8 “欢迎您分享我们的分析报告。”—网络安全专题研究

8.1 2010 年国内网络安全监管动态报告

■ 国内网络安全相关立法动态

1. 《中华人民共和国保守国家秘密法》重新修订，对计算机网络保密管理提出新标准

《中华人民共和国保守国家秘密法》由中华人民共和国第十一届全国人民代表大会常务委员会第十四次会议于 2010 年 4 月 29 日修订通过，于 2010 年 10 月 1 日起正式实施。新修订的保密法从 1995 年开始调研论证，全国人大常委会 3 次进行审议，民众提出修改意见建议达 2000 多条，修改时间长，民众参与多、国际关注度高。针对近年来信息化发展的现状和网络泄密高发的趋势，新修订的保密法对计算机网络保密管理提出了新标准：(1)计算机信息系统将按照涉密程度不同，采取不同强度的管理措施；(2)保密技术设施、设备要按国家标准配备，并与涉密信息系统同步规划、建设、运行；(3)不得将涉密计算机、涉密存储设备接入互联网及其他公共信息网络等；(4)网络运营商、服务商有责任配合有关机关调查泄密事件，发现泄密事件要及时报告。

2. 《电信法》草案上报国务院，关注和重视网络信息安全问题

2010 年 5 月，按照国务院办公厅印发的《国务院 2010 年立法工作计划》要求，工业和信息化部将《电信法》草案上报国务院，并进一步对草案进行了修改完善。制订《电信法》草案是为了维护电信市场秩序，保护电信用户的合法权益，保障电信网络和信息安全，推动三网融合，促进电信市场公平竞争和电信产业发展。《电信法》草案特别关注和重视网络信息安全问题，在“电信网络与信息安全”、“应急通信保障和通信管制”等章节对电信网络的建设和运行管理作了明确的规定。

草案第七十六条规定：“电信业务经营者在电信网络的规划、建设和运行过程中，应当按照国家安全、网络安全、信息安全、应急处置和国防的要求及标准，同步规划、同步建设、同步运行配套的电信网络与信息安全设施、应急通信保障设施，并提供相应技术支持，保障相关设备、设施的正常运行。”

草案第八十五条规定：“电信业务经营者应当根据电信主管部门的要求提供应急通信保障，配备必要的网络资源和电信应急设备，制定通信保障应急预案，健全网络与信息安全应急制度。在发生突发重大网络信息安全事件时，服从电信主管部门的统一指挥与协调，采取相应的安全应急措施。”

3. 全国人大常委会通过议案审议结果，工业信和信息化部已完成《信息安全条例（报送稿）》

2010 年 11 月，全国人民代表大会常务委员会表决通过全国人大财经委员会关于第十一届全国人民代表大会第三次会议主席团交付审议代表提出的议案审议结果，同意由工业和信息化部、公安部通过制定《信息安全条例》等专项法规解决议案所提问题，同时就互联网立法问题展开深入调研，在条例实施和立法调研的基础上，提出综合性的立法方案，解决当前互联网缺乏法律规范的问题。目前，工业和信息化部已完成《信息安全条例（报送稿）》，其中对信息网络环境下法律主体的权利、义务，各种危害网络与信息系统安全行为等内容做出了规定。

4. 工业和信息化部出台《通信网络安全防护管理办法》

2010 年 1 月 21 日，工业和信息化部出台《通信网络安全防护管理办法》（工业和信息化部令第 11 号），完善了通信网络安全保障的法律制度，增强了通信网络安全防护工作的系统性、规范性和科学性。该办法根据《中华人民共和国电信条例》制定，全文共计 31 条。针对通信网络面临的新情况新问题，为提高我国通信网络安全保障水平，增强网络安全事件预防能力，最大限度地减少重大网络安全事件的发生，该办法结合通信技术发展的特点，围绕通信网络安全防护管理工作，按照“积极防御、综合防范、分级保护”的原则，建立了通信网络的定级备案、标准符合性评测、安全风险评估、灾难备份、监督检查等基本制度，明确规定了我国境内电信业务经营者和互联网域名服务提供者的网络安全防护责任，为推进和深化我国通信网络安全防护工作奠定了基础。

5. 文化部出台《网络游戏管理暂行办法》

2010 年 6 月 3 月，文化部出台《网络游戏管理暂行办法》（文化部令第 49 号）。该办法根据《全国人民代表大会常务委员会关于维护互联网安全的决定》和《互联网信息服务管理办法》以及相关法律法规制定，共计 6 章 39 条，首次系统地对网络游戏的娱乐内容、市场主体、经营活动、运营行为、管理监督和法律责任做出明确规定。其中，第二十八条特别规定网络游戏运营企业应当按照国家规定采取技术和管理措施保证网络信息安全，包括防范计算机病毒入侵和攻击破坏，备份重要数据库，保存用户注册信息、运营信息、维护日志等信息，依法

保护国家秘密、商业秘密和用户个人信息。

■ 国内网络安全相关行政管理动态

1. 工业和信息化部组织开展 2010 年度通信网络安全防护检查工作

2010 年 6 月至 10 月，工业和信息化部组织开展了 2010 年度的全国范围内的通信网络安全防护检查工作。自 2006 年起，工业和信息化部每年组织开展一次全行业的通信网络安全大检查和风险评估，发现隐患督促企业落实整改措施，为确保十七大、北京奥运会和国庆 60 周年通信网络安全畅通发挥了重要作用。2010 年，工业和信息化部结合上海世博会和广州亚运会保障工作要求，按照《通信网络安全防护管理办法》有关要求，加大网络安全防护检查力度。在 2009 年网络安全检查的基础上，进一步突出重点，组织基础电信运营企业和中国互联网络信息中心，对移动通信网、IP 承载网络、支撑网、网上营业厅和域名系统等当前存在问题较多的网络和系统进行自查和整改。在企业自查的基础上，组织专业技术力量进行进一步的抽查，督促企业排查安全隐患，并落实整改措施。特别针对上海世博会和广州亚运会通信网络安全保障要求，组织开展对上海、广东等地区的三级（含）以上通信网络单元进行风险评估、技术评测和整改，有效地保障了上海世博会、广州亚运会期间上海、广东地区乃至全国通信网络的安全畅通。

2. 国务院新闻办发表《中国互联网状况》白皮书

2010 年 6 月 8 日，国务院新闻办发表了《中国互联网状况》白皮书，白皮书分为前言、推进互联网发展与普及、促进互联网广泛应用、保障公民互联网言论自由、管理互联网的基本原则与实践、维护互联网安全、积极开展国际交流与合作、结束语 7 部分，全文约 13000 字。白皮书在“五、维护互联网安全”一节中指出“维护互联网安全是互联网健康发展和有效运用的前提。当前，互联网安全问题日益突出，成为各国普遍关切的问题，中国也面临着严重的网络安全威胁。有效维护互联网安全是中国互联网管理的重要范畴，是保障国家安全、维护社会公共利益的必然要求”，并分别从“依法维护互联网安全”、“维护互联网信息的安全流动”、“依法打击网络犯罪”、“反对任何形式的网络黑客攻击行为”四方面进行一一阐述。

3. 工业和信息化部成立互联网网络安全应急专家组

2010 年 8 月 18 日，工业和信息化部互联网网络安全应急专家组在北京成立。国家计算机网络应急技术处理协调中心、工业和信息化部电信研究院、中国互联网络信息中心、国家信息技术安全研究中心、中国信息安全测评中心、基础电信运营企业、通信设备制造商和安全厂商共 20 名专家组委员应邀出席了成立仪式。

该专家组根据工业和信息化部 2009 年颁布的《公共互联网网络安全应急预案》相关规定设立，为互联网网络安全应急管理工作提供技术咨询和决策支撑。

4. 工业和信息化部力推“手机实名制”

2010 年 9 月 1 日，“手机实名制（电话用户实名登记工作）”正式实施。专家普遍认为，实施手机实名制不但有利于抑制短信诈骗等犯罪行为，让受侵害用户便于通过法律手段维护自身权益，同时能保障通信安全，让金融、移动支付能够更加顺利的开展，在进入 3G 时代之后，手机实名制已是势在必行。工业和信息化部要求，电话用户实名登记工作将分两个阶段实施。第一阶段，从 9 月 1 日起对新增电话用户进行实名登记；第二阶段，待电话实名制相关法律法规出台后，用 3 年时间做好老用户的补登记工作。目前，世界上已推出手机实名制的国家有韩国、澳大利亚、泰国、英国、日本、新加坡、南非等。

5. 国家标准化管理委员会批准 18 项信息安全技术国家标准

2010 年 9 月 26 日，由全国信息安全标准化技术委员会组织制定的《公钥基础设施安全支撑平台技术框架》、《证书认证系统密码及其相关安全技术规范》、《信息系统安全等级保护实施指南》等 18 项信息安全技术标准，经国家标准化管理委员会批准发布，并将于 2011 年 2 月 1 日起实施。这批标准的发布实施，对于完善我国信息安全标准体系，规范和指导我国信息安全保障体系建设具有重要意义。

6. 公安部部署开展集中打击黑客攻击破坏活动专项行动

为进化网络环境，公安部于 2010 年部署开展了集中打击黑客攻击破坏活动专项行动，对制作销售网络盗窃木马程序案件、组织僵尸网络案件、帮助他人实施拒绝服务攻击案件以及侵入政府网站案件进行了集中打击。在有关部门支持下，截至 11 月底，全国公安网络安全保卫部门共破获黑客攻击破坏违法犯罪案件 180 起，抓获各类违法犯罪嫌疑人 460 余名，打掉 14 个提供黑客攻击程序、教授黑客攻击犯罪方法并涉嫌组织黑客攻击破坏活动的网站，专项行动取得了预期成效。公安部有关负责人称，当前我国打击网络黑客攻击破坏活动形势仍然非常严峻，境内黑客攻击破坏活动仍然处于高发状态，大量的计算机系统未采取有效的安全保护措施，上网用户安全意识薄弱，防范能力较弱。公安机关将继续加大打击力度，并重点整治打击木马病毒程序制售团伙、以黑客教学为幌子开展的非法培训活动，铲除黑客攻击破坏活动的源头。

8.2 2010 年国外网络安全监管动态报告

在世界发达国家中，互联网早已渗透到其国家政治、经济、军事、文化、生活等各个领域，在社会运转中承担重要角色。所以发达国家面临更为严峻的网络安全挑战，其在应对的过程中有很多先进的经验值得我们认真研究和学习。

■ 美国网络安全监管动态

美国作为互联网的发源地和互联网资源的垄断者，历届政府都非常重视对网络安全的监管，通过多种途径和手段，加强对网络安全的监管，特别是奥巴马政府上台以来，高度重视网络安全在美国家安全战略中的作用，将其列为执政的首要任务。2010 年，奥巴马政府继续延续 2009 年的风格，仍然采取军民并重的网络安全举措，如启动“网络司令部”、组织跨国“网络风暴”演习、发布国家安全战略报告、推出“完美公民”计划等。此外，通过网络安全相关法案也是 2010 年美国网络安全监管的一个亮点。

- 网络安全相关法案

1. 美国众议院通过《加强网络安全法案》

2010 年 2 月 4 日，美国众议院以 422 票对 5 票通过《加强网络安全法案》，这是奥巴马上任以来，众议院通过的首份主要的网络安全法案。该法案要点包括：（1）壮大高素质的网络安全队伍；（2）增加联邦政府在网络安全领域的研发投入；（3）促进网络安全技术的商品化和市场化；（4）加强网络安全教育，提高全社会对网络安全的认识。该法案通过的背景是：2009 年 5 月 29 日，美国形成了《网络空间政策评估》报告，提出了美国网络安全的近期和中期行动计划。2009 年 9 月 23 日和 11 月 4 日，美国众议院科技委员会科学教育分委会和技术、创新分委会分别通过《2009 年网络安全研发法案》和《2009 年网络安全协调与加强法案》。众议院将《2009 年网络安全研发法案》和《2009 年网络安全协调与加强法案》进行整合，吸收《网络空间政策评估》的有关建议，形成并通过了《加强网络安全法案》。

2. 美国参议院商务、科学和运输委员会通过《网络安全法案》

2010 年 3 月 24 日，美参议院商务、科学和运输委员会全票通过了《网络安全法案》，旨在加强美国互联网网络安全，并帮助美国政府机构和企业应对网络威胁。该法案将进入参议院全院表决程序，其主要要点包括：（1）不允许总统单

方面关闭美国的互联网（这与委员会主席杰伊洛克菲勒及参议员斯诺盖恩 2009 年提交的法案草案有所不同）;（2）要求政府机构和企业在网络安全领域加强信息共享，在“网络安全紧急情况”下加强合作（“网络安全紧急情况”在法案中的定义是“相当于战争行为、恐怖袭击或重大自然灾害的网络事件”）;（3）要求通过市场竞争手段，鼓励培养网络安全人才，开发网络安全产品和服务等。

- 网络安全相关战略报告

3. 发布新版《国家安全战略报告》

2010 年 5 月 27 日，美国白宫发布《国家安全战略报告》，该报告是继 2009 年美国白宫发布的《网络空间政策评估——确保可信的强韧的信息通信基础设施》评估报告之后的又一涉及美国网络安全战略的重要报告。该报告专门用一章阐述了网络空间安全的保障问题，认为网络安全威胁是美国国家安全、公共安全和经济面临的最严重挑战之一，而这些威胁可能是来自单独的黑客犯罪分子、有组织的犯罪集团和恐怖分子，甚至是拥有先进技术的国家。报告还认为信息基础设施是国家战略资产，保护信息基础设施同时也是在保护公民隐私和自由，是国家安全的优先事项。

4. 公布《网络空间可信身份国家战略》草案

2010 年 6 月 25 日，美国白宫公布《网络空间可信身份国家战略》（NSTIC）草案，旨在加强网络身份识别和验证。NSTIC 草案是针对 2009 年 5 月奥巴马总统批准的《网络空间政策评估》制定的，核心内容包括指导原则、前景构想、任务目标和行动保障四部分。NSTIC 草案主要的目标任务包括：（1）开发一个综合的身份认证生态系统框架；（2）建立实施一个与身份认证生态系统结合的、互通共用的身份认证基础设施；（3）增强对身份认证生态系统的信任度和参与度；（4）保证身份认证生态系统长期有效的运行。

- 网络安全相关系统体系部署

5. 推出“完美公民”计划，建立全国联网监控对抗网络犯罪

2010 年 7 月 8 日，美国国家安全局宣布推出“完美公民”计划，拟建立一个全面覆盖各类电脑网络的监控体系，以便及时应对网络安全威胁。“完美公民”计划是美国国家安全局保护国家网络安全的技术方案之一，旨在预防潜在的网络威胁入侵政府机构、公共和私营部门。

6. 改造互联网接入系统，防止敏感信息被盗取

随着“维基泄密”风波愈演愈烈,美国政府意识到可能还会有更多类似的“大规模泄密事件”发生。美国国土安全部表示将改造互联网接入系统，并表示此次改造不仅涉及军方网站，未来美联邦政府雇员的所有网络活动(如浏览网页和收发电子邮件)都将通过特别打造的安全网络进行。早年，为了遏制不断升级的黑客袭扰，美国联邦政府就实施了代号为“爱因斯坦”的网络安全工程。据悉，整个项目将持续数年时间完成。届时,美国联邦政府设在互联网上的 2400 多处“接入点”将处于严密保护之下，从而防止黑客盗取各类敏感信息。美国联邦政府设有约 110 个办事机构，目前，只有 20 个部门的 1000 多个“接入点”收到“爱因斯坦”工程的有效保护，其他部门的网络安全接入还在缓慢进行中。

- 网络安全的相关军事举措

7. 美国防部推进“国家网络靶场”工程，加强网络安全研究

2010 年 1 月，美国防部高级研究计划局（DARPA）拨款 5560 万美元推进建立一个原型的高级计算中心——国家网络靶场（NCR），这是 DARPA 为实现布什政府提出的“国家网络综合倡议”（CNCI）的一个重要举措。NCR 将提供一个由先进计算机和数据网络组成的“测试平台”，以实现下列功能：（1）评估信息保障技术和工具；（2）复制各类大型复杂的计算机网络，以支持美国防部的网络战武器和操作；（3）同一时段进行数个大型网络安全试验；（4）模拟真实的美国全球信息网格试验；（5）开发和部署网络测试能力。

8. 启动“网络司令部”

2010 年 5 月 21 日，美国国防部宣布酝酿筹备一年之久的“网络司令部”正式启动。该“网络司令部”隶属于美国战略司令部，位于马里兰州的米德军事基地，编制近千人，主要职责是进行网络防御和网络渗透作战，下辖四个单位：陆军网络指挥部、空军第 24 航空队、海军第 10 舰队和海军陆战队网络空间指挥部。现任国防部国家安全局局长基思·亚历山大担任网络司令部司令，亚历山大是情报军官出身，曾在美军各级情报部门任职，堪称情报界的“元老人物”。目前，美国军方在全球 88 个国家和地区的 4000 多个军事基地内拥有超过 1.5 万个电脑网络和大约 700 万台计算机，一直以来美军各部门都在网络领域孤军作战，而按照计划网络司令部于 10 月全面运作。网络司令部除了要防御和反制敌对国家和黑客的网络攻击外，还具备以下功能：（1）总体控制和协调各情报部门所获取的网络资料；（2）系统分析网络情报资料；（3）将遴选出的最新科技投入生产；（4）影响和限制各国的舆论和政策形成；（5）入侵其他国家的军队网络系统等。

9. 美国防部拟从零构建超级安全网络

2010 年 6 月，美国国防部高级研究计划局（DARPA）宣布推出 CRASH 计划，为专家提供资金从零开始建造超级安全的网络计算机系统。CRASH 计划全称为 Clean-Slate Design of Resilient, Adaptive, Secure Hosts，即重新设计一种自适应、可迅速恢复的安全型计算机系统，主要设想是借助人类生物学技术研发出一套具有高适应性、超智能化的高度安全性网络。例如，CRASH 计划寻求将人类免疫系统的机制移植到计算机环境中。在人类免疫系统中，存在多个独立的机制，它们对病原体进行持续不断的监控，即使在细胞这一等级上，也存在多个备用机制，可对 DNA 的结构进行监控和修复。CRASH 计划将对硬件、系统软件、编程语言和设计环境进行紧密地整合。DARPA 指出，在设计 CRASH 时将对以下六个关键的技术领域进行评估：（1）处理器架构；（2）操作系统；（3）机器学习、自我适应、诊断和恢复；（4）编程语言和环境；（5）形式方法；（6）动态多样性。

10. 联合 12 国举行“网络风暴 III”演习

2010 年 9 月 28 日至 30 日，美国国土安全部召集来自国土安全部、国防部、商务部、能源部、司法部、财政部、交通部等主要联邦机构和商业公司的数千名电脑安全专家，举行了为期 3 天的代号为“网络风暴 III”的反黑客袭击大演习。澳大利亚、英国、加拿大、法国、德国、匈牙利、日本、意大利、荷兰、新西兰、瑞典及瑞士 12 个国家的技术人员也应邀加盟了本次演习。此次演习模拟美国等西方国家诸如电力、供水等重要信息基础设施遭受大型网络袭击，造成政府和私人系统瘫痪的情景，比起前两次演习只涉及能源、运输、银行、通信等行业，涵盖面更广，多达 1500 起以上的模拟攻击事件的想定也更复杂。

11. 宣布谍报机构正式插手民用网络安全

2010 年 10 月 13 日，美国国防部部长罗伯特·盖茨与国土安全部部长纳波利塔诺发表联合声明，宣布两大机构已签署一份备忘录，即日起在保护美国民用网络安全展开合作。合作备忘录指出，准许国家安全局及新成立的网络司令部各派出一队人马(4 至 6 名专家)进驻国土安全部，直接介入该部相关机构的日常运作，协助国土安全部保护民用网络安全及处理网络攻击事故。国土安全部即日起也将派出一队人马进驻国家安全局，该团队由国土安全部负责网络安全的副部长助理领衔，成员包括隐私权、公民权专家及法务人员等。

■ 欧洲地区网络安全监管动态

1. 瑞典多管齐下监管网络

2010 年 1 月，瑞典社会保护和应急署向政府建议在该机构下设立国家信息

技术安全中心，专门负责预防网络攻击，处理所有信息技术案件，旨在应对近年来黑客攻击数量不断增加、利用信息技术盗取、篡改网上信息的案件时有发生的趋势。在互联网迅速普及过程中，瑞典十分重视对网络的监管，设立专门部门负责互联网监管，并不断适应新情况，推动修订立法。在瑞典，社会保护和应急署与国家警察署是网络安全事务的主管部门，前者负责社会信息安全，后者负责网络犯罪案件。瑞典司法部今年年初已向议会递交提案，建议对通过网络色情牟利、传播网络色情、网上付费观看青少年和儿童色情图片及视频等行为进行制裁；法庭严惩涉及青少年儿童的网络色情罪犯，在以往量刑基础上加大刑罚。瑞典也非常重视通过社会监督维护互联网环境健康，呼吁家长、学校和其他社会资源共同行使监督职责，打击网络色情。瑞典学校校园网采取了技术手段，对不良信息进行甄别和过滤。瑞典政府还设立社会热线，接受民众对不良网站和信息的举报。此外，对于电信行业，瑞典政府要求企业严格自律。

2. 欧盟正式发布《欧洲数字化议程》

2010 年 5 月 19 日，欧盟正式发布了《欧洲数字化议程》五年计划，该议程的总体目标是通过在欧盟建立基于高速和超高速互联网及互操作应用的数字单一市场，实现欧洲可持续的经济效益与社会效益。在该议程中，欧盟提出了“在欧盟建立单一的充满活力的数字化市场”、“改进信息通信技术标准的制定，提高可操作性”、“增强网络安全”、“实现高速和超高速互联网连接 ”、“促进信息通信技术前沿领域的研究和创新”、“提高数字素养、数字技能和数字包容”、“利用信息通信技术产生社会效益”等七个重点发展领域及相关措施。其中在“增强网络安全”一节中指出“互联网的便利使得更容易获得私人信息，而且不良信息的传递、网络攻击等都让公民不能完全的信任网络。随着网络间传递的数据不断丰富，新技术不停涌现，如何保护个人数据和隐私也成为了亟待解决的问题。欧盟提出要对网络袭击者进行惩治和加强个人信息的保护，并且要求网络经营商向用户及时通报网络安全方面的信息。”

3. 英国公布国家安全战略报告

2010 年 10 月 18 日，英国政府公布 2010 年英国国家安全战略报告《不稳定时代的强大英国》。该报告将英国的防务重点分为三级，其中第一级就是要应对来自恐怖主义、网络攻击、国家间军事危机、重大事故和自然灾害四大威胁。报告指出，网络犯罪将是英国未来面临的主要威胁之一。据透露，英国将会投资 5 亿英镑（约合 53 亿元人民币）来加强网络安全，其中包括防范恐怖分子对敏感网络系统的攻击以及网上情报的盗取，同时也包括防止电子商务活动的造假和诈骗行为。10 月 19 日，英国政府还公布了《国家战略防务与安全评估报告》，首

次对英国武装部队未来 10 年的定位和能力进行重新评估。该报告反映了英国政府对于本国未来国际战略地位的考虑，特别是如何应对针对英国的安全威胁。

4. 欧洲举行首次网络战演习

2010 年 11 月 4 日 ,由欧洲网络与信息安全署和欧盟联合研究中心承办的“欧洲 2010 网络”演练拉开帷幕，来自欧盟 22 个成员国以及冰岛、挪威、瑞士 3 个非欧盟成员国共 130 名网络专家分 3 组进行了模拟网络战演练 ,这是欧盟首次举行全欧范围内的网络战演习。此次演练是欧盟落实今年 5 月制定的《欧洲数字化议程》而采取的重要措施，旨在提高各国应对网络黑客攻击的能力，并在欧洲各国互联网通信受到严重限制、公民、企业和公共部门的公共互联网上网服务受阻的情况下，避免网络彻底瘫痪。

5. 法国出台《计算机管理风险控制手册》，指导计算机信息安全管理

2010 年 12 月 3 日，法国国家信息系统安全署推出《计算机管理风险控制手册》纸质版和电子版，用以指导政府机构和企业在计算机代理服务方面加强信息安全管理。新《计算机管理风险控制手册》针对代理服务风险等问题设计了安全保证计划蓝本，并罗列一系列有代表性的合同条款，供用户参考。

■ 亚洲、澳洲地区网络安全监管动态

1. 韩国政府将提供免费软件解决网瘾问题

2010 年 3 月 16 日，韩国总理办公室称，韩国将从 2011 年开始向游戏玩家和其他有互联网瘾的人提供免费的软件以限制他们的上网时间。这些免费提供的软件是韩国行政安全部应对互联网瘾计划的一部分。其中，一种软件是双方一致同意关闭程序，适用于监护人和用户设置的使用时间；另一种软件叫做“互联网疲劳”， 将随着时间的流逝使游戏更难玩，从而让游戏玩家感到厌烦。

2. 日本加大监管力度，构筑安全网络社会

2010 年 5 月 11 日，日本政府正式批准制定“保护国民信息安全战略”。该战略将制定 2010 年至 2013 年具体的实施项目 ,重点实施当铁路部门、金融机构的电脑系统等重要基础设施遭受黑客攻击时的早期行动演习，以将损失降到最小。2010 年 7 月，日本总务省公布 2010 年版《信息通信白皮书》,将如何构筑安心、安全的网络社会列为重要内容之一。从《信息通信白皮书》中可以看到，日本已于 2009 年 1 月开始实施安心网络建设项目 ,2009 年 4 月开始实施《青少年网络环境管理法》。

3. 印度建设电脑应用系统和监控系统，以提升国家安全性

2010 年 10 月 11 日，印度政府发言人表示印度计划自主开发一个新的电脑应用系统，以提高电脑应用的安全性。该电脑应用系统由印度国防研究与发展组织研制，主要针对军事系统进行开发，但也可能运用到商业领域中。印度软件安全中心已在班加鲁尔和新德里开始建立，拥有自主知识产权的应用系统将帮助印度抵御黑客袭击。11 月初，印度电信部向印度内阁委员会提交建议书，拟建设一个集中监控和拦截的系统，以通过所有通信平台有效解决国家安全问题。该集中监控系统将整合最新的情报技术和生物识别设备，具备密码分析、语音识别、电网监控、加密和解密、数据挖掘等功能，可通过覆盖国家监测中心许可的每一个区域，实施合法的监听、监测、分析等。根据建议书，该系统的设施部署费用为 54 亿卢比（约 1.22 亿美元），其中 45 亿卢比需要政府拨款，预计 2013 年 6 月 31 日完成设施的部署。

4. 新加坡宣布采取措施加强国家网络安全

2010 年，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人们的网络安全意识，三管齐下加强新加坡的网络安全。新加坡信息通信发展管理局已与各互联网服务供应商合作，制定一套信息通信安全准则，提升信息通信基础设施抵御网络威胁的能力。新加坡信息通信发展管理局将把新准则纳入电信监管架构，规定从业者必须符合基本的网络安全水平，以防范现有和未来的网络威胁。该局也将会定期进行必要的审查工作，以确保互联网服务供应商遵守这套新准则。

5. 澳大利亚成立国家网络安全运行中心并启动 CERT Australia

2010 年 1 月 15 日，澳大利亚国家网络安全运行中心（CSOC）正式宣布落成。成立 CSOC 是澳大利亚 2009 年 5 月份发布的国防白皮书所倡议的，它将为澳政府提供网络安全保障服务，包括：分析网络安全态势、识别和分析恶意网络攻击，以及应对跨政府、重要私营部门系统和基础设施的网络安全事件。同时，澳大利亚国家计算机应急响应官方机构 CERT Australia 启动国家网络安全信息交换机制（National Cyber Security Information Exchange），并与 CSOC 密切合作，支持政府打击网络犯罪和网络恐怖主义威胁。

8.3 2010 年重大活动网络安全保障综述报告

在工业和信息化部的统一部署和指挥下，2010 年 CNCERT 与各基础电信运营商、中国互联网络信息中心等单位一起，以高度的政治责任感和饱满的工作热情圆满完成了多项专项保障工作。在历次专项保障工作中，CNCERT 认真落实工业

和信息化部专项保障工作方案，制定详细工作规范，并安排 7*24 小时现场值守，确保及时发现异常情况、及时通报和处置。

■ 温家宝总理与网民在线交流专项保障

2 月 27 日下午 3 点，温家宝总理接受中国政府网和新华网的联合专访，与网民进行在线交流。CNCERT 于 2 月 24 日至 27 日，从异常流量、域名服务、网页篡改、木马和僵尸网络等各个方面对有关站点开展 24 小时连续监测。结果显示，专项期间未发生针对保障对象的大规模网络安全事件，网络安全态势整体平稳。2 月 26 日，CNCERT 组织基础电信运营商、域名注册管理和服务机构对网上木马和僵尸网络开展了专项治理。在各单位的积极配合下，快速处理境内外活跃控制服务器 94 个（涉及 IP 地址 94 个，域名 37 个）。专项治理后，僵尸网络活跃程度的明显下降，有效保证了专项保障期间良好的网络环境。

■ “两会”网络安全专项保障

3 月 3 日至 14 日，CNCERT 开展了“两会”网络安全专项保障工作，并应全国人大信息中心、国防科工局信息中心要求，为其提供定向技术支撑。专项保障期间网络安全态势整体平稳，未出现大规模攻击的迹象，未发现重要网站被篡改或重要单位主机被木马或僵尸网络控制的情况。此外，得益于“温家宝总理与网民在线交流活动”前进行的木马和僵尸网络专项治理行动，“两会”期间境内外木马受控主机数量和木马控制服务器数量继续呈现下降趋势，这降低了黑客发动大规模攻击的可能性。

“两会”期间，CNCERT 对中国政府网、新华网、人民网、中国网、全国人大网、央视网等多家重点网站进行 7×24 小时监测。CNCERT 监测发现，3 月 3 日 7 点 40 分至 8 点 20 分左右，中国政府网、新华网、人民网、中国网同时出现无法访问情况，研判原因为上述网站的内容分发服务合作商蓝汛公司系统出现故障导致；同日， CNVD 发现微软 IE 浏览器存在一个新型未公开的高危漏洞，CNCERT 于 4 日专门对此向通信行业及相关重要信息系统部门发布了紧急通报，提醒有关部门采取安全防范措施。

■ 上海世博会网络安全专项保障

4 月 16 日至 11 月 15 日，CNCERT 开展了上海世博会网络安全专项保障工作。随着 10 月 31 日 24 点 2010 年中国上海世博会会旗的缓缓降落，历时 184 天的世

博会圆满落幕。成功的世博会背后是成功的保障工作，在千头万绪的世博保障工作中，网络安全保障工作是世博保障的重要组成部分。面对永不落幕的“网上世博”和世博会数十个网络应用系统，整个世博会运行期间，各系统运行稳定，网络安全形势总体可控。

在世博会召开前夕，CNCERT 国家中心组织上海及周边多个省分中心开展了制定应急预案、举办应急演练、对重要信息系统信息进行安全检查等全面的准备工作；在整个世博会保障期间，CNCERT 每日对公共互联网、世博会联网信息系统、国家重要信息系统等进行网络安全监测，并承担电信行业内部的世博保障监测信息汇总和通报工作，共报送日报 188 期，周报 29 期和重要事件和预警信息 8 期，分别为突尼斯上海世博会官方网站主页被黑客两次篡改、世博邮件系统漏洞、世博学习城系统漏洞、世博会城市志愿者服务站点志愿者管理系统漏洞、世博官网漏洞、新疆 2010 上海世博会官方网站被入侵写入恶意脚本后门程序、世博会英国馆网站 SQL 注入漏洞等。

为了营造世博会期间良好的公共互联网安全环境，CNCERT 还分别于 4 月 29 日（世博会开幕式前）、9 月 30 日（国家馆日前）、10 月 29 日（世博会闭幕式前）协调国内基础电信运营企业、域名注册管理和服务机构进行了三次木马和僵尸网络控制端及恶意域名的专项治理，共成功处置境内外 519 个控制端主机 IP 及相关恶意域名。专项治理行动在短时间内对木马、僵尸网络控制端进行了有效清除，大大降低了发动分布式拒绝服务攻击等大规模网络攻击的风险。

■ 广州亚（残）运会网络安全专项保障

10 月 20 日至 12 月 21 日，CNCERT 开展了广州亚（残）运会网络安全保障工作。整个亚（残）运会召开期间，所有亚（残）运会联网信息系统运行稳定，未发生影响用户使用的重大网络安全事件。在亚运会召开前夕，CNCERT 国家中心按照世博会保障的成功经验，又组织广东及周边多个省分中心开展了制定应急预案、举办应急演练、进行安全检查等全面的准备工作，努力将各种安全隐患消灭在前期；在整个亚（残）运会保障期间，CNCERT 每日对公共互联网、亚运会联网信息系统、国家重要信息系统等进行 7*24 小时不间断监测，并派人员在开闭幕式海心沙现场、亚组委信息技术部、亚运场比赛馆驻守候命，有效保障了亚（残）运会系统在互联网上的正常运行。

CNCERT 作为通信行业内网络安全信息通报中心汇总中国电信、中国联通、中国移动、CNNIC 及其他单位报送的信息和自身监测信息，报送日报 34 期，周报 6 期。亚运会开幕式前一天，CNCERT 监测发现亚组委某台主机感染蠕虫病毒

和某亚运相关对外网站感染木马和蠕虫病毒的事件后,立即紧急通知并协助亚组委信息技术部开展相关应急处置工作,对亚组委办公网内机器进行了一系列病毒排查和清除工作。此外,针对亚运会前出现多起借助电子邮件、微博短域名和广州亚运会相似跳转域名等手段对互联网用户进行欺诈的网络仿冒事件, CNCERT 通过网站公告、行业内通报、定向通报等多种方式向有关部门和广大网民发布了安全预警,避免了更多的互联网用户上当受骗。

在亚运会开闭幕式、亚残会开幕式三个敏感时间节点,CNCERT 组织基础电信运营企业、域名注册机构和各省分中心开展了木马、僵尸网络专项治理,对危害较大、活跃度高的木马和僵尸网络控制端进行集中清除。在各基础电信运营企业及域名企业积极配合下,共成功处置境内外 1207 个规模较大的木马和僵尸网络控制端,以及 407 个参与挂马或主机控制的恶意域名,大大降低了不法分子对亚运会在线系统发动大规模拒绝服务攻击的可能性。

8.4“超级工厂”(Stuxnet) 蠕虫分析报告

相较于传统的计算机蠕虫主要破坏计算机网络信息系统,通过迅速的、大规模的扩散来感染更多的计算机不同,2010 年 7 月世界上出现了第一个有针对性的感染现实世界中工业控制系统的计算机蠕虫——Stuxnet,在国内被命名为“超级工厂”、“震网”、“双子”等。这个针对西门子公司的数据采集与监控系统 SIMATIC WinCC 进行攻击的超级蠕虫,由于攻击了伊朗布什尔核电站的工业控制设施并最终导致该核电站推迟发电,而引起了全球媒体的广泛关注,被称为“超级网络武器”、“潘多拉的魔盒”。各界专家纷纷表示,该蠕虫标志着计算机恶意代码已经可以攻击现实世界中的基础设施,这将带来网络战争的军备竞赛。

WinCC 被伊朗广泛使用于基础国防设施中。9 月 27 日,伊朗国家通讯社向外界证实该国的第一座核电站“布什尔核电站”已经遭到攻击。该核电站原计划于今年 8 月开始正式运行,这与 Stuxnet 出现的时间非常接近。据赛门铁克公司的统计,全球有约 45000 个网络被该蠕虫感染,其中 60%的受害主机位于伊朗境内。因此,此次攻击具有明确的地域性和目的性。

CNCERT 监测到 Stuxnet 蠕虫在我国并没有出现大规模爆发的趋势,截止到 2010 年底,我国境内仅有 578 个 IP 被感染,其感染的主机数量比普通蠕虫要少很多。一方面是因为该蠕虫被设计用来进行精确攻击,而不是大范围扩散,我国大部分用户上网的计算机与工业控制系统无关,没有触发该蠕虫传播的条件;另一方面由于该病毒造成的危害已经引起了全球网络安全领域的高度关注,各大杀

毒软件在第一时间将其列入黑名单，普通网民的计算机得到了一定程度的保护。

尽管 Stuxnet 蠕虫并未对我国造成严重影响，但在传统工业与信息技术的融合不断加深、传统工业体系的安全核心从物理安全向信息安全转移的趋势和背景下，此次 Stuxnet 蠕虫的爆发标志着全球网络信息安全进入一个新的时代。我们有必要对其进行深入分析和研究相应对策。

■ Stuxnet 蠕虫攻击原理

西门子公司的 SIMATIC WinCC 系统主要用于工业控制系统的数据采集与监控，一般部署在专用的内部局域网中，并与外部互联网实行物理上的隔离。为了实现攻击，Stuxnet 蠕虫利用了微软 Windows 操作系统中 4 个漏洞（其中 3 个为 0Day 漏洞）和西门子数据采集与监控系统 SIMATIC WinCC 的 2 个漏洞，并采取多种手段进行渗透和传播。该蠕虫首先感染外部主机；然后感染 U 盘，利用快捷方式文件解析漏洞，传播到内部网络；在内网中，通过快捷方式解析漏洞、RPC 远程执行漏洞、打印机后台程序服务漏洞，实现联网主机之间的传播；最后抵达安装了 WinCC 软件的主机，展开攻击。

Stuxnet 蠕虫感染以后会尝试连接 www.windowsupdate.com 和 www.msn.com 两个域名来判断自己是否在内部网络中，然后决定是否通过 U 盘传播，通过对配置数据的修改，它的行为可以被精准控制。当 Stuxnet 蠕虫发现互联网连接可用，就会向 www.mypremierfutbol.com 和 www.todaysfutbol.com 两个域名发送主机信息，包括 IP 地址、操作系统信息和软件版本等，并通过这两个域名实现自身的更新。因此，攻击者能细粒度的选择攻击范围、攻击对象和攻击方法。

感染到西门子公司的 SIMATIC WinCC 工业控制系统后，Stuxnet 通过劫持 DLL 攻击 PLC（可编程逻辑控制器）。它注入的 PLC 代码只有在特定的设备中才能造成攻击，这表明它的针对性极强。因为该蠕虫具有更新能力，所以完全可以被攻击者用来发起针对其它目标的攻击。

Stuxnet 主要通过 MS10-046 快捷方式文件解析漏洞、MS08-067RPC 远程执行漏洞、MS10-061 打印机后台程序服务漏洞漏洞、共享服务和远程访问 WinCC 系统数据库，实现在局域网中的传播与更新。利用的漏洞具体如下：

1.快捷方式文件解析漏洞（MS10-046）

这个漏洞利用 Windows 在解析快捷方式文件（例如.lnk 文件）时的系统机制缺陷，使系统加载攻击者指定的 DLL 文件，从而触发攻击行为。具体而言，Windows 在显示快捷方式文件时，会根据文件中的信息寻找它所需的图标资源，并将其作为文件的图标展现给用户。如果图标资源在一个 DLL 文件中，系统就会加载这个

DLL 文件。攻击者可以构造这样一个快捷方式文件，使系统加载指定的 DLL 文件，从而执行其中的恶意代码。快捷方式文件的显示是系统自动执行，无需用户交互，因此漏洞的利用效果很好。

Stuxnet 蠕虫会将精心构造的快捷方式文件和 DLL 文件复制到所有可移动存储设备中，用户一旦将该设备插到存在漏洞的内部网络计算机上，就会触发漏洞，实现从外部网络向物理隔离的内部网络渗透。这就是所谓的“摆渡”攻击。

2.RPC 远程执行漏洞（MS08-067）与提升权限漏洞

Windows 的 Server 服务在处理特制 RPC 请求时存在缓冲区溢出漏洞，远程攻击者可以通过发送恶意的 RPC 请求触发这个漏洞，导致完全入侵用户系统，以 SYSTEM 权限执行任意指令。对于 Windows 2000、XP 和 Server 2003，无需认证便可以利用这个漏洞；对于 Windows Vista 和 Server 2008，可能需要进行认证。这是 2008 年爆发的最严重的一个微软操作系统漏洞，具有利用简单、波及范围广、危害程度高等特点，目前已经有多个病毒利用该漏洞进行传播。

利用这一漏洞，攻击者可以通过恶意构造的网络包直接发起攻击，无需通过认证地运行任意代码，并且获取完整的权限。因此该漏洞常被蠕虫用于大规模的传播和攻击。

Stuxnet 蠕虫利用这个漏洞实现在内部局域网中的传播。利用这一漏洞时，如果权限不够导致失败，还会使用一个尚未公开的漏洞来提升自身权限，然后再次尝试攻击。

3.打印机后台程序服务漏洞（MS10-061）

这是一个零日漏洞，首先发现被利用于 Stuxnet 蠕虫中。

Windows 打印后台程序没有合理地设置用户权限，攻击者可以通过提交精心构造的打印请求，将文件发送到暴露了打印后台程序接口的主机的%System32%目录中。成功利用这个漏洞可以以系统权限执行任意代码，从而实现传播和攻击。

Stuxnet 蠕虫利用这个漏洞实现在内部局域网中的传播，它向目标主机发送两个文件：winsta.exe、sysnullevnt.mof。后者是微软的一种托管对象格式（MOF）文件，在一些特定事件驱动下，它将驱使 winsta.exe 病毒文件被执行。

■ Stuxnet 蠕虫攻击特点和防范建议

Stuxnet 蠕虫呈现出许多新的手段和特点，值得我们特别关注。

1. 专门攻击工业系统

Stuxnet 蠕虫的攻击目标直指西门子公司的 SIMATIC WinCC 系统。这是一款数据采集与监视控制（SCADA）系统，被广泛用于钢铁、汽车、电力、运输、水

利、化工、石油等核心工业领域，特别是国家基础设施工程。它运行于 Windows 平台，常被部署在与外界隔离的专用局域网中。

一般情况下，蠕虫的攻击价值在于其传播范围的广阔性、攻击目标的普遍性。此次攻击与此截然相反，最终目标既不在开放主机之上，也不是通用软件。这表明攻击者有明确的攻击意图，是一次精心谋划的攻击。此外，无论是要渗透到内部网络，还是挖掘大型专用软件的漏洞，都非普通攻击者所能做到，很有可能是一种“国家”行为。

2. 利用多个零日漏洞

Stuxnet 蠕虫利用了微软操作系统的下列漏洞：

- RPC 远程执行漏洞（MS08-067）
- 快捷方式文件解析漏洞（MS10-046）
- 打印机后台程序服务漏洞（MS10-061）
- 尚未公开的一个提升权限漏洞

后三个漏洞都是在 Stuxnet 中首次被使用，是真正的零日漏洞。如此大规模的使用多种零日漏洞，并不多见。

这些漏洞并非随意挑选，从蠕虫的传播方式来看，每一种漏洞都发挥了独特的作用。比如在基于自动播放功的 U 盘病毒被绝大部分杀毒软件防御的现状下，就使用快捷方式漏洞实现 U 盘传播。

另一方面，在捕获的样本中，有一部分样本的时间戳是 2010 年 3 月。这意味着至少在 3 月份，上述零日漏洞就已经被攻击者掌握，但直到 7 月份大规模爆发，漏洞才首次披露出来，这期间要控制漏洞不泄露，有一定难度。

3. 使用数字签名

Stuxnet 在运行后，释放两个驱动文件：

%System32%\drivers\mrxcls.sys

%System32%\drivers\mrxnet.sys

这两个驱动文件伪装 RealTek 的数字签名以躲避杀毒软件的查杀。目前，这一签名的数字证书已经被颁发机构吊销，无法再通过在线验证，但目前反病毒产品大多使用静态方法判定可执行文件是否带有数字签名，因此有可能被欺骗。

4. 明确的攻击目标

根据赛门铁克公司的统计，7 月份，伊朗感染 Stuxnet 蠕虫的主机只占 25%，到 9 月下旬，这一比例达到 60%。

Stuxnet 蠕虫攻击事件凸显了两个问题，一是即便是物理隔离的专用局域网，也并非牢不可破；二是专用的软件系统，包括工业控制系统，也有可能被攻击。

因此，我们提出下列安全建议：

1. 加强主机（尤其是内网主机）的安全防范，即便是物理隔离的计算机也要及时更新操作系统补丁，建立完善的安全策略；
2. 安装安全防护软件，包括反病毒软件和防火墙，并及时更新病毒数据库；
3. 建立软件安全意识，对企业中的核心计算机，随时跟踪所用软件的安全问题，及时更新存在漏洞的软件；
4. 进一步加强企业内网安全建设，尤其重视网络服务的安全性，关闭主机中不必要的网络服务端口；
5. 所有系统、软件和网络服务均不允许使用弱口令和默认口令；
6. 加强对可移动存储设备（如：U 盘、移动硬盘）的安全管理，严格限制其在敏感计算机或敏感信息系统中的使用；如确需使用则应加强安全防护措施，如：关闭计算机的自动播放功能、使用可移动设备前先进行病毒扫描、为移动设备建立病毒免疫、使用硬件式 U 盘病毒查杀工具等，同时在敏感计算机或信息系统中应采用光盘代替 U 盘进行文件复制。