中美网络安全双边行动

抵御垃圾邮件

建 立 互 信 机 制

EAST WEST INSTITUTE
Forging Collective Action for a Safer and Better World

中国互联网协会
Internet Society of China

中国互联网协会与美国东西方研究所（ISC-EWI）中美联合反垃圾邮件研究报告，第 1 期

本文件主要作者：

卡尔·弗雷德里克·劳舍尔（Karl Frederick Rauscher）

EWI 首席技术官兼特聘研究人员

周勇林

中国互联网协会网络与信息安全工作委员会秘书长

封面照片：Dragan Stojanovksi

中国互联网协会（ISC）成立于 2001 年 5 月 25 日，由国内从事互联网行业的网络运营商、服务提供商、设备制造商、系统集成商以及科研、教育机构等 70 多家互联网从业者共同发起成立。ISC 的主要任务是促进中国互联网的发展和构建先进的信息社会。ISC 希望协调行业间的合作以促进行业发展和互联网用户的利益，发挥行业自律作用，促进会员之间的沟通与协作，为政策的制定提供服务，促进互联网应用和公共意识。

关中国互联网协会的详细信息，请联系：

中国互联网协会

北京市复兴门南大街 2-B 天银大厦 A 东座，邮编 100031

电话：+86-10- 66035712

传真：+86-10- 6603571

邮箱：isc@isc.org.cn

东西方研究所（EWI）是一个国际性的、无党派、非营利性的政策研究机构，主要研究应对重大和平问题的对策。EWI 成立于 1980 年，致力于构建信任关系、提升领导能力、积极促进合作。该所在纽约、布鲁塞尔和莫斯科均设有办事机构。

有关东西方研究所的详细信息，请联系：

东西方研究所

美国纽约州纽约市东 26 街 11 号 20 层，邮编 10010

电话：1-212-824-4100

邮箱：communications@ewi.info

中国互联网协会与美国东西方研究所

网络安全双边活动

抵御垃圾邮件 建立互信机制

作者：卡尔·弗雷德里克·劳舍尔和周勇林

二零一一年六月

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World
30 YEARS

中国互联网协会
Internet Society of China

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.

序

2011 年中美两国首脑会晤上，双方承诺将不断致力于建设“21 世纪积极合作全面的中美关系，这符合两国人民和国际社会利益”，在中美联合声明中也表达了这种愿望。双方就会晤所作的联合声明进一步宣告了两国同意“加强合作以实现网络安全”的立场。

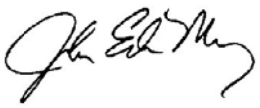
《抵御垃圾邮件建立互信机制》正是说明如何实现这个愿望的绝佳例证。这项及时的双边活动提出了具体可行的建议，如若执行，不仅对中国和美国，对其他国家也将带来直接益处。这项工作反映了对取得有效解决方案所需架构的深刻理解。执行本报告中提出的指导原则需要妥善地平衡行业和政府的力量，从而减少网络中的污染。

垃圾邮件会造成持久的损害，但其所造成的经济冲击和深远影响却被大大低估。由于经常被用作恶意代码和在线欺诈的载体，垃圾邮件对数以十亿计的电脑和网民是一个威胁。正因它关系到大家的共同利益，因此促成了双方在该领域的慎重合作。

尽管开展更多的网络空间合作还将面临很多困难，让我们稍停片刻来共同为这一世界级团队成功解决第一个困难而赞赏和鼓掌！

黄澄清

中国互联网协会 副理事长



约翰．穆洛兹

东西方研究所的创办人，总裁兼 CEO

前言

当您阅读本报告时，您会发现所看到的内容与过去有所不同。过去，中美双方围绕网络空间的观点交流虽然热烈，但都往往停留在口头和书面的讨论上，很少留下具体的成果，但本报告所呈现出的情况却是个例外。当双方在互信关系建设方面蹒跚艰行之时，本报告却提出了为实现共同目标而开展协作、联动和相互支持的倡议。当大多数人只看到网络空间的安全形势越来越严峻时，本报告却充分体现了双方合作的成果，为双方关系的改善带来了希望。

我们彼此都共同认识到互联网是一个仍在不断发展的新事物，它对我们两个国家乃至全球都已经带来了并将继续带来巨大的帮助，同时也带来很多挑战。我们都非常关心在网络空间内的双方关系，并认为与其去纠结一些不确定的问题，不如就一些双方共同面对的、确定的挑战开展真诚合作。

对于下一页所列的各位专家们，我们深表谢意。他们为这一合作付出了大量时间并给出了宝贵的专业意见，没有他们的努力，我们不可能在国际合作进程中取得这一重大进步。

卡尔·弗雷德里克·劳舍尔

美国专家组组长

东西方研究所首席信息官兼特聘研究人员

贝尔实验室院士

纽约市

周勇林

中国专家组组长

中国互联网协会网络与信息安全工作委员会秘书长

国家计算机网络应急技术处理协调中心运行部主任

北京市

劳舍尔和周勇林在东西方研究所全球安全会议
布鲁塞尔　2010 年 2 月

贡献者

中华人民共和国

中国万网 常福刚 韩松 马晓文

中国互联网协会 李红 胡安廷 王朔 徐原 曾明发 朱芸茜

腾讯 金璇 林晋

263 网络通信 李宏宇 田飞

中国联通 梁友

亚太网络法律研究中心 刘德良

中国电信 苏志胜

网易 王明达

绿盟科技 赵粮

新浪 张璐

美利坚合众国

Switch NAP Jeff Ames（退休）

Google Monica Chew

诺斯罗普格鲁曼公司 Gib Godwin

贝尔实验室院士 Suart Goldman（退休）

威瑞信 Ramses Martinez

宾西法尼亚州立大学 Patrick McDaniel

乔治华盛顿大学 Jack Oslund（退休）

康卡斯特有限电视 Dominic Ruffolo

卡内基·梅龙大学软件工程研究所计算机紧急应急小组 Greg Shannon

美国电话电报公司 Fred Stringer

全球网络风险公司 Jody Westby

圣何塞州立大学教授 Weider Yu

考克斯通信公司经理 Jason Zabek

致谢

在此表达高度赞赏和真诚的感谢。

在此特别感谢向东西方研究所提供经济资助的人士，正是您为创建一个更安全和更美好的世界所做的努力使这一项工作得以实施。

感谢 **C.H.Tung 和 Joel Cown** *等对中美关系报以兴趣并提出他们的观点。*

感谢 **Anneleen Roggeman** *在活动全程提供项目管理支持。*

感谢 **Michael O'Rierdan、Jerry Upton** *和* **Linda Marcus** *为本报告的全球推广所做的规划。*

感谢 **Andrew Nagorski、Abigail Rabinowitz** *和* **Dragan Stojanovksi** *对本报告的编辑和印制进行质量控制。*

感谢 **Greg Austin、Terry Morgan** *和* **Vartan Sarkissian** *对本计划的长期支持和鼓励。*

感谢 **Piin Fen-Kok、David Firestein** *和* **Euhwa Tran** *提供对中美关系进行跟踪、研究的成果，并提出自己的观点。*

感谢 **蔡名照、钱小芊、黄澄清、魏正新、刘正荣、James L. Jones** 和 **John Edwin Mroz** *等高层人士对本项目的支持，正是他们的远见为我们带来了这次良机。*

最后，感谢来自北京和华盛顿的众多相关人士的支持，感谢他们对双方联合工作组在项目中所体现的创新性的认可。

目录

图形清单

表格清单

1. 概要

2011 年初，中国主席胡锦涛先生和美国总统奥巴马先生郑重提出要努力改善两国关系，他们在联合声明中特别提到，“加强在一系列问题上的合作…共同加强网络安全。”[1]在合作方面，中国互联网协会和美国东西方研究所在一年多前，就召集了两国的专家开展网络安全议题的双边对话。这份“抵御垃圾邮件建立互信机制”报告，作为专家组的第一份报告，代表了两国就网络空间的重要挑战所进行的首次合作。

垃圾邮件毫无疑问是个重要的问题，因为它污染了我们的网络空间。当前，每天有上千亿的垃圾信息被生成并传遍网络，这大约占到了所有邮件信息的 90%之多。垃圾邮件还会带来其他更为严重的问题，例如它通常被用作恶意代码（如计算机病毒）和网络欺诈的载体。大量用户的计算机在访问垃圾邮件中提供的病毒链接或者带病毒的附件时被植入木马程序，成为黑客所控制的僵尸网络的一部分，而黑客则利用僵尸网络从事更多的恶意行为，包括反过来利用僵尸网络发送海量垃圾邮件而在地下黑客市场中赚取非法收益。此外，垃圾邮件也在传播网络钓鱼和欺诈信息的过程中发挥重要作用。

可能由于垃圾邮件问题不是一个有吸引力的话题，因此这个问题往往被人们低估。它也不是网络运营商或服务供应商在与用户接触中会热切关注的问题，因为它大部分都是一些负面的事情。当网络运营商和互联网服务供应商在将用户可见的垃圾邮件数量降至最低方面取得了巨大进步时，这些垃圾信息仍通过网络传输和处理，在很多方面造成了巨大的损失。这些垃圾邮件消耗了数据中心的大量能源，延长了处理周期，造成重要信息无法正常传输从而引发了用户的抱怨。因此垃圾邮件增加了互联网的运营成本和间接花费。由于资金不得不被用到垃圾邮件管理工作上，因此也间接阻碍了发展和创新。

电子邮件是现代社会必不可少的一项工具，也是处理日常业务的基本工具。然而如我们所知，如果网络运营商、互联网服务供应商（ISP），电子邮件服务提供商（ESP）和安全应用程序开发者们不预先采取应对措施并时刻保持警惕，那么电子信息很可能变得毫无用处。如果没有他们努力对抗泛滥的信息滥用，垃圾邮件很容易达到 99%以上。用户要从成百上千封邮件中才能找到正确的一封，这种情况让人无法忍受。然而解决这方面问题的无名英雄毕竟有限，还需要更多的人共同努力突破各种阻碍。国际合作的不足是治理垃圾邮件的最主要的阻碍之一，本份报告就是致力于提出一种改进国际合作的方法。

本项目的三个首要目标是：（1）双方在网络安全领域开展真诚对话；（2）对两国的网络安全环境加深相互了解；（3）提供共同指导建议，推动减少两国乃至其他国家的垃圾邮件。这些目标目前已经实现。

真诚对话

为此主办方组织 34 位相关专家组成了一支联合团队。在中国、美国和其他国家共举行了 50 场会议进行对话。会议交流形式多样，包括小型和大型的面对面讨论、通过互联网进行实时虚拟会议和大量的电子通信。在整个进程中，团队成员有足够的机会与同行们就基本政策和技术方面的问题进行讨论。

更深一步的了解

联合团队对 500 多个问题进行了讨论。这些讨论涵盖了各种主题，包括：从发送垃圾邮件的动机到互联网服务供应商的业务模式，从社会现象到政府的关切，从网民自我表达的自由到法律的约束，从现有政策的缺陷到世界级的最佳实践，从技术挑战到技术机遇，从国内合作到国际协作等等。以下展示了中美联合小组在加深相互了解方面取得进展的四个例子：

[1]中美联合声明，应对地区和全球挑战，白宫新闻秘书办公室，2011 年 1 月 19 日。

美方专家之于中国的观点（第 3.2 节）

2. 文化转型。互联网改变着全世界，也改变着中国。这是因为之前从来没有过这么多便利的信息技术、通信工具和国际交流机会。中国互联网用户的增长速度和增长规模是令人难以想象的，在认识到互联网的极大便利性和低成本优势后，越来越多的人愿意通过互联网来开展自己的业务，而这对上一辈人来说，甚至是十年前的当代人来说，都是不可想象的。正因为垃圾邮件是一种发布广告信息的最为便宜和便捷的手段，因此虽然招致普遍的反对，但仍然不断吸引人们去使用，而这就反映了中国在互联网管理上面临的挑战。

9. 行业担当主导的关键角色。对很多美国专家来说，中国专家没有主张通过政府干预作为解决垃圾邮件问题的主要途径实在令人吃惊。中国专家组成员所采用的观念和方法相当成熟，因此他们更了解行业在主导反垃圾邮件措施方面所具有的优势。与美国同行们一样，他们也认为，特别是在快速发展的技术行业，政府在制定相应管理政策方面还有大量工作需要去完成。然而他们也担心，在没有惩罚措施的情况下，那些针对潜在发送垃圾邮件行为的自发措施可能效果不佳。中国在反垃圾邮件方面的政策相对来说还不完善，这促使中国专家们在积极采取行动实施行业解决方案的同时，也在考虑选择怎样推动立法工作。

中方专家之于美国的观点（第 3.4 节）

8. 美国反垃圾邮件立法未达到预期目的。在美国，在政策方面最常见的反垃圾邮件方法便是通过立法手段[2]。因此在中国专家看来，美国人相信政府干预能提供统一的应对和惩罚措施来达到制止垃圾邮件的目的。尽管反垃圾邮件法案的效力并不令人满意，但是美国专家并没有对法案进行严厉的批判。中国专家认为由政府颁布有效的惩罚措施确实很重要，但只有行业最有条件发现和执行真正的解决方法。

9. 对中国互联网行业知之甚少。美国专家对中国互联网行业的了解，与中国专家对美国互联网行业的了解相比相对较少。这造成了位于美国的反垃圾邮件组织对中国的 IP 地址抱有偏见，并且对中国的同行不够透明。因此加强双方之间行业层面上的沟通并以发展的角度来看待问题是很重要的。

有关更深一步了解的全面讨论见第 3 节。

联合建议

本报告提出了两点建议，如若执行，将减少两国及其他国家所产生的垃圾邮件。这些建议详见第 4 节，现概述如下。

建议 1　　增进行业间的相互合作

垃圾邮件发送者们充分利用了国际协作中存在的问题，使邮件发送方的身份更难以辨认，垃圾信息更难以识别，进而更难以采取反垃圾的邮件对策。因而，国际合作和国际政策对有效解决垃圾邮件问题至关重要。

近几年来双方均已将反垃圾邮件的国际协作确定为优先考虑的事项。双方接下来的就是为抵制垃圾邮件进行合作。但目前双方仍然缺乏合作，这其中有简单和复杂的原因，从时区和语言的差异性问题到信

[2] 《2003 年控制非法色情信息和商业信息法案（CAN-SPAM）》（《美国法典》第 15 编第 7701 节)。

息分析、处理的交互上的复杂性（见 4.1 节）。在这些问题得到解决之前，垃圾邮件发送者仍然能够不受限制地利用当前环境。因此，双方共同建议：

中美两国的网络运营商，互联网服务供应商，电子邮件服务提供商以及其他国家/地区的同行们应建立一个以减少网络垃圾邮件为目的的、可促进定期合作的论坛。

此项建议提出了可即刻付诸实施、用以解决中美之间缺少反垃圾邮件合作这一问题的指南。双方均有行业专家表示有兴趣立即着手实施此项建议。建议呼吁，各国/各地区现有的各大国际论坛应积极主动地相互协作，并与各网络运营商和服务供应商携手合作。具体来说，这意味着这些组织应调整它们的章程，扩大成员范围，在安排会议地点时应考虑其他国家/地区成员的便利性。

所需承诺：为有效执行此建议，双方的行业之间应积极开展合作，中美两国政府机构则应鼓励开展反垃圾邮件方面的合作；以及建立一个由两国专家广泛参与的国际性的反垃圾邮件组织。

建议 2　　自发采用专家推荐的最佳实践方案

当前反垃圾邮件最佳实践方案对电子信息发送服务的持续发展至关重要。最佳实践方案同样也是改善我们当前局面的希望所在。

专家们齐聚一堂集思广益的情况下最能得出最佳实践方案。这种相聚可以在不同的层面实施，公司或机构，行业或国家/地区，或者国际团体之间。现在只有最后一个层面尚未发展成熟。

为开发最佳实践方案而开展的国际合作已进行数年。然而，中美之间的合作却成果寥寥。此项建议试图填补这个空白，指出 46 项最佳实践方案就是由中美专家团队共同开发的。如若执行，这些最佳实践方案可有效减少垃圾信息的产生、传播和无意打开的几率。此外，鉴于部分实践方案所具有的动态性，随着垃圾邮件发送者为应对现有的反垃圾邮件对策所进行的不断调整，这些实践方案将能持续提供有价值的对策。

中美两国的电子邮件服务提供商、互联网服务供应商、网络运营商和政策制定者与其他国家/地区的同行应在考虑网络配置、业务模式和其他可行性因素的前提下酌情开展合作以发展、维护、自发地实施经双方一致认可的最佳实践方案。

所需承诺：为有效执行此建议，企业需酌情实施最佳实践方案，并为最佳实践方案的优化发展做贡献。建议中美两国相关政府部门酌情实施最佳实践方案，并充分重视企业的专长和需求，以便对最佳实践方案的开发和应用加以指导。

双方达成共识的最佳实践方案

联合团队开发并同意实施 46 项最佳实践方案。每项最佳实践方案均拟自发实行，条件是准备实行这些方案的团体应对当地的情况有所了解并拥有一定的专业知识，可以确定实施该方案是否恰当及可行。下文即提供有四个示例。有关格式解释的说明见第 4.3 节。每项最佳实践方案都已经在使用中，具有很好的效果和操作可行性[3]。

[3]见 4.3 节的最佳实践方案。

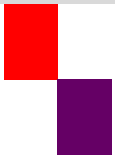
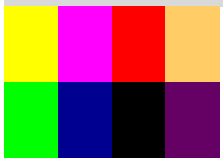
CNCN-US 11-007	对发信密集型业务的识别
 ISPs ESPs NZNs	电子邮件服务提供商和互联网服务供应商应使用可接受使用策略（AUP）。该策略要求有意发送信息的企业注册为此类用户，并在其发送的信息中将其业务类别告知收件人。
CN-US 11-015	**越快越好**
 NOs ISPs ESPs	网络运营商，互联网服务供应商和电子邮件服务提供商应优先采取这样的策略，即在垃圾邮件传播途径上尽可能早地发现并删除它。这会有效地降低此类垃圾信息在互联网传播过程中所带来的成本。
CN-US 11-023	**跨境使用“有效循环反馈（FBL）”机制**
 NOs ISPs ESPs	网络运营商，互联网服务供应商和电子邮件服务提供商应该同其所联接的其它国家的同行一起建立“有效循环反馈（FBL）”机制，以增加有助于进一步管理好垃圾邮件的信息。
CN-US 11-033	**自愿国际协议**
 GPMs NOs ISPs ESPs	政策制定者和行业应考虑在国家之间签订有利于减少垃圾邮件（如关闭发送源）的自愿协议。

表 1 用 7 个数字总结了双方为抵御垃圾邮件建立互信机制所做的努力。第一个和最后一个数字展示了此主题的重要性，中间五个数字则证明本次活动的目标——坦诚对话、加深相互理解和达成一致认识等均已成功实现。

表 1. 概括统计

2	网络大国
2	联合建议
29	更深一步了解的层面
32	专家参与的主题
46	达成共识的最佳实践方案
500+	考虑到的评估参数
X00,000,000,000	每天被过滤的垃圾信息

后续步骤

有关各项建议的推荐后续步骤，可稍后详见各项建议的介绍部分（第 4 节：“后续步骤”标题）。到报告发布时，团队各成员将随着参与实施这些建议而获得更多的新机遇。

参与这些讨论的团体和组织，仍将参与这些后续步骤。按照计划，东西方研究所（EWI）将继续把担任双方建立网络安全互信机制的发起方作为自己的优先工作。此外，EWI 方面的重点工作还包括全球网络安全行动（Worldwide Cybersecurity Initiative，简称 WCI），在该行动中，EWI 将与世界领先的智库、公司、非政府组织（NGO）以及各国政府一起合作，在制定国际协议、标准、政策和规程（ASPR）方面寻求突破。

2. 简介

本节内容主要是介绍本项目的背景，阐述其重要性、概述其目标、定义其范围并描述其方法。

2.1 背景

整个 2008 年，美国高级政府官员和行业的相关方参与了东西方研究所的活动，表达他们对人们越来越依赖快速发展的网络这一现象的深切关注。其中高级军事军官将这个领域的新威胁等同于核武器的危害。此外，高级政治领导人表示了他们对由网络化不确定性的关注。这些都深刻地揭示着国际政策在保障未来网络空间方面将起到的关键作用。在认真审议 EWI 的职责与应对网络安全挑战的关系后，EWI 国际董事会启动了“东西方研究所全球网络安全行动（WCI）”。

WCI的架构和工作重点在第二年显现[4]。WCI将中国、欧盟、印度、俄罗斯和美国[5]这五大最具影响力的互联网国家/地区之间的关系作为最优先考虑事项。WCI 已拟定大致框架，确定了一系列的主题，对于公共安全、经济稳定和国家安全有重大意义。此项活动一方面要制定建立互信机制的战略措施，另一方面要制定先进的互联网冲突解决政策。除此之外，活动还关注基础设施保护和经济稳定性。依此框架作为参照，研究所开始推动两国进行双边活动。

东西方研究所当前关心的最重要问题是中美关系。在向双方与政府相关的人员咨询后，EWI 启动了关于网络安全的合作对话。中国互联网协会被推荐作为对口部门，与东西方研究所开展对话活动。

这一双方活动完成了两国的政策声明中所设定的部分目标。中国相关政府部门在 2010 年出版的《中国互联网状况白皮书》[6]的第六条原则中主张“积极开展国际交流和合作”，这里强调了中国就互联网的相关话题主动促进“双边对话”这一举动。参与该项目的人员可证实中国政府、公司和专家为支持此活动所做出的拥护和努力。对于美国来说，2009 年的白宫网络政策评估报告概括了美国方面的许多优先事项，如评估报告中第七点“近期行动计划”所述号召展开国际合作。具体来说，其目标在于“加强我们的国际伙伴关系来开展活动，从而实现与网络安全相关的一系列的活动、政策和机遇”[7]。

2011 年 1 月中美元首间的会晤加强了这一行动的重要性。在联合声明中，两国共同承诺“ 建立 21 世纪积极合作全面的中美关系”[8]，还特别要求两国“推进合作以实现网络安全”。

抵御垃圾邮件建立互信机制被认为是促进双方关系的一个慎重举措，也确实存在着其复杂性。一方面，中美在经济领域和其他方面有着非常深远依存关系；而另一方面，他们又视对方为竞争者，尤其是在互联网方面。我们写这份报告也是希望网络空间中的合作可以替代竞争。

选择垃圾邮件作为议题并不是武断的。抵御垃圾邮件建立互信机制揭示，垃圾邮件是一个重要问题但却容易被忽略。本报告中提出的联合研究的指导方法，如若实施将对创建更有效和安全的互联网产生重大影响。

我们将减少垃圾邮件作为合作的第一步，双方计划在接下来的报告中考虑更多重要的主题。

2.2 重要性

东西方研究所和中国互联网协会就抵御垃圾邮件建立互信机制的双边活动，其重要性体现为五个方面：第一，它体现了世界上两个互联网大国在网络安全方面面临的共同问题；第二，它解决的是互联网的一个重大的、被低估的及没有被正视的问题[9]；第三，在存在诸多不信任的情况下，它仍然实现了双方之间的合作；第四，这一活动揭示了在网络安全领域的未来合作中还存在新的发展潜力。最后，报告证明了以行业为主导这一活动的有效性[10]。

[4]该行动于 2009 年 4 月在华盛顿美联储召开的会议上启动。
[5]网络五国。WCI 已经形成了网络 40 国（Cyber40），包括 G20 和对网络空间最具影响力的重要国家/地区。
[6]中华人民共和国国务院新闻办公室《中国互联网状况白皮书》第 28 页，2010 年 6 月于北京。
[7]白宫网络政策纵览：《保障可信和强健的信息和通信基础设施》表 1：近期行动计划，2009 年于华盛顿，p.vi。
[8]中美联合声明：《应对地区和全球挑战》，白宫新闻秘书办公室，2011 年 1 月 19 日。
[9]网络运营商和网络服务提供商必须意识到垃圾邮件的问题。然而，由于他们处理工作中的改进，大众其实并不知道被过滤的邮件的数量。
[10]研究所引进了企-公合营制，与以政府为主导的公-企合营制相对。

2.3 目标

此次双边活动设定了三个目标：第一个目标是在两国的相关专家、公司和其他相关者之间**开展真诚对话**。从亲身交流和视频、电话会议总时间达到数百小时来看，团队在这一步已经取得了成功[11]。

第二个目标是由第一个目标发展而来的，旨在**更深一步了解对方的观点**。目前团队成员已经对对方的观点有很好的理解，可以说团队在这一步已经取得了成功。通过对可能影响垃圾邮件的一百多个参数进行系统评估，团队已实现了部分目标。对于任何一个可能参数的调整，双方从理论、有效性、合意性和现实可行性等角度对各个观点进行了权衡分析。团队成员利用这次机会与同行对各个参数的调整进行探讨，并了解为何会得出有益或有害的净评估意见[12]。

当谈到网络安全，鉴于当前的中美关系，双方均意识到单独就前两个目标的成功就意味着已经发生了实质性的进展。但仍有第三个目标尚未实现。第三个目标建立在前两个目标的基础之上，旨在就有关如何减少互联网垃圾邮件的国际政策**达成一致**。第三节“联合建议”，按照两个联合建议和 46 项最佳实践方案的形式给出了指导意见。

2.4 范围

界定此活动范围的最佳参数有 4 个。它们是 1）参与的团体，2）垃圾邮件的定义，3）减少垃圾邮件的措施，4）互信关系的建立。第 1 个和第 2 个参数见此节所述，第 3 个和第 4 个参数分别见第四节和第一节。

参与的团体

该活动由来自中国和美国的相关专家和其他相关方进行。每个专家均是所在国家的公民，并曾经参与了网络安全、网络运营等关键领域的活动[13]。

专家们的经历加起来有五百年之多，涵盖了对主题进行评审所需的一系列专业知识和经验。许多参与活动的人员曾在各自的国家，为国内最大的互联网服务供应商们效力，负责网络安全和处理信息发送泛滥的问题。

由于活动的最后一步旨在进行推广，参与了最后阶段的其他团体包括网络安全专家和其他利益相关者，而且他们还会继续参与。

垃圾邮件的定义

对现有定义进行大量讨论和分析之后，团队一致认为垃圾邮件[14]具备四个基本特征。符合所有特征的邮件才为垃圾邮件。缺少其中任何一个特征便不被认为是垃圾邮件。这四个特征是 **[15]**：

[11]中美团队成员的会议地点包括北京、布鲁塞尔、达拉斯、黎翰谷、纽约和奥兰多。
[12]更多细节请参照 2.9 节：方法。
[13]在个人履历节中附件有每位团队成员的背景介绍。
[14]垃圾电子邮件通常指“垃圾电子邮件”。常用的同义词是不请自来的批量电子邮件（UBE）。团队还发现了其他关于垃圾邮件的定义。很多术语在互联网世界中都不能从语义中推断出，这也就解释了为什么一个术语可能会有几种定义。关于属性的得出是基于两点：现有定义的分析和对对术语对出现的问题的最实用的功能的考虑。
[15] 一些已公布的定义中将垃圾邮件形式定义为电子形式。其他定义可能认为数量多（或“大量”）这一特征便已涵盖了广泛散布这一含义，因此没有另外再规定广泛散布性，但是，发送至同一人的大量信息虽然令人讨厌，但还不属于垃圾邮件。

- **不请自来**[16]
- **发送量大**[17]
- **广泛散布**[18]
- **可为任何形式的电子信息**

电子信息发送的形式包括电子邮件、即时信息、网络搜索引擎、传真、互联网网站公布、移动文本传输、短信服务、博客等其他形式。

尽管与随之而来的问题一样，各种形式的垃圾邮件不断地演变，其程度也在不断加剧，目前大部分的垃圾邮件仍然以电子邮件的形式存在。与垃圾电子邮件的广泛接触使我们对垃圾邮件的这一形式有了新认识。第一个，垃圾信息的源头通常都是隐蔽的。源头信息通常经过了伪造从而无法辨认发送者身份或是不能确定电子邮件传输路线。僵尸网络的使用也使得垃圾邮件问题更加严重，这种网络未经系统或设备所有者的授权而从一台被感染的电脑发送出信息[19]。垃圾信息发送者的动机通常受以下四种利益的驱动：（1）商业利益，例如通过广告、电子出版物和其他宣传材料获得商业利益；（2）通过蓄意欺诈、盗窃和其他非法活动实施犯罪[20]；（3）通过如传播恶意程序或攻击通信网络或计算机系统的方式造成损害；（4）用于散发那些以垃圾邮件之外的方式更难散发的信息，例如色情信息、骚扰广告、观念推广、恐怖主义和种族歧视言论等。这一补充描述使我们对这些垃圾邮件制造者的意图和目的有了更好的了解。这样的认识有助于我们思考可能的对策。

除了垃圾邮件，其他的垃圾信息包括不受欢迎的、大容量并广泛散布的以短信服务（SMS）、垃圾网络电话（SPIT）、网站贴文和传真形式存在的信息。

移动互联网中的恶意软件类型正在急剧增加。恶意软件的类型中包括定购不需要的服务或发送彩信/短信、使用互联网流量、通过互联网远程控制、隐私盗窃、数据破坏和欺骗等方式。手机恶意软件比个人电脑的恶意软件传播的更广。它们包括和互联网、应用程序、短信服务、蓝牙和存储卡的连接。中国的移动服务似乎比美国面临更多的垃圾信息现象。这可能与中国彩信/短信的高使用率和低费用有关。在美国发送一条短信需要 10 美分，大约是中国的 6 倍，这一成本阻碍了批量信息的发送。

有迹象表明，用户的移动设备将成为类似僵尸网络的东西，在美国移动设备本身将成为垃圾邮件的源头，事实上它已经在中国发生了。最新发展表明现已开始出现了大量的被感染的移动设备，一些专家预测在接下来的两年内此类事件会发生较大的增幅。

2.5 垃圾邮件的历史和发展

“垃圾邮件”并不是新事物。在互联网出现之前，“垃圾信件”对西方国家来说已是个普遍的问题——如今仍然如此。垃圾信件的动机与垃圾邮件相似，两者都是将一条信息向许多人进行发送，这是最省钱的方法。

人们认为第一封带有广告性质的垃圾邮件是于 1978 年 5 月 3 日发出的，其面向的人群是高级研究计划署网络（ARPANET）的用户[21]。收信人大概有 600 人。从上世纪末本世纪初开始垃圾邮件的数量暴增。

[16] 其他可替代术语还包括不受欢迎和不请自来。
[17] 例如：发送至若干人的单条不受欢迎的信息不属于垃圾邮件。
[18] 例：发送至同一人的许多不受欢迎的电子邮件不属于垃圾邮件。
[19] 僵尸网络是自动运行的软件程序的集合，它们通常通过多个计算机系统联合在一起而运行。
[20] 对非法活动的定义可由垃圾邮件发送国、接收国或任意的中间国家界定。
[21] 《15 年以来垃圾邮件持续损害电子邮件系统》，Waters、Darren，BBC 新闻，2008 年 3 月 31 日。

现在每天互联网上垃圾邮件大约有数千亿。一些人士估算互联网中的邮件有 85%或者 90%都是垃圾邮件，一些则估计会更高。

关于垃圾邮件的准确数字是很难拿到的。对垃圾邮件的数量只能得到一个估算值——见表 2。现在存在着大量的提供垃圾邮件的来源。然而，在这些数字中简单对照也会发现不一致的地方。这是由于监测垃圾邮件的方法不同，所以是可以理解的[22]。这些不同之处包括部署的设备数量和位置、对于什么是真正的垃圾邮件的定义以及对于垃圾邮件的来源的确定。即使存在着不同，分析中还是存在着一些相似之处。例如，下列的表格提供了公开的垃圾邮件的简单统计，这些数据来源于5家企业。

表 2. 垃圾邮件的主要源发国家和地区

源发国家和地区	A	B	C	D	E	最普通分级
阿根廷	-	17	-	-	-	前 10 名以外
巴西	3	3	5	4	3	**前 5 名**
中国	-		-	-	10	前 10 名以外
哥伦比亚	7	12	-	16	-	前 10 名以外
法国	9	11	9	6	-	前 10 名
德国	-	5	-	3	6	*数据变化大*
印度	1	1	2	2	2	**前 5 名**
意大利	10	8	-	8	-	前 10 名
韩国	4	10	8	9	9	前 10 名
荷兰	-	18	3	13	-	前 10 名以外
波兰	-	14	-	10	-	前 10 名以外
罗马尼亚	8	13	-	11	-	前 10 名以外
俄罗斯	2	4	4	12	4	**前 5 名**
沙特阿拉伯	-	15	-	18	-	前 10 名以外
西班牙	9	16	-	14	-	前 10 名以外
台湾	-	-	7	17	-	前 10 名以外
乌克兰	-	9	-	15	7	*数据变化大*
英国	-	6	10	5	8	前 10 名
美国	6	2	1	1	1	**前 5 名**
乌拉圭	-	-	6	-	-	前 10 名以外
越南	5	7	-	7	5	前 10 名

在上表中可以发现有很有价值的数字，所有其他的条件相同的情况，国家越大，垃圾邮件的数量也会相应更多。绝大数国家都符合这个情况。然而中国却是个很明显的例外。作为拥有世界上最多网民的国家，中国在向其他国家发送垃圾邮件的数量比例较低[23] [24]。

[22] 遗憾的是，覆盖范围和其他限制不会在接下来提供的数据中出现，也不会统计入最后的有效数字内。
[23] 2010 年年底统计的数字是 4.5 亿，是美国的两倍。
[24] 拥有更多的在线用户和在线计算机，导致存在着更大的滥用信息服务的可能性。导致中国垃圾邮件现在情况的因素可能有自然语言的障碍以及政府在管理网络中的作用。

2.6 垃圾邮件的影响

垃圾邮件是全球性问题，它每天占用了网络中数十万亿比特的流量 [25] 污染了我们共有的互联网。垃圾邮件的影响重大，涉及安全、生活、经济、环境、网络运行、网络服务和网络体验等方面。

由于需要花费精力屏蔽垃圾邮件、花费时间人工筛选和删除垃圾邮 [26]，接收者的"网络体验"自然降低。另外，因为部分网络或当地过滤器将非垃圾邮件误报"为垃圾邮件，这样将就往往妨碍了正确信息的流通，也可能会损害用户的体验感受。垃圾邮件给邮件用户和其他邮件订阅者如 SMS 用户带了不佳的体验。

垃圾邮件已经成为一种载体，因为它能作为引进恶意代码或网络钓鱼等利用的工具[27] [28]。垃圾邮件经常传播恶意程序并攻击计算机，从而危害互联网的安全。

垃圾邮件降低了网络运行性能，因为它堵塞了网络通道和网络队列并且延长了处理器时间，进而延误了合法信息在网络空间的传播。研究报告显示垃圾邮件占据了全球所有电子邮件流量的 90%[29]。

垃圾邮件对环境的影响相当于全球每年数十太瓦时的能源消耗量 [30]。

垃圾邮件给互联网用户造成了大概每年 100 亿欧元的联网费 [31]。此外，网络运营商需承担传输、过滤和管理这些邮件而产生的费用[32]。网络运营商和终端用户均必须承担在邮箱中保存这些信息而产生的费用。从业务角度来看，垃圾邮件损害了互联网服务供应商（ISP）和电子邮件服务提供商（ESP）的声誉或互联网内容服务供应商（ICP）的竞争力。它可被看作行业的"烧钱黑洞"，因为它，我们必须建设网络来处理这些流量。另外构建极大规模的网络、运营这些网络、购买和更新硬件及软件、支付技术人员报酬、处理用户投诉、支付许多其他相关和间接相关的费用，这些都带来了较大数量的花费。

垃圾邮件的社会影响在于使人们，尤其是年轻人更容易接触到负面内容，例如色情信息、恐怖主义和种族歧视的信息。和其他媒体不同，垃圾邮件不需要对发送者身份进行辨认。垃圾邮件的发送者充分利用了互联网具有匿名性而无法追究责任的缺点，这一点也使垃圾邮件的发送行为更加无所顾忌。许多公司经常出现性骚扰事件，因为许多露骨的语言和图片被定期发送至职员的邮箱。

最后，垃圾邮件带来的网络安全问题则威胁到企业、基础网络和国家的信息安全，在高负载信息量的压力或恶意代码的威胁下，一些重要在线业务系统可能被损坏。

2.7 减少垃圾邮件过程中遭遇的阻碍

解决互联网中的垃圾邮件会带来巨大回报。然而，解决垃圾邮件问题仍然很艰难。

首先，*垃圾邮件服务于很多业务*。它是轻松联系大量人群的最经济高效的方式。垃圾邮件只需要很低的成本即可发送大量信息。因此即使其点击率很低，投资回报率（ROI）也很可观 [33]。另一因素是不能

[25] 基于对已公布的每日平均邮件数（取 1800 亿）、电子邮件中的垃圾邮件比例（取 85%）和垃圾邮件平均大小（取 5KB）的调查计算得出此数据。
[26] 一般接收者确定一条信息是否为垃圾邮件然后将之删除所需花费的时间估计为大约 5 秒。《垃圾邮件、时间和您：通过 Gmail 发送的一份教育视频》，2007 年 10 月 26 日。
[27] 网络钓鱼是指旨在通过如假装为可信任的实体的欺骗手段来发送电子信息以获得敏感信息（例如密码、信用卡号码）的非法途径。
[28] 根据赛门铁克 MessageLabs 2009 年第 3 季度报告，每 437 封电子邮件中就有 1 封为网络钓鱼攻击邮件。
[29] 根据赛门铁克 MessageLabs 2009 年第 3 季度报告。该报告还计算出美国和加拿大的垃圾邮件水平超过了 91%。
[30] "…相当于 310 万台客车消耗 20 亿加仑天然气的（温室气体）排放量，所消耗的能量相当于 240 万户家庭的用电量。"
[31] 欧共体的《自发的商业通信和数据保护》，2001 年 1 月。
[32] 众所周知，垃圾邮件在创业和促进广告商品的销售方面可带来良好的经济效益。然而，考虑到其低效性，这是一笔不划算的交易。
[33] 大部分垃圾邮件由接入的一大群"软件机器人"或僵尸软件自动生成。

确切界定*广告是否合法*，不同国家对电子信息是否为广告有不同的法律规定[34]。在一些国家你可以尽己所能，无所顾忌地将信息推到潜在客户面前。

虽然不是核心但也比较重要的是向垃圾邮件发送者出售服务的供应商的商业动机。这些供应商在与垃圾邮件发送者的商业关系中获得利润。如果一个用户的流量不违背供应商的可接受使用策略（AUP），那么供应商就很可能会从这种关系中获得净财务效益。像任何商业活动一样，供应商也希望使客户能满意。然而，最近的趋势显示供应商已经不愿意再向垃圾邮件发送者提供服务。

其次，垃圾邮件可向大量人群传播信息[35]。即使用于非商业目的，它也是联系大量人群的最经济高效的方式。利用垃圾邮件可以即时、广泛地分发政治、哲学及其他宣传信息，通常这些邮件是从很远的地点外使用虚假身份进行分发的。

第三，利用垃圾邮件的环境在逐渐发展。垃圾邮件能如此强大主要是因为其具有四大属性。垃圾邮件是：

- ***具有病毒般的扩散潜力，***因而无法阻止其增生扩散[36]
- ***不可追踪***，因而很难跟踪到真正的始作俑者
- ***自动完成，***即使未经所有人授权也可操控计算机
- ***突变性***，因而针对垃圾邮件的预防措施也通常只能是在事情发生后采取应对措施

第四，垃圾邮件利用了法律缺陷，例如国际法律框架尚未统一，全球网络缺少一个归属体系，国际合作也远远不够。由于缺乏跨国合作，许多垃圾邮件发送者利用了这一弱点，他们锁定国外市场，以避免来自任一网络端的政府诉讼。

第五，垃圾邮件的问题之所以没有解决是由于其存在不对称性。出现垃圾邮件现象是由于发送者的成本很低，而通信基础设施和接受者的成本相对较高。这是一种资源的不对称，它也是导致拒绝服务和服务水平降低的根源。反垃圾邮件的主要挑战就在于此，而我们也无法改变这种不对称。一些人员试图去解决这些问题（比如说对每封邮件收取少量费用），但是遭到了市场的否定。

第六，垃圾邮件问题之所以尚未得到解决，还由于不同国家和地区之间存在不同的社会价值观和政治体系。它们提出了严峻的政策上的挑战，要解决这些问题只能通过国家和国际合作。这些问题的核心问题是：

- *个人自由是否能让我们将信息发送到世界上具有不同法律体系的各个国家？*
- *当监测网民互联网行为（如发送邮件）的措施被采用的时候，个人隐私如何去保护？*
- *如果有些事情（如发送邮件广告）很令人厌恶，就一定说它是错的吗？*

世界各地对于这些问题及相关问题的意见还存在不一致性以及道德分歧。

[34] 一个很麻烦的特殊情况是，广播分发电子信息在司法领域可能是一种非法行为，但发出的信息可能涉及到人道主义（即不为经济利益所驱动）

[35] 4.3 节的最佳实践方案中在降低这一影响方面有很好的效果。

[36] 病毒是由新社会媒体网络创造出来的一个术语，用于描述在短时间（如一天）内即传播到超大数量（百万）用户的事物（如网站、视频、信息、应用等）。此术语已从俚语过渡到商业应用，检测内容浏览的软件现在称为病毒检测或病毒测量。

2.8 减少垃圾邮件的期望

考虑到商业环境中存在的合理利用电子信息的情况，摆脱互联网中信息的大量和广泛发送将不是本次计划的目标。实际上，很多阻力恰恰来自合法的商业利益。因而，减少垃圾邮件的目标是要减少那些来自法律范围内不合法的发送方和接收方的邮件。

2.9 方法

八阶段过程

为满足这个特殊的双边约定要求，我们专门制定了一个进程。此进程在设计时结合了本文所概述的目标、范畴、方法以及原则，并且在制定过程中采用了构建问题解决原则、八大元素（8i）框架以及建立广泛的国际共识的经验[37]。因为团队成员意识到这次尝试具有开创性，因而他们从始至终都很注重沟通的准确性。此外，他们还谨慎地对待为了达成共识所依据的确定性。

团队的最后一步是将此双边进程推广到多边国家。团队成员利用各方的相关者的投入来开展这一推广工作。应进行联合规划，以便在适当场所联合提出这次共同制定的建议[38]。

方法

在考虑可进行调整的合适的参数过程中，专家团队采用了以下四种方法保证严密性。严密性在很大程度上增加了劳动量，但却加深了了解。这四个不同的方法如下：

- 商业动机的分析
- 通信理论模型的学习
- 八大元素框架的应用
- 对现有协议、标准、策略与法规（ASPR）的评审

对于第一个方法，专家团队探讨了当前发送垃圾邮件的主要商业动机。他们还探讨了垃圾邮件的演变过程及未来可能的演进方式。然后，在制定反垃圾邮件对策中考虑了潜在的动机因素。

为了分析通信进程的可信模式和基础模式，我们特地查阅了通信的数学理论[39]。这有助于对垃圾邮件信息从发送源到目标的连续进程进行分析。此结构（图 1）的另一个优势是该结构从另一个角度来看待垃圾邮件信息经常以欺骗手段隐蔽其来源或真正意图这一事实。与典型的噪声降低效果最好的通信场景不同，信息发送者在此有意引入了噪音，这是一个明显反常的现象。此噪音使得通信系统难以正确理解和处理信息，使接收器更难以对这一信息做出准确解释。

[37] 此方面成绩现出，可参考 EC ARECI 和 IEEE ROGUCCI 的报告- 见 http://ec.europa.eu/information_society/policy/nis/docs/studies/areci_study/areci_report_fin.pdf 和 www.ieee-rogucci.org。
[38] 例如，信息系统反滥用工作小组，EWI-IEEE 全球网络安全峰会等。
[39] Shannon, Claude E.，《通信数学理论》，《贝尔系统技术杂志》，1948 年。

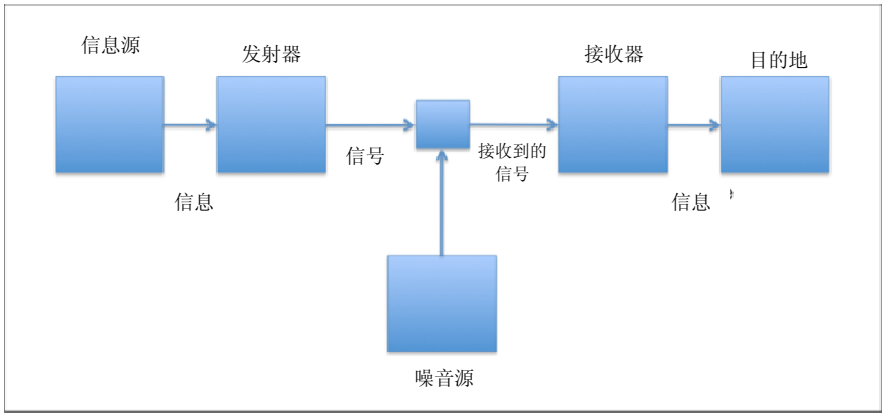


图 1. Shannon 通用通信系统示意图

八大元素(8i)框架对可调整的可用参数（图 2）的系统化分析起着关键作用。由于通过此方法可确定所考虑的大部分参数，因此它是生成最佳实践的最重要来源。

图 2. ICT 基础设施的八大元素框架 [40]

用于确定可调整参数的第四个方法是考虑现有的协议、标准、策略与法规，包括中国、美国及其他国家的相关政策。此外，还要审核此研究所涉及公司的实践。此类分析的结果是，当前的最佳实践，经来自另一国家或源公司以外的专家确认，该实践是有用的。

图 3 概述了各国对可能的垃圾邮件参数进行的调整评估。原有的计划是双方各自的工作组单独对每个参数得出一个分数。然而，双方决定利用两个参数提高分析结论的准确性。中方工作组根据“符合理论”和“符合实践”考虑因素，采用从 0（低）到 9（高）的梯度对每个参数进行评分。美方工作组则以“需求性”和“有效性”为依据，采用从 1（低）到 10（高）的评分梯度。由于各自的首批术语都十分相似，后面的也是如此，所以专家团队决定将其适当保留。只有四个参数评分均高于中线，该参数的调整才被认为是专家为追求良好效果所达成的共识。

[40] 《ATIS 电讯词汇》；*2001 年 IEEE 通信学会技术委员会的通信质量和可靠性(CQR)国际研讨会导论*，RanCNo Bernardo, RausCNer, Karl F，《*保护通信基础设施*》，《贝尔实验室技术杂志国家安全专刊》，第 9 卷，第 2 期，2004 年；《国家安全电信顾问委员会下一代网络任务组报告》，2006 年 3 月 28 日，背景与责任；电讯工业方案联盟网络可靠性指导委员会（NRSC）2002 年度报告；网络可靠性与互操作性委员会（NRIC）VI 国家安全物理安全工作组最终报告，第 3 期，2003 年 12 月；网络可靠性与互操作性委员会 VII 无线网络可靠性工作组最终报告，第 3 期，2005 年 10 月；网络可靠性与互操作性委员会 VII 公共数据网络可靠性工作组最终报告，第 3 期，2005 年 10 月（www.nric.org）。

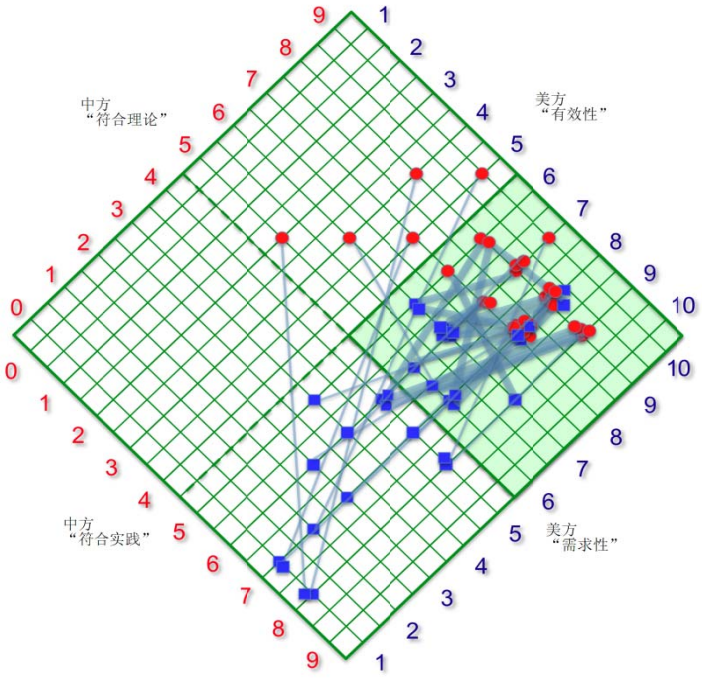


图 3. 双方反垃圾邮件参数调整分析概览

2.10 原则

一个团队

与奥运会不同，奥运会上，中美双方均是选派出最优秀的运动员相互竞赛，而在本次双边活动中，双方参与者共同组成了一个团队，对付互联网中共同的敌人——垃圾邮件。这次活动的参与者主要是些相关专家，他们来自设备供应商、基础设施运营商、网络运营商、互联网服务供应商、电子邮件服务提供商以及研究人员相关人员。这些人员的专业知识和经验跨及科学与工程、商业与法律、学术与军事等众多领域。团队成员的工作体现了他们对这一进程的付出，他们一定程度的知识贡献、寻求双边相互了解中所表现出的耐心以及对实现双方及其他国家互利这一目标的热切渴望都印证了这一点。

双边合作

本次合作对话由非政府组织发起，并给予支持。大部分专家主要来自行业或学术机构。双方分别向他们在北京和华盛顿的政府相关负责人简要汇报。

严谨性

在双方达成一定程度的共识后，团队在整个进程中经常就各种见解进行严谨的讨论。团队成员甚至非常乐于在其它国家成员出席的情况下进行这种严谨的探讨，这样他们更能够发现到分歧和挑战。参与者将这种自由而严谨的探讨视为是能够得出说服力的结论的最有效的方法。

3. 更深入的了解

此次双边活动的第二个主要目标是促进双方对彼此有一个更深入的了解。本节阐明了双方专家获得的关于对方的一些重要观点，以及他们在面对垃圾邮件和相关选择时的挑战。

对话本身并不能保证参与者抓住了所表达的观点、要传递的信息和注意事项。相反，参与者需努力去识别对话中需进行说明的部分并共同力求对某一观点的准确性进行确认。团队在这方面做的很好。有时，对话的进展似乎比较缓慢且过于谨慎。然而，团队这样做是为了设法使对话覆盖与垃圾邮件相关的全部参数和角度。在这一进程中所付出的勤奋和耐心得到了巨大的回报。参与双方均摒弃了对对方固有的表层了解，而获得了对彼此更深入的了解，从而有利于双方进一步的合作。

3.1 美方专家之于美国的观点

下面是美国专家所观察到的有关美国方面情况的六点重要现象。

1. **统计显示相关政策至今无效。**根据统计结果，美国为限制垃圾邮件而制定的相关政策效果并不明显[41]。当前相关政策并没有阻止美国网络上垃圾邮件的与日俱增，也未对国际网络做出任何贡献[42]。

2. **被动局面深入人心。**大家普遍认为反垃圾邮件战主要是一场追踪并进行处理的比赛，而不是主动去预想垃圾邮件下一次将在什么地方发生。我们总是等出现一个新垃圾邮件才做出反应[43]。事实上，需要更加积极主动地规划。

3. **所需人际关系的投入。**美国网络安全工程师此前并未着力培养其与中方伙伴之间的人际关系。而双方的互信关系正是进行反垃圾邮件合作的前提[44]。只有本着小心谨慎的态度相互进行接触才能建立起这种互信关系。

4. **用户拥有各式各样与垃圾邮件相关的经历。** 其原因非常复杂且主要是由以下三个因素共同作用的结果：互联网的复杂性、公司管理邮箱帐号的模式和一些公司滥发信息的行为。 例如，当前流行的免费邮箱服务设计用于发掘帐号持有人的信息内容并向他们出售广告。它们通常不会关心客户的需求。另一方面，依靠提供电子邮件服务获取收入来源的网络运营商则兼顾了客户需求和经济利益，这使得它们的运行更为复杂。事实上，电子信息广告对于某些用户来说是一种经营模式。

5. **经济中的混乱问题。**互联网的层次结构在促进其发展和为每位用户节约成本方面扮演着很重要的角色。然而，层次结构同时也使垃圾邮件的控制变得更为复杂并增添了一笔因使用算法而产生的无效开支。控制垃圾邮件的最佳方法还是从发送垃圾邮件的源头或接收垃圾邮件的接受地址进行控制。然而，网络运营商必须承担发送信息的费用，却只能获取发送字节的收益。这就造成了网络运营商免费发送字节却可能被接收方要求停止发送信息（一旦发送，必然封锁）这样一种局面[45] [46]。

---

[41] 见表 2。.
[42] 2003 年《控制非法色情信息和商业信息法案》（15 U.S.C. 7701）。
[43] 这种现象普遍存在于世界各国，而不仅仅是美国。
[44] Rauser, Karl, F.，欧盟委员会 ARECI 报告，布鲁塞尔，2007 年。
[45] 例如：他们并未对信息内容进行检查。
[46] 这是其与传统的邮寄信件的根本区别，传统邮寄信件的邮费是由发信人承担的。

6. **已适应与垃圾邮件并存。**我们拥有大量致力于减少垃圾邮件的高技术人才和团队，而且他们还在继续为此付出更多的努力。同时，我们还发展和引进了相关方面的先进技术。另一方面，大多数公司已把垃圾邮件视为一种无法避免的干扰和成本消耗。当前尚无可完全消除网络垃圾邮件的有力举措[47]。

3.2 美方专家之于中国的观点

本节详述了9个重要的观察结果，通过这些观察结果美国专家可以更好地了解中国的商业环境、他们的中方伙伴及其在中国进行反垃圾邮件活动的相关经验。

1. **中国当前所面临的网络可扩展性挑战的大小。**在超过十亿的公民中约有5亿网民，新的网上帐号和公司用户正在以亿数量级急剧增长[48] [49]。中国互联网服务供应商甚至使得美国最大的公司开始怀疑他们的进程和操作是否可以发展至如此“极端”的程度。

2. **文化转型。**互联网改变着全世界，也改变着中国。这是因为之前从来没有过这么多便利的信息技术、通信工具和国际交流机会。中国互联网用户的增长速度和当前规模是令人难以想象的，在认识到互联网的极大便利性和低成本优势后，越来越多的人愿意通过互联网来开展自己的业务，而这对上一辈人来说，甚至是十年前的当代人来说，都是不可想象的。正因为垃圾邮件是一种发布广告信息的最为便宜和便捷的手段，因此虽然招致普遍的反对，但仍然不断吸引人们去使用，而这就反映了中国在互联网管理上面临的挑战。

3. **在应对垃圾邮件方面中国正在成为一个好邻居。** 中国在反垃圾邮件方面正处在一个成功的轨道上。来自中国境内某些公司和独立资金来源的公司对垃圾邮件的统计资料，证实中国在减少发送至他国的垃圾邮件方面取得了显著的进步[50]。特别是发送至美国的垃圾邮件数量在过去3年中连续递减。

4. **内容的敏感性。**在探讨垃圾邮件构成内容的对话期间，初次对话主要探讨了垃圾邮件的危险性。中国专家指出了垃圾邮件的各种危害，主要包括传播恶意代码，以及传播影响社会稳定、种族歧视、色情等非法内容[51]。

5. **信息共享。** 为了全面描述垃圾邮件在中国的状态，中国专家与美国专家分享他们的统计数据，这对于针对垃圾邮件的发展趋势阐述各自不同的观点来说非常重要。他们本着合作的态度非常乐意提供相关数据，因为这样有利于项目的开展。

6. **注重操作性。** 中国专家更加注重对话的操作性方面。他们对切实可行的主题有着更浓厚的兴趣，而对未经实践的一些想法似乎兴趣不高[52]。这种务实的态度体现在对所讨论各个方案选项的有效性进行估算。但是，注重实用性并不妨碍接受更有创意的建议。

7. **专业人员的谦虚态度。**中国专家在展示他们的技能和知识时显得非常谦虚。其实，他们在运作网络、理解经营模式和减少垃圾邮件方面显然知识渊博、经验丰富。因此，他们受到了美国方面的高度赞扬。

---

[47] 此外，这项监测在美国还不适用。
[48] 中国已拥有超过13.38亿的人口。
[49] 腾讯和网易各拥有超过3亿的邮箱用户。
[50] 图2。
[51] 2.4节内。
[52] 图4为监测提供了证据。当几率变低时，美国倾向于“需求性”，而中国更倾向于“实践性”。

8. **不一致的了解程度。** 与美国专家对中国公司的了解程度相比，中国专家似乎更加了解美国公司 。这可能是因为美国公司在全球的知名度很高（如：Google、Yahoo!、 Microsoft 等)。

9. **行业主导的重要作用。**对很多美国专家来说，中国专家没有主张通过政府干预作为解决垃圾邮件问题的主要途径实在令人吃惊。中国专家组成员所采用的观念和方法相当成熟，因此他们更了解行业在主导反垃圾邮件措施方面所具有的优势。与美国同行们一样，他们也认为，特别是在快速发展的技术行业，政府在制定相应管理政策方面还有大量工作需要去完成。然而他们也担心，在没有惩罚措施的情况下，那些针对潜在发送垃圾邮件行为的自发措施可能效果不佳[53]。中国在反垃圾邮件方面的政策相对来说还不完善，这促使中国专家们在积极采取活动实施行业解决方案的同时，也在考虑选择怎样推动立法工作[54]。

3.3 中方专家之于中国的观点

下面是中国专家所观察到的有关中国方面情况的五点重要现象。

1. **垃圾邮件犹如过街老鼠，人人喊打。**不论是从互联网用户、互联网运营商，还是从政府主管部门，都鲜明地反对垃圾邮件。互联网用户反对垃圾邮件因为他们会直接受到垃圾邮件的困扰，互联网服务供应商的反对原因则主要由于很多被用来发送垃圾邮件的IP地址段被列入黑名单，影响其运营，政府部门则面对来自公众的压力而力求加强反垃圾邮件工作。

2. **反垃圾邮件的立法不足。**除了《互联网电子邮件服务管理办法》，没有法律和政策专门针对反垃圾邮件。目前，现有的法规大都是对电子邮件的服务商提出了要求，但没有约束电子邮件用户发送垃圾邮件的行为。

3. **在行业自律层面开展了非常重要和有效的工作。**行业内部采取了很多措施，比如清理open-relay服务器、培训邮件服务器管理员、开展垃圾邮件举报和处理工作、公布垃圾邮件黑名单，以及清理僵尸网络等[55]。

4. **应该着力加大国际合作和对外宣传。**中国互联网协会与ITU、OECD、APCAUSE以及其它国际组织建立了联系，但是中国的互联网服务提供商和电子邮件服务提供商与其他国家的直接合作是不够的。但是在互联网服务供应商和电子邮件服务商层面，与相应国际组织的合作明显不足，体现在相关工作没有有效联动，同时没有及时处理来自国际投诉而遭至被封堵IP地址的结果。中国应该进一步加强国际合作，并且通过各种渠道去宣传中国的成就和经验，推动全球的反垃圾邮件工作。

5. **改进法律法规。**中国还需要进一步制定和修改反垃圾邮件的技术标准规范和行业自律条款，以便应对不断出现的新问题，例如正确区别商业信函与垃圾邮件，建立更易于用户理解和操作的反垃圾邮件服务等。

3.4 中方专家之于美国的观点

本节详述了9个重要的观察结果，通过这些观察结果中国专家可以更好地了解美国的商业环境、美方伙伴及其在美国进行反垃圾邮件活动的相关经验，结果分别如下：

[53] 美国专家团队注意到这种观察结果不只限于中国，同时也是适用于欧美国家的一个探讨要素。
[54] 中国团队成员把行业领导的措施或自愿性措施称为“自律”措施。
[55] 英文中“Zombie networks”同“botnets”，都解释为僵尸网络。

1. **框架和方法。**美国专家在进一步深入了解相关问题之前，在进程开始时先花费一定的时间来构建合适的框架，选择合适的方法。通常这种方式会使提出的见解更全面，观点更有创意。与美国专家注重理论和政策不同，中国专家更注重可以解决问题的技术手段。

2. **成熟和丰富的经验。**美国团队拥有各种专家，包括技术和工程专家以及有法律和政策背景的专家。甚至技术专家对政策的讨论也感兴趣。这可能得归功于美国专家相对中国专家而言更长的平均经验和更高的年龄层。这是因为美国的ICT行业比中国的发展得更早。

3. **远程合作。**美国专家组更愿意采用通过互联网的虚拟会议。对虚拟会议进行有效管理，使处于不同地理位置的各个团队成员之间能够精诚合作，共同工作。美国专家更喜欢远程工作，因为他们已熟悉了这种模式。

4. **垃圾邮件统计与协调。**在美国似乎很少有行业组织领导反垃圾邮件协作。在美国并没有类似中国互联网协会反垃圾邮件工作委员会的机构，美国专家所分享的垃圾邮件统计数据通常是来自于第三方的安全服务公司。很多公司尝试用不同的办法来屏蔽垃圾邮件，但在这一领域似乎没有形成一个具体的、统一的规范[56]。

5. **时间范围。**美国专家倾向于通过长时间的努力来慢慢实现设想，这与中国专家的想法有些不同。中国专家则期望在没有太落后于快速发展的技术之前立即采取活动或测试。

6. **相互尊重的讨论氛围。**美国专家和中国专家都克服了语言、文化和观念的障碍，从而使他们之间的对话非常成功。在对话中，美国专家总是对中国专家的观点进行复核，以确保在双方进入不同的探讨方向之前正确地理解了中国专家的观点。同时，美国专家还留有充分的时间供中国专家阐述他们的观点。

7. **专业的研究和工具的使用。**很明显，美国专家采用了非常专业的方法并且充分利用了在他们的研究中能够找到的任何工具。他们有一套非常系统的程序引导他们的团队实现自己的目标。

8. **美国反垃圾邮件立法未达到预期目的。**在美国，最常见的政策方面的反垃圾邮件方法便是立法手段[57]。这使中国专家认为美国人相信政府干预能提供统一的规定和惩罚措施来制止垃圾邮件。尽管反垃圾邮件法案的效力并不令人满意，但是美国专家考虑到后果并没有对法案进行严厉的批判。中国专家认为由政府颁布有效的惩罚措施确实很重要，但行业更有能力找到和执行真正的解决办法。

9. **对中国互联网行业知之甚少。**美国专家对中国互联网行业的了解与中国专家对美国互联网行业的了解相比相对较少。这被认为是一些位于美国的反垃圾邮件组织对中国的IP地址持有偏见且对中国的实践人员不够透明的原因之一。加强中美行业层面上的沟通并以发展的角度来看待问题是很重要的。

[56] 美国很多信息专家都很积极地参与到由反信息滥用工作组主持的行业合作中，该工作组是一个国际组织。对本次论坛或者其他论坛进行的国家层次的协调度并没有中国的中国互联网协会的协调度那么广泛。
[57] CAN-SPAM 法案。

在北京的专家会议

4. 联合建议

前面几节阐述了团队成功地实现了双边活动的前两个目标：*开诚布公地对话和加深双方的了解*。本节将致力于阐述第三个目标——为实现这一目标而就国际间合作的 ASPR（协议、标准、策略与法规）*达成一致*，减少互联网的垃圾邮件及其对收件人的不良影响。随着对国际政策的关注，需注意的是本报告所给指导的重点集中在 ASPR 上[58]。

本报告提交了两条联合建议和 46 项最佳实践方案。每条建议都切实可行，而且在实施后希望能有效减少垃圾邮件。双方专家强烈要求尽快地考虑和实施各建议。

行业先导

这些建议的实施将需要政府、行业和非政府组织的共同领导和支持。然而，双方专家都承认行业对分析问题、发现有效的解决方案和实施这些建议等方面起到的重要作用。这一结论是基于一个简单的事实得出的，即构建、运行和拥有网络的公司以及为这些公司提供服务的公司，他们的工作人员都很擅长关键的专业技术和操作知识[59]。这是公司引导*行业*合作的一个实例[60]。

行业自律

除了上面刚提到的这一点外，其它大部分指导都采取了自愿的最佳实践的形式。这样，很重要的一点就是，应认识到各最佳实践在特定环境下的适用性取决于很多因素，这些因素需要由在最佳实践所涉及的相同领域中拥有适当的经验和专业知识的人员来进行评估。

尽管最佳实践方案遵循了自愿原则，网络运营商，网络服务提供商和电子邮件服务提供商仍应当意识到失职的后果。由于用户服务不佳而可能丢失用户外，或者落后于最佳实践方案部署的曲线，这样他们在无意间将会导致大量垃圾邮件在短期内滋生。

建议展现

作为重大决策，每条建议均言简意赅，维持报告编制的动力和调动行动所需的资源。建议陈述大纲如下所示：

- **标题** – 便于识别且起到概括作用。
- **背景** – 提供与所陈述问题相关背景的一些基本要素。
- **建议** – 确定由谁来做、做什么。.
- **所需承诺** – 清楚地列出重要参与方对成功的。
- **好处** – 涵盖了对于实施建议的价值定位。
- **替代方案及其影响** – 列出其它可选方案以及它们可能带来的结果。
- **下一步骤** – 就保持发展势头和关注给出建议。
- **衡量成功与否** – 提供能够客观评价绩效的方法。

[58] 比如，纯粹技术方面的指导除外。与指导相关的一些政策或合作方面包括在内。
[59] 表 X 详细概述了最佳实践方案以及主要实施任务。
[60] PPP 强调私营机构领导的作用；这是在 2009 年 4 月 27-28 日在塔林召开的欧盟“关键信息基础设施保护”部长级会议上发表的主要讲话中其作者所创造的一个词语；同时，在 2009 年 IEEE 信息和通信基础设施可靠性对话中也提及过。

4.1 行业合作水平提高

背景

垃圾邮件信息通常跨越多个网络进行远距离传播。多个网络之间的信息传播使得网络运营商和服务供应商更加难以追踪信息的路径。当信息通过两个国家之间的接口传播时，这种困难可能更加显著。垃圾邮件制造者发掘出国际协调中存在的弱点，从而使他们的身份难以被发现，垃圾邮件信息难以被识别而且对抗措施难以运用。因此，国际 ASPR（协议、标准、策略与法规） 对于有效处理垃圾邮件非常重要。

几年来，双方均认为在进行反垃圾邮件活动时应优先考虑进行国际合作[61] [62]。这种合作不断扩展，包括现在双方之间的合作。合作中目前存在分歧的原因包括简单因素和复杂因素。简单原因之一便是语言障碍。网络安全工程师之间所进行的垃圾邮件应对措施讨论包含了一些先进的理念和术语，从而使得对话变得晦涩难懂，因此对语言技能的要求非常高。其它简单原因还包括时差问题以及普遍缺乏对他国网络环境的了解[63]。除了这些因素，还有其它一些更简单的原因阻碍了当前反垃圾邮件活动的合作。一个略为复杂的原因便是来自两国的网络安全工程师之间缺少人际关系的发展[64]。另一个原因是两国之间在进行信息通信技术讨论时缺乏信任。在这些问题得到处理前，垃圾邮件发送者仍可能继续有效地利用出这种矛盾。

本建议通过提出立即可行的指导正面解决了这种隔阂。此外，双方行业的专家对快速推动建议的发展有着浓厚的兴趣[65]。本建议呼吁现有的为各国服务的国际论坛主动彼此合作并向各自的网络运营商和服务供应商伸出援助之手。具体地说，这意味着这些组织应调整他们的章程，拓展他们的会员并按照其他国家成员的需求安排会议地址。

建议 1

中美网络运营商和互联网服务供应商，电子邮件服务提供商以及其他国家地区的合作伙伴们应建立一个以减少网络空间的垃圾邮件为目标的，可以促进定期合作的论坛。

所需承诺

为有效落实推荐意见，建议各方做出以下承诺：

- ☐ 中国企业必须致力于他们同美国同行之间的合作。
- ☐ 美国企业必须致力于他们同中国同行之间的合作。
- ☐ 建议中美政府机构进一步致力于鼓励减少垃圾邮件方面的合作。
- ☐ 必须重新建立一个或在已有论坛的基础上建立一个国际反垃圾邮件行业组织，以致力于扩大各国的参与，直至双方均参与到活动中来。

[61] 2005年首尔-墨尔本反垃圾邮件协议：谅解备忘录(MoU)是由澳大利亚、中国大陆、中国香港、日本、韩国、马来西亚、新西兰、菲律宾、泰国和中国台湾共同签署的。
[62] 美国网络运营商和服务供应商积极加入行业发起的国际组织，如反信息滥用工作组（MAAWG）。
[63] 3.1 节美国专家所收集的有关中国方面的观点中的不一致的了解程度。
[64] 人们最终还是相互信任，这使得人际关系对于这种改进至关重要。见 2007 年 3 月欧盟委员会所发布的电子通信基础设施的实用性和稳健性（ARECI）最终报告中第 98 条关键发现。
[65] 报告公布时，双方某些相关团体纷纷表达他们想加入他们伙伴的反垃圾邮件队伍中的热切愿望。

替代方案及其影响

本方法的替代方案包括以下几项：

- 不采取任何措施…*将造成两国之间以及世界范围内的垃圾邮件增多。*
- 将反垃圾邮件活动的合作限制在已有的合作努力范围内…*将错失公开对话和加深了解的良机。*
- 政府机构试图管理行业的交互活动…*将造成与复杂政治因素之间难以处理的不必要的的冲突。*

好处

实施本建议的好处首先是加强了两国相关专家之间的合作。这一合作将使专家能更快地对网络问题作出反应，并加强对垃圾邮件和僵尸网络的识别能力，从而最终减少污染网络的垃圾邮件。此外，在这里建立的谨慎的信任有望发展为更深层次的对于更重要主题上的信任。

下一步骤

所推荐的能形成并保持本建议实施动力的下一步骤包括以下几项：

1-1. 来自中美双方网络运营商，互联网服务供应商和电子邮件服务提供商的反滥用网络安全专家进行会面以确立公司间的联系方式，并就垃圾邮件发展趋势的结果进行比较，还共同分享在反垃圾邮件应对措施的有效性和可行性方面的经历。

1-2. 中美反滥用网络安全专家制定发展互信和共同参与反垃圾邮件活动的程序。

1.3. 来自中国、美国和其它相关团体的反滥用网络安全专家定期会面，以在反垃圾邮件方面进行合作。

衡量成功与否

建议是否得以成功实施可通过下列措施进行衡量：.

A. 联络点已确立。

B. 通过反垃圾邮件和僵尸网络方面的有影响力的合作证明互信关系已建立。

C. 由行业发起的、更加全面的国际反垃圾邮件的管理论坛已建立。

D. 两国制造的垃圾邮件数量有所减少。

4.2 自发采用专家最佳实践方案

背景

若网络运营商、互联网服务供应商、电子邮件服务提供商和安全应用开发商不采取非常先进的应对措施并时刻保持警惕，我们所知的电子信息便无法发送。若我们不努力，电子邮件中垃圾邮件的比重很快就会超过 99%。用户需从成百上千条的信息中筛选出一条合法的信息，这种负担是大多数用户都不能忍受的。因此，当前的最佳实践方案已经证明其对于维护我们所知的电子邮件发送的持续可行性起着至关重要的作用。最佳实践方案同时也是改善当前环境的希望所在。

在专家聚集一堂共同分享各自观点的情况下可制定出最好的最佳实践方案。这可在公司或机构内、

行业间或国内或国际各团体间进行。这是还尚未发展完全的最后一个层面。

通过国际合作来制定最佳实践方案这一方法已实施了很多年[66]。然而，中美之间的合作却成果寥寥。本建议通过由双方联合专家团队共同制定的 46 项最佳实践方案[67]来促进合作。一旦实施，这些最佳实践方案会减少垃圾邮件信息的产生、传播以及被无意打开。而且，因为垃圾邮件发送者会不断进行调整以使当前的反垃圾邮件应对措施失效，故其中的一些实践方案的动态属性应确保能提供应对措施。

建议 2

中美电子邮件服务提供商、互联网服务供应商、网络运营商和政策制定者以及其他国家地区的同行应酌情考虑网络配置、经营模式和其它可行性因素，共同合作制定、维护和自愿采用共识的最佳实践方案。

所需承诺

为有效落实本推荐意见，建议各方做出以下承诺：

- ☐ 企业必须在适当的情况下致力于实施最佳实践方案。
- ☐ 企业必须致力于为最佳实践方案的开发合作提供专门知识。
- ☐ 建议中美政府机构在适当的情况下致力于实施最佳实践方案。
- ☐ 建议中美政府机构考虑对行业的专门知识和经验的需要，以便为最佳实践方案的开发和应用提供指导。

替代方案及其影响

本方法的替代方案包括以下几项：

- o 不采取任何措施…*将造成两国之间以及世界范围内的垃圾邮件增多。*
- o 最佳实践方案的讨论仅限于当前的几方…限制了垃圾邮件可能变得更成熟的机会以及所有最佳实践方案指南的实施。
- o 政府机构强制实行网络管理工作…*将造成网络性能无法达到最佳，行业对所关注问题的反应灵活性降低。*

好处

本建议一旦被实施，将为两国在处理垃圾邮件问题、计算机病毒和互联网欺诈所产生的间接问题方面提供前沿的知识和经验。而且，由于其它多方的努力，专家指导过程将进一步促进开发和实施更好的最佳实践方案。

[66] 当前国际合作实例包括：反信息滥用工作组（MAAWG）、ETIS 反垃圾邮件合作小组和国际反垃圾邮件组织项目。
[67] MAAWG 主席 Michael O'Reirdan 对此次双边行动如此评价："与中国的这次对话是一个最令人欢欣鼓舞的突破—这是真正向前迈进的一步。"2011 年 2 月， http://www.ewi.info/first-china-us-effort-fight-spam。

下一步骤

所推荐的能形成并保持本建议实施动力的下一步骤包括以下几项：

2.1. 中美网络运营商和互联网服务供应商、电子邮件服务提供商对本报告中的各个最佳实践方案进行考虑，并在适当的情况下投入实施。

2.2. 双方和其它有意加入的参与者共同合作，以让最佳实践方案指南得以通用，并对其不断进行改进。

2.3. 基于上面几个步骤的反馈情况，应由一个可靠的中立实体来进行支持协议实施所需的政策和经济上的安排。

衡量成功与否

建议是否得以成功实施可通过下列措施进行衡量：

A. 最佳实践方案已经实施。

B. 最佳实践方案已更新和维持。

C. 垃圾邮件的制造和传播减少。

D. 僵尸网络已被识别出并已关闭。

4.3 双边达成共识的最佳实践方案

本节中介绍了双边为减少垃圾邮件而达成共识的最佳实践方案指南。已根据第 2 节中所列出的方法对 46 项最佳实践方案进行了清晰的描述且就这些方案达成了一致意见。如前所述，这些最佳实践方案都遵循自愿原则，而且其本身就是比较灵活的政策。它们体现了与反垃圾邮件工作相关的某一方（可能是个人或企业或政府机构）对其他相关各方的合理期望。

垃圾邮件的生命周期

考虑垃圾邮件的生命周期对于了解各最佳实践方案的目标非常有利。下面的图 4 列出了一个高水平的大纲，这一大纲是以生命周期为基础建立的，包括生命周期中各阶段的国际背景、主要活动者和对抗措施（如：最佳实践方案）的主要目标。

在生命周期的初期，某一国家的垃圾邮件制作者制作垃圾邮件（阶段 A）。生命周期这一阶段的最佳实践方案着重说明垃圾邮件制作者的动机。生命周期的下一阶段（阶段 B）在电子格式的文件（如电子邮件）中插入垃圾邮件。本阶段应对措施的主要目标是为了减少插入的信息量。在（阶段 C）则由它们网络的互联网服务供应商，网络运营商和电子邮件服务提供商对垃圾邮件进行分配。这一阶段的反垃圾邮件应对措施的主要目标是发现正在发送的垃圾邮件。下一阶段（阶段 D）则是将垃圾邮件从一个网络转移至另一个网络[68]。这通常出现在存在国际壁垒的情况中。针对网络切换的应对措施在这一阶段主要是针对同等网络间的信息共享。

[68] 以同一网络作为目标的垃圾邮件信息当然可能停留在网络内部。

关键要素	国际垃圾邮件质量管理框架					
国家或地区	源头 *			衔接	目标	
Primary Actor:	垃圾邮件制作者		服务供应商和网络运营商		最终用户	
生命周期阶	制作	插入	分配	切换	接收	开启
应 对 措 施 目	减少动机	减少发送量	发现传播	分享数据	信息过滤	滥用报告
	A	B	C	D	E	F

图 4. 国际垃圾邮件质量管理框架

最后两个阶段是为已达到目的地的垃圾邮件而准备的。首先，垃圾邮件被接收（阶段 E）[69]。此阶段有效的应对措施是过滤信息。垃圾邮件信息生命周期的最终阶段则是在它被最终用户打开的时候（阶段 F）[70]。到了这一阶段，也许不会产生任何危害，但也许终端用户的电脑会接触到恶意代码，或最终用户会接触到欺诈信息或攻击性图片。最终阶段的应对措施主要涉及用户的报告以及互联网服务供应商和电子邮件服务提供商对这些报告的处理。此外，应对措施还包括教育和提醒终端用户。

对上述生命周期进行观察后得出的一个重要结论是：从左至右处理垃圾邮件的费用逐渐增多（如：从 A 到 F）。因此尽早处理垃圾邮件是非常有必要的。最好在其它目标实现之前有效地减少动机。同样，我们应当在发现传播或分享数据前减少垃圾邮件的发送量。因为没有任何一组对抗措施会完全有效，因此每个阶段都应有与之相对应的合适措施。

最佳实践方案表述

对每项最佳实践方案的表述采用的格式中含有唯一识别码、指南重点的简短概要、执行的责任方和待解决问题的指明以及应对措施的性质（图 5）[71] [72]。

[69] 接收者可能是公司网络或大学网络。公共互联网服务供应商的策略与公司或大学网络的策略可能不同。
[70] 并不是所有经过过滤的信息都将被打开。这只是为了对完成生命周期进行说明。
[71] 此处所采用的唯一识别码系统的格式为 CN-US 11-001，其中“CN-US”指代中美双方，“YY-XXX”指代具体最佳实践方案被引进或在新版本面世前最新更新的年份（如 11 代表 2011 年）。修订的最佳实践方案可能保留其独特的三位数字，但是 YY 标号可能改变。
[72] 八大问题均按图 3 所示进行排列。即按顺时针方向，由左上角开始的顺序为：能源、软件、有效负荷、人、环境、硬件、网络和政策—另外被称为 ASPR。

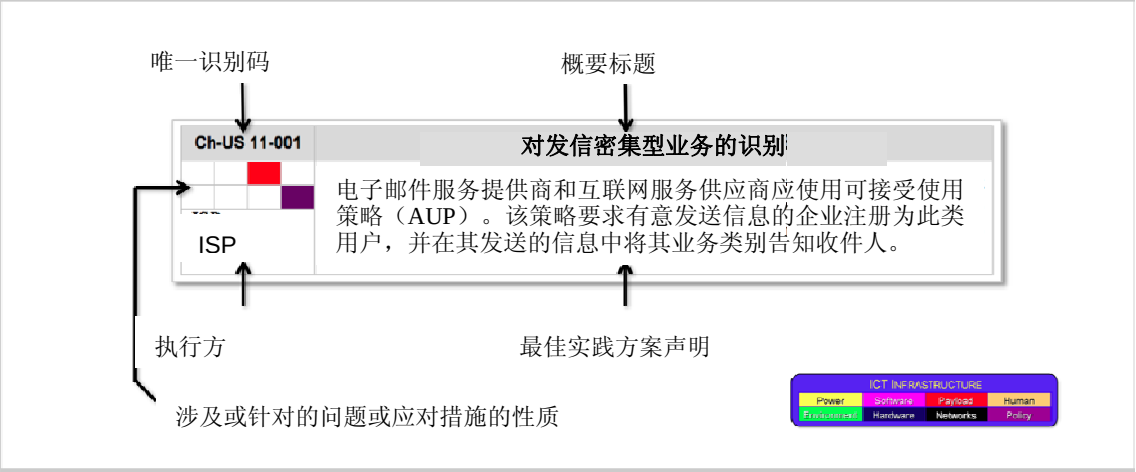


图 5.双方最佳实践方案描述

最佳实践方案原则

双方联合专家团队中在开发这些最佳实践方案的过程中采用了行之有效的方法。此处给出的指导意见符合行业内达成共识的最佳实践方案标准，包括以下 7 项考虑事项[73]：

1. 人们是否执行最佳实践方案[74]
2. 最佳实践方案是否支持“付费”文件、产品或服务[75]
3. 最佳实践方案是否实现了对问题的分类[76]
4. 最佳实践方案是否已被执行[77]
5. 最佳实践方案是否在取得高度共识后得出[78]
6. 最佳实践方案是否经过未参与开发进程的专家验证[79]
7. 通过充分严谨的审核和分析确保了实践方案的概念问题和特殊措辞的准确性后方对最佳实践方案进行表述[80]

表 3 列出了双方共识最佳实践方案的内容以及执行的责任方。

[73] 《劳舍尔最佳实践 7 大原则》，NRIC V 陈述，华盛顿，2001 年。
[74] 最佳实践方案的内容为各行专家所了解并由其所应用。
[75] 最佳实践方案的开发进程不应用于创造商业利益。
[76] 即他们并非具体固定分类。
[77] 并不是说大部分人正在执行实践方案，因为那样就成为了“通用方案”。然而，应证明至少在一个实体机构实践方案是有效可行的。
[78] 只有高度统一的最佳实践方案能被包括在内。进程中每位参与者应有充足机会就他们自己的观点来影响和说服其他同行。
[79] 为避免“群体思维”，应将最佳实践方案草案传播至各相关专家和其他利益相关者，以便其对之进行评述。
[80] 考虑到目标实现过程中的有效性、执行成本和执行风险等因素，不应对最佳实践方案进行全面检验。

表 3. 双方共识最佳实践方案及实施责任

最佳实践方案编号	标题	GPM	ESS	NO	ISP 和 ESP	NZN
CN-US 11-001	减少动机					
CN-US 11-002	顺其自然					
CN-US 11-003	潜在垃圾邮件发送者教育活动					
CN-US 11-004	允许互联网服务提供商和邮件服务提供商收取一定费用					
CN-US 11-005	特定用户协议					
CN-US 11-006	更新策略时保持警惕					
CN-US 11-007	对发信密集型业务的识别					
CN-US 11-008	限制向适当收件人发送					
CN-US 11-009	用户协议高使用限值					
CN-US 11-010	出站垃圾邮件分类					
CN-US 11-011	允许互联网服务供应商区别对待垃圾邮件发送者					
CN-US 11-012	端口 25 输出封锁					
CN-US 11-013	信息识别合作					
CN-US 11-014	剔除不符合要求的信息					
CN-US 11-015	越快越好					
CN-US 11-016	跨境使用 DKIM 机制					
CN-US 11-017	跨境使用 SPF 机制					
CN-US 11-018	联合技术平台					
CN-US 11-019	关闭开放转发					
CN-US 11-020	列入黑名单的互联网服务供应商					
CN-US 11-021	针对统计资料的国际合作					
CN-US 11-022	与同行之间的反馈环路					
CN-US 11-023	跨境使用 FBL 机制					
CN-US 11-024	最佳实践方案清单					
CN-US 11-025	通过 IP 地址追踪僵尸网络					
CN-US 11-026	通过域名追踪僵尸网络					
CN-US 11-027	注册机构反馈					
CN-US 11-028	基于 FBLs 的国际合作					
CN-US 11-029	通过反向搜索向隐藏技术发起挑战					
CN-US 11-030	支持 WHOIS					
CN-US 11-031	隐藏检测					
CN-US 11-032	自愿协议的好处					
CN-US 11-033	自愿国际协议					
CN-US 11-034	合作抑制垃圾邮件					
CN-US 11-035	ASPR 清单					
CN-US 11-036	弥补差距					
CN-US 11-037	反恶意软件支持					
CN-US 11-038	垃圾邮件提醒					
CN-US 11-039	垃圾邮件过滤					
CN-US 11-040	垃圾邮件报告					
CN-US 11-041	垃圾邮件报告中心					
CN-US 11-042	垃圾信息邮箱					
CN-US 11-043	禁用垃圾信息发送帐户					
CN-US 11-044	网民教育活动					
CN-US 11-045	垃圾信息报告管理					
CN-US 11-046	用户服务和教育					

减少动机

由于电子邮件是当前成本很低的有效通信方式，因此垃圾邮件的问题也随之突显出来。当企业对外发送垃圾邮件时，通常会给他们带来明显的经济利益，即充满诱惑的投资回报（ROI）[81]。

防止垃圾邮件产生的根本方法是减少垃圾邮件发送者的动机。只要通过垃圾邮件可产生收益或满足其他需求，就会有人加以利用。许多解决此动机问题的方法都考虑过，但是最终大部分都遭遇到了许多因素的限制，如言论自由、销售电子信息服务的基本经营模式、保持低成本电子信息服务的需求及其使用简单的特征。

解决垃圾邮件发送者的动机问题是下列最佳实践方案的重点：

CN-US 11-001	减少动机
GPMs ISPs ESPs NZNs	电子邮件服务提供商，互联网服务供应商和政策制定者应考虑制定可减少个人或机构发送垃圾邮件动机的协议、标准、策略和法规（ASPR）。但是，此类协议、标准、策略和法规不得妨碍新建合法企业展示其自身实力，也不得侵犯个人表达自我的合法权利。

CN-US 11-002	顺其自然
GPMs	建议政策制定者通过提倡符合企业基本面和社会力量的策略避免对死板规定的依赖，从而为网络容量以及用户服务方面的新发展做好准备。

CN-US 11-003	教育潜在垃圾邮件发送者
GPMs ISPs ESPs NZNs	政府机构，互联网服务供应商和电子邮件服务提供商应考虑开展社区推广活动，以让现有的以及潜在的垃圾邮件发送者认识到国家禁止滥用电子信息系统[82]。

CN-US 11-004	允许互联网服务提供商和邮件服务提供商收取一定费用
GPMs	建议政策制定者考虑研究制定相关政策，允许企业向信息业务量较大的用户收取费用[83][84]。

CN-US 11-005	特定用户协议
ISPs ESPs NZNs	电子邮件服务提供商和互联网服务提供商应通过用户协议对新的电子邮件账户和应用做出具体规定，以创建一种合同机制，严格执行可接受使用策略（AUP），防止邮件滥用现象。

[81] 基于意识形态动机的垃圾邮件发送者除外。
[82] 如海报、传单、促销宣传资料和志愿者指南。
[83] 针对高级企业帐户收取的额外费用产生的效果是有限的。
[84] 政府监管部门已意识到设施、电、硬件、软件、网络容量和人员等是一笔不小的长期运作费用。

CN-US 11-006	更新策略时保持警惕
GPMs ISPs ESPs NOs ESS	政府、网络运营商、互联网服务供应商、电子邮件服务提供商以及设备和软件供应商应对与垃圾邮件有关的有效策略时刻保持密切关注，以便考虑新应用程序和设备的影响。

减少数量

全球网络每天都有数千亿的垃圾邮件。从源头减少垃圾邮件的数量远比经网络传播后再进行处理经济有效得多。

垃圾邮件能够传播的原因之一是其很难被互联网服务供应商、网络运营商和收件人识别。这通常是由于垃圾邮件发送者的故意欺骗所致。因此，团队采取了措施来确定发件人是谁、邮件数量是否巨大、传播范围是否广泛。由于并不是所有批量的商业邮件均为垃圾邮件，因此采取措施时需谨慎小心，以免影响合法的商业活动。降低这种不确定性是下列最佳实践方案的重点[85]。

下列最佳实践方案旨在减少垃圾邮件的数量以及与垃圾邮件有关的欺骗行为。

CN-US 11-007	对发信密集型业务的识别
ISPs ESPs NZNs	电子邮件服务提供商和互联网服务供应商应使用可接受使用策略（AUP）。该策略要求有意发送信息的企业注册为此类用户，并在其发送的信息中将其业务类别告知收件人。

CN-US 11-008	仅发送给合适收件人
NZNs	想要通过发送电子信息进行大数量、大范围通信的网民应将信息仅发送给可能对信息内容感兴趣的收件人。

CN-US 11-009	提高用户协议的使用门槛
ISPs ESPs NZNs	互联网服务供应商和电子邮件服务提供商应考虑对信息业务量较大的用户实施可接受使用策略（AUP），以限制个人和机构发送垃圾邮件。此类协议的管理方式应确保计算机感染僵尸网络病毒的用户不会进行胡乱操作[86]。

[85] 形式通信理论认为通过通信信道传递信息时存在一定程度的不确定性。“香农熵”一词可用来描述上述不确定性。对此基本原理的理解有助于在“信号”清晰度最大化和降低“噪音”等优先次序方面应用基本通信工程原理。

[86] 见附录 B—互联网服务供应商致用户的函件（样本）。

CN-US 11-010	出站前进行垃圾邮件的分类
ISPs ESPs	互联网服务供应商和电子邮件服务提供商应协助在出站前进行垃圾邮件的分类，以便某用户账户被黑客攻击或感染 spambot 病毒后电子邮件供应商可通过禁用该账户来阻止垃圾邮件出站[87]。

CN-US 11-011	允许互联网服务供应商区别对待垃圾邮件发送者
GPMs	建议政策制定者考虑研究制定相关政策，区别对待信息业务量大且传播范围广的用户。这样的实践并不代表需要公开提供这些信息或者由政府来管理。

CN-US 11-012	端口 25 输出封锁
ISPs ESPs	互联网服务供应商和电子邮件服务提供商应考虑在 TCP 端口 25 执行输出过滤操作，并将其设定为默认功能，以阻止僵尸网络非法利用。需要电子邮件服务器的用户可配置静态 IP 地址，并作为例外进行管理。

检测垃圾邮件的传播

良好工程实践的基本原则是有效利用可用的有限资源。处理垃圾邮件时，在源头附件检测垃圾邮件优于在目标地址附件检测垃圾邮件。这样就不会浪费在垃圾邮件的网路传播过程中的资源。这种有形资源浪费包括一些不必要的负担，如硬件容量、软件处理器周期、驱动硬件和维护室内网络设备所需的电能、操作维护此类设备的人员。

能够使垃圾邮件在源头附近得以检测到的三个主要因素如下：有关邮件识别的情报、有关垃圾邮件发送源的情报以及学习和追踪垃圾邮件发送者为避免被检测到而采用的调节装置的效能。检测垃圾邮件在网络上的传播是下列最佳实践方案的重点。

CN-US 11-013	信息识别合作
NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应在国际论坛中相互合作，开发出有效的方法来提高利用邮件标题内容以及信息协议识别合法邮件的有效性[88]。

CN-US 11-014	剔除不符合要求的信息
NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应采用现有机制识别并剔除垃圾邮件。应考虑如何剔除不符合要求的信息。

[87] 识别方法包括内容分析以及检测特定账户发出的信息量是否有增加现象。
[88] 如 DKIM、SPF、IETF RFC 4871。

CN-US 11-015	越快越好
 NOs ISPs ESPs	网络运营商，互联网服务供应商和电子邮件服务提供商应优先采取这样的策略，即在垃圾邮件传播途径上尽可能早地发现并删除它。这会有效地降低此类垃圾信息在互联网传播过程中所带来的成本[89]。

CN-US 11-016	跨境采用 DKIM 机制
 NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应利用可用的域名密钥识别邮件（DKIM）机制，特别是当与国际同行衔接时，以提高网络信息的可信度。

CN-US 11-017	跨境采用 SPF 机制
 NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应利用可用的发件人策略框架（SPF）机制，特别是当与国际同行衔接时，以提高网络信息的可信度。

CN-US 11-018	联合技术平台
 NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应考虑合作开发能协调垃圾邮件的检测和管理的技术平台。

CN-US 11-019	关闭开放转发
 NOs ISPs ESPs	电子邮件服务提供商，互联网服务供应商和网络运营商应考虑关闭开放邮件转发，以便防止垃圾邮件发送者利用其用途隐藏发送源、识别信息[90] [91]。

共享数据

垃圾邮件发送者利用的了互联网的复杂网络系统。他们还进一步开发出了该复杂网络系统的国际性。为了取得成功，互联网服务供应商，电子邮件服务提供商和网络运营商需在信息共享方面密切合作，以赶上垃圾邮件发送者的策略[92]。由于不同的公司其经营模式和可接受使用策略均有所不同，因此合作并不总是一件直截了当的事情，相反，其可能需要经过谈判才能建立双方的利益共同点。

下列最佳实践方案重点关注业界同行中的可靠信息共享问题，尤其是涉及国际接口的行业。

[89] 美国互联网服务供应商已经表示他们在网络入口点对入站邮件的检测率可达到 90%左右。
[90] Lindberg, G., RFC 2505，SMTP MTA 反垃圾邮件建议书，1999 年 2 月。
[91] Klensin, J., RFC 5321，简单邮件传输协议， 2008 年 10 月。
[92] 第 4.1 节— 建议 1：改进行业合作。

CN-US 11-020	列入黑名单的互联网服务供应商
 NOs ISPs ESPs	网络运营商应跨境合作，对将 IP 地址空间块租赁给垃圾邮件发送者的电子邮件服务提供商和互联网服务供应商进行封锁。

CN-US 11-021	针对统计资料的国际合作
 NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应在国际范围内相互合作，积累有助于制定有效协议、标准、策略和法规（ASPR）的全球统计资料，包括趋向信息，从而确保决策者具有足够的信息资料可查阅。

CN-US 11-022	与同行之间的反馈环路
 NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应设立反馈环路机制，便于垃圾邮件的报告和识别，从而提供已确定为垃圾邮件的有关信息。

CN-US 11-023	跨境使用“有效循环反馈（FBL）”机制
 NOs ISPs ESPs	网络运营商，互联网服务供应商和电子邮件服务提供商应该同其所联接的其它国家的同行一起建立“有效循环反馈（FBL）”机制，以增加有助于进一步管理好垃圾邮件的信息[93]。

CN-US 11-024	最佳实践方案清单
 NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应对反垃圾邮件最佳实践方案（包括涉及国际范畴的方案）列表不断更新，并定期通过该列表弥补差距。

CN-US 11-025	通过 IP 地址追踪僵尸网络
 NOs ISPs ESPs	互联网服务供应商和电子邮件服务提供商应确定发送垃圾邮件的僵尸网络的互联网协议（IP）地址，并将之报告给相关网络运营商，以助于关闭僵尸网络活动[94] [95]。

[93] 投诉反馈环路最佳现行实践，MAAWG，2010 年 4 月。
[94] 引用最近的赛门铁克公司报告—俄罗斯近期关闭僵尸网络行动造成垃圾邮件急剧减少。
[95] 见 Conficker 工作小组，www.confickerworkinggroup.org。

CN-US 11-026	通过域名追踪僵尸网络
NOs ISPs ESPs	互联网服务供应商和电子邮件服务提供商应利用发送垃圾邮件的僵尸网络的域名，并将之报告给相关网络运营商，以便关闭僵尸网络活动。

CN-US 11-027	注册机构反馈
NOs ISPs ESPs	互联网服务供应商和电子邮件服务提供商应将流氓网站报告给相关注册机构，以便能够采取适当措施（如关闭域名）。

CN-US 11-028	基于 FBLs 的国际合作
GPMs NOs ISPs ESPs	特定国家的政策制定者，电子邮件服务提供商和互联网服务供应商应认识其所在国的国际化机构，以便国家之间就网络接口策略，如反馈环路（FBL）的使用，进行合作[96]。

CN-US 11-029	通过反向搜索向隐藏技术发起挑战
NOs ISPs ESPs	互联网服务供应商，电子邮件服务提供商和网络运营商应考虑配置自己的邮件交换系统，以便对域名服务器(DNS)入口进行反向搜索，从而确定与 IP 地址关联的指定域名。

CN-US 11-030	支持 WHOIS
NOs ISPs ESPs	互联网服务供应商，电子邮件服务提供商和网络运营商应考虑配置自己的邮件交换系统，以支持 WHOIS 查询，从而确定注册用户或互联网资源代理人[97] [98]。

CN-US 11-031	隐藏检测
NOs ISPs ESPs	互联网服务供应商，电子邮件服务提供商和网络运营商应考虑配置自己的邮件交换系统，以正确识别标识邮件服务器域名且采用适当格式化的标语，从而测定为检测隐藏的身份或发送源而尝试的次数。

[96] 电讯工业方案联盟（ATIS）下一代互连互操作性论坛（NGIIF）持有世界 1 区的无线和有线网络联系人名单。
[97] Daigle, L., RFC 3912，WHOIS 协议说明，IETF，2004 年 9 月。
[98] 互联网资源可能包括域名、IP 地址块或自治系统。

CN-US 11-032	自愿协议的好处
GPMs NOs ISPs ESPs	政策制定者和行业应意识到自愿协议、标准和策略的好处，从而避免对死板政府法规的依赖。

CN-US 11-033	自愿国际协议
GPMs NOs ISPs ESPs	政策制定者和行业应考虑在国家之间签订有利于减少垃圾邮件（如关闭发送源）的自愿协议。

CN-US 11-034	合作抑制垃圾邮件
NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应通过与同行之间的自愿协议相互合作，抑制垃圾邮件（如共享有嫌疑的签名和发送源）。

CN-US 11-035	ASPR 清单
NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应持有一份用于减少垃圾邮件的协议、标准、策略和法规（ASPR）清单，从而追踪预定计划的进程。

CN-US 11-036	弥补差距
NOs ISPs ESPs	网络运营商，电子邮件服务提供商和互联网服务供应商应定期对尚未实施的最佳现有反垃圾邮件措施进行鉴定，以弥补差距。

过滤邮件

一旦垃圾邮件到达其指定地点，离其实现目标就不远了。若没能在垃圾邮件到达其指定地点之前对其进行阻止，则很糟糕，因为在此期间已经产生了隐藏成本[99]。现在，可通过高级软件安全应用程序进行智能过滤，从而识别垃圾邮件，并将其视作威胁加以抑制。

下列最佳实践方案重点关注垃圾邮件的过滤对策。

[99] 对于单独的一条信息而言， 此成本可忽略不计，但是对全球范围的大量信息而言，则是一笔不小的费用。

CN-US 11-037	反恶意软件支持
ESS ISPs ESPs NZNs	如果可行，互联网服务供应商和电子邮件服务提供商应向其用户提供反恶意软件的软件。

CN-US 11-038	垃圾邮件提醒
ISPs ESPs NZNs	互联网服务供应商和电子邮件服务提供商应向其用户提供当前垃圾邮件提醒服务，以减少用户计算机感染僵尸网络病毒的几率。

CN-US 11-039	垃圾邮件过滤
ESS NZNs	网民应使用垃圾邮件过滤器，以防止其计算机感染僵尸网络病毒。

报告垃圾信息

反垃圾邮件的关键在于号召受害者参与。垃圾邮件受害者在增加关于已通过防御的垃圾信息的知识方面起着重要的作用。而此类资料恰好能够帮助互联网服务供应商做出改进。

下列最佳实践方案重点关注终端用户报告以及互联网服务供应商对这些报告的管理[100]。

CN-US 11-040	垃圾邮件报告
ISPs ESPs NZNs	网民应通过反馈环路报告垃圾邮件，以向互联网服务供应商和电子邮件服务提供商提供关于垃圾信息的资料，从而使得这些信息能够被识别和处理。

CN-US 11-041	垃圾邮件报告中心
GPMs NOs ISPs ESPs NZNs	政府和行业应考虑向网民提供一个垃圾信息集中报告方式。

[100] 本次讨论中，互联网服务供应商可以包括所有邮件服务供应商（ESP）。

CN-US 11-042	垃圾信息邮箱
ISPs NZNs	互联网服务供应商和电子邮件服务提供商应提供垃圾信息邮箱（如 abuse@company.com），以便网民一旦发现垃圾信息即可报告[101]。

CN-US 11-043	禁用垃圾邮件发送账户
NOs ISPs ESPs NZNs	互联网服务供应商和电子邮件服务提供商应 勤奋处理来自全球的反馈报告（如 FBL）和垃圾信息报告（如发送至 abuse@company.com 的信息），从而使得有证据证明某托管账户就是垃圾邮件发送源。可对该攻击型账户发出通告，并在情况允许时，随即将其禁用。

CN-US 11-044	网民教育活动
GPMs ISPs ESPs NZNs	政府机构和互联网服务供应商以及电子邮件服务提供商应考虑开展社区推广活动，以提高网民对垃圾邮件识别、打开垃圾邮件的危险以及报告垃圾邮件的可用机制等方面的认识[102] 。

CN-US 11-045	垃圾信息报告管理
ISPs ESPs NZNs	互联网服务供应商和电子邮件服务提供商在对垃圾信息报告进行分析和处理时应进行一定程度的尽职调查，直到将垃圾信息发送者的账户禁用（如果情况允许）。

CN-US 11-046	用户服务和教育
ISPs ESPs NZNs	互联网服务供应商和电子邮件服务提供商应与计算机疑感染僵尸网络病毒的用户合作，以清除其计算机中的恶意代码，并教育用户如何保持其计算机处于健康状态。

[101] RFC 21 42。
[102] 如海报、传单、促销宣传资料和志愿者指南。

5 结论

本报告总结了中美互联网界在网络安全领域建立双边互信机制的一次探索性实践。这个阶段的任务主要是处理网络空间垃圾邮件污染的重要问题。鉴于双方在垃圾邮件方面拥有的共同利益，携手解决这一问题将为构建互信机制提供契机。

此次反垃圾邮件双边活动的三大目标已经实现，体现在以下三个方面：（1）在相关专家和利益相关者之间展开新的对话，（2）实现双方更深入的了解，（3）就减少网络空间垃圾邮件污染建立专家舆论引导。此项活动中联合提出的两大可操作的总体建议，一旦实施，将有效减少两国产生的垃圾邮件。

两大建议中对后续工作步骤进行了概述，其中包括鼓励两国互联网行业更多的专家加入此项活动，以及考虑和采用本文推荐的最佳实践。

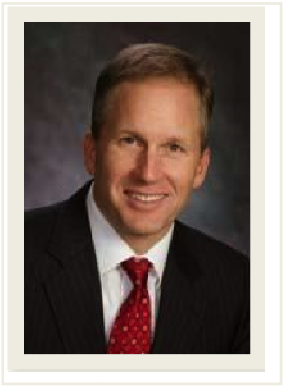
此项活动后续步骤的另一项重要内容是将活动从双边团队推广到其他国家/地区。双边活动中极为重要的第 8 个步骤就是与全球更多性相关专家和团体建立关系。我们双方的参与者全力支持此项活动并为推广活动制定了相关计划。推广活动的目的之一是鼓励适当采用双方一致认可的最佳实践方案。本报告面向公众公布本身就是此推广活动的重要组成部分。因此，我们在本报告最终出版之前就先期公布了报告即将出炉的消息，这个消息得到了广大专家和相关同行的热烈欢迎，我们为此深受鼓舞 [103]。

[103] *中美首次联合反垃圾邮件行动*。http://www.ewi.info/first-CNina-us-effort-fight-spam，美国佛罗里达州奥兰多，2011 年 2 月 23 日。在反信息滥用工作组（MAAWG）第 21 次大会上，此报告的主要作者们通过联合编制的一份特殊声明，宣布此报告面向公众提供。参与此次反垃圾邮件会议的国际观众约有 400 名专家及其他利益相关者。

个人履历

作者

卡尔·弗雷德里克·劳舍尔



卡尔·弗雷德里克·劳舍尔是东西方研究所的首席技术官和资深成员。他之前曾担任过阿尔卡特—朗讯公司贝尔实验室网络可信和安全处的执行理事，以及贝尔实验室的合伙人。卡尔曾经担任过政府高级顾问和五大洲的业界领导者，包括担任向美国总统负责的国家安全电信咨询委员会工业执行委员会的副主席，以及欧洲委员会赞助的课题“电子通信基础设施的可用性和鲁棒性”的带头人。他最新在“IEEE 全球海底通讯电缆的可靠性基础设施”出版了报告。卡尔担任 IEEE 通信质量和可靠性咨询委员会的名誉主席，以及非盈利性无线紧急应急小组的创办人和主席。他在人工智能、关键基础设施保护、应急通信、能量守恒和远程医疗方面有超过 50 项发明创造，他本人发现了现行网络中超过 1000 个软件漏洞，并促进和发展了超过 600 个业界达成共识的专家最佳实践。劳舍尔先生以优异成绩和最高荣誉的身份从罗格斯大学获得电气工程的理学硕士学位，获得了宾夕法尼亚州立大学的理学学士学位以及圣经研究系达拉斯神学的文学硕士学位。他还是麻省理工学院斯隆学院执行发展计划的参与人员。

周勇林

周勇林先生是中国互联网协会网络与信息安全工作委员会的秘书长，他也是国家计算机网络应急技术处理协调中心运行部的主任。他于 1999 年毕业于中国哈尔滨工业大学，获得计算机科学与技术的硕士学位。周勇林先生从事网络安全工作约 12 年。他参加领导了多个关于网络安全监测，漏洞处置和恶意软件分析项目。他带领他的队伍与政府、互联网服务提供商、互联网内容提供商、域名注册机构、安全服务提供商和安全产品供应商在网络安全威胁监测和事件响应等方面密切开展合作，特别是在反垃圾邮件、打击僵尸网络和拒绝服务攻击方面做出了很大贡献。他还带头开展了反网络病毒联盟（ANVA）和国家信息安全漏洞共享平台（CNVD）等行业协作，中国快速增长的互联网行业和用户能够从中得到及时可信和专业的帮助。周勇林先生还应邀担任政府和大学的技术顾问和兼职教授。他是由科学技术部组织的国家 863 项目评估专家组的成员，其工作是帮助审查项目申请以及评估项目结果。 2008 年，他应邀成为北京奥运会组委会的信息网络安全顾问。他在上述研究领域出版了数篇文章。他还积极参加了网络安全领域的国际合作，并发表多次演讲。

特约专家

韩松，中国万网应急响应中心总监

韩松先生毕业于北京交通大学，工商管理硕士研究生，具有十余年的互联网行业技术经历和管理经验，是中国互联网业界资深人士，现担任中国互联网协会反垃圾邮件综合处理平台项目组特聘专家，中国互联网协会自律工作委员会委员，北京通信行业协会互联网分会副会长。韩松曾服务于多家互联网知名行业，自 2002 年起在中国万网工作，现担任应急响应中心总监，负责网络安全、信息安全等突发事件的应急处置，管理万网突发事件应急预案，监管万网用户网站和域名的不良违法信息，并一直坚决致力于反垃圾邮件、反钓鱼网站等净化网络环境事务。韩松先生多次受邀成为特聘专家，代表公司参与国家多项政策法规的制订和修改，如：《互联网电子邮件服务管理办法》、《通信网络安全防护管理办法》、《互联网网络安全信息通报实施办法》、《域名系统安全专项应急预案》等，其出色工作赢得了工信部、部电信研究院、公安部、中国互联网协会等各主管政府部门的充分信任和高度肯定。

马晓文，中国万网邮件研究

马晓文，系统架构设计师高级职称，从事软件行业工作 10 年，有多年丰富的编程经验，资深计算机架构设计和系统分析专家。负责中国万网行业邮局开发和管理工作，曾经参与和负责中国万网多个系统的架构设计和开发工作，例如：万网短信平台、B2B 商务平台、域名注册系统、万网产品生产控制系统。精通多门计算机语言、深入掌握 Linux 系统内核，以及 Linux 文件系统。现在致力于邮件系统以及相关技术的研究，先后带领万网研发团队，突破了邮件在存储、反垃圾，反病毒，安全投递，以及投递成功率方面的技术瓶颈，保持了中国万网邮件系统在行业内的技术先进性。目前全面负责万网云邮箱技术的研发工作，并且完成了云邮箱成功上线。

胡安廷，中国互联网协会反垃圾邮件工作委员会成员

2002 年毕业于中国石油大学计算机科学与技术系，获硕士学位。2005 年加盟中国互联网协会反垃圾邮件工作委员会，开始致力于我国反垃圾邮件事业的实践与研究工作，现任中国互联网协会反垃圾邮件中心副主任。期间，落实建成我国首家权威的中国互联网协会“反垃圾邮件综合处理平台”，向国际电信联盟第 17 研究组（ITU-T SG17）全会提交《反垃圾邮件处理系统的体系结构和接口参考模型的提案》被采纳为国际标准，开展同国际反垃圾邮件组织的交流与合作，积极推进我国垃圾邮件治理工作，成效显著。在此之前，曾就职于中国互联网络信息中心（CNNIC），实施开通中国首个符合 IETF 多语种域名国际标准的中文域名邮件系统，发表《中文域名邮件技术解决方案》等，积极参与多语种域名相关研究和国际标准制定工作等。

李红，中国互联网协会

副研究员。法国格勒诺布尔高等商学院电子商务专业管理学硕士。2003 年留法归国后在国家计算机网络应急技术处理协调中心工作，同时承担中国互联网协会有关工作，主要从事包括与反垃圾邮件相关的互联网研究、管理与国际合作工作，曾兼任协会国际合作与宣传部副部长。2005 年中国互联网协会反垃圾邮件工作委员会正式成立之时当选为工作委员会常务副秘书长，致力于反垃圾邮件工作的深入研究与业界实践。2006 年受工业与信息化部委托筹建“12321 网络不良与垃圾信息举报受理中心”，担任常务副主任，主持建设举报受理平台。2005 年为原信产部起草和颁布《互联网电子邮件服务管理办法》作前期调研。2006 年主持建设中国互联网协会“反垃圾邮件综合处理平台”并主持平台日常工作。2005-2006 年担任“我国动态 IP 状况研究课题小组”副组长主持研究工作。2009 年主持在发改委申请立项“国家反垃圾邮件预警及处置服务平台”成功。此外，开展了一系列颇见成效的研究工作，提出了一些专业性较强的开拓性建议和研究报告。共完成和发表著作、课题研究报告、论文、标准、提案等 10 余篇著，累积约 30 万字，且其中部分主要研究成果已经应用到我国互联网管理的实践当中。

徐原，中国互联网协会网络与信息安全工作委员会

2005 年毕业于北京邮电大学信息与计算科学专业，获得理学学士。2007 年在瑞典林雪平大学获得通信与互动专业的理学硕士学位。归国后在中国互联网协会网络与信息安全工作委员会工作，主要从事网络安全领域的应急研究和国际合作工作。曾经组织参与了亚太经合组织电信工作组 “僵尸网络应对政策与技术手段指南”和国际电联“全球网络安全议程”等项目的研究工作。

曾明发， 12321 网络不良与垃圾信息举报受理中心（www.12321.cn）副主任 。

资深互联网专家，长期致力于互联网治理和推广普及工作，倡导“大禹治水、疏堵结合”的理念治理和发展互联网，多次组织国内外大型会议和交流活动；从 2003 年至今一直从事反垃圾邮件、反垃圾信息等工作，2004 年创办中国互联网协会反垃圾邮件中心网站（www.anti-spam.cn），参与并组织了多项国内及国际有关法规和技术标准的制定，多次接受 CCTV、人民日报、新浪、搜狐、腾讯、网易、赛迪等媒体采访报道，2007 年代表中国赴巴西参加联合国互联网治理论坛（IGF），介绍中国反垃圾邮件的经验，为推动中国的绿色网络事业的发展做出了积极贡献。

金璇，腾讯公司

电子信息工程学士，2007 年加入腾讯公司，任职信息安全策略专家，从事信息安全和互联网行业相关的研究、规划、沟通等工作。积极参与、推动了多项促进中国互联网行业发展的研究项目，在互联网发展规划、法律法规的完善、行业规范的设立、中国互联网相关政策的制定等方面拥有颇丰的实战经验。

林晋，腾讯公司专家

腾讯邮箱中心邮件专家，8 年大型电子邮件系统运营经验，擅长反垃圾邮件策略部署。有别于传统反垃圾策略，主张从收件人的好感和反感程度来判断是否垃圾邮件。其服务的腾讯邮箱是目前垃圾邮件最少的邮件提供商之一。

李宏宇，二六三网络通信股份有限公司 CTO

李宏宇负责二六三网络通信股份有限公司数据通信业务的产品和研发中心事务。在电子邮件及反垃圾邮件领域具有较深的造诣。主持国家 863 计划中的反垃圾邮件相关课题。

田飞，系统工程学博士，二六三网络通信股份有限公司,反垃圾中心开发部经理。

田飞现在负责二六三网络通信股份有限公司反垃圾事务，专注控制行业邮局垃圾邮件接收和外发的控制.另外，他还担负国家反垃圾服务平台的开发工作。

梁友，中国联合网络通信集团有限公司网络运维部互联网处

1993 年就读北京邮电大学计算机科学系获得计算机通信硕士学位，1986 年从武汉大学无线电信息工程系获得无线电电子学学士学位。现任中国联合网络通信集团有限公司网络运维部互联网处经理，从事数据网络和 IP 网络的运行维护、网络管理、技术支撑等工作达 18 年多。在此之前，梁友女士曾在中国网络通信集团公司互联网业务部、网络运行维护部担任数据网络处、互联网处经理，负责 IP 网络和数据网络运行维护管理、网络与信息安全管理等；在北京电信管理局北京电报局担任数据网管中心主任，负责数据网络（如 X.25、FR、ATM）运行维护工作；在北电网络（中国）有限公司数据网络全球技术支撑部门担任资深高级工程师，负责为中国、台湾、香港等地电信运营商提供数据网络技术支持。梁友女士在 IP 网络运行维护和网络安全管理等方面具有丰富的经验，多年来，曾多次参与国内大型活动通信网络安全保障及应急指挥协调工作，曾参与 2008 年北京奥运会网络与信息安全保障专家组工作。

刘德良，北京大学互联网法律研究中心

刘德良教授的研究方向为民商法，在《法学研究》等学术杂志上公开发表学术论文 60 余篇；出版专著三部，主持国家社科基金、国家 242、教育部人文社科基金、司法部等国 家级和省部级课题五项。刘德良教授在网络与电子商务法、信息法与信息财产权、电信法、网络时代的知识产权问题等领域内有独到的见解，是国内网络与电子商务法领域的权威专家，应邀 曾经多次为上海、广东和北京市网络与电子商务和信息化立法提供专家意见。目前，在信息法与信息财产权、网络时代的民商法基本理论问题等领域内的研 究居于国内外领先水平。其“论个人信息的财产权保护”一文（《法学研究》2007.3）在国内首次提出个人信息财产权保护理论， 其博士论文《论个人信息的财产权保护》（人民法院出版社 2008.7 版）是国内外首次系统研究个人信息财产权保护理论的专著。 其《网络时代的民法学问题》（人民法院出版社 2004.1 版）是大陆法系首次系统研究网络时代的民法学基本理论问题的专著。 另外，刘德良教授还在国内首次提出“网络公共安全”及其法律治理理论。

苏志胜，中国电信

2005 年从北京邮电大学信息网络中心获得硕士学位，1998 年从北京邮电大学获得学士学位。现任中国电信集团公司高级业务主管，一直从事互联网网络安全工作，是中国电信互联网网络安全体系(SOC)主要构架者和创始人，并对大型运营商的网络安全架构、战略规划、网络安全运维等方面积累了丰富的经验。

王明达，网易公司

王明达是网易公司的一个Linux系统管理员，他有10多年的工作经验在互联网领域，他的工作目标是建立一个更大、更快和更加可靠的网站。

赵粮，绿盟科技首席战略官。

1997 年从北京大学电子学系获得博士学位，1994 年和 1991 从北京大学物理学系分别获得硕士和学士学位。高级工程师，现任绿盟科技首席战略官。长期从事网络安全和电信行业相关的研究、开发、策划、规划、沟通等工作。赵博士是云安全联盟 CSA 的主要贡献者之一，也是中国分会的发起者和主要创始人之一。 在此之前，赵博士曾在联想集团任 IT 架构师和安全运营总监、在 CA 中国任首席顾问、在安氏互联网安全系统（中国）有限公司任首席战略官、在中国电信数据局任高级工程师，负责网络安全工作。赵博士于 2002 年获得 CISSP 证书，在 2003 年获得了 ITIL 认证证书，成为最早的将 IT 治理和安全管理结合方面进行探索的专家之一。赵博士在行业 IT 和安全架构、战略规划等方面具有丰富的经验，其国际视角和沟通能力使其成为国内安全业界在全球化方面的先驱之一。他积极参与并指导云计算安全、安全度量、安全智能与信誉、网络空间犯罪与立法等方面的若干国际项目。赵博士先后在国内外著名报刊、核心期刊和行业会议上发表过数十篇文章和报告，他的研究兴趣覆盖了网络安全、云计算和虚拟化技术、IT 治理与企业 IT 架构等领域。

杰弗里·A·埃姆斯（Jeffery A. Ames）：斯维奇通讯集团有限责任公司（Switch Communications Group, LLC）创始成员、前任技术总监

近期，杰弗是斯维奇通讯集团有限责任公司的创始成员，并曾任其技术总监（CTO），该公司是主要数据中心和网络接入点（NAP）。20 世纪 80 年代，杰弗加入负责特种武器试验诊断和数据采集的光子学研究团队，担任其现场管理员，为能源部采用高速电光系统，以协助劳伦斯利弗莫尔实验室和内华达试验基地。从政府离任后，杰弗在内华达联合小型企业管理局推行小型新兴科技公司的项目。他曾为摩托罗拉、能源部（DOE）、交通部（DOT）、美国垦务局、林业部、劳伦斯利弗莫尔实验室等多家高科技单位参与设计整合信息系统。1993 年，杰弗在内华达组建了该州第一家互联网服务公司（ISP）。他曾加入网景首个增值分销商（VAR）咨询委员会，帮助建立了数家 ISP 和网页网站设计公司。杰弗制定了北拉斯

维加斯市光纤基础设施计划，先后担任宽带研发实验室管理人、国家竞争性本地交换运营商（CLEC）方法程序项目管理人、塞拉太平洋通讯公司（Sierra Pacific Communications）客户工程服务及新业务开发主管，还曾在考克斯通讯公司（Cox Communications）业务服务部工作。目前他担任多个科技促进与咨询委员会主席，并为数家非盈利机构及商业公司的技术项目提供支持。

莫妮卡·陈（Monica Chew）

莫妮卡·陈是谷歌公司 gmail 垃圾邮件的工程师。她是垃圾邮件、仿冒和电子邮件认证方面的专家。在 gmail 的工作中，她开发了谷歌的安全浏览器，也从事了针对恶意软件和广告点击仿冒的相关工作。她对政策和可用性方面的事物很感兴趣。她获得了加利福尼亚大学伯克利分校的计算机科学的博士学位和旧金山音乐学院的钢琴音乐学硕士学位。

吉卜·高德温（Gib Godwin）：诺斯洛普格鲁曼信息系统公司（Northrop Grumman Information Systems）防御系统部海军系统集成机构副总裁

吉卜•高德温现任诺斯洛普格鲁曼信息系统公司防御系统部内设海军系统集成机构副总裁，负责监督跨部门合作工作，该工作旨在充分利用部门情况了解、沟通、相互支持工作所构成的协力。这拓展了商业机会，发挥各部门的优势，统一客户服务标准，推进“一个诺斯洛普格鲁曼””的倡议。在此之前，高德温先生担任动力分析及实验公司（Dynamic Analytics and Test）副总裁，负责模型模拟及分析业务。他在雅典娜科技公司（Athena Technologies）担任相似的职务，职责包括针对人工及自动系统设计的导航和控制系统全套生产线的联邦航空管理局（FAA）认证和寿命周期支持，人工及自动系统得到公司的生产支持。高德温先生取得美国杜兰大学土木工程工学学士学位，持有绝密级许可证，并获国防采办大学项目管理 3 级认证。

斯图尔特·高德曼（Stuart Goldman）

他在信息与通讯技术领域积累了超过 45 年的丰富经验。他曾先后在 ITT、AGCS、朗讯（Lucent）、阿尔卡特朗讯（Alcatel-Lucent）等公司任职。目前，斯图任美国政府特殊通讯需求顾问，并受聘为贝尔实验室终身研究员。他已获 21 项美国专利证书，另有 55 项专利正在申请之中。他曾先后担任世界无线通讯解决方案联盟（ATIS）数据包技术与系统委员会（PTSC）互操作性（IOP）下属委员会主席；世界无线通讯解决方案联盟网络互操作性论坛（NIIF）主席；世界无线通讯解决方案联盟数据包技术与系统委员会信令、架构与控制（SAC）下属委员会副主席；世界无线通讯解决方案联盟网络互操作性论坛联合主席，此外还曾在电信标准部门（ITU-T）的信令 11 研究组（SG 11）、互联网工程任务组担任各种职务。斯图还参加了欧洲委员会特许设立的电子通讯基础设施可用性与坚固性（ARECI）研究院、美国国家安全电信顾问委员会（NSTAC）和对澳大利亚司法部长办公室的研究。

拉姆西·马蒂尼（Ramses Martinez）：

拉姆西·马蒂尼担任威瑞信公司信息安全部部长一职。在这一职位上，马蒂尼先生领导团队负责信息安全策略、政策和日常运作各方面的工作，以便按工作要求保护.net、.com、.tv、.cc 及.gov 域名的全球 DNS 基础设施。此团队还负责保护公司运营的全球 DNS 安全扩展密钥管理与签发基础设施。

在过去的十五年里，马蒂尼先生与数家美国及国际公司合作，为保护 IT 网络基础设施建立安全计划和制定解决方案。此项合作包括为抵御垃圾邮件，恶意软件和其他网络攻击事件而设计和运行复杂的系统。在国际法律实施和网络犯罪案例信息调查研究方面，包括一些备受关注的僵尸网络的移除，马蒂尼先生也拥有 10 多年的工作经验，。在投身私营部门前，马蒂尼先生在美国海军服役六年。

马蒂尼先生是反钓鱼工作组（APWG）及信息技术信息共享和分析中心（IT-ISAC）委员会成员。他同时还积极在欧洲委员会、事件反应论坛（FIRST）、国际反数字犯罪联盟等多家安全及政策组织从事演

讲活动与担任网络犯罪顾问的工作。他具有计算机科学专业学士学位及信息安全专业硕士学位。

帕特里克·麦克丹尼尔（Patrick McDaniel）：宾夕法尼亚州立大学计算机科学与工程系副教授

帕特里克•麦克丹尼尔是系统与互联网基础设施安全实验室创立人，并担任主任一职，同时在宾夕法尼亚州立大学计算机科学与工程系任副教授，在纽约大学斯特恩商学院任兼职教授。来到宾夕法尼亚州任教之前，他是AT&T研究的高级技术人员。麦克丹尼尔教授主要研究网络及计算机安全，已在主要学术期刊上发表数篇研究成果，涉及通信安全、安全路由与地址管理、正式安全策略、数字权限管理、分布式系统安全等众多方面。

他活跃在从事安全研究的学术界。由他撰写的书籍、论文和报告超过 100 本（篇），应邀参加的演讲也超过 100 次。帕特里克还兼任《美国计算机学会（ACM）互联网技术汇刊（TOIT）》主编及《美国计算机学会信息及系统安全汇刊》、《美国电气和电子工程师协会（IEEE）软件工程汇刊》、《美国电气和电子工程师协会计算机汇刊》副编辑。他曾在美国电气和电子工程师协会举办的主题为安全与隐私的讨论会、高等计算机系统协会讨论会等主要计算机安全会议上任技术程序主席，在过去的五年里参加了 50 多个项目委员会。

罗伯特（杰克）·奥斯伦德（Robert (Jack) Oslund）

罗伯特（杰克）•奥斯伦德博士在政府、企业和国内安全和国际通信的学术领域内有超过 40 年的经验。他获得美国大学国际服务学院国际研究专业的博士学位。奥斯伦德博士曾执教于国防情报学院，并任通讯政策白宫办公室国际参谋，在通信卫星公司担任高级管理职位。奥斯伦德还参加了美国国家安全电信顾问委员会，同时在乔治•华盛顿大学兼职教授进行教学。他还是该大学的国土安全政策研究所的高级会员。

多米尼克·洛夫罗：康卡斯特公司（Comcast）信息工程部资深总监

多米尼克•洛夫罗现任康卡斯特公司（Comcast）信息工程部资深总监。他负责公司的信息传送系统的运行，包括电子邮件、语音邮件、短信息及反滥用技术。他的工作成果包括设计和实施大规模的消息平台，成功迁移超过 25M 的电子邮箱账户——在当时是互联网史上之最。

多米尼克之前曾任贝尔实验室——朗讯的工程师，宽带接入技术是其团队工作的重点。在任期内，多米尼克协助开创了光纤入户业务（当地首批光纤入户业务之一），并助使多个大型宽带业务成功签约。开发制定的相关工具和方法有很多为出版文稿或申请专利提供了依据。除此之外，多米尼克还曾在 AT&T 任工程师和经理，负责公司的国内通讯网络基础设施及其监测。他还为新网络技术制定设计要求。多米尼克获威得恩大学电气工程及物理专业学士学位及克莱姆森大学电气工程专业硕士学位。

格莱格·沙侬（Greg Shannon）：卡内基梅隆大学软件工程学院 CERT®项目首席科学家

格莱格•沙侬博士现任卡内基梅隆大学软件工程学院 CERT®项目首席科学家，该学院为联邦政府资助的研发中心。在此职位上，他与 CERT 管理人员和工作人员合作开发改进研究的可观察性、措施、战略以及政策。在为该项目工作之余，他还致力于引导国家研究计划，促进了网络安全的数据驱动技术发展。在加入 CERT 项目之前，沙侬博士曾在两家创业公司（反风暴公司（CounterStorm）和工程与科技联合公司（Science, Engineering and Technology Associates））任首席科学家，负责内部威胁、网络安全技术及统计异常检测工作。更早以前，沙侬博士在朗讯科技、鲁美塔（Lumeta）、恒升通讯 (Ascend Communications)、洛斯阿拉莫斯国家实验室、印第安纳大学以及自己开办的创业公司任职，领导网络安全和数据分析的应用研究开发工作。沙侬博士曾在爱荷华州立大学获得计算机科学的学士学位，并辅修数学、经济学和统计学。之后他获帕卡德基金会奖学金资助，取得普渡大学计算机科学专业硕士和博士学位。

乔迪·R·维斯比（Jody R. Westby）

维斯比女士涉足技术、法律、政策、商业 20 余年，见解独特，为全球公共和私营部门的客户提供咨询和法律服务，涉及隐私、安全、网络犯罪、违约管理、法院调查及 IT 管理等多个领域。目前她还在卡

内基梅隆大学信息技术安全教育与研究中心任兼职研究员。维斯比女士是哥伦比亚特区、宾夕法尼亚和科罗拉多律师协会会员，并担任美国律师协会隐私和计算机犯罪委员会主席。目前，她还是全球科学家联盟信息安全常设监察小组的副主席以及国际电信联盟网络安全高级专家小组成员。维斯比女士促进发展了在互联网犯罪立法方面的国际电信联盟工具包，是 2010 年全球科学家联邦和国际电信联盟出版物——《追寻网络和平》的编辑和合著者。她还合作撰写并编辑了四本有关隐私、安全、网络犯罪、企业安全项目的书籍。她在全球范围演讲，并著有大量文章。她以优异的成绩毕业于塔尔萨大学，获学士学位，之后以优等生的身份毕业于乔治城大学法律中心，获法学博士学位，跻身高级律师阶层。

威德尔·D·余（Weider D. Yu）

威德尔·D·余是加利福尼亚圣荷西（硅谷）的圣荷西州立大学计算机工程学院的副教授。余教授在以下领域进行教学和研究活动，如：通信软件的质量和安全移动，基于手机和网络的软件工程，互联网安全和隐私，安全工程，分布式系统，电子医疗保健和移动医疗保健技术。他获得纽约州立大学奥尔巴尼分校的计算机科学理学硕士学位，西北大学电气工程和计算机科学的博士学位。他还参加了芝加哥大学的商学研究院的 MBA 计划，并获得了卡内基梅隆大学颁发的信息安全工程师的证书。余博士还曾是贝尔实验室杰出研究人员，伊力诺依大学电气工程系和计算机科学系的兼职副教授。

杰森·扎贝克（Jason Zabek）：考克斯通讯公司（Cox Communications）客户安全经理

扎贝克先生现任考克斯通讯公司“客户安全经理”，该公司是美国第四大电缆供应商。他曾在考克斯驻加州橘郡办公室工作五年，负责为公司商业客户运行邮件服务器和 DNS 服务器，并为高端（光纤）客户提供技术支持。2003 年，他受聘于考克斯驻亚特兰大佐治亚办公室，带领客户安全团队制定执行高速数据使用策略，与法律执行部门紧密合作，帮助客户清理受病毒感染的设备。目前，扎贝克先生为“反垃圾邮件工作组”提供帮助，该工作组由安全团队和邮件管理员组成，讨论抵御垃圾邮件的办法。他加入消息与反滥用工作组已有六年，四年前又成为 Infragard 成员（Infragard：联邦调查局联手私营企业建立的合资公司，旨在阻止网络诈骗）。他获得思科公司（Cisco）和瞻博公司（Juniper）认证证书。他拥有多年的反垃圾邮件和反网络诈骗实际经验，最清楚客户在这个真实世界里遇到的问题。

缩略词

8i	八大元素（ICT 基础设施框架）
ARPA	地址路由和参数区
AS	自治系统
ASPR	协议、标准、策略与法规
AUP	可接受的使用策略
BGP	边界网关协议
BP	最佳实践
CAN-SPAM	《控制非法色情信息和商业信息法案》
CNCERT/CC	中国国家计算机网络应急技术处理协调中心
DoS	拒绝服务
DDoS	分布式拒绝服务
DHCP	动态主机配置协议
DKIM	域名密钥识别邮件
DNS	域名服务器
DNSBL	DNS 黑名单
EHLO	扩展 HELLO（SMTP 命令）
ESMTP	扩展 SMTP
ESS	设备与软件供应商
EWI	东西方研究所
FBL	反馈环路
FIRST	事件响应和安全团队论坛
FQDN	完全限定域名
GPM	政策制定者
GSM	全球移动通信系统
GSMA	GSM 协会
HELO	HELLO（SMTP 命令）
HTTP	超文本传输协议
ICT	信息通讯技术

IEEE	电气电子工程学会
IETF	互联网工程任务组
IIA	互联网行业协会（澳大利亚）
IMAP	互联网信息存取协议
ISC	中国互联网协会
ISP	互联网服务供应商
HTML	超文本标记语言
MAAWG	反信息滥用工作组（MAAWG）
MoU	谅解备忘录
MTA	邮件传输代理
MX	邮件交换
NO	网络运营商
NGO	非政府组织
NRIC	网络可靠性与互操作性委员会
NZN	网民
OECD	经济合作与发展组织
PC	个人计算机
POP	邮局协议
*P*PP	*私—公合作*
PPP	公—私合作
PRC	中华人民共和国
RFC	评审请求
RIR	地区性互联网注册机构
ROI	投资回报率
SCIO	国务院新闻办公室
SMS	短信服务
SMTP	简单邮件传输协议
SMTPS	带传输层安全的简单邮件传输协议
SPF	发送方政策框架
SPIT	垃圾网络电话

SSL	安全套接层
TCP	传输控制协议
U.S.	美国
WCI	全球网络安全行动
WHOIS	who is；RFC 3912 中记录的请求与响应协议
WWW	万维网

参考文献

反垃圾邮件行业自律工作委员会联盟，中国互联网协会，2005 年。

《ATIS 电讯词汇》，www.atis.org，2007 年。

《2003 年控制非法色情信息和商业信息法案（CAN-SPAM）》(《美国法典》第 15 编第 7701 节)。

《减少网络信息系统滥用的最佳通用实践》，反信息滥用工作组（MAAWG），2010 年 8 月。

Blokker, Jaco，《反垃圾邮件最佳实践》，ETIS，2010 年 10 月。

《申诉反馈环路之当前最佳实践》，反信息滥用工作组（MAAWG），2010 年 4 月。

《Conficker 工作组》，conficjerworkinggroup.org。

《网络空间政策评估：保障可信和强健的信息和通信基础设施》，白宫，2009 年。

Daigle, L，RFC 3912，《WHOIS 协议规范》，互联网工程任务组，2004 年 9 月。

Gross, Grant，“《控制非法色情信息和商业信息法案》奏效吗？”《个人计算机世界》，2009 年 3 月 21 日检索。

《反互联网和无线通讯垃圾邮件法（FISA）》，C-28 议案，加拿大，2010 年。

GSM 协会，www.gsmworld.com

《中国互联网状况白皮书》，中华人民共和国国务院新闻办公室，北京，2010 年 6 月。

Kigerl, Alex C。（2009 年 12 月），“《控制非法色情信息和商业信息法案》：一次经验分析”，《网络犯罪学国际期刊》第 3 期(2)：566–589 页。

Klensin, J.，RFC 5321，简单邮件传输协议，互联网工程任务组，2008 年 10 月。

Lindberg, G.，RFC 2505，简单邮件传输协议之邮件传输代理反垃圾邮件建议，互联网工程任务组，1999 年 2 月。

M86 安全，《安全实验室报告》，2010 年 1 月。

McMillan, Robert，《中国清理垃圾邮件的问题》，《个人计算机世界》，2011 年 2 月。

《互联网电子邮件服务管理办法》，工业和信息化部，北京，2006 年。http://miit.gov.cn/n11293472/n11294912/n11296542/12165060.htm

反信息滥用工作组（MAAWG），www.maawg.org

《国家安全电信顾问委员会给总统的有关国际通信的报告》，美国国家安全电信顾问委员会（NSTAC），2007 年 8 月。

OECD 反垃圾邮件工具包

Palmer, Maija，《有关披露的网络不正当行为的秘密战争》，《金融时报》，2009 年 6 月 14 日。

《木马和僵尸网络监测与处置机制》，工业和信息化部，2009 年。

Rauscher, Karl. F.，《电信基础设施的可用性与强劲性（ARECI）—最终报告》，欧洲委员会，2007 年 3 月。

Rauscher, Karl F.，《保护通信基础设施》，《贝尔实验室技术杂志—专刊：国家安全》，第 9 卷，第 2 期，2004 年。

Rauscher, Karl F.、Krock, Richard E.、Runyon, James P.，《通信基础设施的八大元素：增强网络可靠性与安全性的系统化综合框架》，《贝尔实验室技术杂志》，第 11 卷，第 3 期，2006 年。

《首尔—墨尔本反垃圾邮件协议》，2005 年。

Shannon, Claude E.，《通信的数学理论》，《贝尔系统技术杂志》，1948 年。

Spamhaus 项目，www.spamhaus.org

网络不良和垃圾信息举报受理中心，中国互联网协会。

SpamLinks.com

《中美联合声明》，白宫新闻秘书办公室，2011 年 1 月 19 日。

附录 A 中美联合声明

2011 年 1 月 19 日

白宫新闻秘书办公室，华盛顿

1．应美利坚合众国总统贝拉克·奥巴马邀请，中华人民共和国主席胡锦涛于二 0 一一年一月十八日至二十一日对美国进行国事访问。访问期间，胡主席会见了美国副总统约瑟夫·拜登，将会见美国国会领导人，并访问芝加哥。

2．两国元首回顾了自奥巴马总统二 0 0 九年十一月对中国进行国事访问以来中美关系取得的进展，并重申致力于建设二十一世纪积极合作全面的中美关系，这符合两国人民和国际社会的利益。双方重申，中美三个联合公报为两国关系奠定了政治基础，并将继续指导两国关系的发展。双方重申尊重彼此主权和领土完整。两国元首还重申了对二 0 0 九年十一月《中美联合声明》的承诺。

3．中美致力于共同努力建设相互尊重、互利共赢的合作伙伴关系，以推进两国共同利益、应对二十一世纪的机遇和挑战。中美正在安全、经济、社会、能源、环境等广泛领域开展积极合作，需进一步深化双边接触与协调。两国领导人还一致认为，需要与国际伙伴和机构进行更加广泛、深入的合作，以形成和落实可持续的解决方案并促进世界和平、稳定、繁荣和各国人民的福祉。

加强中美关系

4．鉴于两国面临重要的共同挑战，中美决定继续建设伙伴关系，以推进共同利益、处理共同关切、强调国际责任。两国领导人认识到，中美关系既重要又复杂。中美已成为不同政治制度、历史文化背景和经济发展水平的国家发展积极合作关系的典范。双方同意进一步努力培育和深化战略互信，以加强双边关系。双方重申要深化对话，拓展务实合作，确认需共同努力，处理分歧、扩大共识、加强在一系列问题上的协调。

5．美方重申，美方欢迎一个强大、繁荣、成功、在国际事务中发挥更大作用的中国。中方表示，欢迎美国作为一个亚太国家为本地区和平、稳定与繁荣做出努力。两国领导人支持通过合作努力建设二十一世纪更加稳定、和平、繁荣的亚太地区。

6．双方强调台湾问题在中美关系中的重要性。中方强调，台湾问题涉及中国主权和领土完整，希望美方信守有关承诺，理解并支持中方在此问题上的立场。美方表示奉行一个中国政策，遵守中美三个联合公报的原则。美方赞扬台湾海峡两岸《经济合作框架协议》，欢迎两岸间新的沟通渠道。美方支持两岸关系和平发展，期待两岸加强经济、政治及其他领域的对话与互动，建立更加积极稳定的关系。

7．双方重申，尽管两国在人权问题上仍然存在重要分歧，但双方都致力于促进和保护人权。美方强调，促进人权和民主是美国外交政策的重要组成部分。中方强调，不应干涉任何国家的内政。中美强调，各国及各国人民都有权选择自身发展道路，各国应相互尊重彼此选择的发展模式。双方本着平等和相互尊重的精神处理人权问题上的分歧，按照国际文书促进和保护人权，并同意在第三轮中美战略与经济对话前举行下一轮中美人权对话。

8．中美同意在下一轮人权对话前恢复举行法律专家对话。双方还同意将加强两国的法律合作和法治交流。两国正积极探讨关于加强妇女在社会中作用的交流和讨论。

9．中美两国确认，一个健康、稳定、可靠的两军关系是胡锦涛主席和奥巴马总统关于积极合作全

面中美关系共识的重要组成部分。双方一致认为，有必要加强各层次的实质性对话和沟通，以减少误解、误读、误判，增进了解，扩大共同利益，推动两军关系健康稳定可靠发展。双方注意到美国国防部长罗伯特·盖茨本月早些时候对中国进行了成功访问，美方欢迎中国人民解放军总参谋长陈炳德上将于二０一一年上半年访问美国。双方重申，中美国防部防务磋商、国防部工作会晤、海上军事安全磋商机制未来将继续作为两军对话的重要渠道。双方表示，将继续推动二０００九年十月中国中央军委副主席徐才厚上将与美国国防部长盖茨就发展两军关系达成的七项共识得到落实。

１０．中美同意采取具体行动，深化在航天领域的对话和交流。美方邀请中方代表团于二０一一年访问美国国家航空航天局总部和其他合适的设施，以作为对美国国家航空航天局长二０一０年对中国富有成果的访问的回访。双方同意继续在透明、对等、互利的基础上讨论在航天领域开展务实合作的机会。

１１．《中美科技合作协定》是两国最早签署的双边协定之一，双方认可在该协定框架下取得的成果并欢迎签署该协定延期议定书。中美将继续在农业、卫生、能源、环境、渔业、学生交流、技术创新等广泛领域进行合作，以增进双方福祉。

１２．中美双方欢迎中美执法合作联合联络小组在反恐等诸多领域加强执法合作取得的进展。双方同意通过双边和其他途径加强反腐败合作。

促进高层交往

１３．双方认为，强有力的中美关系离不开高层交往，密切、频繁、深入的对话对推进双边关系以及国际和平与发展十分重要。本着这一精神，两国元首期待在二０一一年再次会面，包括在美国夏威夷州举办的亚太经合组织领导人非正式会议期间会晤。中方欢迎拜登副总统于二０一一年访华。美方欢迎习近平副主席此后访美。

１４．双方积极评价中美战略与经济对话这一两国政府间十分重要的协调机制，同意二０一一年五月在华盛顿举行第三轮对话。战略与经济对话在帮助两国建立互信方面发挥了重要作用。双方还同意二０一一年春在美国举行第二轮中美人文交流高层磋商，二０一一年下半年在中国举行第二十二届中美商贸联委会。双方同意两国外长通过互访、会晤等方式保持密切沟通。

１５．双方强调两国议会继续保持交往的重要性，包括中国全国人民代表大会与美国参议院和众议院之间的机制化交流。

应对地区和全球挑战

１６．双方认为，中美两国在促进亚太及其他地区和平安全方面拥有共同利益，同意加强沟通与协调，应对紧迫的地区和全球挑战。双方致力于采取行动保护全球环境，在全球性问题上协调合作，维护和促进各国及各国人民的可持续发展。具体而言，中美同意在下述领域增进合作：应对暴力极端主义，防止核武器扩散、其他大规模杀伤性武器及其运载工具的扩散，加强核安全，消除传染性疾病和饥饿，消灭极端贫困，有效应对气候变化挑战，打击海盗，预防和减少灾害，应对网络安全问题，打击跨国犯罪，打击贩卖人口。中美将与其他各方一道，努力加强合作，应对共同关切、促进共同利益。

１７．中美强调致力于最终实现无核武器世界，强调需要加强国际核不扩散体系以应对核扩散和核恐怖主义等威胁。在此方面，双方支持《全面禁止核试验条约》尽早生效，重申支持日内瓦裁谈会尽早启动“禁止生产核武器用裂变材料条约”谈判，并愿为此进行合作。双方注意到在华盛顿核安全峰会后中美在核安全领域合作深化，签署了关于在华建立核安保示范中心的谅解备忘录。

１８．中美一致认为，正如六方会谈“九·一九”共同声明和联合国安理会相关决议所强调，保持朝鲜半岛和平稳定至关重要。双方对近期事态发展导致半岛局势紧张表示关切。双方注意到两国在半岛问题

上保持了密切合作。中美强调改善半岛南北关系的重要性，都认为朝韩开展真诚和建设性对话是非常重要的一步。鉴于半岛无核化对维护东北亚地区和平与稳定至关重要，中美双方重申，有必要采取切实有效步骤实现无核化目标，并全面落实六方会谈“九·一九”共同声明中的其他承诺。在此背景下，中美对朝鲜宣称的铀浓缩计划表示关切。双方反对所有违反六方会谈“九·一九”共同声明和相关国际义务和承诺的活动。双方呼吁采取必要步骤，以尽早重启六方会谈进程，解决这一问题及其他相关问题。

１９．中美重申，将致力于寻求全面长期解决伊朗核问题的办法，以重建国际社会对于伊朗核计划仅限于和平目的的信心。双方同意伊朗根据《不扩散核武器条约》拥有和平利用核能的权利，同时伊朗也应履行该条约规定的相应国际义务。双方呼吁全面执行联合国安理会所有有关决议。双方欢迎并将积极参与六国与伊朗进程，强调包括伊朗在内的各方应致力于建设性的对话进程。

２０．双方同意全力支持苏丹北南和平进程，包括全面有效落实《全面和平协议》。双方强调各方应尊重自由、公平和透明的公投结果。中美双方对达尔富尔问题表示关注，认为应推动达尔富尔地区政治进程取得进一步实质性进展，以促进该问题早日得到全面妥善解决。整个地区继续保持和平稳定符合中美双方利益。

２１．双方同意，本着相互尊重和合作的精神加强在亚太地区的沟通和协调，并通过多边机构等渠道和其他亚太国家一道促进和平、稳定与繁荣。

建设全面互利的经济伙伴关系

２２．胡锦涛主席和奥巴马总统认识到共同努力建设相互尊重、互利共赢的经济合作伙伴关系对两国和世界经济极其重要。两国领导人同意推进全面经济合作，并将依托现有对话机制，基于以下要素，到将于今年五月举行的第三轮中美战略与经济对话时进一步确立全面经济合作框架。

２３．为推进中美两国和世界经济强劲、可持续、平衡增长，双方同意加强宏观经济政策沟通与合作：

（１）美国将重点减少中期联邦赤字，确保长期财政可持续性，并对汇率过度波动保持警惕。美联储近年来已采取重要步骤增强其传递未来展望和长期目标的清晰度。

（２）中国将继续加大力度扩大内需，促进服务部门的私人投资，更大程度地发挥市场在资源配置中的基础性作用。中国将继续坚持推进人民币汇率形成机制改革，增强人民币汇率弹性，转变经济发展方式。

（３）双方同意继续实施前瞻性货币政策并关注其对国际经济的影响。

两国支持欧洲领导人为增强市场稳定性和促进可持续长期增长所做出的努力。

２４．双方认识到开放的贸易和投资对促进经济增长、创造就业、创新和繁荣的重要意义，重申将采取进一步措施推进全球贸易和投资自由化，反对贸易和投资保护主义。双方也同意愿本着建设性、合作性和互利性的态度，积极解决双边贸易和投资争端。

２５．两国领导人强调将指示其谈判代表进行跨领域的谈判，在维护世界贸易组织多哈发展回合授权、锁定已有成果的基础上，促使多哈回合谈判尽快取得成功、富有雄心、全面和平衡的结果。双方同意加强和扩大两国谈判代表的参与度以完成谈判。

２６．两国领导人同意实现更加平衡的贸易关系的重要性，并高度赞扬包括近期在华盛顿举行的第二十一届中美商贸联委会在此方面取得的进展。

２７．中方将坚持保护知识产权，包括进行审计以确保各级政府机关使用正版软件，并依法公布审

计结果。中国的创新政策与提供政府采购优惠不挂钩。美方欢迎中方同意在世界贸易组织政府采购委员会二０一一年最后一次会议前提交一份强有力的新的修改出价，其中包括次中央实体。

２８．两国领导人认识到培育开放、公平和透明的投资环境对两国经济和世界经济的重要性，重申双方继续致力于推进双边投资协定谈判。双方认识到成功的双边投资协定谈判将通过促进和保护投资，为双方投资者增强透明度和可预见性，支持开放的全球经济。中方欢迎美方承诺通过中美商贸联委会以一种合作的方式迅速承认中国市场经济地位。中方欢迎中美双方讨论美国正在推进的出口管制体系改革，以及在符合美国国家安全利益的前提下这一改革对美向包括中国在内的主要贸易伙伴出口的潜在影响。

２９．双方进一步认识到双边商贸关系广阔和强有力的特点，包括此访所达成的合同，双方欢迎双边商贸关系经济上的互利性。

３０．双方同意继续通过将要举行的中美战略与经济对话、中美商贸联委会等进程致力于推进双边经济关系取得具体进展。

３１．双方认识到企业在两国基础设施建设中发挥积极作用的潜力，并愿加强在这一领域的合作。

３２．双方承诺深化在金融部门投资和监管领域的双边和多边合作，在符合审慎监管并与国家安全要求一致的情况下，支持为金融服务和跨境证券投资领域营造开放的投资环境。美方承诺确保“政府支持企业”具有足够资本和能力以履行其财务责任。

３３．中美双方认同纳入特别提款权的货币应仅为在国际贸易和国际金融交易中广泛使用的货币。鉴此，美方支持中方逐步推动将人民币纳入特别提款权的努力。

３４．双方承诺致力于加强全球金融体系和改革国际金融框架。双方将继续强有力的合作以提高国际货币基金组织和多边开发银行的合法性和有效性。为实现联合国千年发展目标，双方将共同促进国际社会援助发展中国家、特别是最不发达国家的努力。双方还将与多边开发银行协作，寻求合作支持包括非洲在内的全球减贫、发展和区域一体化，为包容和可持续的经济增长做出贡献。

３５．双方重申支持二十国集团强劲、可持续和平衡增长框架，重申在二十国集团首尔峰会公报中的承诺，包括采取一系列措施巩固全球经济复苏、减少过度外部失衡并将经常账户失衡保持在可持续水平。双方支持二十国集团在国际经济和金融事务中发挥更大作用，并承诺加强沟通协调，落实二十国集团峰会承诺，推动戛纳峰会取得积极成果。

气候变化、能源和环境合作

３６．双方认为气候变化和能源安全是当今时代两大重要挑战。中美同意继续就应对气候变化行动进行密切磋商，为实现两国和世界人民的能源安全而开展协调，加强现有清洁能源合作，确保市场开放，在气候友好型能源领域推动互利投资，鼓励清洁能源，推动先进清洁能源技术开发。

３７．双方积极评价中美清洁能源研究中心、可再生能源伙伴关系、《中美能源安全合作联合声明》和中美能源合作项目启动以来两国在清洁能源和能源安全领域合作取得的进展。双方重申继续就能源政策进行交流，在石油、天然气（包括页岩气）、民用核能、风能和太阳能、智能电网、先进生物燃料、清洁煤、能效、电动汽车及清洁能源技术标准等领域进行合作。

３８．双方积极评价《中美能源和环境十年合作框架》自二００八年启动以来取得的进展。双方同意在该框架下进一步加强务实合作，落实水、大气、交通、电力、保护区和湿地、能效等优先领域的行动计划，开展政策对话，实施绿色合作伙伴计划。双方高兴地宣布两个新的绿色合作伙伴计划。双方欢迎两国地方政府、企业、研究机构参与十年合作框架，共同探索中美能源环境合作的创新模式。双方对根据十年合作框架将于二０一一年开展的合作项目和活动表示欢迎。

３９．双方对坎昆协议表示欢迎，认为应对气候变化的努力也应促进经济社会发展。双方同意与其他国家一道，积极推动《联合国气候变化框架公约》的全面、有效、持续落实，包括落实坎昆协议，并支持今年的南非会议达成积极成果。

扩展人文交流

４０．中美两国一贯支持开展更加广泛深入的人文交流，这也是双方建设相互尊重、互利共赢中美合作伙伴关系努力的一部分。双方同意采取切实步骤加强人文交流。双方满意地注意到，二０一０年上海世博会取得成功，中方对美国馆的成功展示向美方表示祝贺。双方宣布建立中美省州长论坛，决定进一步支持两国地方各级在一系列领域开展交流合作，包括增强友好省州和友好城市关系。中美还同意采取切实措施，特别是通过“十万人留学中国计划”，加强两国青年之间的对话与交流。美方热忱欢迎更多中国学生赴美留学，并将继续为他们提供签证便利。双方同意讨论扩大文化交流的途径，包括探讨举办中美文化年及其他活动。双方强调将进一步推动相互旅游并为此提供便利。双方认为，所有上述活动都有助于深化了解、互信与合作。

结语

４１．胡锦涛主席感谢奥巴马总统和美国人民在他访问期间给予的热情款待。中美两国元首认为，此访进一步推进了两国关系，双方决心共同努力建设相互尊重、互利共赢的合作伙伴关系。两国元首均深信，一个更加强有力的中美关系不仅符合两国人民的根本利益，也有利于整个亚太地区乃至全世界。

附录 B 互联网服务供应商致客户函（样例）

兹此向制作此通用信函模板的 Cox 通信公司表示感谢！此函已在最佳实践 CN-US 11-005“*用户协议高使用阈值*”中被引用。

尊敬的[公司]互联网用户：

作为随访跟踪，我们向您发送了此封邮件，对防木马、防病毒和安全软件提供几点建议。我们及其他[公司]客户发现，此款软件在清理病毒和木马感染上很实用。而且，它还有助于保护计算机将来不受感染。[公司]的很多员工都在其个人系统上安装了这些程序，这也是我们能够推荐它们的原因。

请注意，我们乃是出于对您系统的安全考虑而向您推荐这些实用程序，但[公司]并不保证这些程序可以正常工作，亦不对您可能遭受的任何负面影响承担责任。此外，[公司]也无法为这些实用程序提供支持。如果您在安装或使用这些应用程序时需要技术支持或帮助，请联系厂商/制造商，以获取技术支持或资料。

没有任何一款安全软件是 100%有效的。必要的时候，可能需要同时使用数款应用程序，才能尽可能地保持您的系统安全无虞。例如，您应该拥有一个防病毒安全软件套件（例举产品）和一款好的间谍软件删除程序（例举产品）。应注意，也有一些安全软件套件可以提供所有这些功能。

以下是一篇文章的链接，可帮助您确定最适合您的安全软件：[提供网址]

[公司]**免费**向我们的现有用户提供一款一站式安全软件套件。请阅读 Cox 支持站点中的这篇文章，以了解更多信息：[网址]

在开始安装该安全程序前，确保您的重要数据已进行备份（应定期进行备份）。可以手动（通过拖拉方式）或使用一款系统备份软件实用程序备份文件。可以将您的文件备份到 U 盘（AKA USB 密钥）、CD/DVD 光盘、移动硬盘或网络文件服务器。

首先应该运行的工具是（例举产品）。它是 Microsoft 为查找和清除黑客最常用的病毒和木马而开发的一款产品。可在此处下载该工具：[提供网址]

更新您的防病毒扫描仪。不管您是使用 McAfee、AVG、Norton 等工具中的哪款工具，更新病毒库并运行全盘扫描。这些实用程序中的大部分程序都可在该程序自身内部进行更新，因此请参考帮助文件，确保您拥有最新的防病毒库。

安装一款软件或者同时安装两款软件后，请运行全盘扫描并删除或隔离在您系统上检测出的所有恶意间谍软件。并非所有间谍软件都是恶意的，例如，跟踪 cookie 尽管很令人讨厌，但相对而言是无害的。您的间谍软件实用程序将通知您哪个间谍软件真正有害，哪个确定要予以删除。Ad-Aware 对其发现到的软件会给出从 1 到 10 的评级。例如，任何评级为 3 及以下的软件均被视为低级威胁。

[产品]是一款反恶意软件程序，以其基于行为的威胁检测而著称。它可对您系统上所有运行着的应用程序和运行过程的行为进行检测。它将提醒您和/或阻止任何“异常”活动，如出站端口扫描、密钥登记或发出数万封垃圾邮件等。这是一款出色的应用程序，它可与您的防病毒、反间谍软件及其他安全工具协作，为您提供额外的保护层。

[产品]是另外一款反恶意软件程序，可监测各种过程行为并保护您的系统不受恶意活动入侵。Threatfire 可提供出色的即时保护，因此可更好地确保您个人计算机和宝贵数据的安全。

[产品]也是一款出色的反恶意软件程序，它可检测到并清除恶意软件。

* 如果这些程序无法清除您系统上的威胁，可能需要重新格式化和重新安装操作系统。*

帮助您保持系统安全的一些建议：

1. 使用带网络地址转换功能（NAT）的路由器

连接路由器的所有系统均使用一个公共 IP 地址连入互联网，即您的广域网（WAN）网关。使用一款带有电缆调制解调器的路由器将帮助您阻断从互联网主动提供的流量。如果黑客试图从互联网连接到您的计算机，由于您的计算机没有发起连接请求，因此会拒绝该连接。这样即可阻止“周末”黑客攻击您的网络和/或计算机。

2. 使用防火墙

防火墙可以是软件设备或硬件设备，可对所有入站网络流量进行监测。它将准许获您批准的流量进入，拒绝任何主动提供的流量。防火墙可通过终止所有主动提供的入站互联网请求使您的计算机看似对互联网“不可见”。[公司]推荐在您的电缆调制解调器（或 NID）后使用硬件防火墙，在您专有网络上的每个计算机系统上安装软件防火墙。

3. 启用自动更新！

确保您的操作系统已全面更新并安装补丁。

[厂商]在每月的第二个星期二定期发行补丁。在 XP 系统下，点击“开始>设置>控制面板>安全中心”，然后点击“自动更新”，接着点击“自动”（推荐）单选按钮。

几乎所有供应商都存在安全问题并且会持续发布补丁。

以下是另外一些有用的链接：[提供链接]

如需更多帮助，请访问[网址]中的“数据—安全”部分。

谢谢！

[公司]客户安全事业部