10 “邀请您参加我们的活动”—国内外网络安全重要活动

10.1 国内重要网络安全会议和活动

■ CNCERT 和 CNNIC 联合举办 2009 年全国网民网络信息安全状况调查活动

2010 年 3 月 30 日，CNCERT 和 CNNIC 联合召开新闻发布会，发布《2009 年全国网民网络信息安全状况调查报告》。本次调查活动由国家互联网应急中心和中国互联网络信息中心联合主办，并邀请国内安全企业、增值电信运营企业、网络游戏公司、安全论坛以及非经营性互联单位等共 12 家单位作为支持单位参与。本次网民网络信息安全状况调查活动采用在线调查问卷方式，样本目标是中国大陆（除港、澳、台三地）网民，共得到有效数据样本 25472 个。调查问卷设计以公益性和普及性为基本设计原则，设问范围涵盖当前网民网络信息安全认知及相关应用情况，以期为政府部门、行业企业以及关心我国网络信息安全状况的研究机构提供翔实可靠的参考数据，并通过宣传和推广调查活动成果，引导网民提升安全防护水平。基于取得的有效调查数据样本，报告侧重于解读 2009 年网民网络信息安全意识状况，包括网民安全防护软件使用情况、网民遭遇网络信息安全事件情况及对事件的关注度、网民安全防范意识、网民安全应用认知情况等。

■ 工业和信息化部召开《通信网络安全防护管理办法》宣贯会

2010 年 4 月 20 日，工业和信息化部通信保障局在西安召开《通信网络安全防护管理办法》宣贯会。工业和信息化部通信保障局局长王秀军强调，各级通信主管部门要突出非传统安全管理，依法履行好监管职责，抓好该办法的贯彻落实，不断提高通信网络安全防护水平，维护我国通信网络安全。当前，通信行业产业分工越来越细，网络价值逐渐从底层传输向上层应用转移，应用层网络安全事件造成的社会影响愈来愈大。为此，该办法首次将域名注册管理机构、注册服务机构、域名权威解析服务提供者纳入通信网络安全管理范畴，适用范围从基础电信运营企业扩大到提供公众通信服务的各通信网络（系统）运行单位。该办法还首次以立法形式明确了通信网络运行单位是本单位网络安全工作的责任主体，这有利于纠正当前通信行业存在的“重发展、重效益、轻安全”的倾向。

■ 国家信息安全漏洞共享平台 2010 年春季工作会议在北京召开

2010 年 4 月 20 日，国家信息安全漏洞共享平台（China National Vulnerability

Database，简称 CNVD）2010 年春季工作会议在北京召开，工业和信息化部、国家互联网应急中心、国家信息技术安全研究中心、中编办电子政务中心的相关领导到会并发言，CNVD 工作委员会、技术合作组、用户支持组全体成员单位代表，以及中国电信、中国移动、中国联通的领导和专家出席了会议。CNVD 于 2009 年 10 月成立，半年来 CNVD 共收集整理漏洞信息 26605 条，其中高危漏洞 12607 个，零日漏洞 22 个；收集补丁信息 206 条；验证可利用远程攻击代码 2456 个；发布重大漏洞公告 6 期，有效地发挥了预警作用。

会上，CNVD 对在 2009 年度信息安全漏洞库共建工作中表现突出的启明星辰、神州绿盟、知道创宇、东软、安氏领信、恒安嘉新、安天科技七家网络安全企业进行了表彰。会议期间，在与会代表的共同见证下，正式开通了 CNVD 网站（www.cnvd.org.cn）。最后，来自北京启明星辰信息安全技术有限公司、微软（中国）有限公司和国家互联网应急中心的专家分别作了题为“漏洞的进化”、“Windows 7 安全”、“2010 年一季度网络安全状况分析”的技术报告。

■ 中国反网络病毒联盟工作会议在京召开

2010 年 8 月 6 日，中国反网络病毒联盟（ANVA）在北京召开工作会议，中国电信、中国移动、中国联通、神州绿盟、启明星辰、天融信、奇虎、瑞星、腾讯、百度、新浪等联盟成员单位出席了本次会议。ANVA 是由中国互联网协会网络与信息安全工作委员会发起、国家互联网应急中心具体组织运行的行业自律组织，致力于联合基础互联网 运营企业、域名注册服务提供商、网络内容和应用服务提供商、网络安全企业等互联网行业机构，共同开展网络病毒的防范、治理工作，净化网络空间，维护公共互联网网络安全。

本次会议由中国互联网协会网络与信息安全工作委员会秘书长周勇林主持。他在会议总结中对各成员单位的积极工作表示感谢和肯定，并强调了反网络病毒工作的重要意义，希望各成员单位能够坚持不懈的积极配合联盟秘书处开展工作，共同推动反网络病毒工作和联盟的共同发展。随后，各成员单位的代表汇报了本单位上半年的反网络病毒工作情况，并就联盟组织建设、网络病毒信息共享、专项技术研究、恶意域名清理等下一阶段重点工作展开热烈讨论。与会代表一致认为，借助反网络病毒联盟的机制，联合防范、应对网络病毒黑色产业链，促进社会网络安全意识提升，对构建绿色、和谐的互联网网络环境并促进网络安全产业的健康发展具有重要意义。

■ 2010 中国计算机网络安全年会暨 FIRST 技术研讨会胜利召开

2010 年 9 月 12 日至 15 日，由 CNCERT 主办的“2010 中国计算机网络安全

年会暨 FIRST 技术研讨会”在北京国家会议中心胜利召开。工业和信息化部杨学山副部长出席大会开幕式并作大会主旨报告，提出应通过加强法制建设、建立网络空间行为规范、提升网络安全保障能力和开展国际合作这四个方面的工作，共同打造安全、可靠、放心的网络空间；国家信息化专家咨询委员会周宏仁副主任为大会作专题报告；相关政府部门、专业机构和重要信息系统单位的领导出席了开幕式；来自国内外网络安全科研和产业机构，银行、电信等重要信息系统单位，以及 FIRST、APCERT 等国际网络安全组织的近 400 名代表参加了本次年会。本次年会以“对话、合作、联动——共筑网络安全”为主题，围绕“信息基础设施安全”、“网络安全产业发展”、“网络应用安全”、“新技术和新挑战”四个分论坛，并联合国际权威网络安全组织“事件响应与安全组织论坛（FIRST）”同期举办了 FIRST 技术研讨会，通过专场培训、技术报告、会间交流等形式与参会代表进行全方位互动。本次年会为促进网络安全事业发展，推动国际交流与合作，共筑全球互联网安全贡献了积极力量。

10.2 国际重要网络安全会议和活动

■ APCERT 2010 年度应急演练顺利进行

2010 年 1 月 28 日，CNCERT 参加了由 APCERT 组织的年度应急演练。本次演练的主题是“打击金融领域的网络犯罪行为”，通过演练检验各 CERT 组织应对和处理金融领域网络安全事件的能力以及各国和地区间协调合作的实效。14 个国家和地区的 16 个 CERT 组织参加了演练，包括澳大利亚、文莱、中国大陆、中国台湾、中国香港、印度、印度尼西亚、日本、韩国、马来西亚、新加坡、斯里兰卡、泰国和越南。

CNCERT 首次作为 APCERT 演练的组织者之一，参与了本次演练的内容设计和模拟系统搭建的工作。演练的背景是，提供在线交易服务的金融类网站，如电子银行、电子拍卖和股票交易等网站，经常受到网络犯罪分子和集团的各类攻击，他们通过仿冒在线业务盗取用户的账号、密码直至钱财。由于网络在线业务的日益普及，犯罪分子已将此类渠道作为地下黑色经济的一个重要收入来源。犯罪分子已经变得非常职业化，他们开发和利用僵尸网络取得用户的登录权限，植入网络钓鱼网站，或发动分布式拒绝服务攻击。当用户浏览此类挂马网站，其电脑就会中招而成为僵尸网络的一员。由于僵尸网络和钓鱼网站往往都是跨国界的，因而发生的拒绝服务攻击和网络钓鱼事件也是跨国界的。单凭一国之力难以处理这些事件，迫切需要各个国家和地区 CERT 组织之间的通力合作。在本次演

练过程中，各 CERT 组织积极响应模拟的安全事件，共享恶意代码的检测和分析结果，并采取措施关闭钓鱼网站或阻断参与拒绝服务攻击的僵尸网络服务器。

■ 第七届世界安全会议在比利时召开

2010 年 2 月，CNCERT 应邀赴比利时出席了由美国东西方研究所(EastWest Institute)主办的第七届世界安全会议（Worldwide Security Conference）。期间，来自各国各地区的近百位人士参加了研讨，从政府决策、法律规范、技术研究、协作机制等多个角度就加强网络安全管理、增进网络安全协作水平提出了各自见解。CNCERT 参加了世界安全会议闭门专家会议、全体会议以及亚洲网络安全分论坛等重要议程，并在全体会议上就“网络威胁与金融、经济安全”主题发表了演讲。

会后，CNCERT 应邀与比利时国家级网络研究组织——BELNET 会见。BELNET 是比利时主管教育网络的机构。CNCERT 主要介绍了在网络安全应急处置方面开展的工作，BELNET 则介绍了比利时教育网络安全运行情况、安全事件处置情况。双方的会谈还涉及基础网络运行管理、热点安全领域研究、应急处置技术等多方面内容，并就将来在网络安全事件(如：恶意域名、拒绝服务攻击、网络仿冒等)的跨国协作达成了口头意向。

■ 中美网络安全对话机制正在持续开展

中美网络安全对话机制是在美国知名智库——东西方研究所提议下，经工业和信息化部、国务院新闻办推荐，由中国互联网协会牵头就反垃圾邮件、黑客攻击等多个专题与其开展交流和沟通活动，从而增进中美双方在网络安全问题上的相互了解、进一步促进合作。中国互联网协会指定其网络与信息安全工作委员会（秘书处设在 CNCERT）具体承办。自 2010 年 3 月起，CNCERT 先后组织召开中美网络安全对话机制反垃圾邮件专题中美双方会议、电话会议及中方专家组内部会议共十四次，中方专家组成员主要来自中国互联网协会反垃圾邮件中心、北京邮电大学、中国电信、中国联通、新浪公司、网易公司、263 公司、腾讯公司、万网志成公司、绿盟公司等单位，美方专家组成员则来自 Switch NAP、Google、Northrop Grumman、Bell Labs、Comcast Cable Communications、VeriSign、Pennsylvania State University、George Washington University、CERT at CMU Software Engineering Institute、AT&T、Global Cyber Risk、San Jose State University、Cox Communications 等机构。截止 2010 年 12 月底，双方已就反垃圾邮件专题充分交换了意见，并形成了反垃圾邮件建议联合报告的初稿。

■ 2010 年中日信息技术与产业政策交流会胜利召开

2010 年 4 月 9 日 ,工业和信息化部与日本经济产业省在北京共同举行了 2010 年中日信息技术与产业政策交流会。双方就信息产业最新政策、绿色 IT、新技术发展与应用政策、软件服务业、网络信息安全及电子信息产品标准和计算机技术与软件专业技术资格 (水平) 考试等议题广泛交换了意见。会议由工业和信息化部国际合作司和日本经产省商务情报政策局共同主持 ,工业和信息化部相关司局、国务院信息化专家咨询委员会、国家互联网应急中心 (CNCERT) 、中国电子信息产业研究院及日方相关人员参加了会议。CNCERT 在下午的网络信息安全议题中，代表中方介绍了 CNCERT 的监测和事件处置情况、在网络安全领域的国际合作情况，以及中日 CERT 的合作及提议。随后，日方经济产业省和 JPCERT 的代表分别介绍了日本网络信息安全的现状和 JPCERT 的国际合作情况，并对 CNCERT 的提议表示支持，赞扬了 CNCERT 在网络安全信息共享和事件处置等方面的积极合作。

■ 第二十二届计算机安全事件处理年会在美国召开

2010 年 6 月 13 日至 18 日，第二十二届计算机安全事件处理年会在美国迈阿密市召开，CNCERT 参加了本次会议。该年会由 FIRST (Forum of Incident Response and Security Team,事件响应与安全小组论坛) 组织举办，是各国政府与民间计算机安全应急处理组织之间广泛交流和深入探讨计算机安全事件应急处理方法的重要活动，主要包括 FIRST/ICANN 研讨会、网络安全事件响应技术培训、网络安全事件响应案例介绍与网络安全事件响应管理等内容。

■ CNCERT 受邀参加“中国-东盟电信监管圆桌讨论会”

2010 年 7 月 7 日至 8 日，CNCERT 受邀陪同工业和信息化部有关部门赴越南出席了东盟电信监管理事会第十六次会议，重点参加了其中的“中国-东盟电信监管圆桌讨论会”。中方作为东盟电信监管理事会对话伙伴，出席了 7 月 8 日下午举行的“中国-东盟电信监管圆桌讨论会”。会议由本届东盟电信监管理事会会议主席越南信息与通信部副部长 Le Nam Thang 主持，中国和东盟除菲律宾以外的九国电信监管机构共约 80 多名代表出席。

Le Nam Thang 先生代表东盟电信监管理事会欢迎中方参加第五次“中国-东盟电信监管圆桌讨论会”，并邀请中方代表发言。工信部通信保障局领导代表我方感谢东盟的友好邀请和主办方越南信息与通信部的热情接待 ,一是简要回顾了自 2006 年来中国应邀参加东盟电信监管理事会的主要成果；二是介绍了工业和信息化部近年来开展网络安全工作的情况；三是总结了 2009 年 10 月中国-东盟电信部长会议上正式签署《中国-东盟电信监管理事会关于网络安全问题的合作

框架》以来，中国和东盟在网络安全领域的合作情况。

随后，我方表达了愿同东盟各成员国共同促进本地区网络安全领域合作与信息通信领域繁荣发展的愿望，并提出 2009-2010 年度中国-东盟在网络安全领域合作活动的建议。中方介绍后，马来西亚等国代表相继发言表示支持中方的提议，愿意与中方开展持续性合作，并对中方多次参加东盟网络安全应急演练及 CNCERT 成功主办的 “中国-东盟网络安全研讨会”表示赞赏。

■ CNCERT 受邀参加“亚太经合组织（APEC-TEL）电信工作组会议”

2010 年 5 月和 8 月，CNCERT 受邀陪同工业和信息化部有关部门参加了 APEC-TEL 第 41 次会议和第 42 次会议，重点参加了其中的网络安全工作组会议。会议通报了 APEC-TEL 在网络安全意识提升、公钥基础设施（PKI）应用、网络反恐、移动终端安全、反垃圾邮件、海光缆保护等方面的最新工作进展，并探讨如何应对当前网络安全新威胁。我方参加了基础电信运营企业网络安全行动规范、儿童上网安全保护等专题研讨会，并发表了演讲，介绍了我国互联网行业主管部门、基础电信运营企业和网络安全组织近年来网络安全工作开展情况。

鉴于我方于 2008 年完成的 APEC 项目“僵尸网络应对政策和技术手段指南”，各经济体对源于我国垃圾邮件数量持续降低的情况及僵尸网络治理措施很感兴趣，我方筹划进一步申请“僵尸网络培训”项目，扩大与 APEC 各经济体在网络安全领域的共识，共同面对日益严峻的内外部网络安全威胁，深化在网络安全事件处置方面的合作。第 42 次会议后，CNCERT 还为 2010 年 10 月举行的 APEC 第八次电信部长会议网络安全宣传海报展设计了一幅反映我国网络安全行业自律联盟和提高网络安全意识活动的海报，得到了参会者的关注和好评。

■ CNCERT 与东盟 CERT 组织完成年度应急演练

2010 年 9 月 21 日，CNCERT 参加了由东盟 CERT 组织的年度网络安全应急演练，这是 CNCERT 连续第四年参加该项演练。参加本次应急演练的 CERT 组织来自东盟成员国及其对话伙伴国等十个国家，包括文莱 BruCERT、中国 CNCERT、印度 CERT-In、印尼 ID-SIRTII、日本 JPCERT、马来西亚 MyCERT、缅甸 mmCERT、新加坡 SingCERT、泰国 ThaiCERT 和越南 VNCERT 共十个国家级 CERT 组织。

近来，恶意 PDF 文件成为黑客入侵的重要工具之一，PDF 解析器漏洞成为各国 CERT 组织重点关注的威胁。本次演练搭建了一个调查和响应 PDF 感染事件的平台，各国 CERT 组织按照各自的事件应急处理流程，对模拟发生的 PDF 感染事件进行分析研判，完成信息通报、代码分析、发现目标并协调关闭控制服

务器。本次演练成功检验和提升了各国 CERT 组织在网络安全突发事件中的应急处置效率和协同配合能力。

■ 微软第二届反数字犯罪协作会议在加拿大召开

2010 年 10 月 12 日至 15 日，微软第二届反数字犯罪协作会议在加拿大蒙特利尔举办。该会议由微软公司主办，是各国应急组织、民间团体、安全企业、研究机构共同讨论网络安全事件处理、网络犯罪打击、网络安全技术交流的重要国际性会议，其前身为在国际上具有重要影响力的微软反僵尸网络大会。本次会议共有来自美国、加拿大、日本等多个国家的四百多名代表参加，会议针对影响伊朗核设施的“震网”病毒、“宙斯”网银大盗等热点技术进行深入的探讨和分析。

会上，CNCERT 做了关于中国网络安全形势的报告，详细介绍了国际黑客利用僵尸网络、木马等手段控制我国大量计算机的事实，分析了伊斯兰世界相关黑客攻击我国大量政府网站的现状，并深度剖析了 2010 年 3 月 Google 被来自中国黑客攻击的事实真相。与会代表反映，第一次听到 Google 被攻击的真实说法并感到震惊，同时感谢中国应急组织做了大量富有成效的工作，指出中国恶意域名的数量今年锐减，已经从去年的排名第一跌出前五名，这和中国政府在网络环境治理方面的努力密不可分。会议还表彰了 2010 年 4 月在协同处置 Waledac 全球大型僵尸网络中做出突出贡献的相关单位，授予 CNCERT、美国华盛顿大学、威瑞信(Verisign)等六个单位“Waledac 处置英雄奖”，并颁发了奖杯。