1 2010 年网络安全状况综述

1.1 总体状况

当前，互联网在我国政治、经济、文化以及社会生活中发挥着愈来愈重要的作用，作为国家关键基础设施和新的生产、生活工具，互联网的发展极大地促进了信息流通和共享，提高了社会生产效率和人民生活水平，促进了经济社会的发展。互联网的影响日益扩大、地位日益提升，维护网络安全工作的重要性日益突出。回顾 2010 年，在政府相关部门、互联网服务企业、网络安全企业和网民的共同努力下，我国互联网网络安全状况总体平稳，但互联网所面临的安全威胁呈现出一些新的特点和趋势。本综述将从基础网络安全、重要联网信息系统安全、公共网络环境安全和国际网络安全动向等方面分析归纳 2010 年的互联网网络安全态势。

一、基础网络安全

2010 年，基础网络运行总体平稳。互联网骨干网各项监测指标正常，未发生重大网络安全事件。但不容忽视的是，域名系统仍然是互联网安全的薄弱环节。2010 年 1 月 12 日，由于在境外注册的域名信息被篡改，百度网站发生近 4 小时的访问故障，引起网民广泛关注。9 月 10 日，安徽电信公共域名服务器（DNS）遭受网络攻击，省内互联网用户上网受到一定影响。此外，2010 年还多次发生针对新网、万网等域名注册服务机构的网络攻击事件，对域名注册和解析服务造成影响。

二、重要联网信息系统安全

（一）政府网站安全防护薄弱。据国家互联网应急中心监测，2010 年中国大陆有近 3.5 万个网站被黑客篡改，数量较 2009 年下降 21.5%，但其中被篡改的政府网站高达 4635 个，比 2009 年上升 67.6%。中央和省部级政府网站安全状况明显优于地市以下级别的政府网站，但仍有约 60%的部委级网站存在不同程度的安全隐患。政府网站安全性不高不仅影响了政府形象和电子政务工作的开展，还给不法分子发布虚假信息或植入网页木马以可乘之机，造成更大的危害。

（二）金融行业网站成为不法分子骗取钱财和窃取隐私的重点目标。网络违法犯罪行为的趋利化特征明显，大型电子商务、金融机构、第三方在线支付网站成为网络钓鱼[1]的主要对象，黑客仿冒上述网站或伪造购物网站诱使用户登陆和

[1]网络钓鱼是通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、

交易，窃取用户账号密码、造成用户经济损失。2010 年，国家互联网应急中心共接收网络钓鱼事件举报 1597 件，较 2009 年增长 33.1%；“中国反钓鱼网站联盟”处理钓鱼网站事件 20570 起，较 2009 年增长 140%。

（三）工业控制系统安全面临严峻挑战。2010 年 9 月，伊朗布什尔核电站遭到 Stuxnet 病毒攻击，导致核电设施推迟启用。Stuxnet 病毒是一种蠕虫病毒，利用 Windows 系统漏洞和移动存储介质传播，专门攻击西门子工业控制系统。业界普遍认为，这是第一次从虚拟信息世界对现实物理世界的网络攻击。工业控制系统在我国应用十分广泛，工业控制系统安全值得高度关注。

三、公共网络环境安全

（一）木马和僵尸网络依然对网络安全构成直接威胁。2010 年，由于扩大了监测范围[2]，国家互联网应急中心全年共发现近 500 万个境内主机 IP 地址感染了木马和僵尸程序，较 2009 年大幅增加。2010 年，在工业和信息化部的指导下，国家互联网应急中心会同基础电信运营企业、域名从业机构持续开展木马和僵尸网络专项打击行动，成功处置境内外 5384 个规模较大的木马和僵尸网络控制端和恶意代码传播源。监测结果显示，相对 2009 年数据，远程控制类木马和僵尸网络的受控主机数量下降了 25%，治理工作取得一定成效。然而，黑客也在不断提高技术对抗能力。根据工业和信息化部互联网网络安全信息通报成员单位报告，2010 年截获的恶意代码样本数量特别是木马样本数量，较 2009 年明显增加，木马和僵尸网络治理工作任重道远。

（二）手机恶意代码日益泛滥引起社会关注。随着移动互联网智能终端的普及，手机恶意代码开始出现并快速蔓延。不法分子利用手机恶意代码窃取用户隐私信息、恶意订购各类增值业务或发送大量垃圾短信，危害用户利益和网络安全。据“中国互联网协会反网络病毒联盟（ANVA）”的监测数据，2010 年新截获手机恶意代码 1600 余个，累计感染智能终端 800 万部以上。其中，“毒媒”木马全年累计感染约 200 万多个用户手机，“手机骷髅”病毒累计感染 83 万余个用户手机。另外，从手机平台来看，Symbian 平台是手机恶意程序感染的重点对象，约有 69%的恶意程序针对该平台手机，其次分别是 J2ME 平台（27%）和 Android 平台（3%）。手机恶意代码增长速度快、传播范围广、造成危害大，移动互联网网络环境治理工作亟待加强。

（三）软件漏洞是信息系统安全的重大隐患。网络设备、服务器系统、操作

手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人秘密信息（如银行帐号和帐户密码）。

[2] CNCERT 根据木马和僵尸网络的发展情况，不断调整监测范围，新增了下载者木马、窃密木马、盗号木马、流量劫持木马、部分新型远程控制木马等木马监测类型。

系统、数据库软件、应用软件乃至安全防护产品普遍存在安全漏洞，高危漏洞会带来严重的安全隐患。2010 年，国家互联网应急中心发起成立的“国家信息安全漏洞共享平台（CNVD）”共收集整理信息安全漏洞 3447 个，其中高危漏洞 649 个（占 18.8%）。典型的高危漏洞有：论坛建站软件 Discuz!高危漏洞、MySQL yaSSL 库证书解析远程溢出漏洞、Microsoft IE 对象重用远程攻击漏洞、Microsoft Windows 快捷方式‘LNK’文件自动执行漏洞、IBM 公司 Lotus Domino/Notes 群件平台密码散列泄露漏洞、工业自动化控制软件 KingView6.5.3 缓存区溢出漏洞等。CNVD2010 年收集整理的漏洞中，应用程序漏洞占 62%，操作系统漏洞占 16%，WEB 应用漏洞占 9%，分列前 3 位。

（四）DDoS 攻击危害网络安全。2010 年，分布式拒绝服务（DDoS）攻击呈现转嫁攻击[3]和大流量攻击的特点。2010 年，某些政府网站的流量异常事件以及腾讯业务系统多次遭受攻击事件，都是缘于游戏私服[4]网站在遭到攻击后将其网站域名恶意指向上述系统所致。另一方面，DDoS 攻击流量越来越大，如针对“456 游戏”网站的攻击流量峰值甚至超过 100Gbps，对公共互联网的安全运行造成较大冲击。由于攻击源多采用虚假源 IP 地址，对攻击行为的溯源和应急处置工作面临很大困难。

（五）我国垃圾邮件治理成效显著。在互联网行业的共同努力下，过去一年中，源于中国的垃圾邮件数量呈稳步下降之势。据英国网络安全公司 Sophos2010 年第 1 季度监测报告显示，源于中国的垃圾邮件数量仅占全球垃圾邮件总量的 1.9%，排名从 2009 年第 4 季度的第 7 位大幅下降至第 15 位；2010 年后 3 个季度的 Sophos 报告显示，我国已不在全球垃圾邮件源发大国之列。

（六）互联网应用层服务的市场监管和用户隐私保护工作亟待加强。2010 年，发生了以“3Q 大战”[5]为代表的多起终端安全软件与互联网应用服务之间的商业争端，以及终端安全软件之间的商业争端，反映出互联网应用层服务的市场竞争失序，用户隐私保护立法工作亟待加强，社会各界要求加强管理的呼声强烈。

四、国际网络安全动向

（一）网络安全事件的跨境化特点日益突出。2010 年，国家互联网应急中心监测发现共近 48 万个木马控制端 IP，其中有 22.1 万个位于境外，前三位分别是美国（占 14.7%）、印度（占 8.0%）和我国台湾（占 4.8%）；共有 13782 个僵

[3]转嫁攻击是指某些网站在受到攻击后，通过修改域名指向等方式，将攻击流量嫁祸给第三方网站从而危害第三方网站安全的行为。

[4] 游戏私服是指未经网络游戏制作商的法定许可，私自存在并运营的游戏服务器，其目的是向玩家收费而获利。

[5] “3Q 大战”是指，2011 年 11 月两大互联网增值服务商——奇虎 360 公司和腾讯公司借安全名义发生争端，最终发展到各自在互联网终端软件采取互斥技术，导致双方大量用户使用受到影响。

尸网络控制端 IP，有 6531 个位于境外，前三位分别是美国（占 21.7%）、印度（占 7.2%）和土耳其（占 5.7%）。另据工业和信息化部互联网网络安全信息通报成员单位报送的数据，2010 年在我国实施网页挂马、网络钓鱼等不法行为所利用的恶意域名半数以上在境外注册。2010 年国家互联网应急中心协调境外网络安全组织和域名机构处理多起针对境内的恶意扫描、网络钓鱼等网络安全事件，得到美国、韩国、澳大利亚等国应急组织和“国际反网络钓鱼联盟”等组织的配合。总体上看，跨境网络安全事件呈现快速增长趋势，国际网络安全合作需进一步加强。

（二）发达国家政府普遍加强网络安全管理。美国政府出台《加强网络安全法案》等相关网络安全法律文件，推进网络安全立法；推出“完美公民”计划，拟建全美联网监控体系对抗网络犯罪。欧盟正式发布《欧洲数字化议程》五年规划，提出增强网络安全相关举措。瑞典政府拟设国家信息技术安全中心，以应对网络攻击及处理信息技术案件。日本政府批准制定“保护国民信息安全战略”，加大监管力度，构筑安全网络社会。新加坡信息通信发展管理局通过制定新准则、加强信息分析能力以及提高公民网络安全意识加强新加坡网络安全。澳大利亚启动国家计算机应急响应官方机构 CERT Australia，支持政府打击网络犯罪和网络恐怖主义威胁。

部分发达国家加强网络攻防建设。继美军方成立网络司令部、白宫设立网络安全专员之后，美国国土安全部与国防部签署网络安全合作协议，还依托北约集团打造网络战联盟，并连续举行三次“网络风暴”演习。2010 年 11 月，欧盟举行了由欧盟成员国和冰岛、挪威、瑞士 3 个非成员国参加的“欧洲 2010 网络”演练。

1.2 数据导读

多年来，国家互联网应急中心对我国网络安全宏观状况进行了持续监测，以下是 2010 年抽样监测获得的主要数据分析结果。

- 木马与僵尸网络监测
  - 2010 年木马控制服务器 IP 总数为 479626 个，较 2009 年下降 21.3%。其中，境内木马控制服务器 IP 数量为 258623 个，较 2009 年下降 41.9%；境外木马控制服务器 IP 数量为 221003 个，较 2009 年增长 34.1%。
  - 2010 年木马受控主机 IP 总数为 10317169 个，较 2009 年大幅增长 274.9%。其中，境内木马受控主机 IP 数量为 4514312 个，较 2009 年大幅增长 1620.3%；境外木马受控主机 IP 数量为 5802857 个，较 2009 年增长 133.1%。木马受控主机 IP 数量的大幅增长主要是由于自 2010

年 6 月起，国家互联网应急中心的监测范围新增了下载者木马、窃密木马、盗号木马、流量劫持木马、部分新型远程控制木马等。

- 2010 年僵尸网络控制服务器 IP 总数为 13782 个，较 2009 年下降 39.6%。其中，境内僵尸网络控制服务器 IP 数量为 7251 个，较 2009 年增加 72.9%；境外僵尸网络控制服务器 IP 数量为 6531 个，较 2009 年下降 65.0%。
- 2010 年僵尸网络受控主机 IP 总数为 5622023 个，较 2009 年下降 52.8%。其中，境内僵尸网络受控主机 IP 数量为 470120 个，较 2009 年下降 43.9%；境外僵尸网络受控主机 IP 数量为 5151903 个，较 2009 年下降 53.4%。

■ “飞客”蠕虫监测

- 仅 12 月一个月的监测就发现全球互联网已经有超过 6000 万个主机 IP 感染“飞客”蠕虫，其中，境内感染“飞客”蠕虫的主机 IP 有超过 900 万个。

■ 移动互联网安全监测

- 在手机恶意代码的监测方面，全国感染“毒媒”的用户达 200 万余个，感染“手机骷髅”的用户达 83 万余个，感染“FC.MapUp.A”的用户达 21 万余个，感染“Boothelper.A”的用户达 1431 个。

■ 网站安全监测情况

- 2010 年境内被篡改网站数量为 34845 个，较 2009 年下降 17.1%。
- 2010 年境内被篡改政府网站（gov.cn 域名网站）数量为 4635 个，与 2009 年相比增加 67.6%。2010 年被篡改的政府网站占整个境内被篡改网站总数的 13.30%。在国家互联网应急中心监测的政府网站列表中，2010 年被篡改的政府网站比例达到 10.3%，即全国有十分之一的政府网站被篡改。
- 2010 年国家互联网应急中心共接到 1566 件网页仿冒事件报告，经归类合并后国家互联网应急中心成功处理了 631 件。在国家互联网应急中心接收到的这些网页仿冒事件中，被仿冒的大都是电子商务网站、金融机构网站、第三方在线支付站点、社区网站等。

■ 信息系统安全漏洞公告及处理

- 2010 年 CNVD 共收集新增漏洞信息 3447 个。其中，高危漏洞 649 个（占 19%）。此外，2010 年 CNVD 共收录漏洞补丁 2310 个。

- 网络安全事件接收与处理

  - 2010 年国家互联网应急中心共接收了 10433 件非扫描类网络安全事件报告，其中国外报告事件数量为 5070 件。所报告的网络安全事件集中在信息系统漏洞（占 33.0%）、恶意代码（占 19.6%）、网页挂马（占 21.4%）和网页仿冒（占 15.0%）等类型。
  - 2010 年国家互联网应急中心共成功处理各类网络安全事件 3236 件，较 2009 年增长了 175%。其中，恶意代码事件（占 45.2%）、网页挂马事件（占 20.0%）、网页仿冒事件(占 19.5%)和网页篡改事件(占 12.7%)处置较多。

- 网络安全信息发布情况

  - 2010 年国家互联网应急中心共收到通报行业各单位报送的网络安全月度信息 674 份，事件信息和预警信息 728 份。全年共编制并向各单位发送《互联网网络安全信息通报》28 期，《网络安全信息与动态周报》48 期。
  - 2010 年国家互联网应急中心通过发布网络安全专报、周报、年报和在期刊杂志上发表文章等多种形式面向行业外发布报告 101 个。