国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1240

(04/2008)

X系列：数据网、开放系统通信和安全性

电信安全

用于打击垃圾电子邮件的技术

ITU-T X.1240 建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	
业务和设施	X.1-X.19
接口	X.20-X.49
传输、信令和交换	X.50-X.89
网络概貌	X.90-X.149
维护	X.150-X.179
管理安排	X.180-X.199
开放系统互连	
模型和记法	X.200-X.209
服务限定	X.210-X.219
连接式协议规范	X.220-X.229
无连接式协议规范	X.230-X.239
PICS书写形式	X.240-X.259
协议标识	X.260-X.269
安全协议	X.270-X.279
层管理对象	X.280-X.289
一致性测试	X.290-X.299
网间互通	
概述	X.300-X.349
卫星数据传输系统	X.350-X.369
以IP为基础的网络	X.370-X.379
报文处理系统	X.400-X.499
号码簿	X.500-X.599
OSI 组网和系统概貌	
组网	X.600-X.629
效率	X.630-X.639
业务质量	X.640-X.649
命名、寻址和登记	X.650-X.679
抽象句法记法1(ASN.1)	X.680-X.699
OSI 管理	
系统管理协议子集和结构	X.700-X.709
管理通信服务和协议	X.710-X.719
管理信息的结构	X.720-X.729
管理功能	X.730-X.799
安全	X.800-X.849
OSI 应用	
托付、并发和恢复	X.850-X.859
事务处理	X.860-X.879
远程操作	X.880-X.889
ASN.1的一般应用	X.890-X.899
开放分布式处理	X.900-X.999
电信安全	**X.1000-**

欲了解更详细信息，请查阅 *ITU-T*建议书目录。

ITU-T X.1240建议书

用于打击垃圾电子邮件的技术

摘要

ITU-T X.1240建议书对垃圾电子邮件和用于打击垃圾电子邮件的技术的基本概念、特点和影响做了说明，还介绍了不同标准制定机构和打击垃圾电子邮件相关机构现用的解决方案和开展的有关活动。该建议书向希望制定打击垃圾电子邮件技术解决方案的用户提供了指导原则和信息，因而将被用作进一步制定打击垃圾电子邮件技术建议书的依据。

来源

ITU-T 第17研究组（2005-2008年）根据世界电信标准化全会（WTSA）第1号决议规定的程序，于2008年4月18日批准了ITU-T X.1240建议书。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准 ITU-T 建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2009

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页

1 范围 1
2 参考 1
3 定义 1
4 缩略语 1
5 常用语 2
6 有关打击垃圾电子邮件的介绍 2
6.1 垃圾信息的概念和特性 2
6.2 打击垃圾电子邮件的方法 3
7 反垃圾信息技术 3
7.1 综述 4
7.2 工具/技术场景的重要性 4
7.3 综合测试 5
7.4 反垃圾信息技术类型 5
7.5 发送域的存在及应对回应的争取 6
7.6 指针记录的存在（PTR） 6
7.7 黑名单/白名单 7
7.8 发送服务器地址被视为“动态”或“居民” 7
7.9 过滤 8
7.10 HELO/CSV 9
7.11 灰名单 10
7.12 令牌/密码 10
7.13 各种手段 10
7.14 如何利用这些技术和因素考虑问题 11
7.15 在SMTP会话中的拒绝 12
7.16 沉默拒绝 12
7.17 通过发送DSN（发送状态通知或“反弹”）拒绝 12
7.18 向垃圾信息邮箱的投递 12
7.19 标识 12
附录I – 有关打击垃圾电子邮件的活动 13
I.1 引言 13
I.2 有关打击垃圾信息的国际活动 13
I.3 反垃圾信息技术规范的制定 15
I.4 行业联盟名单和打击垃圾信息举措 16
参考文献 20

引言

按照WTSA-2004第52号决议“用技术手段打击垃圾信息”的要求，为制定有助于通过技术手段打击垃圾信息的ITU-T建议书已开展了标准化工作。本建议书是一系列打击垃圾电子邮件的ITU-T建议书中的一份，这些建议书包括指导方针、要求、技术框架和技术战略。其它用于打击在IP电话、即时消息和大会等IP多媒体应用中垃圾信息的ITU-T建议书另见其它文件。

ITU-T X.1240建议书

用于打击垃圾电子邮件的技术

1 范围

本建议书具体介绍了打击垃圾电子邮件使用的技术。它介绍了目前的解决方案以及各标准制定机构和相关打击垃圾电子邮件组织所开展的有关活动。本建议书的目的是为希望制定有关打击垃圾电子邮件技术解决方案的用户提供有益信息。本建议书将用作进一步编制反垃圾电子邮件技术建议书的依据。

注－本建议书所用的“身份”（identity）一词，并不是指其绝对意义，尤其是它不构成任何确有把握的认证。

2 参考

无。

3 定义

本建议书对以下术语做出定义：

3.1 钓鱼攻击者（Phisher）：发动钓鱼攻击的实体或个人。

3.2 钓鱼（phishing）：钓鱼攻击使用社会工程学和技术规避手段盗取消费者个人身份数据及财务账户凭证。社会工程学手段使用盗用地址的（“spoofed”）电子邮件引导消费者至旨在诱骗其批露信用卡号、账号用户名、密码和社会保障号码等财务数据的假冒网页。钓鱼攻击者劫持银行、网上零售商和信用卡公司品牌，劝服接收者做出响应。采用技术规避手段是将犯罪软件植入个人电脑以便直接盗取证书。一般情况下，使用特洛伊木马键盘记录器（keylogger）间谍软件。

3.3 垃圾信息（spam）：“垃圾信息”一词的含义取决于各国根据其国家技术、经济、社会和实际情况对隐私和垃圾信息构成的看法。值得一提的是，随着技术的发展，其含义不断变化并拓宽，为滥用电子通信创造了新的可乘之机。尽管在全球范围内没有有关垃圾信息的一致定义，但该术语一般用来描述为推销商业化产品或服务通过电子邮件或移动消息批量传送的推介性电子通信。

3.4 垃圾信息制造者（spammer）：制造并发送垃圾信息的实体或个人。

4 缩略语

本建议书使用以下缩略语：

API	应用程序接口（Application Programming Interface）
DKIM	域钥识别邮件（DomainKeys Identied Mail）
CSV	认证的服务器确认（Certified Server Validation）
DNS	域名系统（Domain Name System）
DSN	投递状态通知（Delivery Status Notification）

HTML	超文本标记语言（HyperText Markup Language）
IM	即时消息（Instant Messaging）
ISP	互联网服务提供商（Internet Service Provider）
META	传输授权消息增强（Message Enhancements for Transmission Authorization）
MMS	彩信业务（Multimedia Message Service）
MTA	邮件传送代理（Mail Transfer Agent）
OECD	经合发组织（Organization for Economic Co-Operation and Development）
OPES	开放式可插拔边缘服务（Open Pluggable Edge Services）
PGP	良好隐私（Pretty Good Privacy）
PTR	指针记录（Pointer Record）
SMS	短信业务（Short Message Service）
SMTP	简单邮件传送协议（Simple Mail Transfer Protocol）
SPF	发送人政策框架（Sender Policy Framework）
TEOS	可信赖的电子邮件开放标准（Trusted Email Open Standard）

5 常用语

无。

6 有关打击垃圾电子邮件的介绍

6.1 垃圾信息的概念和特性

尽管垃圾信息没有普遍达成一致的定义，但该词通常用于描述为推销商业产品或服务而通过电子邮件、移动消息（SMS、MMS）和即时消息服务进行的推介性电子通信。

尽管广而皆知的垃圾信息形式是垃圾电子邮件，该词还适用于对其它媒体的滥用，如，移动电话垃圾消息、IP电话垃圾信息、即时消息垃圾信息、网上新闻垃圾信息、网页搜索引擎垃圾信息及博客垃圾信息。垃圾信息的内容从产品广告至令人反感的色情资料无处不在。垃圾电子邮件对于电子邮件服务使用者和互联网服务提供商造成多方面的不良影响：

– 垃圾信息接收者和ISP为识别、删除并过滤垃圾信息投入大量时间、资金和精力。

– 垃圾电子邮件可能包含诱惑垃圾信息接收者的欺骗性内容或儿童不宜的成人内容。

– 电子邮件业务使用者和ISP浪费了互联网资源和存储空间。

– 病毒和间谍软件的传播可对网络安全造成威胁。

– 垃圾电子邮件使人忽略了正常和重要的电子邮件。

最近日趋猖獗的一个现象是，垃圾邮件被用来支持欺诈和犯罪活动－包括通过将信息伪装成发自可信赖的公司（“品牌地址盗用”或“钓鱼”）以获取财务信息（如，账号和密码）－并作为传播病毒和蠕虫的工具。

钓鱼攻击使用社会工程学和技术规避手段盗取消费者个人身份数据及财务账户凭证。社会工程学手段使用盗用地址的（“spoofed”）电子邮件引导消费者至旨在诱骗其批露其信用卡号、账号用户名密码和社会保障号码等财务数据假冒网页。钓鱼攻击者劫持银行、网上零售商和信用卡公司品牌，劝服接收者做出响应。采用技术规避手段就是将犯罪软件植入个人电脑以便直接盗取证书。一般情况下，使用特洛伊木马键盘记录器（keylogger）间谍软件。网址嫁接（Pharming）犯罪软件误导用户至欺骗性网站或代理服务器，一般通过域名系统（DNS）拦截或感染进行。

垃圾信息制造者自身为防止被发现表现出高超的创造力，采用伪造电子邮件来源和对内容进行随机化的方式以逃避垃圾信息过滤器。由于该问题蔓延之广，很多国家都在迅速颁布反垃圾信息法律－尽管各国所采用的手段和补救方式不同。与此同时，人们日益认识到，打击垃圾信息需要国际协调和合作。

6.2 打击垃圾电子邮件的方法

由于垃圾电子邮件对电子邮件服务使用者、ISP及网络运营商造成严重伤害，许多国家为有助于打击垃圾信息开发了技术并通过了规定。然而，仅凭一项打击措施，如过滤或合法惩罚难以有效打击垃圾信息，因为打击垃圾信息不是一个简单的问题。为此，应同时采用不同方法有效打击垃圾信息：

– 法规：应通过反垃圾信息法规方便服务使用者对垃圾电子邮件做出适当响应，并增强过滤等反垃圾信息技术的效应。此外，法规可帮助保护服务使用者和ISP免受非法垃圾信息的影响。

– 技术：反垃圾信息技术的开发对于有效打击大批量垃圾电子邮件至关重要。应开发不同技术，以防止传送垃圾信息并有效识别和过滤垃圾信息。

– 行业行动：ISP或网络运营商等行业参与者应开发和安装包括黑名单或白名单及过滤功能的各种反垃圾信息技术。ISP还可以通过有关打击垃圾电子邮件的政策。

– 国际合作：由于电信网络无国界，而且垃圾信息的生成和影响也不局限于各国国内，因此需要国际合作。同时，国际合作对于实现法规的有效批准、反垃圾信息技术开发和服务使用者及提供者在培训方面的信息共享非常有益。

– 教育：为将垃圾电子邮件造成的影响降至最低，对服务使用者和ISP开展教育至关重要。希望通过教育帮助电子邮件使用者对垃圾电子邮件采取适当行动，而ISP则采取反垃圾信息政策和技术。

对于上述各种反垃圾措施，本建议书将重点阐述打击垃圾信息的技术手段，如反垃圾信息技术的开发和应用。

7 反垃圾信息技术

OECD垃圾信息任务组的报告[b-OECD TF]为打击垃圾电子邮件提供了很多内容，包括规则方法、执法问题及技术解决方案。本建议书在本段话中引用了报告的一部分（第四项－反垃圾信息技术）。该内容需要审议，因为反垃圾信息工具包是于2006年5月公布的，并且至今尚未更新。

这段话论述了不同反垃圾信息技术及其现有能力以及收到垃圾信息后的应对方法。有效打击垃圾信息的所有尝试，都需要合理地协同使用一系列上述技术。没有哪种技术能够单枪匹马地取得成功。当有效地综合采用一系列反垃圾信息技术时，便可以产生大幅度降低垃圾信息对系统的影响的效果。

7.1 综述

垃圾信息为技术带来重大挑战，因此，为消除垃圾信息需要适当的技术措施所支持的解决方案。尽管政府的行为和立法会发挥有益作用，但这些不足以应对垃圾信息所带来的挑战。事实上，垃圾信息主要是由于SMTP协议中的一个错误而产生的技术问题。由于该问题的技术性质使其很难让执法者发现垃圾信息制造者，并对其进行相应的惩罚。

无论垃圾信息如何定义，还有一些技术和手段可以用来控制无用电子邮件的问题。本句话旨在从中立的角度概述各种技术手段和方法以及在落实这些手段和方法前应考虑的因素。本节专门阐述手段，而不是解决方案。尽管技术的开发旨在解决由垃圾信息造成的诸多问题，并且可能能够实际“解决”一些与垃圾信息相关的具体问题，但是要彻底解决垃圾信息问题必须采用包括技术、政策（酌情包括法规）、实践和教育等多个方面的方法。

反垃圾信息手段用于多个层面－发送点、骨干网、网关和接收端计算机，可单独使用或联合使用。有关最新信息和资源可在工具包网页www.oecd-antispam.org上查阅。

这一段话特别针对邮件服务器管理人员，让其了解各种过滤技术的利弊，使其根据计划的架构按照其电子邮件政策和需求选择软件。本段话重点放在对进入邮件的做法，尽管减少发出垃圾信息的做法亦非常有用。除接收服务器的运营商外，发送服务器的运营商亦可发挥作用。发送服务器的运营商可采用限制出局速率及端口25阻拦和其它手段以减少从其服务器发出的垃圾信息。

处理垃圾信息的工具不仅要注重邮件，同时还要重视围绕邮件的行为。鉴于上述多重因素，很多工具和方法都基于单独可行或综合利用的可辨别可疑电子邮件的成套规则或假设。随着时间的推移，垃圾信息的规模不断扩大，包含了更多的病毒和恶意软件。由此，防护技术不仅需要基于文本的工具，还需要可分析行为或场景因素的工具，从而决定是否接收或拒绝某个邮件，甚至是连接尝试。考虑到垃圾信息带来的日益巨大的安全危胁，我们希望，反垃圾信息技术将包含更多的、先进的安全及认证技术，或与这些技术的联合使用。

7.2 工具/技术场景的重要性

本段话讨论的一些工具/技术是专门针对电子邮件平台入口而设计的，而其它工具/技术布署在收到信息后，但在投递到最终用户之前则更加有用。重要的是，一些工具还可以放在接收者的计算机中。在过滤应用的各个阶段，实施规则的目的可能是拒绝电子消息，或只是对其进行标识或将其投递到最终用户的垃圾信息邮箱。

各项规则的相关性及益处只能根据具体的适用场景、在消息传播过程中的使用情况以及对最终通信所产生的影响而加以评定。

7.3 综合测试

技术是所有打击垃圾信息手段的基石。人们应认识到，以下几段话所探讨的技术中没有所谓“灵丹妙药”或解决垃圾信息问题的一站式解决方案。事实上，所有的技术是相辅相成的，只有在相互配合时才能得到最有效地实施。减少垃圾信息对系统造成的有害影响必须综合利用多种技术。

对测试不一定采用“要么全用，要么一个不用”的模式。相反，最好能综合各种测试以便使拦截的垃圾电子邮件数量最大化，并减少被恶意劫持或拒绝的合法电子邮件数量。

– 全拒绝或无拒绝－这是使用黑名单的服务可能做出的一种响应。任何测试失败的消息均可遭到拒绝。但是，错误的出现取决于规则在传播过程中所处的位置。
– 接入权－这是使用白名单的服务器可能做出的一种响应。消息通过测试则被接受。没有合法信息被拒绝的风险，但是可能会出现误报情况。举例而言，如果发件人的域未经认证（使用发送人政策框架（Sender Policy Framework）或域钥识别邮件（DKIM）），域名白名单没有真正意义。
– 很多垃圾消息或蠕虫声称来自经认可的消费者品牌，期望获得接入权。
– 计分－这是程序综合测试的方法。为避免“所有或全无”测试产生的不利之处，建议采用计分方法。但是，该方法耗费机器资源，而且需要不断更新计分因数以便增加点击，同时减少漏报。

常规方法是进行若干次“所有或全无”测试，然后对允许进入的消息打分。

7.4 反垃圾信息技术类型

7.4.1 电子邮件的认证

邮件认证方法分为不同规则类别，尽管这些方法有助于打击垃圾信息，但不能构成具体反垃圾信息技术。

为清楚起见可以举例而言。身份卡不是信任标志。行骗人亦可以拥有身份卡。但是，透明度的要求对于合法发送人来说比对垃圾信息制造者更有意义。

7.4.2 SPF和/或Sender-ID

垃圾信息迅速增加的一个主要原因是垃圾信息制造者能够将其消息的真实回复地址隐藏起来。电子邮件从架构而言并非意味着在发送人和接收人之间存在事先的联络。因此，不能依靠系统认证。令人愈加关注的问题是，钓鱼欺骗使用假冒地址勾引消息接收人披露其信用卡号码和其它个人信息。

这种技术的使用仍处于初级阶段，因此缺少标准化，但可采用认证的方法，对无法验证真实发送人的电子邮件消息进行旗标。接收服务器可以选择阻拦非认证的消息，但技术本身没有这个要求。技术所做的仅是对消息增加旗标。域层面认证的关键优势在于，它可以大大减少漏报情况，基于声誉进行更可靠的过滤。发信人的付出可以从有保障的消息投递上得到补偿（如发信人得到认证并合法使用系统或面临品牌滥用的法律风险时）。验证程序的具体情况根据所选择的模式而不同，目前已存在若干服务器认证模式。最普遍的两种模式是发送人政策框架（SPF）和Sender-ID。

这两种技术可以共同探讨，因为他们有很多共性。但是，至于选择哪一种技术并非轻而易举。

SPF和Sender-ID可用来检测一个电子邮件服务器是否得到认证，代表某个域发送电子邮件。这是通过在域名系统（DNS）中公布一个记录来完成的，它将经授权的电子邮件服务器列在一个域中。两个技术的主要区别在于所测试的身份的选择。SPF测试的是来自[b-IETF RFC 2821]信封邮件，而Sender-ID测试的是字头[b-IETF RFC 2822]。

服务器管理员采取两项行动－他们在DNS中公布SPF记录并在条目上予以测试。根据最近的报告[B-Lyris]，不适当的使用SPF记录现已严重影响消息的投递。

通过核对发送人服务器的IP地址授权电子邮件将有助于未来对垃圾信息的管理。这可能需要在认证之上创建服务，例如专用白名单、信誉评等服务和认证服务。

7.4.3 DKIM和/或META

DKIM和传输授权消息增强（META）通过电子邮件服务器自动增加的加密签名手段对发送人域进行认证。采用消息加密签名认证电子邮件有助于在未来减少并应对垃圾信息。

DKIM是这些模式中最为人熟知的一种。这种模式要求对所有发出消息使用数字签名或专用密钥。进入消息在域及邮件服务器层面通过确保专用密钥与文件中已存在的公众密钥相匹配而得到认证。这种方法可能保证该消息只能来自原有的ISP。DKIM有利于发送域，因为它能确保向运行DKIM算法的ISP的发送。最近，互联网工程任务组已将DKIM批准为一项RFC，由此使其成为一项IETF标准。

7.5 发送域的存在及应对回应的争取

很多垃圾信息制造者以不存在的发送人地址发送邮件。可以采用规则拒绝这些消息，如后缀指令reject_unknown_sender_domain或j-chkmail指令BadMX。另一种可能性是验证给定域中“from”消息字段内进入服务器（MX）的记录。一些垃圾信息制造者伪造MX记录以避免愤怒的抗议回复（例如MX至意为本地发送人的127.0.0.1）。

这些规则要求DNS流量少，这是在回复中无论如何都可能出现的情况，这些规则还可以拒绝一定量的垃圾信息。

7.6 指针记录的存在（PTR）

DNS的指针记录可用来将发送人服务器的IP地址转换成为一个名称，尽管不一定核对该名称是否与发送人域一致。

增加此类记录并非一直在发送人域的控制之内（如IP未分配addr.arpa）。这样做即使是合法的，可能也无法满足规定要求。这些记录可用来确定电子邮件消息来源以及在多大程度上这些邮件可以得到信赖。这些记录还可以用来决定一份电子邮件是否来自一个居民用IP地址或将一份错误消息转发至正确的服务器。

7.7 黑名单/白名单

传统的过滤以及对用户群的投诉跟踪可最终产生可接受发送人的白名单和可疑垃圾信息制造人的黑名单。白名单/黑名单的方法对于多数使用者来说往往是一个过于极端的解决方案。制造白名单耗费时间，而且需要不断更新。黑名单同样需要监测。所有名单都需要更新使用的机制和程序，以应对漏报问题以及对名单的欺骗性投诉。盗用地址和开放式中继也会产生问题，使邮件看上去源于一个错误地址。

黑名单基于列举垃圾信息来源的原则。该名单可包含机器名称、IP地址或电子地址。它可以通过一实体加以落实以便共用，或由满足自身需求而使用的服务器引入并维护。

使用当前的邮件传送代理（MTA），此测试可在SMTP会话中进行。因此，甚至可能在消息发送之前便遭到拒绝。一些名单包含不仅发送垃圾信息的开放中继。其开放中继配置可被发送消息的平台视为非法行为。

黑名单的质量根据编制人的专业化水平差异相差甚远。很多名单管理不当、被放弃或其真实性受到质疑：名称可以迅速增加，但采用的标准不够清楚，辙出名单根本不可能或必须付费。产生这一问题的主要原因是缺少行为准则或任何对黑名单的运行进行规范和限制的规定。如将来采用这种解决方案，需要合作建立一份优良做法清单，明确规定可列入黑名单的地址以及辙出名单的条件。

黑名单不可避免地包含不准确信息，使一些合法消息无法到达消费者。这种被称之为误报的问题在合法发送人认为他们被错误的置于ISP的黑名单时引发法律纠纷。此外，个人用户的误报问题可对完全依赖传统的过滤技术停止垃圾信息的方法造成严重影响。然而，误报可能产生于多种反垃圾信息措施。域层面的认证应限制误报情况。

尽管黑名单的使用引发很多令人担扰的问题，但对于拒绝其行为危害发送电子邮件平台的安全或服务质量的机器连接或拒绝某些发送人的信息而言是一个快捷的解决方案。

7.8 发送服务器地址被视为“动态”或“居民”

这是一种特殊的黑名单形式，加入名单的标准是，被阻拦的IP地址对应于一个ISP的个人用户机器，而不是一个组织的邮件服务器。其原理是，一个普通的用户不会在SMTP中直接发送邮件，而是通过其提供商的PTA。一般情况下，这意味着受阻拦的机器正在从垃圾信息制造者处直接发送垃圾信息，或者更加普遍的情况是，信息是在所有者不知情的情况下发送的（即，为发送消息机器已遭到破坏并转化成为“僵尸”）。

这些地址的名单并非永远可靠，因为多数名单采用启发性手法，例如在机器名称中使用了“adsl”。管理这些名单也耗费很大资源。

相反，一些名单，特别是使用这些名单的服务器所编制的名单可用来区分获得授权的域中服务器与居民用名单。此外，一些域公布其居民地址范围。

这种测试可以被看作区别“单纯的消费者”和“提供商”的方法。后者认为域所有者拒绝将其机器与居民地址相连（因为这些地址是目前垃圾信息的主要来源）的政策是合法的。但消费者认为，垃圾信息固然存在，使用电子邮件的自由必须得到保护。

7.9 过滤

过滤是最为司空见惯的反垃圾信息技术。过滤的主要好处是方便实施，而且使用者可以灵活地决定将哪些信息视为垃圾信息，启发性过滤器要求使用者规定标准，例如密码或发送人地址，由此启动过滤器阻拦一些消息进入到消费者信箱。有意误拼字词或使用不同语言拼写的垃圾信息制造者可以轻而易举地逃避密码方法。贝斯过滤器以经验为基础，在一个识别表中产生有关消息的统计数据，供个人使用者未来使用，从而区别垃圾信息和合法邮件。过滤器只允许与使用者前一个合法邮件类似的信息通过。美国联邦贸易委员会[b-FTC]2005年进行的调查研究显示，过滤器可阻拦90%的垃圾信息。

7.9.1 启发性过滤器

这些过滤器基于测试消息中是否存在某些典型的垃圾信息特点的原则，例如只使用HTML或邮件发送的消费者类别。该测试是通过对一套已知垃圾信息邮件和一套已知合法邮件的了解过程进行加权（因此，计分不是人为计算的结果，从而降低了主观性）。

这些过滤器存在的风险是，使用垃圾信息制造技术的消息－HTML中的异常消息－将被划分为垃圾信息。此外，应指出的是，这些过滤器使用大量机器资源。

这些过滤器可以发现多数垃圾信息邮件，它们不需要培训或配置。但是，由于这些过滤器使用了大量测试，应了解的是，可以更换正在运行的测试以及用来界定垃圾信息的计分。

7.9.2 关键词过滤器

这些是搜索关键词（“Viagra”等）的二进制过滤器。漏报的可能性非常大，但可以通过空格、更换字符和误拼避免这些问题。

7.9.3 摘要或散列值（hash value）过滤器

散列值过滤器对所提交的消息制造散列值，同时说明该消息是否已被确认为垃圾信息。有很多误报情况，因为很多垃圾信息邮件在被服务器中的散列值过滤器扫描到后尚未被识别。另外，有些消息差异很大，足以产生不同的散列值。解决这种问题的方法是推迟邮件（采用灰名单做法），这样可生成较少的误报情况。

7.9.4 贝斯过滤器

贝斯过滤器的工作原理是通过审查系列已知的垃圾电子邮件和一系列已知合法的电子邮件启动其引擎。之后，在从已知名单中的垃圾信息制造者身上学到词汇后，使用贝斯概率计算一条消息是否为垃圾信息。对于组过滤器，这种学习往往由系统管理员进行。

由于以垃圾信息词汇概念为基础，这些过滤器在共用的情况下可能会造成问题。在小范围和高度统一的环境中（如每个人在同一个域内采用类似词汇表工作的一个公司或大学中的一个系），这是可行的。但是，对于一个大的电子邮件提供商，特别是一个公众提供商，除非该集团为每个使用者提供其邮箱定制过滤器，这种做法令人质疑。因为，对一些使用者来说可接受的词汇，如被某集团确定为垃圾信息词汇，就可能触动过滤器。

尽管在集团层面上可能存在问题，这些过滤器用于个人使用者时相当有效，是为数不多的经适当培训后再单独使用时可过滤到几乎所有垃圾邮件的解决方案之一。

7.9.5 行为过滤器

这种过滤器审查远程服务器的行为，如单位时间内发出的邮件数量。速率限制就是一种这样的过滤。其原理是，普通的邮件是单独发送的或少数邮件一起发送，而垃圾邮件往往是特大批量发送的。

这种过滤很脆弱，因为，一般情况下，无法区别垃圾信息制造者和合法传播清单中的服务器，如新闻组。

一些专家认为，一个平台拒绝一些批量邮件是合法的，主要因为其规模有限，或有责任确保网络安全。让批量邮件发送人承担传播消息的费用，而不是过快地发送批量文件，使自己免于承担使用电子邮件这种通信手段本应承担的费用，从而节省远端平台资源也是合理合法的。

7.10 HELO/CSV

发送计算机通过SMTP “EHLO”或“HELO”指令，在每个SMTP交易开始时向接收计算机用名称通报身份。

认证服务器验证（CSV）为邮件接收服务器评估邮件发送服务器提供了一种机制。它采用现有服务提供商的做法，对发送系统连接的网络进行认证。

HELO测试核对远端MTA是否得到适当配置，但这些测试不能说明是否有垃圾信息。CSV测试对名称增加了概率测试：它是否与域对应？与SPF或DKIM不同的是，CSV不对发送消息的域进行认证，而是对电子邮件服务器域进行认证，（当提供商拥有大量客户时，情况可能有所不同）。

配置指南 – 如后缀指令reject_invalid_hostname – 测试服务器宣布的名称。使用常规HELO测试会使大量合法消息遭到拒绝。但是，目前几乎没有站址知道如何修改HELO以便使其正常工作。这种情况将来可能会发生变化，因为越来越多的站址将测试HELO，由此激励人们对此予以改进。

7.11 灰名单

当遇到一个新的发送人时，有意发送一个SMTP 4xx误码（相对于5xx确定误码的一个临时误码，见[b-IETF RFC 2821]）。如果是一个正常的MTA，新的发送人将会在晚些时候重新尝试（一般在15分钟以后），其消息也将随之得到接受。大多数垃圾信息软件程序不做多次发送尝试。这种手段非常有效，可以阻拦不通过开放中继或由提供商的MTA发送的所有垃圾邮件。它防止收到来自不良配置服务器的某些消息，特别适合与白名单一同使用。

7.12 令牌/密码

这些手段的目的是将密码纳入电子邮件发送地址或使用挑战/应对系统，如图灵测试垃圾信息制造者的软件不认识该密码，因此无法通过该测试。

这些技术没有误报问题－除非垃圾信息制造者决定雇用数千名低成本人员完成这项工作。

一些合法使用者将拒绝或无法通过测试。因此，会出现很多的漏报情况。已收到批量邮件（包括合法邮件）的接收人或希望减少自由通信范围内所收到的邮件数量的接收人对这些技术非常关注，需要注意的是，并非所有发送人将接受所实施的测试。让使用者了解该技术的好处并进行上述测试可帮助减少不可接收率。

7.13 各种手段

本段话涉及尝试最多的或测试不足的各种手段。

7.13.1 信封测试（退信地址验证（BATV）和签署的邮件发送人（SES））

这些技术是最近的开发成果，布署量很小，尚不值得考虑。

7.13.2 大宗邮件的认证 – 发送人信誉

尽管有效的发送人认证将使ISP在处理垃圾信息时可以更加直接了当地完成工作，但认证对于消除垃圾信息而言仅仅迈出了第一步。在识别发送人后，需要确定信誉并认证来决定是否将一条消息在其到达用户前确定为垃圾信息。独立机构负责确定认证程序和标准，由不同部门代表构成的监督委员会将对认证机构予以监督。

为此，可信赖的电子邮件开放标准（TEOS）已由ePrivacy’s Group制定完成。TEOS产生于旨在将合法电子邮件与垃圾信息相分离的行业自律计划。TEOS不仅采用认证，还为电子邮件发送人根据在电子邮件字头中的签名创建可信赖的身份。与DKIM的认证签名不同的是，TEOS签名是在消息中能看见的签印，证明发送人符合规定标准。

为减少将大宗邮件错误过滤为垃圾信息的问题，行业内一直讨论大宗邮件认证机制作用。举例而言，合法的大宗邮件可在ISP层面使用经服务器认可的标签进行识别，由此使人们更加有信心地使用电子邮件过滤器。一些标准亦可用于认证程序的输入，如尊重隐私的做法。例如，法国正在与其数据保护机构（CNIL）合作为通知使用客户记录的发送人提供认证。

各ISP将保持一份认证客户白名单。建议要求在各ISP之间就认证程序达成一致，不得掺杂外部干预。但是，这种方法需要大多数ISP的参与以便行之有效，并应基于ISP之间的信任，因为该认证程序没有外部监督。此外，为大宗邮件确定数量可能会造成问题。狡滑的垃圾信息制造者可以使用多个免费电子邮件账户发送大量垃圾信息，而每个账户发出的信息数量恰好低于大宗邮件预先规定的门限数量。

7.13.3 认证发送人的服务器？

FFS。

7.13.4 PGP签名

FFS。

7.13.5 系统配置

行业和个人在端口、防火墙、网络、路由器、代理、接入、密码、允许密钥保护和软件安装方面的最佳安全做法均为反垃圾信息技术中使用的系统配置方法。通过系统配置阻拦无用邮件，人们只能捕获部分垃圾信息。然而，随着越来越多的系统安装这些机制，垃圾信息制造者将会变得更加聪明，但是他们对制造垃圾信息也将越来越失去兴趣，因为障碍越来越多。现在人们知所以制造垃圾信息，是因为这很简单、快捷而且成本低廉。随着这种情况的变化（成千上万的系统管理员正在努力改变现状），制造垃圾信息将难以成功。

7.13.6 反病毒工具

反病毒工具是降低垃圾邮件感染计算机系统风险的重要技术。一般来说，有害垃圾电子邮件的附件中带有启动病毒文件。反病毒软件可以对邮箱进行扫描，防止病毒感染。

一些ISP正在使用交换服务器进行监督并更新反病毒应用程序接口（API）、VSAPI。该技术为用户邮箱提供反病毒扫描，将扫描延伸至网络边缘，从而减少病毒及感染病毒的电子邮件对网络基础设施所造成的影响。同时，通过扫描进入邮件以外的发出邮件，还可以防止受到感染的电子邮件离开一个组织。

7.14 如何利用这些技术和因素考虑问题

任何工具的实用性取决于需求、技术能力和同一工具用户的基础设施。这些工具应布署在系统的不同部分并满足不同需求。使用者应在选择和布署反垃圾信息工具时深入思考其需求及防范策略。工具从成熟度、效用、可靠性和布署来说各不相同。一些工具更容易产生漏报问题，而其它工具则在某些领域内更加有效，还有一些工具则可能在成本、基础设施、带宽/容量方面付出更多代价，因而需要技术专长。尽管列出的思考因素五花八门，但使用者应针对具体的计划应用选择适当的工具。

上述一些测试旨在打击垃圾信息，而其它测试则用来防止某些威胁安全、浪费邮件发送平台的资源或仅仅是不符合发送电子信息的规则的行为。在收到构成即将发送的消息的数据后规则得到落实，但如何处理消息还有待进一步决定。这将明显取决于所进行的测试结果。一些测试相对于其它来说更加可靠，因此可以为采取更加严厉的措施提供依据。此外，对于某些消息，可以决定进行其它或更加昂贵的测试。

根据规则实施之处而处理消息的不同方法见下文。

7.15 在SMTP会话中的拒绝

这种拒绝的关键在于不对电子消息负责，电子消息的传播由远端服务器负责。此外，这种做法节省带宽，因为首先，消息并未收到。第二，远端服务器不必发送消息可能生成的投递状态通知（DSN），即针对拒绝生成的消息，见[b-IETF RFC 3461]。发出这样一个未投递消息的任务转给了发送人。

但是，这种拒绝意味着，无法保留消息副本（因此，无法检索可能已被接收的合法消息或对拒绝进行调查）。

另外，并非目前所有的SMTP服务器均可以在SMTP会话中运行某些测试。但是，这种情况随着新产品特别是发送邮件“milter”和后缀“政策服务器”等界面或未来的OPES的广泛使用将发生变化，将任何程序连接到SMPT会话之中。

7.16 沉默拒绝

这种方法往往使普通用户感到困惑，他们希望其电子邮件得到投递或至少得到其邮件已被拒绝的通知。“投递或通知”的选择是电子邮件发送的一个重要原则，但由于假冒无关用户发送的电子邮件数量巨大，这一原则可能不得不被放弃。

理想的情况是，在这种情况下销毁的电子邮件记录应得到保护，由此可以使用[b-IETF RFC 3885] 所描述的消息跟踪协议规定的消息跟踪技术，让使用者了解其消息所发生的情况（像一般包裹投递公司所提供的包裹跟踪系统一样）。

7.17 通过发送DSN（发送状态通知或“反弹”）拒绝

这是传统电子邮件中使用的方法。但是，由于出现了joejob，有可能会惩罚无辜的发送人，可能像反病毒程序误发送DSN一样。

7.18 向垃圾信息邮箱的投递

如果少有信息被阻挡在平台入口，垃圾信息邮箱可以承载大量信息，使使用者不愿意阅读。虽然消息未被销毁，但使用者有机会对漏报情况进行补救。

7.19 标识

服务器不做任何决定，但仅在电子邮件上放置一说明。这种技术使使用者获得全部控制权，同时也强制使用者下载垃圾信息邮件。

请注意，电子邮件服务提供商可以向用户提供对邮件进行标识的选择，否则便将其发送至垃圾信息邮箱。这样管理相对容易。

附录I

有关打击垃圾电子邮件的活动

（本附录不构成本建议书的重要组成部分）

I.1 引言

此附录阐述了最近以来包括ITU-T在内的各组织打击垃圾电子邮件的活动、技术规范、行业联盟和举措。这里列举的各组织正在建议制定阶段就打击垃圾电子邮件积极开展工作。因此，技术规范的范围及验证情况以及所列各组织的状况在未来都将发生变化。

I.2 有关打击垃圾信息的国际活动

I.2.1 国际电联

在2003年12月于日内瓦召开的信息社会世界峰会（WSIS）第一阶段会议[b-WSIS-2003]上通过的《原则宣言》中，垃圾信息被看作是全面使用互联网和电子邮件业务的潜在威胁。为此，WSIS与会者认识到，垃圾信息是“用户、网络和互联网面临的越来越严重的问题”，为增强使用ICT的信心并提高安全度，有必要“在国家和国际层面采取适当行动”。

于2004年10月在巴西弗洛里亚诺波利斯召开的国际电联世界电信标准化全会（WTSA）强调指出，垃圾信息问题关乎国际电联成员国利益。在全会中，国际电联成员批准了两项涉及国际电联未来在垃圾信息领域所开展的活动的决议。

第一份有关打击垃圾信息的决议，第51号决议，责成国际电联三个部门主任及秘书长就打击垃圾信息的有关国际电联和其它国际举措向理事会2005年会议紧急拟定一份报告，并通过成员国和部门成员所做出的贡献，建议可能采取的跟进行动，供理事会审议。该决议进一步请各成员国在其国家法律框架内采取适当步骤，确保为打击垃圾信息采取适当而有效的措施。

第二份有关利用技术手段打击垃圾信息的决议，第52号决议，确认指出，“垃圾信息造成电信网安全问题，成为传播病毒和蠕虫的途径”。该决议还确认了有关ITU-T现有的一些建议书。这些建议书可以为未来该领域的发展提供指导，因此，责成相关ITU-T研究组，通过与互联网工程任务组（IETF）及其它相关各组的合作，作为一项紧急事项，酬情制定有关打击垃圾信息的技术建议书。同时，向电信标准化顾问组定期报告工作进展。该工作应得到电信标准化局主任的全力支持。该局主任将就此项议题向国际电联理事会做出报告。

I.2.2 经合组织

垃圾信息正在对数字经济造成不良影响，使经合和非经合组织国家付出了重大经济和社会代价。鉴于随着通信技术的融合该问题将愈发严重，而且通信和移动互联网将无处不在，经合组织成员国必须找到打击垃圾信息的有效途径，为应对这一挑战，经合组织信息、计算机和通信政策委员会（ICCP）在2003年3月3-4日的会议中对此项重要活动表示支持，要求将这项工作放入快速轨道，并指出这是一项全球性问题。消费者政策委员会（CCP）对经合组织在此议题上所开展的工作表示关注。在垃圾信息方面所做出的初步问题探索已拟定成为一份背景文件。由欧洲委员会主办的有关垃圾信息的研讨会在2004年2月在布鲁塞尔举行。

垃圾信息是影响到网络利用率、拥塞问题及IP网络问题、隐私和网络安全问题及消费者保护问题的多重性问题。为更好地协调有关垃圾信息的工作并为打击垃圾信息而迅速达成一个政策框架，经合组织委员会于2004年7月同意成立一个平面化“打击垃圾信息任务组”。该任务组将在2006年7月前向CCP和ICCP做出报告。

该任务组的主要目标是将指定的反垃圾信息政策协调员联合起来，以便制定打击垃圾信息迫切需要的最有效政策手段，从更广的层面上解决问题并受益于经合发组织多方面的专业技能。

该任务组被责成研究编写并推广现有及即将出台的反垃圾信息政策。认识到打击垃圾信息没有“灵丹妙药”，该任务组于2006年4月开发了一个反垃圾信息工具包“（工具包）”。该工具包基于这样一个前提，为帮助制定和发展在技术、监管及执行领域的反垃圾信息策略和解决方案并推进国际合作，应在垃圾信息问题上考虑到多种协调一致的因素。经合组织工具包旨在将内容一致和相辅相成的政策和其它（如执行）举措结合起来。工具包的制定和落实主要依赖于利益攸关方在不同领域的输入。该工具包由八个相互关连的内容组成：

– 反垃圾信息监管
– 国际执行合作
– 行业推动的反垃圾信息解决方案
– 现有和即将出台的反垃圾信息技术
– 教育和提高认识
– 和反垃圾信息合作伙伴关系
– 垃圾信息指标
– 全球合作（走出去）

任务组起草的背景报告涉及工具包的若干内容。本附录概述了任务组所开展的工作及其结论。本附录得到OECD委员会有关反垃圾信息跨边界执法合作的建议书及OECD反垃圾信息网站www.oecd-antispam.org 的补充。

I.2.3 亚太经合组织

亚太经济合作组织（APEC）在电信和信息工作组（TEL WG）讨论了垃圾信息问题。TEL WG致力于改善本地区的电信和信息基础设施，并推进有效合作、自由贸易和投资及可持续性发展。

在网络安全和基础设施领域，TEL努力在网络安全问题上与其它组织合作，在为信息社会创建安全在线环境方面加强工作，处理诸如垃圾信息等问题，打击网络威胁，将跟进行动纳入APEC打击垃圾信息行动原则和APEC打击垃圾信息行动实施指导方针，同时与国际电联、OECD和东南亚联盟（ASEAN）等国际和区域性组织开展合作。有关信息请查阅APEC TEL WG网站（http://www.apectelwg.org/）。

I.3 反垃圾信息技术规范的制定

I.3.1 ITU-T

世界电信标准化全会（2004年，弗洛里亚诺波利斯）在第52号决议中责成相关研究组与IETF和其它相关各组合作，酌情制定包括打击垃圾信息所需要的定义在内的技术建议书，并向世界电信标准化顾问组定期就进展情况做出报告。

有关电信安全的牵头研究组并负责支持WTSA第50、51和52号决议活动的第17研究组，有责任研究潜在的打击垃圾信息的各种技术措施，因为这涉及到电信网络的稳定性和稳健性。ITU-T第17研究组成立了一个专门报告人组，Q.17/17，以便为打击垃圾信息提供技术解决方案。初步的工作主要集中在就打击垃圾电子邮件制定技术规范。之后又为IP电话等IP多媒体应用进一步制定了打击垃圾信息的技术解决方案。技术规范涉及或计划涉及打击各种类型垃圾信息的指导原则、要求、技术框架和技术手段。

I.3.2 IETF

IETF已制定了若干有关打击垃圾电子邮件的RFC，从如下的指导原则到技术规范：

– [b-IETF RFC 2505] “用于SMTP MTA的反垃圾信息建议书”：

  本 RFC 为SMTP、MTA（邮件转发代理）给出了若干实施建议，使其更加具备减少垃圾信息影响的能力。这些建议书的目的是在用于互联网上足够多的SMTP MTA后帮助清洁垃圾信息环境，并作为不同MTA厂商的指导原则。这并不是最终的解决方案。但是，如果这些建议用于所有的互联网SMTP MTA，情况将大有改善，从而赢得时间设计更加长期的解决方案。有关未来工作一段阐述了可能作为长期解决方案一部分的内容。尽管最终解决方案可能是一个集社会、政治和法律为一体的方案，而不是单纯的技术方案。实施者应认识到，拒绝服务攻击的增加可能导致DNS服务器查询数量的增加并扩大登录文件的规模，从而造成系统超载或在攻击过程中崩溃。

– [b-IETF RFC 2635] “DON’T SPEW 关于批量推介性邮件和公布（垃圾信息*）的指导原则”：

  本 RFC对批量推介性电子邮件消息为何损害互联网络社会做出解释。它为用户、系统管理员、新闻管理员和邮寄名单管理员处理非推介性邮件提供了一套指导原则。同时，它还提出了可供互联网服务提供商遵循的建议。

– [b-IETF RFC 3685]“SIEVE 电子邮件过滤：垃圾信息测试和病毒测试扩展”：

  SIEVE‘垃圾信息测试’和‘病毒测试’扩展使用户能够使用简单、便捷指令用于测试电子邮件消息上的垃圾信息和病毒。每项扩展提供了一个新的测试，使用匹配，而不是用数字“计分”实际核对的工作是由底层的SIEVE的落实来实现的，由此产生测试返回的数值。

– [b-IETF RFC 4686]“启动域钥识别邮件（DKIM）威胁的分析”：

本 RFC分析了旨在由基于签名的邮件认证，特别是域钥识别邮件处理的互联网邮件威胁。它探讨了不良行为的性质和位置，能力及通过攻击所要达到的目的。

除此之外，一些草案正在制定之中，描述适用于打击垃圾电子邮件的域层面认证问题。

I.4 行业联盟名单和打击垃圾信息举措

以下列出了世界各地的行业举措。该清单并不完整，但由此可以看出各组织为以协调和有效的方式打击垃圾信息而开展的多种多样的活动和项目。

I.4.1 反钓鱼工作组

反钓鱼工作组（APWG）[b- APWG]是一个全球性泛行业执法协会，主要是清除因日益嚣张的钓鱼、网址嫁接和电子邮件盗用问题而产生的欺诈和身份盗窃。该组织为讨论钓鱼问题提供了一个论坛，从实际和潜在成本定义了钓鱼问题的范围，同时为消除该问题共享信息和最佳实践。适当时，APWG也希望与执法机构共享这一信息。

I.4.2 认证和在线信任联盟

电子邮件认证组织成立于2004年10月，现演变成为认证和在线信任联盟（AOTA Inc.）。AOTA的使命是增强对各种形式的电子消息、电子商务、电子银行和互联网的信赖和信任，帮助提高安全度和对企业和消费者提供在线保护。其目标包括推进最佳做法、数据共享和电子邮件及互联网认证的布署及实施、身份和信誉标准及解决方案以及域防护战略，在一个厂商中立的环境中提供可行的生态系统及可落实的建议。AOTA由领先的企业、行业及非营利组织构成。这些机构努力改善人们对电子消息、互联网和电子商务的信赖和信任。由于钓鱼和虚假电子邮件的破坏，这种合作对于确保电子邮件的可靠性和可投递性至关重要，它将加强在线信任和信赖并保护世界各地企业的品牌及域名。

在2004年早期，由Bigfoot Interactive、电子邮件发送人和提供商联盟（ESPC）、微软及Sendmail牵头的企业、行业和市场领导者开始聚集起来，为电子邮件认证和提高用户信心寻求解决方案。继美国联邦贸易委员会于2004年11月召开的由商务部国家标准和技术学会共同赞助的峰会后，做出决定为推进经认证的电子邮件采取果断性行动并建立了www.emailauthentication.org网站。随着钓鱼和欺骗性电子邮件对用户和企业信心的进一步伤害，2006年9月emailauthentication.org以AOTA正式成立。

在专注于电子邮件的认证和技术领导地位的同时，AOTA的使命已扩大帮助解决更广泛的问题及影响在线信赖和信任的威胁问题。

I.4.3 垃圾信息主管部门联络网（CNSA）

有关欧洲委员会的举措，由各国管理机构组成的一个非正式小组称为“打击垃圾邮件机构联络网（CNSA）”，其职责是执行第2002/58/EC号隐私和电子通信指令的第13条。

在CNSA，各国之间交流有关打击垃圾信息的做法，包括接收和处理投诉信息和情报以及调查和打击垃圾信息的最佳做法。该委员会负责承担CNSA的秘书处工作。CNSA得到协调员的帮助。协调员推动CNSA之间的信息交流并对委员会的秘书处工作提供支持。目前的协调员是法国总理办公室。CNSA定期在布鲁塞尔召开会议（每年3-4次）。CNSA还与伦敦行动计划每年召开联合会议。

CNSA已建立了一项合作程序，以便在各国管理机构之间推动有关投诉信息和其它相关情报的传送。

I.4.4 Digital PhishNet

Digital PhishNet（DPN）作为一家合作性执法机构成立于2004年12月8日，它将技术、银行、金融业务和在线拍卖领域的行业领先机构与执法部门结合起来以便对“钓鱼”（一种破坏性和日趋猖獗的在线身份盗窃形式）进行打击。

钓鱼是一种特别有害的并具有欺骗性的在线威胁，往往通过虚假或“盗用”垃圾电子邮件指使消费者进入到虚假网站，输入诸如信用卡号和密码等个人财务信息。其它行业小组着重于识别钓鱼网站并分享最佳做法和案例信息，而DPN是第一个将工作重点放在辅助执法和惩罚那些通过钓鱼对消费者犯下罪行的人们的小组。DPN将行业和执法机构结合为一体，由此可以实时地汇编重要的打击钓鱼数据，提供给执法部门。

I.4.5 电子邮件发送人和提供商联盟

电子邮件发送人和提供商联盟（ESPC）是由行业领先企业组成的一个合作性团体。它为解决日益猖獗的垃圾信息问题及不断出现的不可传送问题提供解决方案。ESPC成员已认识到，有必要制定强有力的打击垃圾信息解决方案，确保合法电子邮件的传递。ESPC成员一直积极从事打击垃圾信息的工作。ESPC通过合法宣传、技术开发和制定行业标准努力为打击垃圾信息和解决不可投递问题寻求解决方案。

ESPC由四个分委员会构成：

– 立法委员会 – 指导ESPC就联盟和各洲打击垃圾信息的立法开展游说工作。
– 接收人关系 – 帮助促进更好地了解情况并在发送人和接收人之间开展对话。
– 技术 – 评估并制定技术解决方案，对垃圾信息做出更精确的响应（减少误报情况）。该委员会已成立了一个技术工作组，探索并建议这种解决方案。该组在需要时召开会议，也定期举办面对面会议。
– 宣传 – 为该联盟提供广泛的公共事务策略。

I.4.6 垃圾信息和互联网公共政策学会（ISIPP）

垃圾信息和互联网公共政策学会（ISIPP）致力于就行业有关垃圾信息、电子邮件、电子邮件传递性和互联网的公共政策和程序等问题提供分析、信息和磋商。ISIPP还提供广泛使用的电子邮件发送人认证服务SuretyMail，还组织和赞助电子邮件管理圆桌会议、电子邮件投递性峰会和“垃圾邮件与法律”大会等论坛。

I.4.7 伦敦行动计划

伦敦行动计划是为打击垃圾信息、钓鱼和相关在线威胁而建立的全球执法机构和行业代表网络。美国联邦贸易委员会和英国公平贸易办公室牵头于2004年成立了伦敦行动计划。伦敦行动计划现拥有20多个国家的成员。自成立以来，伦敦行动计划已加强了各执法机构之间的双边和多边关系，由此促进了在多项垃圾信息调查中的国际合作。2005年伦敦行动计划与其它一些政府伙伴联合开展了“垃圾信息僵尸行动”。在此举措中，全球的机构向互联网服务提供商发出信函敦促其采取保护性措施，防止消费者计算机因发送垃圾信息而受到劫持。

如上所述，伦敦行动计划每年与CNSA举行联合年会。最近，伦敦行动计划与CNSA于2007年10月9-11日在华盛顿特区举办了第3次联合研讨会。LAP-CNSA研讨会是与第11届MAAWG全会同期举办的。LAP和CNSA与MAAWG就很多相关问题召开了若干次联合会议。

在2007年的研讨会上，伦敦行动计划还为各执法机构举办了培训会议，探讨了公众私营部门合作举措的好处，并探索了增强跨边界执法合作的途径。来自20多个国家的执法和私营部门代表参加了联合研讨会。

I.4.8 消息处理反滥用工作组（MAAWG）

消息处理反滥用工作组（MAAWG）是一个全球组织，主要工作是保护电子消息免受在线破坏和滥用，从而增强用户信赖和信心，并确保合法消息的传送。拥有代表6亿多邮箱的互联网服务提供商（ISP）和网络运营商、关键技术提供商和发送人等代表的MAAWG通过重点研究技术、行业合作和公众政策举措解决消息滥用问题。

MAAWG的宗旨是将消息行业联合起来通过合作成功解决垃圾消息、病毒攻击、拒绝服务攻击和其它滥用形式的消息滥用问题。为完成这项工作，MAAWG正在为解决消息滥用问题所必需的三个领域开展举措：合作、技术和公共政策。

I.4.9 Spamhaus

Spamhaus项目是一个非营利国际组织，其任务是追查垃圾信息制造者、垃圾信息团伙和垃圾信息业务，为IP网络提供可依赖的实时反垃圾信息保护，同时与执法机构合作识别并跟踪全球范围内的垃圾信息制造者，为制定有效反垃圾信息立法向各国政府进行游说。Spamhaus建立于1998年，总部分别设于瑞士日内瓦和英国的伦敦。该机构是由工作在九个国家的25个调查人员组成的。

Spamhaus出版已知垃圾信息操作登录表（ROKSO）－一个全世界范围内已知的200个最坏垃圾信息团伙情况和证据的数据库。ISP使用该数据库以防止已知垃圾信息制造者注册并滥用其网络，而执法机构使用该数据库帮助寻找并惩罚专业垃圾信息制造者。

Spamhaus公布了若干实时垃圾信息阻拦数据库，包括Spamhaus阻拦名单（SBL），使用阻拦清单（XBL）和政策阻拦清单（PBL）。Spamhaus清单从位于17个国家的40个DNS服务器网络上进行广播，得到众多互联网主要服务提供商、公司、大学、政府和军方网络使用。

资金来自赞助和捐赠。国际基础设施的资金通过提供垃圾信息阻拦清单同步服务（“Spamhaus数据输入”）加以筹集。此项服务由一家单独的后勤机构向大的IP网络和商用垃圾信息过滤公司提供。

I.4.10 停止垃圾信息联盟

停止垃圾信息联盟是一个联合举措以收集有关打击垃圾信息的信息和资源。此项举措由APEC、欧洲联盟的CNSA、国际电联、伦敦行动计划、OECD和首尔-墨尔本反垃圾信息集团共同完成。

根据WSIS《突尼斯议程》－[b-WSIS-2005] －即要求成员“有效处理日益严重的垃圾信息问题”并呼吁各利益攸关方通过多方面手段打击垃圾信息－停止垃圾信息联盟的网页可以链接到打击垃圾信息立法和执法活动、消费者和企业教育、最佳实践及国际合作方面的相关举措。

描述由相关组织举办的有关垃圾信息和相关威胁的国际活动的“共同活动议程”亦可在网上查询http://stopspamalliance.org/。

I.4.11 可信赖的电子通信论坛（TECF）

可信赖的电子通信论坛（TECF）是一个跨行业、跨地理区域的联合体。它致力于对打击钓鱼、地址盗用、身份盗窃的技术、手段和最佳做法进行标准化。TECF的重点是高效而有效地创建、布署和批准由成员通过研究和分析而得出的解决方案。工作组和各委员会有责任拟定和/或验证专门针对TECF所列举的高风险威胁的技术和手段。

参考文献

[b-WSIS-2003] WSIS First Phase (2003), *Declaration of Principles*. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>

[b-WSIS-2005] WSIS Second Phase (2005), *Tunis Agenda for the Information Society*. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>

[b-APWG] Anti-Phishing Working Group, <http://www.antiphishing.org/>.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*. <http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*. <http://www.ietf.org/rfc/rfc2635.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*. <http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*. <http://www.ietf.org/rfc/rfc2822.txt>

[b-IETF RFC 3461] IETF RFC 3461 (2003), *Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*. <http://www.ietf.org/rfc/rfc3461.txt>

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*. <http://www.ietf.org/rfc/rfc3685.txt>

[b-IETF RFC 3885] IETF RFC 3885 (2004), *SMTP Service Extension for Message Tracking*. <http://www.ietf.org/rfc/rfc3885.txt>

[b-IETF RFC 4686] IETF RFC 4686 (2006), Analysis of Threats Motivating DomainKeys Identified Mail (DKIM). <http://www.ietf.org/rfc/rfc4686.txt>

[b-FTC] United States Federal Trade Commission, *Email Address Harvesting and the Effectiveness of Anti-Spam Filters*, November, 2005. <http://www.ftc.gov/opa/2005/11/spamharvest.pdf>

[b-Lyris] Lyris Technologies, Inc., *Email Advisor: ISP Email Deliverability Report Card*, 2nd quarter, 2007. <http://www.lyris.com/resources/reports/deliverability_report_Q22007.pdf>

[b-OECD TF] OECD Task Force on Spam (2006), *Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures*. <http://www.oecd.org/dataoecd/63/28/36494147.pdf>

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	电信系统使用的语言和一般性软件情况

瑞士印刷
2009年，日内瓦