits

The benefits of implementing this recommendation begin with enhanced cooperation between subject matter experts from the United States and China. This cooperation will enable a more rapid response to network problems, enhanced identification spam and botnet sources and an ultimate reduction in the spam that pollutes cyberspace. In addition, the careful trust built here may advance the level of trust on increasingly more significant challenges in cybersecurity.

### **Next Steps**

Suggested next steps to generate and maintain the momentum for implementing this recommendation include the following:

- 1-1. The anti-abuse network security experts from network operators, ISPs and ESPs of China and the U.S. meet to establish points of contact between companies, compare observations of spam trends and share experiences regarding the effectiveness and feasibility of spam fighting countermeasures.
- 1-2. Chinese and U.S. anti-abuse network security experts develop procedures for developing trust and interacting on spam fighting initiatives
- 1-3. Anti-abuse network security experts from China, the U.S. and other interested parties meet regularly to cooperate in fighting spam.

### **Measures of Success**

The successful implementation of this recommendation can be gauged by the following measures:

- A. Points of contact established.
- B. Trust evidenced by meaningful cooperation in fighting spam and botnets.
- C. The establishment of a industry-led, inclusive international forum for anti-spam governance
- D. The reduction in spam generated from both countries

## 4.2 Voluntary Implementation of Expert Best Practices

### Background

Electronic messaging as we know it would be impractical if it were not for very advanced countermeasures and constant vigilance on the part of network operators, ISPs, ESPs and security application developers. Without their efforts, spam could easily comprise more than 99% of all email messages. Most users would find the resulting burden of sifting through one hundred or one thousand messages to find a single legitimate one to be unacceptable. Thus, existing best practices have proven vital for the continued viability of electronic messaging. Best practices are also the hope for improving the current situation.

Best practices are best developed when experts come together and share insights. This can be done within a company or agency, across an industry or country, or among international parties. It is the last level that has not yet been fully developed.

International cooperation to develop best practices has been underway for several years.<sup>66</sup> However, cooperation between the West and China, and more specifically, the U.S. and China has been insufficient.<sup>67</sup> This recommendation aims to improve cooperation by pointing to 46 Best Practices developed jointly by the combined China-U.S expert team. If implemented, these best practices would reduce the origination, propagation and unintentional opening of spam messages. Further, the dynamic nature of some of these practices would offer countermeasure value, as spammers continuously adapt to defeat existing anti-spam countermeasures.

### RECOMMENDATION 2

The Email Service Provider, Internet Service Providers, Network Operators and Government Policy Makers of China and the United States, along with peers in other nation-states, should cooperate to develop, maintain, and voluntarily implement consensus Best Practices as appropriate, with consideration of network configurations, business models and other feasibility factors.

### Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Industry companies must be committed to implementing best practices, where appropriate.
- ☐ Industry companies must be committed to contributing expertise to best practice development collaboration.
- ☐ Chinese and U.S. government agencies must be committed to implementing best practices, where appropriate.

<sup>66</sup> Examples of existing international cooperation include the Message Anti-Abuse Working Group (MAAWG), ETIS Anti Spam Cooperation Group, and the Spamhaus Project.

<sup>67</sup> *"This dialogue with China is a most welcomed breakthrough – a real step forward."* – statement from MAAWG Chairman Michael O'Reirdan, in reference to this bilateral initiative. <http://www.ewi.info/first-china-us-effort-fight-spam>, February 2011.



- Chinese and U.S. government agencies must respect the need for industry expertise and experience to guide the development and application of best practices.

### **Alternatives and Their Consequences**

Alternatives to this approach include the following:

- Do nothing . . . *resulting in increased spam between the two countries and throughout the world.*
- Confine best practice discussions to current parties . . . limiting the potential maturity and implementation of the aggregate best practice guidance.
- Government agencies mandate network management practices . . . *resulting in suboptimum network performance and reduced industry flexibility to respond to concerns.*

### **Benefits**

If implemented, this recommendation will provide cutting-edge expertise and experience to help both countries fight spam, and the related problems of computer viruses and Internet fraud. Further, as the effort extends to other parties, this expert guidance process will be leveraged to develop and deploy even better best practices.

### **Next Steps**

Suggested next steps to build and maintain the momentum for implementing this recommendation include the following:

- 2-1. The network operators, ISPs and ESPs of China and the U.S. consider each of the best practices described in this report and, where appropriate, implement them.
- 2-2. China, U.S. and other willing parties collaborate to maintain and continuously improve upon the best practice guidance.
- 2-3. Based on feedback from the above steps, a trusted neutral entity should address the political and financial arrangements needed to support the implementation of the agreement.

### **Measures of Success**

The successful implementation of this recommendation can be gauged by the following measures.

- A. Best practices are implemented.
- B. Best practices are updated and maintained.
- C. Spam generation and transmission is reduced.
- D. Botnets are identified and shut down.

### 4.3 The Consensus Best Practices

This section introduces the consensus best practice guidance for reducing spam. 46 Best Practices were articulated and agreed upon based on the methodologies outlined in Section 2. As stated earlier, these best practices are intended to be voluntary and, as such, are flexible policies. They represent reasonable behaviors for one party to expect another party with whom they interface or interact.

#### Spam Lifecycle

In order to appreciate the purpose of each best practice, it is helpful to consider the lifecycle of spam. Figure 4 below provides a high-level outline that builds on the lifecycle to include the international context, primary actors and principle objective of countermeasures (i.e. best practices) for each stage of the lifecycle.

At the beginning of the lifecycle, spam is created by a spammer in a given country (Phase A). Best practices to address this stage of the lifecycle are best focused on addressing the motivation of the spammer. In the next stage (Phase B) of the lifecycle, that spam is inserted in some electronic format (i.e. email) by the spammer. The primary objective of countermeasures in this phase is to reduce the volume of messages being inserted. The spam is then distributed by ESPs, ISPs and network operators in their networks (Phase C). Countermeasures that fight spam at this stage are chiefly aimed at detecting the spam being transmitted. The next step is for spam to be handed off from one network to another (Phase D).<sup>68</sup> This is typically where it may encounter international barrier(s). Countermeasures that can assist network hand-offs often are built around information sharing between network peers.

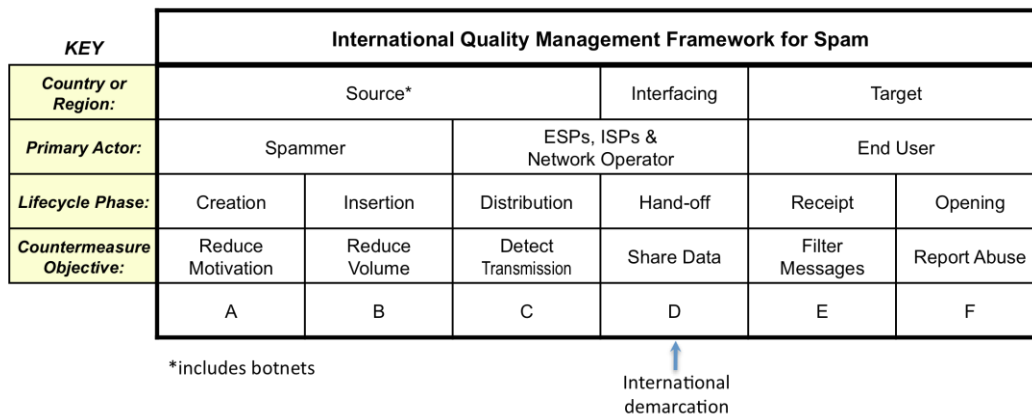


Figure 4. An International Quality Management Framework for Spam

The final two phases are reserved for spam that has reached its target destination. First, the spam is received (Phase E).<sup>69</sup> Effective countermeasures at this phase mainly filter messages. At the final phase of its lifecycle, the spam message is opened by the end user (Phase F).<sup>70</sup> At this point

<sup>68</sup> Spam messages targeting the same network would of course possibly stay within that network.

<sup>69</sup> The recipient may be a corporate or university network. Policies of public ISPs can be different from that of corporate or university networks.

<sup>70</sup> Not all messages that pass filters will be opened. This is for illustrative purposes to complete the lifecycle.

the result may be harmless, or the end user computer may be exposed to malicious code, or the end user may be presented with a fraudulent message or offensive images. The countermeasures for this final phase deal with end user reporting, and ESP and ISP management of these reports. In addition, they include educating and raising awareness among end users.

A critical observation regarding the above lifecycle description is that the cost of dealing with spam increases as you move from left to right (A to F). Thus, it is imperative that spam be countered as early as possible. It is *better to effectively reduce the spammers' motivation* above all other goals. Likewise, we should prioritize reducing the volume of spam being inserted over detecting its transmission or sharing data about it. Since no countermeasure suite will be completely effective, it is necessary to have measures in place at each phase.

### Best Practice Presentation

Each of the best practices is presented in a format intended to provide a unique identification, a short summary of guidance provided, the parties responsible for implementation, and an indication of which ingredients are being addressed and the nature of the countermeasure (Figure 5).<sup>71 72</sup>

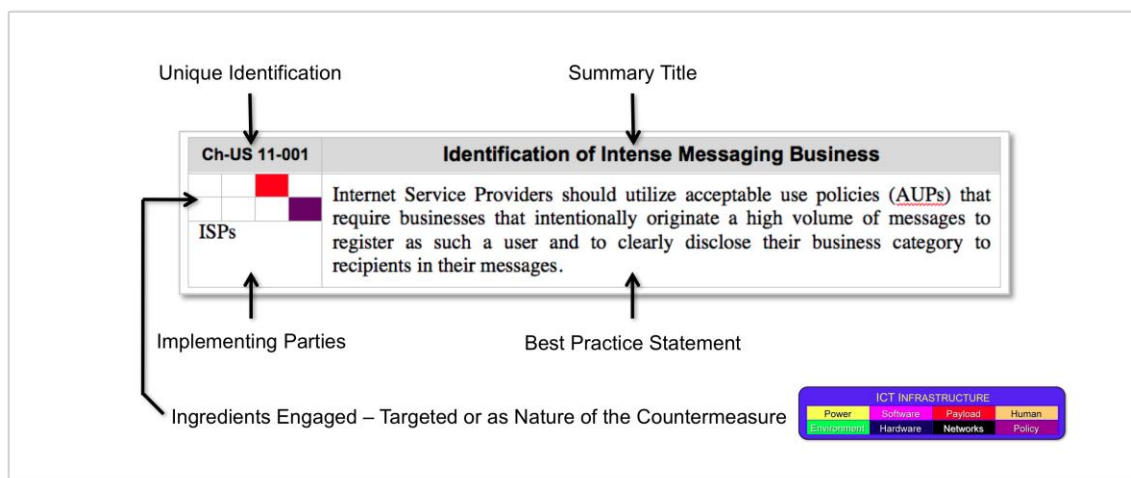


Figure 5. Presentation of China-US Consensus Best practices

### Best Practice Principles

The joint China-U.S. expert team utilized proven methods in their development of these best practices. The guidance presented here meets the standards for industry consensus best practices, including the following seven considerations.<sup>73</sup>

<sup>71</sup> The Unique Identification system introduced here is of the format CN-US 11-001, where “Ch-U.S.” designates the China-U.S. bilateral and the “YY-XXX” provides an indication of the year (i.e., 11 for 2011) the specific Best Practice was introduced or last updated, when future revision are made. The last three digits are unique identifiers. A revised BP would retain its unique three digit number but the YY designations could change.

<sup>72</sup> Each of the eight ingredients are arranged as shown in Figure 3. That is, clockwise, starting the upper left corner: Power, Software, Payload, Human, Environment, Hardware, Networks and Policy – otherwise known as ASPR.

<sup>73</sup> Rauscher's 7 Principles of Best practices, NRIC V Presentation, Washington, D.C., 2001.

1. People implement best practices<sup>74</sup>
2. Best practices do not endorse "pay for" documents, products or services<sup>75</sup>
3. Best practices address classes of problems<sup>76</sup>
4. Best practices are already implemented<sup>77</sup>
5. Best practices are developed by high degree of consensus<sup>78</sup>
6. Best practices are verified by experts who were outsiders to the development process<sup>79</sup>
7. Best practices are presented only after sufficient rigor and deliberation has warranted inclusion of both the conceptual issue and the particular wording of the practice.<sup>80</sup>

Table 3 provides a list of the consensus best practices along with an indication of who the primary responsible party is regarding implementation.

---

<sup>74</sup> Best practices (BPs) are written to be broadly understood by experts in their field and likewise applied by the same.

<sup>75</sup> The BP development process should not be used to promote commercial interests.

<sup>76</sup> i.e., they are not specific fixes.

<sup>77</sup> This is not to say that most are doing them, as that would be "common practices." However, the practices should be proven effective and feasible by at least one entity.

<sup>78</sup> Only BPs that achieve a high degree of agreement should be included. Each participant in the process should have ample opportunity to influence and persuade peers regarding their point of view.

<sup>79</sup> To avoid "groupthink" the draft BP language should be circulated for critical review by subject matter experts and other stakeholders.

<sup>80</sup> Best practices should not be thoroughly examined with considerations that include such factors as effectiveness in achieving objective, cost to implement and risk of not implementing.

**Table 3. Consensus Best Practices with Implementation Responsibilities**  
(Government Policy Maker, Equipment or Software Supplier, Network Operator,  
Email Service Provider, Internet service provider, Netizen)







BP ID	TITLE	GPM	ESS	NO	ESP & ISP	NZN
CN-US 11-001	Reduce the Motivation					
CN-US 11-002	Go With the Flow					
CN-US 11-003	Education Campaign for Potential Spammers					
CN-US 11-004	Enable ESPs & ISPs to Charge					
CN-US 11-005	Specific User Agreements					
CN-US 11-006	Vigilance in Updating Policies					
CN-US 11-007	Identification of Intense Messaging Businesses					
CN-US 11-008	Limited Distributions to Appropriate Recipients					
CN-US 11-009	Subscriber Agreement High Use Thresholds					
CN-US 11-010	Outbound Spam Classification					
CN-US 11-011	Enable ISPs to Treat Spammers Differently					
CN-US 11-012	Port 25 Egress Blocking					
CN-US 11-013	Message Identification Coordination					
CN-US 11-014	Drop Noncompliant Messages					
CN-US 11-015	Sooner is Better					
CN-US 11-016	Utilize DKIM Mechanisms Across Borders					
CN-US 11-017	Utilize SPF Mechanisms Across Borders					
CN-US 11-018	Joint Technology Platform					
CN-US 11-019	Closing Open Relays					
CN-US 11-020	Blacklisting ISPs					
CN-US 11-021	International Cooperation for Statistics					
CN-US 11-022	Feedback Loops with Peers					
CN-US 11-023	Utilize FBL Mechanisms Across Borders					
CN-US 11-024	Best Practices Checklist					
CN-US 11-025	Botnet Tracking Via IP Addresses					
CN-US 11-026	Botnet Tracking Via Domain Names					
CN-US 11-027	Registrar Feedback					
CN-US 11-028	International Coordination on FBLs					
CN-US 11-029	Challenging Cloaking with Reverse Lookups					
CN-US 11-030	Support WHOIS					
CN-US 11-031	Cloaking Detection					
CN-US 11-032	Benefits of Voluntary Agreements					
CN-US 11-033	Voluntary International Agreements					
CN-US 11-034	Cooperation for Spam Suppression					
CN-US 11-035	ASPR Checklist					
CN-US 11-036	Gap Closure					
CN-US 11-037	Anti-Malware Support					
CN-US 11-038	Spam Alerting					
CN-US 11-039	Spam Filtering					
CN-US 11-040	Spam Reporting					
CN-US 11-041	Spam Reporting Center					
CN-US 11-042	Abuse Mailboxes					
CN-US 11-043	Disabling Abusive Accounts					
CN-US 11-044	Education Campaign for Netizens					
CN-US 11-045	Abuse Report Administration					
CN-US 11-046	Customer Service and Education					

## Reducing the Motivation

Spam is a problem because it is currently an effective way of communicating with many people for a very low cost. When a business makes use of spam, there is usually a perceived financial advantage – i.e. an attractive return on investment (ROI).<sup>81</sup>

A fundamental factor in preventing the creation of spam concerns spammers' motivations. As long as spam is an attractive option for revenue generation or meeting other needs, then spammers will use it. The team considered a broad range of ideas for making spam less attractive. Ultimately, most of these ideas looked at important restraints, such as freedoms of speech, the basic business model for selling an electronic messaging service, and the desirability to keep the cost of electronic messaging services low and its use uncomplicated.

Addressing the incentive for those inserting spam into networks is the focus of the following Best practices.

CN-US 11-001		Reduce the Motivation
GPMs ESPs & ISPs NZNs		Email Service Providers, Internet Service Providers and government policy makers should consider agreements, standards, policies and regulations (ASPR) that will reduce the motivation for individuals and organizations to send spam. Such ASPR should not impede opportunities for new legitimate business opportunities or infringe on the legal rights of individuals to express themselves.
		
CN-US 11-002		Go With the Flow
GPMs		Government policy makers should avoid dependence on slow and inflexible regulation by advocating strategies aligned with business fundamentals and social forces in order to be prepared for new developments in network capabilities and consumer services.
CN-US 11-003		Education Campaign for Potential Spammers
GPMs ESPs & ISPs NZNs		Government agencies, Internet Service Providers and Email Service Providers should consider the use of community outreach in order to raise the awareness of existing or potential spammers regarding prohibitions against abusing electronic messaging systems. <sup>82</sup>
		
		

<sup>81</sup> Exceptions to this include spammers who are ideologically motivated.

<sup>82</sup> E.g., posters, flyers, promotions and volunteer-led tutorials.

CH-US 11-004

### Enable ISPs to Charge



Government policy makers should consider policies that would enable industry to impose financial costs on customers with high-volume message practices.<sup>83</sup>

<sup>84</sup>

CN-US 11-005

### Specific User Agreements



ESPs & ISPs  
NZNs

Email Service Providers and Internet Service Providers should make use of user agreements with specific provisions for new messaging accounts and applications in order to provide a contractual mechanism to strictly enforce the AUP against messaging abuse.

CN-US 11-006

### Vigilance in Updating Policies



GPMs  
ESPs & ISPs  
NOs  
ESSs

Governments, Network Operators, Internet Service Providers, Email Service Providers and equipment and software suppliers should continuously monitor effective policies on spam in order to weigh the impacts of new applications and devices.

## Reducing Volume

The volume of spam messages inserted each day into networks around the world is on the order of hundreds of billions. Reducing spam volume at the front end of the process is much more cost-effective than dealing with it later, after the spam has been transported through networks.

One of the reasons spam is effective is that it is hard to identify by ESPs, ISPs, network operators and message recipients. This is often due to intentional deception by spammers. Therefore, the team explored measures to provide more certainty about who is sending a message and whether or not it is part of a high-volume, wide distribution campaign. Because not all bulk commercial messaging is spam, care needs to be taken to avoid measures harmful to legitimate business endeavors.<sup>85</sup>

The following best practices aim to reduce the volume of inserted messages and reduce the deception associated with spam:

<sup>83</sup> The additional cost for a premium business account was considered of limited effect.

<sup>84</sup> Government regulators recognize the nontrivial ongoing operational cost of facilities, electricity, hardware, software, network capacity and personnel.

<sup>85</sup> Formal Communications Theory recognizes that there exists a degree of uncertainty when information is transmitted in a communication channel. The term 'Shannon Entropy' can be used to describe this uncertainty. Understanding this basic principle can be helpful in enabling basic communications engineering principles to be applied regarding such priorities like maximizing 'signal' clarity and reducing 'noise.'

CN-US 11-007

### Identification of Intense Messaging Business

ESP  
s & ISP  
s  
NZNs

Email Service Providers and Internet Service Providers should utilize acceptable use policies (AUPs) that require businesses that intentionally originate a high-volume of messages to register as such a user and to clearly disclose their business category to recipients in their messages.

CN-US 11-008

### Limited Distributions to Appropriate Recipients

NZNs

Netizens intending to use electronic messaging as a vehicle for high-volume, wide distribution communications should target messages only to recipients who are likely to appreciate the content.

CN-US 11-009

### Subscriber Agreement High Use Thresholds

ESP  
s & ISP  
s  
NZNs

Email Service Providers and Internet Service Providers should consider acceptable use policies (AUP) for customers with high-volume message practices in order to restrict individuals and organizations from sending spam. Such agreements must be managed in a way that subscribers with botnet-infected computers are not mishandled.<sup>86</sup>

CN-US 11-010

### Outbound Spam Classification

ESP  
s & ISP  
s

Email Service Providers and Internet Service Providers should support outbound spam classification so that if one of their customer's accounts gets hijacked or they are infected with a spambot, the mail provider should stop the outbound spam by disabling the account.<sup>87</sup>

CN-US 11-011

### Enable ESPs and ISPs to Treat Spammers Differently

GPMs

Government policy makers should consider policies that would enable different treatment to customers with high-volume, wide-distribution message practices. Such a practice does not imply that this information needs to be made public, provided to or managed by the government.


<sup>86</sup> See Appendix A, *Sample ISP Letter to Customers*.

<sup>87</sup> Methods of identification may include content analysis or detecting an increase in message volume from a particular account.



CN-US 11-012

### Port 25 Egress Blocking

 Email Service Providers and Internet Service Providers should consider performing egress filtering on TCP Port 25 as a default in order to impede its unauthorized utilization by botnets. Subscribers requiring a mail server can be managed as exceptions and provided with a static IP address.

ESPs & ISPs


### Detecting Transmission

A fundamental principle of good engineering practice is make efficient use of the limited resources. When dealing with spam, detecting spam nearer to its source is preferred to detecting it nearer to its target, so as not to waste resources carrying spam across networks. This waste includes unnecessary strain on hardware capacity, software processor cycles, the energy needed to power the hardware and maintain buildings housing network gear, and the staff to operate and maintain this equipment.

There are three primary factors that enable spam to be detected close to its source: intelligence regarding message identification, intelligence regarding the source and effectiveness in learning and tracking adjustments employed by spammers to avoid detection. The following best practices focus on detecting the transmission of spam in networks.

CN-US 11-013


### Message Identification Coordination

 Network Operators, Internet Service Providers and Email Service Providers should collaborate in international forums to develop methods of increasing the effectiveness of identifying legitimate messages utilizing message header contents and message protocols.<sup>88</sup>

NOs  
ESPs & ISPs

CN-US 11-014


### Drop Noncompliant Messages

 Network Operators, Internet Service Providers and Email Service Providers should use existing mechanisms to identify and drop spam. Consideration should be given to dropping noncompliant messages.

NOs  
ESPs & ISPs

CN-US 11-015

### Sooner is Better

 Network Operators, Internet Service Providers and Email Service Providers should prioritize anti-spam strategies that detect and remove spam messages as early in their intended transmission path as possible, in order to reduce the inefficiency and cost of transporting such messages across the Internet.<sup>89</sup>

NOs  
ESPs & ISPs

<sup>88</sup> E.g., DKIM, SPF, IETF RFC 4871.

<sup>89</sup> U.S. ISPs have indicated that they can achieve detection rates at the network entry point on the order of 90% for inbound messages.

**CN-US 11-016**

### **Utilize DKIM Mechanisms Across Borders**

  
NOs  
ESPs & ISPs

Network Operators, Internet Service Providers and Email Service Providers should make use of available Domain Keys Identified Mail (DKIM) mechanisms, especially when interfacing with international peers, in order to improve the confidence that the messages are from a reputable network.

**CN-US 11-017**


### **Utilize SPF Mechanisms Across Borders**

  
NOs  
ESPs & ISPs

Network Operators, Internet Service Providers and Email Service Providers should make use of available Sender Policy Framework (SPF) mechanisms, especially when interfacing with international peers, in order to improve confidence that the messages are from a reputable network.

**CN-US 11-018**

### **Joint Technology Platform**

  
NOs  
ESPs & ISPs

Network Operators, Internet Service Providers and Email Service Providers should consider cooperating to develop technology platforms that can be used to facilitate coordination in detecting and managing spam.

**CN-US 11-019**

### **Closing Open Relays**

  
NOs  
ESPs & ISPs

Internet Service Providers, Email Service Providers and Network Operators should consider closing open mail relays, in order to prevent spammers from exploiting their use to hide source and identify information.<sup>90 91</sup>

## **Sharing Data**

Spammers take advantage of the world's complex web of interconnected networks. They further exploit the international aspect of this complexity. To keep up with the spammers' tactics, ESPs, ISPs and network operators need to cooperate to share information.<sup>92</sup> Because different companies have different business models and acceptable use policies, cooperation is not always straightforward, but rather, may require negotiations to build on common areas of interest.

Each of the following best practices focuses on trusted information sharing among industry peers, especially for those involving international interfaces.

<sup>90</sup> Lindberg, G., RFC 2505, Anti-Spam Recommendations for SMTP MTAs, February, 1999.

<sup>91</sup> Klensin, J., RFC 5321, Simple Mail Transfer Protocol, October, 2008.

<sup>92</sup> Recommendation 1, *Improved Industry Cooperation*, Section 4.1.

CN-US 11-020

### Blacklisting ISPs

NOs  
ESPs & ISPs



Network Operators should cooperate across borders to block Internet Service Providers and Email Service Providers that lease blocks of IP address space to spammers.

CN-US 11-021

### International Cooperation for Statistics

NOs  
ESPs & ISPs



Network Operators, Internet Service Providers and Email Service Providers should collaborate at an international level to aggregate worldwide statistics, including trend information, that can be useful in developing effective agreements, standards, policies and regulations (ASPR) by ensuring that decision makers are sufficiently informed.

CN-US 11-022

### Feedback Loops with Peers

NOs  
ESPs & ISPs



Network Operators, Internet Service Providers and Email Service Providers should provide feedback loop mechanisms to facilitate the reporting and identification of spam, in order provide intelligence on messages that have been identified as spam.

CN-US 11-023

### Utilize FBL Mechanisms Across Borders

NOs  
ESPs & ISPs



Network Operators, Internet Service Providers and Email Service Providers should make use of available feedback loop (FBL) mechanisms with the countries with which they interface with in order to increase the information available to them to manage spam.<sup>93</sup>

CN-US 11-024

### Best Practices Checklist

NOs  
ESPs & ISPs



Network Operators, Internet Service Providers and Email Service Providers should maintain an updated list of best practices, including those dealing with international aspects, for fighting spam and periodically make use of the list towards the aim of gap closure.

CN-US 11-025

### Botnet Tracking Via IP Addresses

NOs  
ESPs & ISPs



Internet Service Providers and Email Service Providers should identify the internet protocol (IP) addresses of botnets sending spam and report to the related Network Operator in order help shut down the botnet activity.<sup>94 95</sup>

<sup>93</sup> *Complaint Feedback Loop Best Current Practice*, MAAWG, April, 2010.

<sup>94</sup> Seitzer, Larry, *How Microsoft Took Down Rustock*, PCMag.com, March 2011.

<sup>95</sup> see Conficker Working Group, [www.confickerworkinggroup.org](http://www.confickerworkinggroup.org).

CN-US 11-026

### Botnet Tracking Via Domain Names

  
NOs  
ESPs & ISPs

Internet Service Providers and Email Service Providers should use the domain names of botnets sending spam and report them to the related Network Operator to help shut down the botnet activity.

CN-US 11-027


### Registrar Feedback

  
NOs  
ESPs & ISPs

Internet Service Providers and Email Service Providers should report rogue web sites to the associated registrars in order that appropriate action can be taken (i.e. shutting down the domain name).

CN-US 11-028

### International Coordination on FBLs

  
GPMs  
NOs  
ISPs

Government policy makers and Internet Service Providers within a specific country should recognize their country's international-facing agencies to enable coordination between nation-states on network interface policies, like utilization of Feedback Loops (FBLs).<sup>96</sup>

CN-US 11-029


### Challenging Cloaking with Reverse Lookups

  
NOs  
ESPs & ISPs

Internet Service Providers, Email Service Providers and Network Operators should consider configuring their mail exchanges to perform reverse Domain Name Server (DNS) entry lookup, in order to confirm the designated domain name associated with an IP address.

CN-US 11-030

### Support WHOIS

  
NOs  
ESPs & ISPs

Internet Service Providers, Email Service Providers and Network Operators should consider configuring their mail exchanges to support WHOIS lookups, in order to enable the confirmation of registered users or assignees of Internet resources.<sup>97 98</sup>

CN-US 11-031

### Cloaking Detection

  
NOs  
ESPs & ISPs

Internet Service Providers, Email Service Providers and Network Operators should consider configuring their mail exchanges to correctly verify a properly formatted banner that identifies the mail server's domain name, in order to detect attempts to detect identity or source-cloaking.


<sup>96</sup> Alliance for Telecommunications Industry Solutions (ATIS) Next Generation Interconnection Interoperability Forum (NGIIF) maintains a world zone 1 list of contacts for wireless and wireline networks.

<sup>97</sup> Daigle, L., RFC 3912, *WHOIS Protocol Specification*, IETF, September, 2004.

<sup>98</sup> Internet resources may include domain names, IP address blocks or autonomous systems.

CN-US 11-032


### Benefits of Voluntary Agreements

 Government policy makers and industry should recognize the benefits of voluntarily implemented agreements, standards and policies to avoid dependence on slow government regulations.

GPMs  
NOs  
ESPs & ISPs

CN-US 11-033


### Voluntary International Agreements

 Government policy makers and industry should consider voluntary agreements across nation-state borders that might help reduce spam (e.g., closing down sources).

GPMs  
NOs  
ESPs & ISPs

CN-US 11-034


### Cooperation for Spam Suppression

 Network Operators, Internet Service Providers and Email Service Providers should use voluntary agreements with their peers to cooperate in suppressing spam (e.g., sharing suspected signatures and sources)

NOs  
ESPs & ISPs

CN-US 11-035


### ASPR Checklist

 Network Operators, Internet Service Providers and Email Service Providers should maintain a checklist of agreements, standards, policies and regulations (ASPR) used to reduce spam in order track progress against the intended plan.

NOs  
ESPs & ISPs

CN-US 11-036

### Gap Closure

 Network Operators, Internet Service Providers and Email Service Providers should regularly identify the best existing anti-spam measures not yet implemented for gap closure.

NOs  
ESPs & ISPs

## Filtering Messages

Once a spam message has arrived at its target destination, the spammer is close to achieving his or her objective. It is unfortunate that the spam message was not stopped earlier, as it has incurred hidden cost.<sup>99</sup> Intelligent filtering by advanced software security applications are now relied upon to identify the spam and neutralize its threat.

<sup>99</sup> For a single message, this cost is negligible, but for the aggregate of messages at a global level it is quite substantial.

The following best practices focus on filtering countermeasures:

**CN-US 11-037**

### **Anti-Malware Support**

ESSs  
ESPs & ISPs  
NZNs

Internet Service Providers and Email Service Providers should provide anti-malware software for their subscribers, when feasible.

**CN-US 11-038**

### **Spam Alerting**

ESPs & ISPs  
NZNs

Internet Service Providers and Email Service Providers should deploy current spam advisory services for their subscribers in order to reduce the chance of their computers becoming infected with botnets.

**CN-US 11-039**

### **Spam Filtering**

ESSs  
NZNs

Netizens should make use of junk mail filters in order to avoid chances of becoming infected by a botnet.

## **Reporting Abuse**

An essential aspect of fighting spam is soliciting the participation of its victims. These end users can help increase ISP knowledge by revealing which abusive messages passed through their defenses. It is precisely this type of information that can enable ISPs to make improvements.

The following best practices focus on end user reporting and the ISP's management of these reports:<sup>100</sup>

**CN-US 11-040**

### **Spam Reporting**

ESPs & ISPs  
NZNs

Netizens should make use of feedback loops to report spam in order to provide intelligence to Internet Service Providers and Email Service Providers about annoying messages so that these messages can be identified and addressed.

<sup>100</sup> For purposes of this discussion, the ISPs can be inclusive of Email service providers (ESPs).

CN-US 11-041

## Spam Reporting Center

GPMs  
Nos, ESPs &  
ISPs NZNs

Government and industry should consider providing netizens with a centralized reporting option for abusive messaging.

CN-US 11-042

## Abuse Mailboxes

ESPs & ISPs  
NZNs

Internet Service Providers and Email Service Providers should offer abuse mailboxes (e.g., abuse@company.com) for the reporting of abusive messaging activity.<sup>101</sup>

CN-US 11-043

## Disabling Abusive Accounts

NOs  
ESPs & ISPs  
NZNs

Internet Service Providers and Email Service Providers should diligently process feedback reports (e.g., FBLs) and abuse reports (e.g., messages to abuse@company.com), including those from international sources, to compile the evidence needed to prove that a hosted account is the source of spam. The offending account can then be notified and subsequently disabled, if appropriate.

CN-US 11-044

## Education Campaign for Netizens

GPMs  
ESPs & ISPs  
NZNs

Government agencies, Internet Service Providers and Email Service Providers should consider the use of community outreach in order to raise netizen awareness regarding spam identification, the dangers of opening spam messages and the available mechanisms for reporting spam.<sup>102</sup>

CN-US 11-045

## Abuse Report Administration

ESPs & ISPs  
NZNs

Internet Service Providers and Email Service Providers should perform an appropriate level of due diligence in analyzing and acting on abuse reports, up to disabling the accounts of abusive message senders, when appropriate.

CN-US 11-046

## Customer Service and Education

ESPs & ISPs  
NZNs

Internet Service Providers and Email Service Providers should work with subscribers whose computers are suspected of being infected with a botnet in order to remove malicious code from their computer, and educate subscribers on practices to keep their computers healthy.

<sup>101</sup> RFC 21 42

<sup>102</sup> E.g., posters, flyers, promotions and volunteer-led tutorials.

## 5. Conclusion

A simple truth is that, given the profound economic and other critical interdependencies between China and the United States, their mutual mistrust in cyberspace cannot be ignored. It is a very imposing impediment for their shared future.

This paper has captured the early, careful steps of a new China-U.S. Track 2 trust-building program in the cybersecurity arena. This first installment dealt with the big issue of spam pollution in cyberspace. Given the common interests of both countries regarding spam, jointly addressing this issue presented an opportunity to cautiously build trust.

The three objectives of this anti-spam bilateral initiative were achieved, as is evidenced in the (1) opening of new dialogue among subject matter experts and stakeholders, (2) achievement of a deeper understanding between both countries, and (3) development of expert-based consensus guidance for reducing spam pollution in cyberspace. Two joint overarching recommendations are presented that are actionable, and if implemented, will be effective in reducing the spam generated from both countries.

The next steps are outlined in the two recommendations and include new engagements between industry experts from both China and the U.S., as well as the consideration and voluntary implementation of best practices.

Another important part of the next steps for this initiative is for the bilateral team to conduct outreach to other countries. The important 8<sup>th</sup> step of the bilateral process is to engage the broader worldwide community of subject matter experts and other stakeholders. Participants from both countries are committed to supporting this activity and have developed a plan to conduct this outreach. One of the purposes of this outreach is to encourage the adoption of these consensus best practices, as appropriate. The public availability and distribution of this report is in itself a key part of this outreach. As such, the announcement of the report's availability has already begun prior to final publication, and the reception to this news by experts and stakeholders has been very encouraging.<sup>103</sup>

---

<sup>103</sup> *First China-U.S. Effort to Fight Spam*. <http://www.ewi.info/first-china-us-effort-fight-spam>, Orlando, Florida, February 23, 2011. The forthcoming availability of this Report was announced at the 21<sup>st</sup> General Meeting of the Messaging Anti-Abuse Working Group (MAAWG). The announcement was made in a special presentation jointly prepared by the lead authors. The international audience of spam-fighting was on the order of 400 experts and other stakeholders.



## Biographies

### *About the Authors*

#### KARL FREDERICK RAUSCHER



Karl F. Rauscher is Chief Technology Officer and a Distinguished Fellow at the EastWest Institute, serving its mission to convene conversations, reframe issues and mobilize resources for a safer and better world. He led the IEEE Reliability of Global

Undersea Communications Cable

Infrastructure (ROGUCCI) Study, which provides guidance for improving the resilience of the critical international infrastructure that underpins the Internet. Karl recently served as the Executive Director of the Bell Labs Network Reliability & Security Office of Alcatel-Lucent and is a Bell Labs Fellow, cited for the first achievement of “6 9’s” for a public network system (i.e. 99.9999% uptime), for being instrumental in shaping the post-September 11, 2001 U.S. strategy for communications infrastructure protection, and for being at the forefront in the development of hundreds of world-recognized consensus best practices. Karl has 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 (NSTAC) industry executive committee and as leader of the European Commission-sponsored study on the Availability and Robustness of Electronic Communications Infrastructures (ARECI), whose guidance is serving as a catalyst for European information and communications technology security. Karl serves as the chair-emeritus of the IEEE Communications Quality & Reliability (CQR) advisory board, which has advised the International Olympic Committee on ultra-high reliability and security.

#### ZHOU YONGLIN



ZHOU Yonglin is the Director of Network and Information Security Committee, Internet Society of China. Also, he is leading the Operation and Administration department of CNCERT/CC, the national computer emergency response team of China. He graduated from Harbin Institute of Technology (HIT) of China in 1999 with master

degree of computer science. Now he has been working on network security for about 12 years. He has led or joined tens of projects on network security monitoring, vulnerability handling and malware analysis. Leading his team, he works closely with government, ISPs, ICPs, domain name registrars, security service providers and product vendors on cybersecurity threat and incident watching and response, especially makes great efforts on stopping spam, botnet and DDos attacks. The recently industry collaboration they initiated include Anti-Network-Virus Association (ANVA) and China National Vulnerability Database (CNVD), from which the quickly growing Internet industry and users in China could get timely, trusted and professional assistance. Mr. Zhou has been invited to work as technical consultant and part-time professor by government and universities. He is the Member of National 863 Project Evaluation Expert Group which organized by the Ministry of Science and Technology of China to help review the project application and evaluate the results. In 2008, he was invited as an Information Network Security Advisor of Beijing Olympic Games Organizing Committee. He has published tens of papers around his research area. He has actively joined international cooperation on network security and given presentations at many conferences.

## Contributing Subject Matter Experts

### **Jeffery A. Ames, Chief Technical Officer (CTO), Original member of Switch Communications Group, LLC**

Jeff is Chief Technical Officer (CTO) and an original member of Switch Communications Group, LLC, the premier data center and Network Access Point (NAP). Using high-speed Electro-optic systems for the Department of Energy during the 80's in support of Lawrence Livermore Labs and the Nevada Test Site: Jeff was Field Administrator for the photonics research team responsible for the diagnostics and data acquisition of specialized weapons testing. After leaving the government Jeff ran a program to expand a small emerging technology companies in Nevada in conjunction with the Small Business Administration. Jeff participated in designing and integrating information systems for high-tech environments such as Motorola, DOE, DOT, U.S. Bureau of Reclamation, Department of Forestry, Lawrence Livermore Laboratory. In 1993 Jeff formed the first Internet Service Provider (ISP) in Nevada. Jeff sat on the first VAR advisory council for Netscape, helped several ISP's and web productions companies get started. Jeff wrote the City of North Las Vegas Fiber Infrastructure plan, was manager of the broadband R&D Lab and Methods and Procedures Program at a national CLEC, served Sierra Pacific Communications (SPC) as Director of Customer Engineering Services and New Business Development, and also worked with Cox Communications in the Business Services division. Jeff also chair several Technology Advancement and Advisory Boards and supports several non-profit organizations and commercial companies technical programs.

### **Monica Chew**

Monica Chew is a Gmail spam engineer at Google. She is an expert in spam, phishing and email authentication. Prior to working on Gmail she developed Google Safe Browsing and has also done work linking malware and ad click fraud. She is also interested in policy and usability issues. She holds a PhD in computer security from the University of California at Berkeley and a Master of Music in piano performance from the San Francisco Conservatory of Music.

### **Gib Godwin, Vice President, Naval Systems Integration of Defense Systems Division, Northrop Grumman Information Systems**

Gib Godwin, Vice President of Cybersecurity and Systems Integration, is leveraging his expertise in acquisition and military information systems to emerge as a thought-leader and innovator in the development of new approaches to cyber-assurance for the Defense Systems and Defense Technology Divisions within NGIS. In this role, he oversees a cross-sector collaboration effort designed to capitalize on the synergies of sector situational awareness, communication and mutual support. In turn, this expands business opportunities, leverages the strengths of individual sectors, provides a single voice to the customer and furthers One Northrop Grumman initiatives. Previously, Mr. Godwin served as vice president at Dynamic Analytics and Test in its Modeling Simulation and Analysis business. He held a similar role at Athena Technologies, where his responsibilities encompassed FAA certification and life cycle support of the entire product line of navigation and control systems for manned and unmanned systems, which Athena supported in production. Mr. Godwin holds a Bachelor of Science degree in civil engineering from Tulane University, and he is PM Level 3 certified by the Defense Acquisition University.

### **Stuart Goldman**

Stu Goldman brings over 45 years of information and communications technology experience. His corporate experience includes ITT, AGCS, Lucent, and then Alcatel-Lucent. Stu has served as an advisor for special communications needs of the U.S. government and is a lifetime Bell Labs Fellow. Stu has been granted 28 US patents, with 52 additional patent applications pending. His positions have included serving as Chair of the Alliance for Telecommunications Industry Solutions (ATIS) Packet Technologies and Systems Committee (PTSC) Interoperability (IOP) subcommittee, Chair of the ATIS Network Interoperability Forum (NIIF), Vice Chair of the ATIS PTSC Signaling, Architecture, and Control (SAC) subcommittee, Co-Chair of the ATIS Network Interconnection Interoperability Forum (NIIF), and various roles within the ITU-T SG 11, Internet Engineering Task force (IETF). Stu has participated in the European Commission-chartered Availability and Robustness of Electronic Communications Infrastructures ARECI Study, the U.S. President's National Security Telecommunications Advisory Committee (NSTAC), and a study for the Australian Attorney's General office.

### **HAN Song**

Mr. Han Song, Director of Hichina Emergency Response Team, graduated from the Beijing Jiaotong University, MBA and is a veteran of the Chinese Internet industry, with more than ten years experience in Internet industry technology and management. He currently serves as an expert of the Anti-spam Integrated Processing Platform Project Team of

Internet Society of China, is a member of Self-discipline Working Committee of Internet Society of China, and is a vice president of the Internet branch of the Beijing Communication Industry Association. Mr. Han Song, who has served many well-known Internet companies and worked for HiChina since 2002, is currently the director of Hichina Emergency Response Team, responsible for emergency handling on network security and information security, emergency management of HiChina, and regulation on illegal information in websites and domain names of HiChina's clients. He has been strongly committed to cleaning Internet environment affairs such as anti-spam, anti-phishing sites. Mr. Han Song has been invited to be an expert many times, on behalf of the company, involved in the formulation and modification of national policies and regulations, such as: "Measures for Administration of Email Service on Internet," "Measures for the Administration of Communication Network Security Protection," "Measures for Information Reporting of Internet Security," and "Contingency Plan for Domain System Security." His excellent work won the full trust of and high recognition from government departments including the Ministry of Industry and Information Technology, the China Academy of Telecommunication Research of MIIT, the Ministry of Public Security, and the Internet Society of China, among others.

#### **HU Anting**

Hu Anting graduated and obtained his Master's degree from the Department of Computer Science and Technology at the China University of Petroleum in 2002. He went on to join in the Anti-spam Committee of Internet Society of China in 2005 and from there he began to be devoted to the practice and research work of anti-spam. At present, he holds the office of Vice Director of the Anti-Spam Center of Internet Society of China. During this period, he participated in and put the Anti-Spam Platform of ISC into practice, which is the first authoritative platform in China. At the same time, he submitted the "Proposal for the Architecture and Interface Reference Model of Anti-Spam Processing System to the plenum of ITU-T SG17," which was finally adopted as an international standard. He also made a remarkable achievement in conducting exchanges and cooperation with international anti-spam organizations. Before this, Hu ever worked in the China Internet Network Information Center (CNNIC). He performed and opened the Email System of Chinese Domain Name, which is the first email system in line with IETF's International Domain Name of international standards. He issued some dissertations such as the Technical Solutions for Chinese Domain Name Mail. And he also took an active part in research on international domain names and the work of setting international standards.

#### **JIN Xuan**

JIN Xuan, BSc in Electronics and Communications Engineering, joined Tencent in 2007 as an Information Security Strategy Expert. Jin is engaging in research, planning and communication work related to information security and Internet industry, and is actively involved in numerous research programs that promote the development of Internet industry in China. Jin also has rich field experience in development planning, perfection of laws & regulations, establishment of industrial norms and policy-making for the Internet industry in China.

#### **LI Hongyu**

Hongyu Li is Chief Technology Officer of 263 Network Communications Co., Ltd. and is responsible for all products and R&D center business affairs in data communications. He is skilled in email and anti-spam. Moreover, he is responsible for anti-spam issues of the National 863 Plan.

#### **LIANG You**

Ms. LIANG You obtained an M.Eng. Degree from Beijing University of Posts & Telecommunications at Computer Communication in 1993, and obtained the B.Sc. degree from Wuhan University at Radio & Electronics in 1986. She has over 18 years of professional experience on IP and data network operations and maintenance, and in the telecom network security area. Currently, Liang works for Network Operation and Maintenance Dept. of China Unicom as Director of Internet Division. Before her current position, she was the Director of Data Network Division of Operation & Maintenance Dept. in the China Network Communication Group (CNC Group), responsible for the IP & data network operations, maintenance, security and management from 2002 to Dec. 2008. Before working for the CNC Group, she worked for Nortel networks (China) Limited as a Senior Engineer of Global Technical Support of Data Network from 1999 to 2002. From 1993 to 1999, she worked for the Beijing Telegraphic Office of Beijing Telecom Administration as the manager of the data network management center. Ms. Liang has rich experience in IP network operations, maintenance and network and information security. She has participated in many important telecommunication network security guarantee activities. She was a member of the Safeguard Expert Group of Network & Information Security for the 2008 Olympic Games in Beijing.

**LIN Jin**

Parco Lin, an expert at Tencent Ltd QQ Mail Center, has worked for eight years on large-scale email system operations and master disposing anti-spam strategy. Unlike traditional anti-spam strategies, this idea rests on the favor or antipathy of recipients. QQMail is one of the email service providers with the least spam.

**LIU Deliang**

Dr. Deliang Liu is the professor of Law School in Beijing Normal University (BNU). He is also the founder and the director of Asia-Pacific Institute for Cyber-law Studies (<http://www.apcyber-law.com>); a researcher in the Internet Legal Research Center, Peking University; and China's chief legal expert in China-EU Information Society Project. Liu has been a visiting scholar at the London School of Economics and Political Science, Edinburgh University and Advanced Legal Research Institute of London University, and an arbitrator of Chinese E-commerce Online Expert Arbitration Commission; a member of the committee of the legislation expert commission on Cyber and Information in Beijing, Shanghai and Guangdong; invited expert of High and New Technology and Intellectual Property Commission in All China Lawyers Association; a member of the committee of the legislation seminar of Ministry of Information Industry of PRC, Ministry of Industry and Information Technology of PRC and Beijing Internet and Information legislation; and a legal expert of network governance of the Political and Judiciary Commission under the Central Committee of the Communist Party of China. With a focus on civil and commercial law, Liu has published more than 60 papers in academic journals, as well as three monographs, and led five research projects at the national, provincial and ministerial levels, such as the National Social Science Foundation of China, National 242, Humanities Social Science Foundation of Ministry of Education and Ministry of Justice. Professor Liu has a unique perspective in the fields of cyber and e-commerce Law, information law and information property, telecommunication law and intellectual property in the Internet age. He is the authoritative expert in fields of cyber law and e-commerce law in China and has been invited to make suggestions for the legislations of cyber, e-commerce and information in Shanghai, Guangdong and Beijing. His paper "The Protection of Property Rights in Personal Information" (Legal Research, 2007.3) first proposed the theory of the protection of property rights of personal information in China, and his doctoral dissertation "The Protection of Property Rights in Personal Information" is the first academic monograph that systematically researched the topic. His "Civil Law Issues in the Network Age" (People's Court Press, version 2004) is the first monograph on basic civil theoretical issues in the network age in the field of civil law. Liu has been interview by well-known medias outlets including: China Central Television, China Education Television, Central People's Broadcasting Station, China Radio International, Guangming Daily, People's Daily, Xinhua News Agency, China Legal Daily, Procuratorial Daily, People's Court News, Hong Kong "South China Morning Post," "Mirror" and *The New York Times*, *USA Radio International*, *The Christian Science Monitor*, *Mai Qi Newspaper*, *The Financial Times*, *Le Figaro*, Italy's *Southern Weekly*, Japan's *Sankei Shimbun*, and Al Jazeera. Professor Liu has also been a special guest and keynote speaker at international academic conferences on cyber and information law in Europe and America.

**MA Xiaowen, Senior System Architect**

Ma Xiaowen is an expert in computer architecture design and system analysis, and has had ten years of programming experience in the software industry. He is currently responsible for the management and development of the HiChina Post Office. He participated in and took charge of several HiChina system architecture designs and products, such as HiChina SMS system, B2B business platform, domain name registration system, and HiChina production control system. Ma is proficient in many computer languages, Linux system kernel and Linux file system. He is devoting himself to mail system technology and research, and leading his R&D team to overcome difficulties in storage, anti-spam, anti-virus, and safe and robust delivery, so as to make HiChina's mail system the best in the industry. He is in charge of the HiChina Cloud Mail System, the first version of which was recently released to great success.

**Ramses Martinez**

Ramses Martinez is the Director of Information Security of VeriSign Inc. In this role Mr. Martinez leads the team that is responsible for all aspects of information security strategy, policy and operational work required to protect the global DNS infrastructure for the .net, .com, .tv, .cc and .gov domains. This team is also responsible for the protection of the global DNSsec cryptographic key management, signing and distribution infrastructure operated by VeriSign. For the last fifteen years Mr. Martinez has worked with a number of U.S. and international companies creating security programs and developing solutions to protect IT network infrastructure. This work includes designing and implementing complex systems that deal with SPAM, malware and other network based attacks. Mr. Martinez also has over ten years of experience working with international law enforcement and the intelligence community in the investigation of cybercrime cases, including some very high profile botnet takedowns. Prior his private sector experience, Mr. Martinez served for six years in the US Navy. Mr. Martinez is a board member of the anti-phishing working group (APWG) and of the IT-ISAC. He is also actively involved as a speaker and cybercrime advisor in a number of security and policy organizations like Council of Europe, the Forum for Incident Responders (FIRST) and

the Digital Crimes Consortium. Mr. Martinez holds an MS degree in information assurance and a bachelor's degree in Computer Science.

**Patrick McDaniel, Associate Professor of Computer Science and Engineering, Pennsylvania State University**

Patrick McDaniel is the co-director and founder of the Systems and Internet Infrastructure Security Laboratory, an Associate Professor of Computer Science and Engineering at The Pennsylvania State University, and an Adjunct Professor of The Stern School of Business at New York University. Before coming to Penn State, he was a senior technical staff member at AT&T-Research. Professor McDaniel's research focuses on network and computer security. This research has led to major publications in, among others, telecommunications security, secure routing and address management, formal security policy, digital rights management, and distributed systems security. Patrick is active in the academic security research community. He has authored over 100 books, papers, and reports and given over 100 invited talks. Patrick is the editor-in-chief of the ACM Journal Transactions on Internet Technology (TOIT), and serves as associate editor of the journals ACM Transactions on Information and System Security, IEEE Transactions on Software Engineering, and IEEE Transactions on Computers. He has served as the technical program chair for several leading conferences in computer security including the IEEE Symposium on Security and Privacy and the USENIX Security Symposium, and participated in over 50 program committees in the last five years.

**Robert (Jack) Oslund**

Jack Oslund has over 40 years of experience in government, industry and academia in the areas of national security and international communications. Oslund holds a Ph.D. in International Studies from the School of International Service of the American University. He was a faculty member at the National Defense Intelligence College, was on the international staff at the White House Office of Telecommunications Policy, and has held senior management positions at the Communications Satellite Corporation. Oslund also participated in the National Security Telecommunications Advisory Committee (NSTAC) and has taught as an adjunct professor at George Washington University. He was a Senior Fellow at the University's Homeland Security Policy Institute.

**Dominic Ruffolo, Senior Director, Messaging Engineering, Comcast**

Dominic Ruffolo is Director of Messaging Engineering at Comcast. He is responsible for Comcast's messaging systems including email, voicemail, SMS and anti-abuse technologies. His contributions include the design and implementation of large-scale messaging platforms and the successful migration of over 25M email accounts – at the time the largest in Internet history. Previously, Dominic was an engineer at Bell Laboratories – Lucent Technologies where his team focused on broadband access technologies. During his tenure, Dominic supported the introduction of one of the first commercial deployments of fiber-to-the-home and helped secure several large scale broadband services engagements. Many of the associated tools and methodologies that were developed became the basis for publications or patents. Dominic also served as an engineer and manager at AT&T. He was responsible for infrastructure and monitoring of the company's national communications network. He also developed design requirements for new network technologies. Dominic earned bachelor degrees in Electrical Engineering and Physics from Widener University, and his master's degree in Electrical Engineering from Clemson University.

**Greg Shannon, Chief Scientist, CERT® Program, Software Engineering Institute, Carnegie Mellon University**

Dr. Greg Shannon is the chief scientist for the CERT® Program at Carnegie Mellon University's Software Engineering Institute, a Federally Funded Research and Development Center. In this role, he works with CERT management and staff to establish and enhance CERT's research visibility, initiatives, strategies, and policies. Outside of CERT, he works to influence national research agendas and promote the data-driven science of cyber security. Prior to joining CERT, Dr. Shannon was the chief scientist at two startups (CounterStorm, and Science, Engineering and Technology Associates.), where he worked on insider threats, the science of cyber security, and statistical anomaly detection. In earlier positions, Dr. Shannon led applied research and development efforts in cyber security and data analysis at Lucent Technologies, Lumeta, Ascend Communications, Los Alamos National Laboratory, Indiana University, and his own startup company. Dr. Shannon received a BS in Computer Science from Iowa State University with minors in Mathematics, Economics, and Statistics. He earned both his MS and PhD in Computer Sciences at Purdue University, on a fellowship from the Packard Foundation.

**Fred Stringer**

Fred Stringer is a Security Systems Engineer and Network Architect in AT&T's Chief Security Office. He designs systems for the protection of the AT&T's customers and the network infrastructure. Mr. Stringer has extensive experience with AT&T's packet networks, having worked on X.25 through Frame Relay and ATM. He is one of the founding engineers of AT&T's common IP backbone network. During a nine year break in Fred's AT&T career, he was a Consulting Engineer with Juniper Networks, defining high performance routers for the carrier markets. His work

on network vulnerability assessments and Cybersecurity best practices with NRIC's (Network Reliability and Interoperability Council) instilled in him a passion to contribute to the security of the Internet and AT&T has enabled that work. Fred was appointed a Bell Laboratories Distinguished Member of Technical Staff for his work on data network design tools, methods and practices. In addition to his work on network security Fred worked extensively in systems architecture for reliability and network availability.

#### **SU Zhisheng**

Su Zhisheng obtained B.Sc and M.Sc. degrees from the Beijing University of Posts and Telecommunications, from 1998 to 2002. He currently works for China Telecom in the network maintenance department, and is responsible for the infrastructure architecture of Internet network security. He is an experienced network security architect, and adept at strategic planning and network security operations.

#### **TIAN Fei**

Dr. Tian is the Doctor of System Engineering and Manager of the Anti-Spam Department of 263 Network Communication Company. He concentrates on the anti-spam efforts of the 263 Network Communication Company, especially the spam emails sent to and from enterprise email service providers. He is also responsible for developing the work of the NASP (National Anti-spam Service Platform).

#### **WANG Mingda**

Mingda Wang is a Linux system administrator of at NetEase.com, Inc. He has over ten years of professional experience on different areas of the Internet. He aims to build a bigger, faster and more reliable website.

#### **Jody R. Westby**

Drawing upon a unique combination of more than twenty years of technical, legal, policy, and business experience, Jody Westby provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, cybercrime, breach management, forensic investigations, and IT governance. She also serves as Adjunct Distinguished Fellow for Carnegie Mellon CyLab. Ms. Westby is a member of the bars of the District of Columbia, Pennsylvania, and Colorado and serves as chair of the American Bar Association's Privacy and Computer Crime Committee. She co-chairs the World Federation of Scientists' (WFS) Permanent Monitoring Panel on Information Security and is a member of the ITU Secretary-General's High Level Experts Group on Cybersecurity. Ms. Westby led the development of *the ITU Toolkit on Cybercrime Legislation* is an editor and co-author of the 2010 WFS-ITU publication, *The Quest for Cyber Peace*. Ms. Westby is also co-author and editor of four books on privacy, security, cybercrime, and enterprise security programs. She speaks globally and is the author of numerous articles. B.A., summa cum laude, University of Tulsa; J.D., magna cum laude, Georgetown University Law Center; Order of the Coif.

#### **Dr. Weider D. Yu**

Dr. Weider D. Yu is an associate professor in the Computer Engineering Department at San Jose State University, San Jose (Silicon Valley), California. Dr. Yu performs his teaching and research activities in the areas of communication software quality and security, mobile-based and web-based software engineering, web service security and privacy, security engineering, distributed systems, e-Healthcare and mobile-Healthcare technologies. He received an M.S. in Computer Science from the State University of New York at Albany, and a Ph.D. from Northwestern University in Electrical Engineering and Computer Science. He also attended the MBA program in the Graduate School of Business at University of Chicago and received a certificate in information security engineering from Carnegie Mellon University. Prior to the university, Dr. Yu was a Distinguished Member of Technical Staff at Bell Laboratories and an adjunct associate professor in the department of Electrical Engineering and Computer Science, University of Illinois at Chicago.

#### **XU Yuan**

Ms. XU Yuan obtained a Bachelor degree in Information and Computer Science at the Beijing University of Posts and Telecommunications in 2005. Then, she studied at Linkoping University in Sweden, majoring in Communications and Interactivity. After receiving an M.S., Xu worked at the Network and Information Security Committee of the Internet Society of China, and was mainly engaged in the field of network security research in emergency response and international cooperation. She organized and participated research projects including "Guide on Policy and Technical Approaches against Botnet" in the APEC Telecommunications Working Group and "Global Cybersecurity Agenda" with the ITU.

**Jason Zabek, Manager, Customer Safety, Cox Communications**

Mr. Zabek is currently Customer Safety Manager at Cox Communications, the United States' 4<sup>th</sup> largest cable provider. He spent five years at the Cox office in Orange County California running the mail server and DNS servers for their business customers along with technical support for their high-end (fiber) customers. In 2003, he was offered a position at the Cox Corporate office in Atlanta, Georgia, managing the Customer Safety team where the company sets and enforces its high-speed data use policy, working closely with law enforcement and assisting customers in cleaning infected machines. Mr. Zabek is a contributor to the Anti-spam Working Group, which includes security teams and mail administrators who discuss ways to fight spam. He has been a member of the Messaging and Anti-Abuse Workgroup for 6 years and member of Infragard for the past 4 years (Infragard is a joint venture between the FBI and private business to stop online fraud). He is Cisco and Juniper certified. With many years of hands-on experience fighting spam and online fraud, his best asset is knowing what happens in the real world to real customers.

**ZENG Mingfa**

Mr. Mingfa Zeng, Director of the Anti-Spam Center and Vice Director of 12321 Reporting Center of the ISC (Internet Society of China), is a senior Internet security expert. He devotes himself to working against spam and other harmful information on the Internet. Similar to the method of the legendary Chinese ancestor Da Yu who fought against the pre-historic flood, Mr. Zeng believes that to assure Internet security and cleanliness we should "dredge or block" according to the specific situation. Since 2003, Mr. Zeng has been engaging in anti-spam and anti-harmful information activities by participating in and organizing large-scale, high-end conferences and forums. In 2004, Mr. Zeng built the ISC's anti-spam website ([www.anti-spam.cn](http://www.anti-spam.cn)) and participated in the formulation of juristic regulations, as well as setting technical standards both domestically and internationally. Mr. Zeng has been covered by media including CCTV, People's Daily, Sina, Sohu, Netease and CCID. As a member of the Chinese delegation, Mr. Zeng attended the Internet Governance Forum (IGF) of UN in Brazil in 2007, where he shared China's experience on anti-spam work. Mr. Zeng has made positive contributions to the process of building China's green network.

**ZHAO Liang**

Dr. Richard Zhao obtained his B.S., M.S. and PhD degrees from Peking University in 1991, 1994, 1997 respectively, majoring in physics and fiber-optic communications. He has over 13 years of professional experience on telecommunications and network security areas. He owns certifications in CISSP, ITIL and BS7799. Currently, he works for NSFOCUS as the Chief Strategy Officer. Before his current position, he was the Director of Architect and Security Operations at Lenovo, responsible for infrastructure architecture and information security operations from 2006 to August 2009. Before Lenovo, he worked for Computer Associates as the Principal Consultant at China from 2003 to 2006. From 2000 to 2003, he worked for iS-One as Chief Strategy Officer, responsible for R&D and the security consulting service. From 1997 to 2000, he worked for China Telecom, as the chief of network security affairs. Dr. Zhao is an active contributor to the Cloud Security Alliance and an initiator of the Greater China Chapter of CSA. His research interests include information security metrics, cloud computing and security, and security compliance.. More details about his career and thoughts could be found on LinkedIn (<http://www.linkedin.com/in/zhaol>) and on his blog at <http://sbin.cn/blog>.

## ACRONYMS

8i	Eight Ingredient (Framework of ICT Infrastructure)
APCAUSE	Asia Pacific Organization on Anti-spam
ARPA	Address Routing and Parameter Area
AS	Autonomous System
ASPR	Agreements, Standards, Policies and Regulations
AUP	Acceptable Use Policy
BGP	Border Gateway Protocol
BPs	Best practices
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CNCERT/CC	National Computer Network Emergency Response Technical Team/Coordination Center of China
EWI	EastWest Institute
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Email
DNS	Domain Name Server
DNSBL DNS	Black List (or Block List or Black hole)
EHLO	Extended Hello (an SMTP Command)
ESMTP	Extended SMTP
ESS	Equipment and Software Suppliers
EWI	EastWest Institute
FBL	Feedback Loop
FIRST	Forum of Incident Response and Security Teams
FQDN	Fully Qualified Domain Names
GPM	Government Policy Maker



GSM	Global Systems Mobile
GSMA	GSM Association
HELO	Hello (an SMTP Command)
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIA	Internet Industry Association (Australia)
IMAP	Internet Message Access Protocol
ISC	Internet Society of China
ISP	Internet service provider
ITU	International Telecommunications Union
HTML	Hypertext Markup Language
MAAWG	Messaging Anti-Abuse Working Group
MoU	Memorandum of Understanding
MTA	Mail Transfer Agent
MX	Mail Exchange
NO	Network Operator
NGO	Non-Government Organization
NRIC	Network Reliability and Interoperability Council
NZN	Netizen
OECD	Organization for Economic Cooperation and Development
PC	Personal Computer
POP	Post Office Protocol
PPP	<i>Private</i> -Public Partnership
PPP	Public-Private Partnership
PRC	People's Republic of China
RFC	Request for Comments

RIR	Regional Internet Registry
ROI	Return on Investment
SCIO	State Council Information Office
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol with transport layer security
SPF	Sender Policy Framework
SPIT	Spam over Internet Telephony
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
U.S.	United States (of America)
WCI	Worldwide Cybersecurity Initiative
WHOIS	The query and response protocol documented in RFC 3912
WWW	World Wide Web

## REFERENCES

- Alliance on Anti-Spam Self-Discipline Working Committee, Internet Society of China, 2005.
- ATIS Telecom Glossary, [www.atis.org](http://www.atis.org), 2007.
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 (15 U.S.C. 7701).
- Best Common Practices for Mitigating Abuse of Web Messaging Systems*, MAAWG, August, 2010.
- Blokker, Jaco, *Best Practices in Anti-Spam*, ETIS, October, 2010.
- China Internet Network Information Center (CNNIC), [www.cnnic.net.cn](http://www.cnnic.net.cn).
- Complaint Feedback Loop Best Current Practice*, MAAWG, April, 2010.
- Conficker Working Group, [conficjerworkinggroup.org](http://conficjerworkinggroup.org).
- Cranor, Lorrie Faith and LaMacchia, Brian A. *Spam!* Communications of the ACM. Vol. 41, No. 8, August 1998.
- Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, White House, 2009.
- Daigle, L., RFC 3912, WHOIS Protocol Specification, IETF, September, 2004.
- Fighting Internet and Wireless Spam Act (FISA)*, Bill C-28, Canada, 2010.
- Gross, Grant, "Is the CAN-SPAM Law Working?". PC World. Retrieved March 21, 2009.
- Global Threat Trend Analysis*, 1H 2010, Trend Micro TrendLabs, 2010.
- GSM Association, [www.gsmworld.com](http://www.gsmworld.com)
- Internet in China, The*, Information Office of the State Council of the People's Republic of China, June, 2010, Beijing.
- Kigerl, Alex C. (December 2009), "CAN SPAM Act: An Empirical Analysis", International Journal of Cyber Criminology 3 (2): 566–589
- Klensin, J., RFC 5321, Simple Mail Transfer Protocol, IETF, October, 2008.
- Lindberg, G., RFC 2505, Anti-Spam Recommendations for SMTP MTAs, IETF, February, 1999.
- M86 Security, *Security Labs Report*, January 2010.
- McMillan, Robert, *China Cleans Up Spam Problem*, PCWorld, February 2011.
- Measures for the Administration of Internet Email Services*, MIIT, Beijing, 2006. <http://miit.gov.cn/n11293472/n11294912/n11296542/12165060.htm>
- MessageLabs Intelligence: 2010 Annual Security Report, MessageLabs, 2010.

Messaging Anti-Abuse Working Group, MAAWG, [www.maawg.org](http://www.maawg.org)

*NSTAC Report to the President on International Communications*, The President's National Security Telecommunications Advisory Committee (NSTAC), August, 2007.

OECD Anti-Spam Toolkit

Palmer, Maija, *Secret War on Web Crooks Revealed*, Financial Times, June 14, 2009.

*Policy of Trojan and Botnet Handling Mechanisms*, Internet Society of China, 2009.

Rauscher, Karl F., *Availability and Robustness of Electronic Communications Infrastructures (ARECI) Final Report*, European Commission, March 2007.

Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal – Special Issue: Homeland Security, Volume 9, Issue 2, 2004.

Rauscher, Karl F., Krock, Richard E., Runyon, James P., *Eight ingredients of communications infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security*, Bell Labs Technical Journal, Volume 11, Issue 3, 2006.

Seitzer, Larry, *How Microsoft Took Down Rustock*, PCMag.com, March 2011.

Seoul-Melbourne Anti-Spam Agreement, 2005.

Shannon, Claude E., *A Mathematical Theory of Communication*, Bell System Technical Journal, 1948.

Spamcop.net

Spamhaus Project, The, [www.spamhaus.org](http://www.spamhaus.org)

Spam Reporting Center, Internet Society of China.

SpamLinks.com

*U.S.-China Joint Statement*, White House, Office of the Press Secretary, 19 January 2011. [www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement](http://www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement)

*\*Several subject matter experts were consulted who requested to remain anonymous.*

## **APPENDIX A. U.S.-China Joint Statement, 19 January 2011**

### **The White House Office of the Press Secretary Washington, D.C.**

1. At the invitation of President Barack Obama of the United States of America, President Hu Jintao of the People's Republic of China is paying a state visit to the United States of America from January 18-21, 2011. During his visit, President Hu met with Vice President Joseph Biden, will meet with U.S. Congressional leadership, and will visit Chicago.
2. The two Presidents reviewed the progress made in the relationship since President Obama's November 2009 State Visit to China and reaffirmed their commitment to building a positive, cooperative, and comprehensive U.S. - China relationship for the 21st century, which serves the interests of the American and Chinese peoples and of the global community. The two sides reaffirmed that the three Joint Communiqués issued by the United States and China laid the political foundation for the relationship and will continue to guide the development of U.S. - China relations. The two sides reaffirmed respect for each other's sovereignty and territorial integrity. The Presidents further reaffirmed their commitment to the November 2009 U.S. - China Joint Statement.
3. The United States and China committed to work together to build a cooperative partnership based on mutual respect and mutual benefit in order to promote the common interests of both countries and to address the 21st century's opportunities and challenges. The United States and China are actively cooperating on a wide range of security, economic, social, energy, and environmental issues which require deeper bilateral engagement and coordination. The two leaders agreed that broader and deeper collaboration with international partners and institutions is required to develop and implement sustainable solutions and to promote peace, stability, prosperity, and the well-being of peoples throughout the world.

#### **Strengthening U.S. - China Relations**

4. Recognizing the importance of the common challenges that they face together, the United States and China decided to continue working toward a partnership that advances common interests, addresses shared concerns, and highlights international responsibilities. The two leaders recognize that the relationship between the United States and China is both vital and complex. The United States and China have set an example of positive and cooperative relations between countries, despite different political systems, historical and cultural backgrounds, and levels of economic development. The two sides agreed to work further to nurture and deepen bilateral strategic trust to enhance their relations. They reiterated the importance of deepening dialogue aimed at expanding practical cooperation and affirmed the need to work together to address areas of disagreement, expand common ground, and strengthen coordination on a range of issues.
5. The United States reiterated that it welcomes a strong, prosperous, and successful China that plays a greater role in world affairs. China welcomes the United States as an Asia-Pacific nation that contributes to peace, stability and prosperity in the region. Working together, both leaders support efforts to build a more stable, peaceful, and prosperous Asia-Pacific region for the 21st century.
6. Both sides underscored the importance of the Taiwan issue in U.S. - China relations. The Chinese side emphasized that the Taiwan issue concerns China's sovereignty and territorial integrity, and expressed the hope that the U.S. side will honor its relevant commitments and appreciate and support the Chinese side's position on this issue. The U.S. side stated that the United States follows its one China policy and abides by the principles of the three U.S.-China Joint Communiqués. The United States applauded the Economic Cooperation Framework Agreement between the two sides of the Taiwan Strait and welcomed the new

lines of communications developing between them. The United States supports the peaceful development of relations across the Taiwan Strait and looks forward to efforts by both sides to increase dialogues and interactions in economic, political, and other fields, and to develop more positive and stable cross-Strait relations.

7. The United States and China reiterated their commitment to the promotion and protection of human rights, even as they continue to have significant differences on these issues. The United States stressed that the promotion of human rights and democracy is an important part of its foreign policy. China stressed that there should be no interference in any country's internal affairs. The United States and China underscored that each country and its people have the right to choose their own path, and all countries should respect each other's choice of a development model. Addressing differences on human rights in a spirit of equality and mutual respect, as well as promoting and protecting human rights consistent with international instruments, the two sides agreed to hold the next round of the U.S.-China Human Rights Dialogue before the third round of the Strategic and Economic Dialogue (S&ED).

8. The United States and China agreed to hold the next round of the resumed Legal Experts Dialogue before the next Human Rights Dialogue convenes. The United States and China further agreed to strengthen cooperation in the field of law and exchanges on the rule of law. The United States and China are actively exploring exchanges and discussions on the increasing role of women in society.

9. The United States and China affirmed that a healthy, stable, and reliable military-to-military relationship is an essential part of President Obama's and President Hu's shared vision for a positive, cooperative, and comprehensive U.S.-China relationship. Both sides agreed on the need for enhanced and substantive dialogue and communication at all levels: to reduce misunderstanding, misperception, and miscalculation; to foster greater understanding and expand mutual interest; and to promote the healthy, stable, and reliable development of the military-to-military relationship. Both sides noted the successful visit of Secretary of Defense Robert Gates to China earlier this month, and that the United States welcomes Chief of the PLA General Staff General Chen Bingde to the United States in the first half of 2011. Both sides reaffirmed that the Defense Consultative Talks, the Defense Policy Coordination Talks, and the Military Maritime Consultative Agreement will remain important channels of communication in the future. Both sides will work to execute the seven priority areas for developing military-to-military relations as agreed to by Secretary Gates and General Xu Caihou, Vice Chairman of the Central Military Commission in October 2009.

10. The United States and China agreed to take specific actions to deepen dialogue and exchanges in the field of space. The United States invited a Chinese delegation to visit NASA headquarters and other appropriate NASA facilities in 2011 to reciprocate for the productive visit of the U.S. NASA Administrator to China in 2010. The two sides agreed to continue discussions on opportunities for practical future cooperation in the space arena, based on principles of transparency, reciprocity, and mutual benefit.

11. The United States and China acknowledged the accomplishments under the bilateral Agreement on Cooperation in Science and Technology, one of the longest-standing bilateral agreements between the two countries, and welcomed the signing of its extension. The United States and China will continue to cooperate in such diverse areas as agriculture, health, energy, environment, fisheries, student exchanges, and technological innovation in order to advance mutual well-being.

12. The United States and China welcomed progress by the U.S.-China Joint Liaison Group on Law Enforcement Cooperation (JLG) to strengthen law enforcement cooperation across a range of issues, including counterterrorism. The United States and China also agreed to enhance joint efforts to combat corruption through bilateral and other means.

### **Promoting High-Level Exchanges**

13. The two sides agreed that high-level exchanges are indispensable to strong U.S.-China relations, and that close, frequent, and in-depth dialogue is important to advance bilateral relations and international peace and development. In this spirit, both Presidents look forward to meeting again in the coming year, including in the state of Hawaii for the U.S.-hosted 2011 Asia-Pacific Economic Cooperation (APEC) Leaders' meeting. China welcomed Vice President Biden for a visit in 2011. The United States welcomed a subsequent visit by Vice President Xi Jinping.

14. The two sides praised the S&ED as a key mechanism for coordination between the two governments, and agreed to hold the third round of the S&ED in Washington, D.C., in May 2011. The S&ED has played an important role in helping build trust and confidence between the two countries. The two sides also agreed to hold the second meeting of the High-Level Consultation on People-to-People Exchange in the United States in the spring of 2011, and the 22nd meeting of the U.S.-China Joint Commission on Commerce and Trade (JCCT) in China in the second half of 2011. The two sides agreed to maintain close communication between the foreign ministers of the two countries through mutual visits, meetings, and other means.

15. The two sides emphasized the importance of continued interaction between their legislatures, including institutionalized exchanges between the National People's Congress of China and the U.S. Senate and House of Representatives.

### **Addressing Regional and Global Challenges**

16. The two sides believe that the United States and China have a common interest in promoting peace and security in the Asia-Pacific region and beyond, and agreed to enhance communication and coordination to address pressing regional and global challenges. The two sides undertake to act to protect the global environment and to work in concert on global issues to help safeguard and promote the sustainable development of all countries and peoples. Specifically, the United States and China agreed to advance cooperation to: counter violent extremism; prevent the proliferation of nuclear weapons, other weapons of mass destruction, and their means of delivery; strengthen nuclear security; eliminate infectious disease and hunger; end extreme poverty; respond effectively to the challenge of climate change; counter piracy; prevent and mitigate disasters; address cyber-security; fight transnational crime; and combat trafficking in persons. In coordination with other parties, the United States and China will endeavor to increase cooperation to address common concerns and promote shared interests.

17. The United States and China underlined their commitment to the eventual realization of a world without nuclear weapons and the need to strengthen the international nuclear non-proliferation regime to address the threats of nuclear proliferation and nuclear terrorism. In this regard, both sides support early entry into force of the Comprehensive Nuclear Test Ban Treaty (CTBT), reaffirmed their support for the early commencement of negotiations on a Fissile Material Cutoff Treaty in the Conference on Disarmament, and agreed to work together to reach these goals. The two sides also noted their deepening cooperation on nuclear security following the Washington Nuclear Security Summit and signed a Memorandum of Understanding that will help establish a Center of Excellence on Nuclear Security in China.

18. The United States and China agreed on the critical importance of maintaining peace and stability on the Korean Peninsula as underscored by the Joint Statement of September 19, 2005 and relevant UN Security Council Resolutions. Both sides expressed concern over heightened tensions on the Peninsula triggered by recent developments. The two sides noted their continuing efforts to cooperate closely on matters concerning the Peninsula. The United States and China emphasized the importance of an improvement in North-South relations and agreed that sincere and constructive inter-Korean dialogue is an essential step. Agreeing on the crucial importance of denuclearization of the Peninsula in order to preserve peace and stability in Northeast Asia, the United States and China reiterated the need for concrete and effective steps to achieve the goal of denuclearization and for full implementation of the other commitments made in the September 19, 2005 Joint Statement of the Six-Party Talks. In this context, the United States and China expressed concern regarding the DPRK's claimed uranium enrichment program. Both sides oppose all activities inconsistent with the 2005 Joint Statement and relevant international obligations and commitments. The two sides called for the necessary steps that would allow for early resumption of the Six-Party Talks process to address this and other relevant issues.

19. On the Iranian nuclear issue, the United States and China reiterated their commitment to seeking a comprehensive and long-term solution that would restore international confidence in the exclusively peaceful nature of Iran's nuclear program. Both sides agreed that Iran has the right to peaceful uses of nuclear energy under the Non-Proliferation Treaty and that Iran should fulfill its due international obligations under that treaty. Both sides called for full implementation of all relevant UN Security Council Resolutions. The United States and China welcomed and will actively participate in the P5+1 process with

Iran, and stressed the importance of all parties – including Iran – committing to a constructive dialogue process.

20. Regarding Sudan, the United States and China agreed to fully support the North-South peace process, including full and effective implementation of Sudan's Comprehensive Peace Agreement. The two sides stressed the need for all sides to respect the result of a free, fair, and transparent referendum. Both the United States and China expressed concern on the Darfur issue and believed that further, substantive progress should be made in the political process in Darfur to promote the early, comprehensive, and appropriate solution to this issue. Both the United States and China have a continuing interest in the maintenance of peace and stability in the wider region.

21. The two sides agreed to enhance communication and coordination in the Asia-Pacific region in a spirit of mutual respect and cooperation, and to work together with other Asia-Pacific countries, including through multilateral institutions, to promote peace, stability, and prosperity.

### **Building a Comprehensive and Mutually Beneficial Economic Partnership**

22. President Obama and President Hu recognized the vital importance of working together to build a cooperative economic partnership of mutual respect and mutual benefit to both countries and to the global economy. The two leaders agreed to promote comprehensive economic cooperation, and will develop further a framework of comprehensive economic cooperation, relying on existing mechanisms, by the third round of the S&ED in May, based on the main elements outlined below:

23. The two sides agreed to strengthen macroeconomic communication and cooperation, in support of strong, sustainable and balanced growth in the United States, China and the global economy:

- The United States will focus on reducing its medium-term federal deficit and ensuring long-term fiscal sustainability, and will maintain vigilance against excess volatility in exchange rates. The Federal Reserve has taken important steps in recent years to increase the clarity of its communications regarding its outlook and longer run objectives.
- China will intensify efforts to expand domestic demand, to promote private investment in the service sector, and to give greater play to the fundamental role of the market in resource allocation. China will continue to promote RMB exchange rate reform and enhance RMB exchange rate flexibility, and promote the transformation of its economic development model.
- Both sides agree to continue to pursue forward-looking monetary policies with due regards to the ramifications of those policies for the international economy.
- The two sides affirmed support for efforts by European leaders to reinforce market stability and promote sustainable, long-term growth.

24. The two countries, recognizing the importance of open trade and investment in fostering economic growth, job creation, innovation, and prosperity, affirmed their commitment to take further steps to liberalize global trade and investment, and to oppose trade and investment protectionism. The two sides also agreed to work proactively to resolve bilateral trade and investment disputes in a constructive, cooperative, and mutually beneficial manner.

25. The two leaders emphasized their strong commitment to direct their negotiators to engage in across-the-board negotiations to promptly bring the WTO Doha Development Round to a successful, ambitious, comprehensive, and balanced conclusion, consistent with the mandate of the Doha Development Round and built on the progress already achieved. The two sides agreed that engagement between our representatives must intensify and expand in order to complete the end game.

26. The two leaders agreed on the importance of achieving a more balanced trade relationship, and spoke highly of the progress made on this front, including at the recent 21st Meeting of the JCCT in Washington, D.C.

27. China will continue to strengthen its efforts to protect IPR, including by conducting audits to ensure that government agencies at all levels use legitimate software and by publishing the auditing results as required by China's law. China will not link its innovation policies to the provision of government procurement preferences. The United States welcomed China's agreement to submit a robust, second revised offer to the WTO Government Procurement Committee before the Committee's final meeting in 2011, which will include sub-central entities.



28. The two leaders acknowledged the importance of fostering open, fair, and transparent investment environments to their domestic economies and to the global economy and reaffirmed their commitment to the ongoing bilateral investment treaty (BIT) negotiations, recognizing that a successful BIT negotiation would support an open global economy by facilitating and protecting investment, and enhancing transparency and predictability for investors of both countries. China welcomed the United States' commitment to consult through the JCCT in a cooperative manner to work towards China's Market Economy Status in an expeditious manner. China welcomed discussion between the two sides on the ongoing reform of the U.S. export control system, and its potential implications for U.S. exports to its major trading partners, including China, consistent with U.S. national security interests.

29. The two sides further acknowledged the deep and robust nature of the commercial relationship, including the contracts concluded at this visit, and welcomed the mutual economic benefits resulting from the relationship.

30. The two sides agreed to continue working to make concrete progress on the bilateral economic relationship through the upcoming S&ED and the JCCT process.

31. The United States and China recognized the potential for their firms to play a positive role in the infrastructure development in each country and agreed to strengthen cooperation in this area.

32. The two countries committed to deepen bilateral and multilateral cooperation on financial sector investment and regulation, and support open environments for investment in financial services and cross-border portfolio investment, consistent with prudential and national security requirements. The United States is committed to ensuring that the GSEs have sufficient capital and the ability to meet their financial obligations.

33. The United States and China agree that currencies in the SDR basket should only be those that are heavily used in international trade and financial transactions. In that regard, the United States supports China's efforts over time to promote inclusion of the RMB in the SDR basket.

34. The two countries pledged to work together to strengthen the global financial system and reform the international financial architecture. The two sides will continue their strong cooperation to strengthen the legitimacy and improve the effectiveness of the International Monetary Fund and Multilateral Development Banks (MDBs). The two sides will jointly promote efforts of the international community to assist developing countries, in particular the Least Developed Countries to achieve the Millennium Development Goals (MDGs). The two sides will also, in partnership with the Multilateral Development Banks, explore cooperation that supports global poverty reduction and development, and regional integration including in Africa, to contribute to inclusive and sustainable economic growth.

35. The two countries reiterated their support for the G-20 Framework for Strong, Sustainable and Balanced Growth and reaffirmed their commitments made in the Seoul Summit Declaration, including using the full range of policies to strengthen the global recovery and to reduce excessive imbalances and maintain current account imbalances at sustainable levels. The two sides support a bigger role for the G-20 in international economic and financial affairs, and pledged to strengthen communication and coordination to follow through on the commitments of the G-20 summits and push for positive outcomes at the Cannes Summit.

### **Cooperating on Climate Change, Energy and the Environment**

36. The two sides view climate change and energy security as two of the greatest challenges of our time. The United States and China agreed to continue their close consultations on action to address climate change, coordinate to achieve energy security for our peoples and the world, build on existing clean energy cooperation, ensure open markets, promote mutually beneficial investment in climate friendly energy, encourage clean energy, and facilitate advanced clean energy technology development.

37. Both sides applauded the progress made in clean energy and energy security since the launch of the U.S.-China Clean Energy Research Center, Renewable Energy Partnership, U.S.-China Joint Statement on Energy Security Cooperation, and Energy Cooperation Program (ECP). Both sides reaffirmed their ongoing exchanges on energy policy and cooperation on oil, natural gas (including shale gas), civilian nuclear energy, wind and solar energy, smart grid, advanced bio-fuels, clean coal, energy efficiency, electric vehicles and clean energy technology standards.

38. The two sides commended the progress made since the launch of the U.S.-China Ten Year Framework on Energy and Environment Cooperation (TYF) in 2008. They agreed to further strengthen practical cooperation under the TYF, carry out action plans in the priority areas of water, air, transportation, electricity, protected areas, wetlands, and energy efficiency, engage in policy dialogues, and implement the EcoPartnerships program. The United States and China were also pleased to announce two new EcoPartnerships. The two sides welcomed local governments, enterprises, and research institutes of the two countries to participate in the TYF, and jointly explore innovative models for U.S.-China energy and environment cooperation. The two sides welcomed the cooperation projects and activities which will be carried out in 2011 under the TYF.

39. The two sides welcomed the Cancun agreements and believed that it is important that efforts to address climate change also advance economic and social development. Working together and with other countries, the two sides agreed to actively promote the comprehensive, effective, and sustained implementation of the United Nations Framework Convention on Climate Change, including the implementation of the Cancun agreements and support efforts to achieve positive outcomes at this year's conference in South Africa.

### **Expanding People-to-People Exchanges**

40. The United States and China have long supported deeper and broader people-to-people ties as part of a larger effort to build a cooperative partnership based on mutual respect and mutual benefit. Both sides agreed to take concrete steps to enhance these people-to-people exchanges. Both sides noted with satisfaction the successful Expo 2010 Shanghai, and the Chinese side complimented the United States on its USA Pavilion. The two sides announced the launch of a U.S.-China Governors Forum and decided to further support exchanges and cooperation at local levels in a variety of fields, including support for the expansion of the sister province and city relationships. The United States and China also agreed to take concrete steps to strengthen dialogue and exchanges between their young people, particularly through the 100,000 Strong Initiative. The United States warmly welcomes more Chinese students in American educational institutions, and will continue to facilitate visa issuance for them. The two sides agreed to discuss ways of expanding cultural interaction, including exploring a U.S.-China cultural year event and other activities. The two sides underscored their commitment to further promoting and facilitating increased tourism. The United States and China agreed that all these activities help deepen understanding, trust, and cooperation.

### **Conclusion**

41. President Hu Jintao expressed his thanks to President Obama and the American people for their warm reception and hospitality during his visit. The two Presidents agreed that the visit has furthered U.S.-China relations, and both sides resolved to work together to build a cooperative partnership based on mutual respect and mutual benefit. The two Presidents shared a deep belief that a stronger U.S.-China relationship not only serves the fundamental interests of their respective peoples, but also benefits the entire Asia-Pacific region and the world.

(Distributed by the Bureau of International Information Programs, U.S. Department of State. Web site: <http://www.america.gov>)

Source: <http://www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement>

## APPENDIX B. Sample ISP Letter to Customers

Appreciation is expressed here to Cox Communications for their making this generic letter template available. This letter is referenced by Best Practice CN-US 11-005, *Subscriber Agreement High Use Thresholds*.

Dear [Company] Internet Subscriber,

As a followup, we are sending you this email with several suggestions for Anti-Trojan, Anti-Virus and Security Software, which we and other [Company] Customers have found useful in cleaning virus and Trojan infections. This software will also help keep your computers safe from future infections. Many of us at [Company] use these programs on our personal systems, which is why we are able to recommend them.

Please be aware that even though we are suggesting these utilities for the safety of your systems, [Company] makes no guarantee that they will work and takes no responsibility for any negative affects you may incur. Unfortunately, [Company] cannot provide support for these utilities either. If you should need information or assistance for installing or using these applications, please contact the vendor/manufacturer for technical support or documentation.

No security software is 100% effective. Sometimes the use of several applications may be necessary to keep your systems safe as possible. For example, you should have one Anti-Virus Security Suite [sample products cited] and a good Spyware Removal Program [sample products cited]. Note that some Security Suites provide all of these features.

Here is a link to an article that may help you determine which Security Software is best for you: [provide web site]

[Company] provides, at NO CHARGE to our current residential subscribers, an all-in-one Security Suite. Please read this article on our Support Site for more information: [web site link]

Before you begin, be sure to back up your important data. (You should do this on a regular basis) You can back up your files manually (drag and drop) or using a System Back-up Software Utility. You can back your files up to a USB Thumb Drive (aka USB Key), a CD/DVD, an external hard drive or a network file server.

The first tool to run is the [cite product]. It has been developed by [cite vendor] to find and remove the most common viruses and Trojans used by hackers. You may download it here: [provide web site].

Update your anti-virus scanner. Most of these utilities can be updated from within the program itself so consult the help files to ensure you have the latest anti-virus definitions.

Once you've installed these utilities, run a FULL system scan and delete or quarantine any malicious spyware detected on your system. Not all spyware is malicious. For instance, tracking cookies, although annoying, are relatively harmless. Your spyware utility should inform you as to which spyware is truly harmful and which should definitely be removed. [Cite product] gives a rating on its findings, on a scale of 1 to 10. For example, anything rated 3 and below, is considered a minor threat.

[Cite product] is an anti-malware program best known for its behavioral based threat detection. It monitors the behavior of all applications and processes running on your system. It will alert you of and/or stifle any activity considered "out of the ordinary", such as outbound port scans, key logging or sending out thousands of spam emails. This is an excellent program and it works in tandem with your antivirus, anti-spyware and other security tools to give you an additional layer of protection.

[Cite product] is another anti-malware program that monitors process behaviors and protects your system from being exploited for malicious activity. It provides immediate protection, so your PC and valuable data will be better secured.

[Cite product] is also a good Anti-Malware program that detects and removes malicious software.

\*If these programs do not remove the threat(s) from your system(s), you may need to re-format and re-install your operating system\*

Some other tips to help keep you safe:

1. Use a Router with NAT (Network Address Translation).

All systems connected to a router use one public IP address to connect to the Internet. This is known as your WAN Gateway. Using a router with your cable modem will help stop unsolicited traffic from the Internet. If a hacker is trying to connect to your computer from the Internet, the connection will be denied because your computer did not request this connection. This can stop a "weekend" hacker from attacking your network and/or computer.

2. Use a Firewall.

A firewall can be software or a hardware device that monitors all incoming network traffic. It will permit traffic you have approved and deny any unsolicited traffic. A firewall can make your computer appear "invisible" to the Internet by dropping all inbound, unsolicited Internet requests. [Company] recommends using a hardware firewall behind your cable modem (or NID) and software firewalls on each computer system on your private network.

3. Enable Automatic Updates!

Make sure that your operating system is fully patched and updated.

[Vendor] issues regular patches on the second Tuesday of every month. Just about all vendors have security issues and patches are released on a consistent basis.

Here are some other helpful links:

[provide links]

More assistance is available at [provide web site] under our data - security section.

Thank you,

[Company] Customer Security





Founded in 1980, the EastWest Institute is a global, action-oriented, think-and-do tank. EWI tackles the toughest international problems by:

**Convening** for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel “Track 2” diplomacy, and also organizes public forums to address peace and security issues.

**Reframing** issues to look for win-win solutions. Based on our special relations with Russia, China, India, the United States, Europe, and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

**Mobilizing** networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) non-profit organization with offices in New York, Brussels and Moscow. Our fiercely-guarded independence is ensured by the diversity of our international board of directors and our supporters.

**EWI Brussels**  
59-61 Rue de Trèves  
Brussels 1040  
Belgium  
32-2-743-4610

**EWI Moscow**  
7/5 Bolshaya Dmitrovka Str.  
Bldg. 1, 6th Floor  
Moscow 125009  
Russia, 7-495-234-7797

**EWI New York**  
11 East 26th Street  
20th Floor  
New York, NY 10010  
U.S.A. 1-212-824-4100

[www.ewi.info](http://www.ewi.info)