8 网络安全专题分析

8.1 2011 年国内网络安全监管动态

一、国内网络安全相关立法动态

(一) "两高"联合发布了《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》

中国最高人民法院、最高人民检察院 2011 年 8 月 29 日联合发布了《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(以下简称《解释》)。该《解释》自 2011 年 9 月 1 日起施行，共有十一条，主要规定了以下几个方面的内容：一是明确了非法获取计算机信息系统数据、非法控制计算机信息系统罪，提供侵入、非法控制计算机信息系统程序、工具罪，破坏计算机信息系统罪等犯罪的定罪量刑标准；二是规定了对明知是非法获取计算机信息系统数据犯罪所获取的数据、非法控制计算机信息系统犯罪所获取的计算机信息系统控制权，而予以转移、收购、代为销售或者以其他方法掩饰、隐瞒的行为，以掩饰、隐瞒犯罪所得罪追究刑事责任；三是明确了对以单位名义或者单位形式实施危害计算机信息系统安全犯罪的行为，应当追究直接负责的主管人员和其他直接责任人员的刑事责任；四是规定了危害计算机信息系统安全共同犯罪的具体情形和处理原则；五是明确了“国家事务、国防建设、尖端科学技术领域的计算机信息系统”、“专门用于侵入、非法控制计算机信息系统的程序、工具”、“计算机病毒等破坏性程序”的具体范围、认定程序等问题；六是界定了“计算机信息系统”、“计算机系统”、“身份认证信息”、“经济损失”等相关术语的内涵和外延。

(二) 工业和信息化部出台《规范互联网信息服务市场秩序若干规定》

为规范互联网信息服务市场秩序，保护互联网信息服务提供者和用户的合法权益，促进互联网行业的健康发展，工业和信息化部于 2011 年 12 月 29 日公布了《规范互联网信息服务市场秩序若干规定》(简称《若干规定》)，该规定自 2012 年 3 月 15 日起施行。《若干规定》主要对互联网信息服务活动中的下述事项进行

了规范：一是明确了禁止实施的侵犯其他互联网信息服务提供者权益的行为。二是规范了互联网“评测”活动。三是明确了禁止实施的侵犯用户合法权益的行为。四是规范了在用户终端上安装、运行或者捆绑软件的行为。五是规范了广告窗口弹出行为。六是强化了对用户个人信息的保护。另外，为了保证电信管理机构及时发现和处理互联网信息服务中的违法事件，保护互联网信息服务提供者和用户的合法权益，《若干规定》还对违反相关规定的行为设定了相应的法律责任。

(三) 深圳人大表决通过网络信息安全保护条例议案

深圳市五届人大常委会第七次会议表决通过了《深圳市人大常委会 2011 年度立法计划》，将《网络信息安全保护条例》增加作为立法调研项目。据了解，制定《网络信息安全保护条例》是 2011 年 1 月召开的市五届人大二次会议的 1 号议案，该议案称，2010 年以来，我国互联网企业之间的竞争异常激烈，罔顾法律、甚至背弃商业道德恶意攻击竞争对手的事件不断发生，现有法律制度无法跟上社会的发展，新型的侵权行为没有在法律中明确规定，相关制度的缺失致使政府监管缺位，规范竞争秩序的法律制度难以适应市场快速发展的需要，亟待进行完善。因此，为了防止互联网企业之间再度发生类似的恶性竞争，该议案建议制定《网络信息安全保护条例》，为网络信息安全护航。议案同时还附上了近 3000 字的《网络信息安全保护条例（草案）》。

(四) 两会关注信息安全，提案直指净化网络环境

2011 年两会期间，代表委员们直接关注网络信息安全，在各代表递交的相关提案中，虽然具体表述略有区别，但是所指的方向趋于一致，即将信息安全纳入到社会管理体系，提升信息化管理水平，净化网络信息环境。他们指出当明显的侵权行为（指网络热帖“贾君鹏”事件）变为广泛参与的娱乐，网络暴力随时可以让任何一个人变成下一个受害者；对那些为获取点击率、提高关注度而不履行管理职责的人，应当追责；网络社会其实跟现实社会一样，需要约束和规范。一旦进入网络世界，就像新生儿出生在社会一样，必须拥有一张出生证，上面有你的名字和信息，从此你必须负起应有的法律责任。同时应加快制定一部关于我国互联网络的基本法等。

二、国内网络安全相关行政管理动态

(一) 国务院办公厅下发《关于进一步加强政府网站管理工作的通知》

4 月 21 日，国务院办公厅下发《关于进一步加强政府网站管理工作的通知》，要求各省、自治区、直辖市人民政府，国务院各部委、各直属机构充分发挥政府网站的信息公开、互动交流作用，切实加强和规范政府网站管理。该通知在网络安全方面，要求全面检查“网站安全防范工作是否到位，是否采取了防攻击、防篡改、防病毒等安全防护措施并制定了应急处置预案”，并指出“对于缺乏技术保障力量的政府网站，上级政府、部门和主管单位要主动协调有关方面提供技术支持，帮助其做好网站的安全防范工作”。

(二) 国务院会议强调加强网络安全保障

国务院总理温家宝 11 月 23 日主持召开国务院常务会议，研究部署加快发展我国下一代互联网产业。会议明确了今后一个时期我国发展下一代互联网的路线图和主要目标。2013 年年底前，开展国际互联网协议第 6 版网络小规模商用试点，形成成熟的商业模式和技术演进路线；2014 年至 2015 年，开展大规模部署和商用，实现国际互联网协议第 4 版与第 6 版主流业务互通。在此过程中，形成一批具有较强国际影响力的下一代互联网研究机构和骨干企业，全面增强互联网产业对消费、投资、出口和就业的拉动作用，增强对信息产业、高技术服务业、经济社会发展的辐射带动作用。同时，会议确定了一些重点任务，包括加强资源共建共享，建设宽带、融合、安全、泛在的下一代国家信息基础设施，推动网站系统升级改造。加强网络与信息安全保障，强化网络地址及域名系统的规划和管理，全面提升下一代互联网安全性和可信性。

(三) 工业和信息化部发布《信息安全技术个人信息保护指南（征求意见稿）》

为提高个人信息保护意识，保护个人合法权益，促进个人信息的合理利用，指导和规范利用信息系统处理个人信息的活动。2011 年 2 月 10 日，工业和信息化部发布《信息安全技术个人信息保护指南（征求意见稿）》，并向社会公开征求意见。该“指南”包括前言、引言、范围、术语和定义、个人信息处理原则、个人信息主体的权利、个人信息保护要求等方面，并对包括收集、加工、转移、使用、屏蔽、删除等处置信息的行为进行了定义。

(四) 工业和信息化部印发《关于加强工业控制系统信息安全管理的通知》

针对工业控制系统安全事件愈发频繁的情况，工信部在 2011 年 9 月专门印发了《关于加强工业控制系统信息安全管理的通知》（以下简称《通知》），对重点领域工业控制系统信息安全管理提出了明确要求。《通知》明确，重点加强核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环

境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关领域的工业控制系统信息安全管理，在连接管理、组网管理、配置管理、设备选择与升级管理、数据管理和应急管理六个方面落实安全管理要求。同时，《通知》提出，不仅要建立工业控制系统安全测评检查和漏洞发布制度，还要进一步加强工业控制系统信息安全工作的组织领导。

(五) 工业和信息化部印发《移动互联网恶意程序监测与处置机制》

11 月 18 日，工业和信息化部印发《移动互联网恶意程序监测与处置机制》（以下简称《机制》），这是工业和信息化部首次出台移动互联网网络安全管理方面的规范性文件，引起了业界的广泛关注。《机制》界定“ 移动互联网恶意程序 ”是指运行于包括智能手机在内的具有移动通信功能的移动终端之上，存在窃听用户通话、窃取用户信息、破坏用户数据、擅自使用付费业务、发送垃圾信息、推送广告或欺诈信息、影响移动终端运行、危害互联网网络安全等恶意行为的计算机程序，其内涵比通常意义的手机病毒更广。《机制》规定，依据《移动互联网恶意程序描述格式》行业标准开展移动互联网恶意程序的认定和命名工作，由各单位对恶意程序样本进行初步分析，并将信息汇总到 CNCERT，由 CNCERT 统一认定和命名。移动通信运营企业负责本企业网内恶意程序的样本捕获、监测处置和事件通报，CNCERT 负责恶意程序跨网监测、汇总通报和验证企业处置结果。

(六) 工业和信息化部组织开展“2011 年度互联网网络安全应急演练”

为切实提高互联网网络安全保障能力，营造建党 90 周年庆祝活动的良好网络环境，6 月 17 日，工业和信息化部组织中国电信、中国移动、中国联通三家基础电信运营企业和 CNCERT、CNNIC，开展了“2011 年度互联网网络安全应急演练”。演练以重点网站网络安全保障为场景，模拟重点网站遭受大规模流量攻击、域名劫持、网页篡改以及权威域名解析服务器瘫痪等网络攻击和系统故障时，通信行业各单位按照《公共互联网网络安全应急预案》要求和工业和信息化部（指挥部）命令，迅速采取应急处置措施，及时有效消除网络安全事件带来的影响，确保重点网站正常运行。通过演练，有效检验了通信行业各单位的网络安全应急工作水平，提高了网络安全保障能力，达到了预期效果。

(七) 中国反网络病毒联盟制定我国首个手机病毒技术规范

目前国内外安全厂商、网络安全组织对手机病毒的定义、命名、描述存在较大差异，会混淆互联网用户对手机病毒种类、影响范围和危害情况的认知，不利于提高手机用户的安全意识。对此，中国互联网协会反网络病毒联盟（ANVA）于 5 月 24 日发布了我国首个关于手机病毒命名及描述的技术规范——《移动互

联网恶意程序描述规范》, 同时在中国反网络病毒联盟内有 20 余家基础电信运营企业、研究机构、安全企业和互联网企业表示将遵循并启用该规范。该规范主要约定了移动互联网恶意程序定义、属性定义及分类、命名规范等内容。按照危害等级和特定属性，将移动互联网恶意程序依次分为恶意扣费、隐私窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈、流氓行为等八大类。目前，基于该规范文本已经形成了通信行业标准《移动互联网恶意程序描述规范（报批稿)》，有望成为我国首个手机病毒相关的行业标准。

8.2 2011 年国外网络安全监管动态

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。

一、美洲地区网络安全监管动态

（一） 美国网络安全监管动态

1. 美国网络安全相关战略计划

- 美国白宫发布《网络空间国际战略》

美国白宫当地时间 5 月 16 日发布了新的互联网安全规定《网络空间国际战略》，就日后美国如何应对互联网安全等事务提出具体方案。新规表示，美国将与全球其它国家加强合作，追求网络安全与自由，美国各个执行部门还将就此展开密切合作。文件最“ 强硬 ”的一条规定是，白宫明确表示，如果未来遭到威胁美国国土安全的网络攻击，美国可以动用军事实力反击。

- 美国提出网络身份证国家战略

在美国总统奥巴马的推动下，作为国家网络安全战略重要组成部分，美国商务部启动网络身份证战略。奥巴马提出的网络身份证国家战略，也称“ 网络空间可信身份标识国家战略 ”（NSTIC)。美国这一国家战略将确定以下四项主要具体目标：建立一个综合的身份标识生态系统框架；建立可互操作的身份标识基础设施；增强用户信心和参与身份标识生态系统的意愿；确保身份标识生态系统的长远成功。

- 美国白宫公布网络安全研究与发展项目战略计划

2011 年 12 月 7 日消息，美国白宫公布了一份路线图，名为《可信赖的网络空间：联邦网络安全研究与发展项目战略计划》（以下简称《战略计划》），该计划确定了网络安全研究与发展的重点，以确保美国网络基础设施的安全，促进美国处理网络安全问题方式的改变。该《战略计划》在经过公共与私营部门网络的安全专家历时七年的审查及论证后确定了四个战略重点：首先，运用所谓的“改变比赛规则（game-changing）”的思维来理解目前网络安全缺陷的根源，并找到解决这些问题的新方法。这方面的研究包括建立更多的“移动靶子”，使黑客难以渗透到计算机网络。第二，像对待其他科学实践一样，为网络安全构建科学基础，诸如定律、假设检验、重复实验设计、标准化的数据收集方法、指标、常用术语等。第三，确保各研究机构进行合作、协调，综合安排有关改进网络安全的活动，最大限度地发挥研究影响，并确保网络安全研究与研究机构的目标挂钩。最后，缩短网络安全从研究到投入实践的时间。

2. 美国网络安全相关法令政策

- 美国白宫为联邦远程工作人员制定信息安全规则

2011 年 7 月 25 日报道，美国白宫发布了关于联邦雇员远程办公的信息安全指导方针。美国行政管理和预算局（OMB）指示各机构按照《联邦信息安全管理法 （FISMA）的要求，为信息和信息系统提供“与风险相称的”保护。各机构最低限度必须采取以下信息安全措施：控制对机构信息与信息系统的访问；保护机构信息（包括个人身份信息）与信息系统；限制漏洞侵入；保护用于远程办公但不在机构控制之下的信息系统；维护用于远程办公的无线及其他电信设施；防止不适当地使用官方时间或资源。美国行政管理和预算局还指示每个机构的首席信息官与美国国土安全部设立一个技术联络点，以协助远程办公安全要求的实施。

- 美国总统奥巴马签署法令 收紧数据安全政策

受到维基揭密泄露机密文件的影响，美国总统奥巴马于 2011 年 10 月 7 日签署了一项法令，旨在加强美国的数据安全，避免 2010 年令美国政府大为尴尬的文件大规模泄露事件的重演。该法令概括了联邦机构的几项结构性改革，包括成立一个高级筹划指导委员会，负责监督信息保护和信息共享。法令要求，该委员会必须在 90 天内向总统提交一份报告，并在此后每年至少提交一次报告，评估联邦政府在保护政府计算机网络的机密信息方面的成败。该法令还呼吁成立一个

“内部人员威胁处理任务组”，由美国总检察长和美国国家情报委员会主席牵头，负责检测漏洞、防止机密信息从政府和军方各级机构中泄露。

3. 美国网络安全相关军事举措

- 美国发布《网络空间行动战略》以扩大网络空间优势

美国国防部 2011 年 7 月 14 日发布首份《网络空间行动战略》，以加强美军及重要基础设施的网络安全保护。根据美国国防部在其网站公开的部分文件内容，该战略包括五大支柱：第一，将网络空间列为与陆海空及太空并列的“行动领域”，国防部以此为基础进行组织、培训和装备，以应对网络空间存在的复杂挑战和巨大机遇。第二，变被动防御为主动防御，从而更加有效地阻止、击败针对美军网络系统的入侵和其他敌对行为。第三，加强国防部与国土安全部等其他政府部门及私人部门的合作，在保护军事网络安全的同时，加强重要基础设施的网络安全防护。第四，加强与美国的盟友及伙伴在网络空间领域的国际合作。第五，重视高科技人才队伍建设并提升技术创新能力。

- 美国陆军网络司令部打造“2020 年网络陆军”战略计划

2011 年 8 月 25 日消息，虽然美国陆军网络司令部/第二集团军（2nd Army）运转了不足一年，但该机构已经开始打造“2020 年网络陆军”，为未来的行动提出清晰的构想。陆军网络司令部司令瑞特·赫尔南德斯中将表示，陆军网络司令部不仅要协调陆军的情报行动，还要担任陆军的网络支持者角色。除了高层活动外，该司令部还在建设下属网络旅，该旅将在陆军的网络任务中充当作战力量。他表示，到 2020 年，陆军必须拥有整合全方位的网络能力，确保行动的指挥能力，同时实现其在网络领域的行动自由。这意味着陆军的网络行动将会与陆地行动有同等的自由。

- 美国国防部将为国防承包商提供试点网络保护

2011 年 9 月 26 日报道，美国网络安全官员曾警告称，针对美国国防公司的网络攻击日益复杂，包括偷窃重要的国防武器系统和飞机的数据。为此，美国国防部将实行一个试点工程来帮助保护其主要的国防承包商，防范黑客和敌对国家入侵网络和窃取敏感数据。美国国土安全部官员正在评估该项目，希望将相似的保护措施推广至电厂、电网等其他重要基础设施。到目前为止，这项试点项目包括了至少 20 家美国国防承包商，并且被延长至 11 月中旬，同时还在研究如何将其拓展到更多的公司和转包商。事实上，奥巴马政府一直在极力推动对美重要部

门的网络保护工作，与私营部门共享情报，帮助公司更好地保护自己的系统，国防部的这一试点项目代表了这项工作的一个突破。

- 美拟研发网络攻击与防御武器 为网络战争备战

2011 年 11 月 7 日，美国政府官员表示五角大楼研究人员打算加强努力，积极为网络战争发展攻击武器，这反映数字威胁使美国政府日益感到不安。美国国防先进研究计划署 (DARPA)署长杜根说，美国政府必须投资发展攻击和防御性网络工具，以拥有更多更好的选择，确保国家敏感的计算机网络免于受到攻击。

- 美国国防部报告称美国保留使用军事力量打击网络攻击的权利

美国五角大楼 11 月 15 日发布的一份报告称，美国保留使用军事力量打击针对美国的网络攻击的权利，正在努力提高追踪攻击来源的能力。这份报告是迄今为止，美国对自己的网络安全政策以及军方在美国资产受到来自网络空间的攻击时所发挥的作用所做的最清楚的阐述之一。报告中的内容包括：1、得到授权后，美国将利用一切手段应对恶意网络攻击。美国保留使用包括外交、情报、军事、经济等所有必要手段保卫国家、盟友、合作伙伴以及美国的利益的权利；2、国防部保有运用武力响应针对网络空间以及其他领域的攻击的能力，并正在发展这种能力；3、进行军事响应的关键是能够快速确认攻击来源，而由于互联网的匿名特性，要达到这一点，十分具有挑战性。为解决这一问题，美国国防部正在支持追踪攻击的物理源的研究，并利用基于行为的算法来评估攻击者的可能身份。

- 美国网络司令部完成首次大型网络攻防演习

2011 年 11 月 30 日消息，美国网络司令部成功完成了首次大型网络攻防演习，此次演习的任务是保护美国国防部网络免受网络攻击，为期一个多星期。此次演习在内华达州的内利斯空军基地的空军红旗实验室内进行，共有来自各地的 300 名参与者汇聚在一个专用虚拟网络上，演练了他们的防御技能。演习者被分为“好人”和“坏人”两队，运用其攻、防网络技能进行对抗。“坏人”团队试图使用恶意软件和其他网络入侵形式侵入网络司令部的网络。网络司令部公共事务办公室的约翰森承认，“好人”团队不能防御所有的网络攻击，不过他指出，绝大多数的攻击被识别出来并被及时处理。

- 美国网络司令部拟成立网络“猎人队”

2011 年 12 月 13 日消息，美国防高级研究计划局举办了为期一天的“网络讨论会”，国防部高级官员和信息技术产业单位数百人与会，共商如何更好地保护军用和商用网络空间。美国网络司令部司令和国家安全局主任基思•亚历山大

陆军将军透露，国防部正在考虑创建特别的“猎人队（hunter teams）”，积极寻找计算机病毒和恶意软件。这个团队将是“一个充满活力的”外围防御网络的一部分。国防部在发展与企业合作伙伴关系以及盟友的合作方面可以做得更多，以保护网络领域。将军事网络防御升级并节约开支的另一个变化，就是要适应云计算平台。他指出，测试显示，使用云网络系统，可以使潜在的国防部信息技术节省 30%。

4. 美国其他网络安全相关举措

- 美国国防部计划投入 5 亿美元进行网络安全新技术研究

2011 年 2 月 16 日美国国防部副部长威廉·林恩表示，美国国防部计划投入 5 亿美元进行包括云计算和加密数据处理在内的网络安全新技术研究。林恩在旧金山举行的技术会议上表示，“国防部将为企业提供‘种子基金’用于发展能服务网络安全需要的军民两用技术。网络防御不同于领空防御，它不是军事任务，责任不能全由军方承担。我们国家大部分的关键基础设施，包括互联网本身都在私人手中，要通过公私合作来保护我们的网络。”这 5 亿美元是美国国防部 2012 财年用于改善国防部网络能力的 23 亿美元预算计划和被称为“网络 3.0”（Cyber 3.0）的综合网络战略的一部分。军方正与企业沟通，寻求最新技术和专家的支持来保护五角大楼的计算机网络免受网络攻击和间谍活动的侵袭。林恩表示，他已经会见了英特尔公司和谷歌公司的官员，并计划与微软公司官员会谈。

- 美国联邦调查局成立新的计算机取证实验室以打击网络犯罪

2011 年 1 月 7 日报道，美国联邦调查局（FBI）在加利福尼亚州成立了一个计算机取证实验室。该实验室有 25 个工作站，占地 2.1 万平方英尺。FBI 局长罗伯特·穆勒称，这个投资达 700 万美元的实验室将帮助警方打击日渐增长的计算机网络犯罪。司法鉴定人员处理证据时将使用精密的取证软件，该软件可以从计算机、手机和其它设备上提取数据。官方人员称该实验室将加快完成对犯罪嫌疑人调查取证的过程并早日绳之以法。之后，地方检察官的实验室将被并入当地的计算机取证实验室。穆勒表示，此举意在节约资源，精简多家机构共同开展调查工作时的操作步骤。

- 美国国家安全局协助金融业与黑客作战

2011 年 10 月 27 日消息，美国国家安全局（NSA）已开始向华尔街的银行提供有关外国黑客的情报，这一迹象显示美国对金融业遭破坏的担心在日益增加。

根据对美国官员、安全专家和国防工业管理人员的采访，为了防御网络攻击，上述举措只是美国银行业和其他金融公司向美国军方和私营国防合同商寻求帮助的努力的一部分。美国联邦调查局（FBI）也对银行业发出警告，特别应提防黑客利用安全漏洞对全球市场造成严重破坏，导致经济混乱。目前还不清楚黑客是否具备隐藏在银行的网络中致使股票、债券、现金等交易系统瘫痪，引发闪电崩盘，大笔资金被转走或所有的 ATM 机都被关闭等能力，不过 FBI 表示，该机构已数次协助银行确定网络漏洞，帮助其避免了几次大型网络攻击。负责美国军方网络运营及保护涉密的政府网络免受攻击的 NSA 局长凯斯·亚历山大表示，应金融公司的请求，NSA 已向其提供了有关网络攻击的专门技术知识。亚历山大表示，NSA 正在与金融公司谈判，可能将目前开展的一个向国防行业提供类似数据的试验项目拓展至金融行业,共享有关恶意软件方面的电子信息。不过，亚历山大没有提供双方协作的进一步细节。

- 美国商务部宣布新的针对商业企业的互联网安全计划

2011 年 6 月 8 日报道称，美国商务部宣布了一项打击网络黑客和网络欺诈行为的计划，并敦促企业自愿采纳互联网安全标准，但是没有提出任何具体要求。这份由商务部互联网政策工作小组完成的报告还呼吁增强互联网最佳做法和网络风险公众教育方面的国际合作。工作小组表示，政府在互联网安全中的责任应是“积极推动业界主导的网络安全工作和被广泛接受的标准。”美国民主和科技中心负责公共政策的副主席吉姆·登普塞表示，该报告正试图通过确定互联网上哪些部分不需要过多监管来划分政府管理互联网的界线。

- 美国 FCC 建立专业网站以帮助小型企业防范网络威胁

2011 年 5 月 17 日消息，美国联邦通信委员会（FCC）主席格纳考斯基宣布，为帮助小型企业“堵住”每年损失额高达数十亿美元的“安全漏洞”， FCC 建立了一个名为“小型企业网络安全”的网站，作为帮助小企业抵御网络攻击的若干方案之一。该网站提供一个包含厂商、非盈利及官方资源等的名单链接，并提出 10 条网络安全重要建议，包括培训员工、安装补丁程序、限制访问及定期更换密码等。此外， FCC 还同美国商会、SCORE 基金会、全美城市联盟（NUL），以及网络安全公司赛门铁克、McAfee 合作，为美国小企业提供网络安全提示及网络资源。在不久的将来，美国 FCC 还将同 SCORE 基金会支持的“电子商务即时计划（eBusiness Now Program）”开展合作，以提供有关网络安全方面的专业知识或技能。

- 美俄两国签订网络安全合作协定

2011 年 7 月 12 日报道，作为奥巴马政府与俄罗斯紧密关系重建工作的一部分，美国计划开始定期与俄罗斯分享网络安全信息，以消除两国在网络安全政策方面的意见分歧。两国发布的联合声明称，双方签订了一份网络安全合作协定，其中包括网络空间作战方面的军事意见交换以及两国计算机应急响应小组（CERT）之间的定期信息交流。两国还计划利用两国间现有的危机预防联系渠道建立网络安全通信协议。官员们表示，随着两国在网络空间方面对国家安全事宜的相互了解不断加深，这些措施将帮助两国政府在网络威胁方面更好地沟通，在应对这些威胁方面开展更好的协作，并在响应危机事件方面防止事态恶化。两国达成一致，将在 2011 年底开始实施这些网络安全措施。

（二） 美洲其他国家网络安全监管动态

1、 加拿大计划整合政府网络服务以提高网络攻击应对能力

为加强网络安全，加拿大政府 8 月 4 日公布计划，拟在两年时间内对该国政府机构复杂的电子邮件系统和互联网服务进行加强及整合，从而转变信息系统注重防御的设计理念，并期望节省高达 1-2 亿美元的开支。加拿大公共及政府服务部长安布丝表示，为保证信息更加安全、成本更低，将对目前联邦政府各机构用的超过 100 个的电子邮件系统进行整合，“ 化百为一 ”。此外，加政府还将把目前的 300 个数据中心减少到不足 20 个，并对 3000 多个政府及政府间电子网络进行精简。安布丝表示，这些努力及改变将有助于提高政府的数据安全，从而保护该国民众的根本利益。

2、 古巴要推行网络防御战略 为应对互联网安全威胁

古巴政府视互联网为国家安全的最大威胁之一，因此要求制定新的“ 政治战略 ”，开展“ 积极的网络防御 ”。普通古巴民众使用互联网的条件很糟糕，哈瓦那当局将此归咎于美国的贸易禁令，尽管如此，古巴现在也强调“ 占领网络 ”的重要性。古巴外交部长罗德里格斯要求更加积极地介入网络并采取更有力的防御机制来打击古巴所认为的主要媒体的敌对态度。

二、 欧洲地区网络安全监管动态

（一） 北约各成员国国防部长就共同应对网络威胁达成共识

2011 年 3 月 10 日在比利时布鲁塞尔召开的会议上，北约的国防部长们在一

项提高北约的防御能力以应对不断增长的网络威胁的政策上达成了共识。一位北约官员表示，目前第一步的想法是通过一项新的网络安全政策，以取代 2008 年制定的现行政策。新政策将仔细考量“ 网络防御正在快速发展的事实以及提升能力应对网络威胁的必要性。” 他还表示，作为北约政策的一部分，北约的计算机安全事件响应中心按计划将于 2012 年前全面投入运转。这意味着北约将进行设备投资、创建网络响应小组以帮助那些要求援助的成员国。此外，北约还将把各类网络威胁整合到北约的防御规划之中。预计，北约各成员国的国防部长将在 6 月召开的下一次会议上批准通过修订后的北约网络防御政策，并制定一项战略。

（二） 欧盟成立新机构以监视大型 IT 系统

2011 年 6 月 10 日欧盟成立了一个委员会，旨在监控一些在成员国范围内运营的大型 IT 系统。欧盟 27 个成员国 6 月 10 日达成一个政治协议，决定在 2012 年夏季开始运营这一新的 IT 机构。该机构将在爱沙尼亚首都塔林外的地区运营，其开发及管理部门将设在法国的斯特拉斯堡，此外，还将在奥地利的蓬高地区建立一个备份网站。欧盟表示，新的 IT 监督机构将管理的 IT 系统包括：一个国家级执法数据库——申根信息系统；跟踪跨境活动的签证信息系统；以及用于识别庇护申请人及非法移民的指纹数据库——欧盟数字指纹识别系统（EURODAC）。新机构还将监视未来可能涉及自由、安全、争议领域内的任何其他的 IT 系统，而整合其他的系统将需要欧洲议会投票决定。

（三） 欧洲委员会成员国达成协议保护关键基础设施和互联网言论自由

2011 年 9 月 26 日消息，欧洲国家一致同意，如果企业未能保护关键基础设施及互联网上的言论自由，用户可以根据人权法案起诉政府。在法国斯特拉斯堡召开的欧洲委员会会议上，47 个成员国的部长通过了有关互联网治理的建议，明确了现行法案所赋予他们的责任，并向前迈进一步，将这些责任以互联网条约的形式固化下来。部长们达成协议支持互联网治理的 10 条原则：保护人权、民主与法律原则；多方治理原则；国家责任原则；用户授权原则；普遍性原则；完整性原则；分散管理原则；开放标准、互操作性和端到端技术原则；开放网络原则；文化与语言多样性原则。他们还同意，有必要进行合作，以保持跨境互联网在应对网络攻击时的完整性。不过，各国一直不太情愿分享有关漏洞方面的情报。

（四） 欧洲网络信息安全局发布《如何进行有效的 IT 安全公私合作指南》

2011 年 10 月 11 日欧洲网络信息安全局（ENISA）发布新指南，就成功打造有效的公私合作，构建有弹性的 IT 安全提出了 36 条建议。欧洲多数成员国的关键基础设施都由私营行业运营，因此，业界和政府必须共同合作，为公民和企业

提供安全、可靠的系统接入。由于地理因素和电信运营商之间的竞争，欧洲的关键信息基础设施（CII）呈碎片化状态。因此，对于欧洲来说，提高 CII 弹性十分重要。为满足这种需求，公私合作（PPP）不断发展，在不同时间、在不同的法律框架下保护众多成员国的数字经济。这种自发的演进方式导致各国对 PPP 的构成缺乏共性的认识。欧洲网络与信息安全管理局 ENISA 出台的新 PPP 指南，其中包括了如何成功打造 PPP 的 36 条建议，凸显了在欧洲范围内达成共识的必要性。这对于欧盟发起的一个项目——欧洲公私合作增强复原能力（EP3R）项目尤为重要，该项目旨在将各国有关关键信息基础设施保护（CIIP）方面的公私合作建立起联系。

（五） 英国公布新反恐战略 严防恐怖分子“网络圣战”

英国政府新的反恐战略 7 月 13 日正式公布，战略中指出恐怖分子正越来越多地利用网络制造攻击，策划在未来针对英国等西方国家发动“网络圣战”。内务大臣特里莎•梅(Theresa May)指出，科技的进步意味着当局的反应必须同步加快，恐怖分子可能正利用网络科技，包括“谷歌地图”和“谷歌街景”来制定攻击计划。为了应对恐怖分子越来越多地利用这些高新技术手段（如电话声音加密技术、文字操作程序和云计算技术等）的可能性，英国当局必须将技术相应地进行配套和跟进。

（六） 英国政府拨款 10 亿美元打造全新网络安全战略

2011 年 11 月 25 日消息，为应对日益猖獗的网络犯罪和黑客活动，英国政府将拨款 6.5 亿英镑（约 10 亿美元）打造一个全新网络安全战略。该项战略旨在用 4 年时间提升该国的网络安全水平，维护网上交易安全。英国国家打击犯罪局将在 2013 年前成立新的网络犯罪小组，与伦敦警察厅的中央电子犯罪小组和英国严重有组织犯罪局展开合作。战略要求还包括大量投入和开展协作，使各方及时交流信息并处理各类威胁。英国政府的目标是，到 2015 年，大多数英国公民能够享受基本的安全保护，能够识别和上报网络威胁，在网上使用个人及敏感信息时具有更强的安全意识，将网络犯罪的报告用时从 20—30 分钟减少至 15 分钟。

（七） 英国研究开发网络武器

2011 年 6 月 1 日消息，为了应付日益增长的网络威胁，维护国家安全，英国正在研究开发网络武器，此项网络武器开发计划的目的是让英国政府在遭遇网络攻击时有更多的攻击性选择，而不只是被动地抵抗黑客的攻击。对于网络武器何时可以使用、谁有权下令使用的问题，英国武装力量大臣尼克•哈维表示，网

络武器和其他军事资产的保管和使用准则完全一样，英军特种部队就是这种武器的榜样。

（八） 国际网络安全保护联盟（ICSPA）在英成立

随着网络技术的日益发展，网络犯罪已成为一个全球性问题，网络犯罪给各国造成的损失逐年增加。为有效打击网络犯罪，在英国政府支持下，一个全球性非营利组织——国际网络安全保护联盟（ICSPA）7 月 5 日在伦敦举行新闻发布会宣告正式成立。ICSPA 是一个全球性非营利组织，目前其成员包括 McAfee、TrendMicro 等数家全球知名企业。该组织将致力于整合国际间商业团体、法律执行机构以及各国政府的努力，通过国际网络犯罪援助项目、国家及地区网络犯罪援助项目以及网络犯罪相关法律培训和信息共享机制，提升打击网络犯罪的国际执法能力，保护广大企业及其顾客免受网络犯罪活动侵害。

（九） 德国组建 IT 安全特别工作组以帮助中小型企业保护 IT 基础设施

2011 年 3 月 30 日报道，德国联邦经济与科技部长莱纳·布鲁德雷组建了一支负责 IT 安全的专责小组，该工作组的目标是加大对德国中小企业开展 IT 基础设施保护的扶持力度。该工作组将与业界伙伴合作开展更多保护措施以保证 IT 安全。工作小组也受到德国信息技术、电信和新媒体协会（Bitkom）的欢迎，该协会与德国软件公司 Datev、安全公司 Sophos 与软件公司 Sap 工业为德国网络安全协会 DsIN 完成的一份研究显示，如果电脑系统崩溃，只有 1/4 的德国中小企业有应急预案，3/4 的中小型企业没有对他们的员工提供有关信息安全技术的定期教育或相关信息。

（十） 德国国家网络防御中心正式成立

2011 年 6 月 16 日消息称，德国正式成立了国家网络防御中心，用于识别来自网络世界的威胁并做出相应的反应。联邦刑事犯罪调查局、联邦警察局、联邦海关总署以及联邦国防军共同参与网络防御中心的工作。国家网络防御中心的任务包括识别来自网络世界的威胁并做出相应的反应。联邦内政部长弗里德里希最担心德国重要的基础设施领域遭到黑客袭击，例如能源、饮水供应系统以及通讯网络等等。联邦信息技术安全局负责人表示，下一步要做的工作是将经济领域纳入网络防御范围。“ 经济领域是民生之外网络防御中心的又一工作重点，因为 80% 的重要基础设施都在经济领域占据着一席之地。”

（十一） 以色列国防军成立新部门加强网络防御力量

2011 年 6 月 28 日消息，面对日益增加的针对以色列的网络威胁，以色列国防军（IDF）近日成立了一个新部门以加强其防御能力。新成立的部门隶属于 C4I

部（注：C4I 部由以色列国防部队的 C4I 处和通信、电子和计算机部队组成，主要负责完成以色列国防部队的 4 项主要的 C4I 项目：创建国家保密光缆网络、将光缆网连入以色列国防部队的移动电话网络、在地面机动部队部署宽带通信、拓展以色列国防部队的卫星通信能力），负责保护军用网络免受敌方黑客攻击。

三、 亚洲、澳洲地区网络安全监管动态

（一） 日本表决通过针对计算机病毒的犯罪管理刑法修正案

日本参议院在 6 月 17 日表决通过了针对计算机病毒的犯罪管理刑法修正案《为应对信息处理高级化而对部分刑法内容所作的修正法案》，并宣布自 2011 年 7 月开始执行。该法案的特点是明确包含了所谓的“ 计算机病毒罪 ”。无正当理由，“ 开发 ” 病毒或“ 提供 ” 病毒，擅自在他人计算机上执行程序的情形，处以 3 年以下有期徒刑或 50 万日元(约 4 万元)以下罚金。同时，无正当理由，“ 获取 ” 病毒或“ 保存 ” 病毒，擅自在他人计算机上执行程序的情形，处以 2 年以下有期徒刑或 30 万日元(约 2.4 万元)以下罚金。

（二） 日本警察厅发 2011 年版《警察白皮书》

2011 年 7 月 22 日，日本警察厅发布了 2011 年版《警察白皮书》。这是该白皮书时隔 5 年再次发布网络犯罪特集。《白皮书》指出，现在，在互联网上骗取个人信息的“ 钓鱼 ” 犯罪以及蹭用他人无线网络以混淆发信地址等使用新型犯罪手法的犯罪行为频频发生，“ 网络监管工作未能取得同现实世界中的监管工作一样的进展 ”。

（三） 日本防卫相要求军工企业采取防范黑客入侵新措施

日本防卫相一川保夫 11 月 16 日在记者会上正式宣布了要求军工企业采取防止黑客攻击的新措施，其中包括每周至少使用相应软件查毒一次。防卫省将于 11 月 24 日面向企业举办说明会。新措施修改了与企业签署装备合同时签订的《有关确保信息安全的特约条项》，要求对防卫机密等“ 应保密信息 ” 是否泄露进行全天候监视，并至少保存三个月的链接记录；当确认感染病毒或遭遇非法入侵时，相关企业须立刻向防卫省报告。

（四） 韩国发布《国家网络安全总体规划》

8 月 8 日，韩国通信委员会（KCC）发布了 15 家政府机构集体参与编撰的《国家网络安全总体规划》。在这一规划中，网络空间将被视为韩国领土的一部分，政府将对未能遵守新的网络标准的企业进行问责，同时也将加强黑客入侵检测能力。目前，韩国政府的 15 个部门正分头细化相关方案，有望于本月底整合后正

式实施。根据这一总体规划，如果发生网络袭击事件，韩国将以“国家网络安全中心”为核心，由政府相关部门和民间组织、机构联手采取应对措施。“国家网络安全中心”将由国家情报院负责运营，韩国广播通信委员会、国防部、行政安全部、金融委员会等机构也将参与其中。为预防网络袭击事件的发生，韩国政府将要求政府部门和民间企业对重要信息加密，主要设施具备数据备份中心，构筑“灾难”恢复系统。

（五） 马来西亚网络安全机构启动多项措施应对网络攻击

2011 年 4 月 27 日消息，马来西亚科学、技术和创新部下属的马来西亚网络安全机构（CyberSecurity Malayasia）表示，为应对日益严重的网络攻击，该机构启动了多个网络安全项目。首先，根据马来西亚国家通讯社的报道，该机构启动了“网络 999”公共服务，以提供网络安全突发事件的应急响应。在 2011 年第一季度，“网络 999”服务台收到了 3563 件网络安全事件举报。其中，1273 件涉及到网络欺诈，包括 400 件针对马来西亚银行的钓鱼攻击。其次，该机构启动了一个公私伙伴关系——信任标记（Trust Mark）计划。公司通过增强他们的网络安全措施来获得一个“信任标记”图标并放在他们的网站上。第三，马来西亚网络安全机构首席运营官佐里表示，政府正向互联网用户提供被称为“DontPhishme（拒绝网络钓鱼）”的浏览器插件来检测虚假的银行网站，用户可以从 Mozilla 的火狐和谷歌的 Chrome 官方下载库中下载浏览器插件。

（六） 印度出台《国家网络安全策略（草案）》强调发展本土 IT 产品

2011 年 4 月 10 日消息，印度政府出台了《国家网络安全策略（草案）》（NCSP），认为发展本土 IT 产品对于应对进口高科技产品可能带来的威胁至关重要。《国家网络安全策略（草案）》称，“研发的本土化是国家信息安全措施的重要组成部分，首先是因为发达国家对尖端产品设定了出口限制，其次是为了树立自信，这样进口的 IT 安全产品就不会变成一项潜在的安全威胁。”《草案》要求政府确认对国家而言风险最高的网络威胁类型、关键 IT 基础设施的漏洞和网络安全存在的问题，并在此基础上开展协同一致的研发工作，满足关键研究所需。《草案》认定专利技术也存在风险，要求推广那些基于印度开放标准的产品。《草案》称，“为了使依赖专利 IT 产品的风险最小化，要鼓励开放式标准。政府和私营企业需要组成一个联盟，提高对基于开放式标准的可认证 IT 产品的使用率。”《草案》建议，将印度境内的战略基础设施连接起来组成一个全国范围的内联网，并让印度计算机应急响应小组（CERT-In）监督该内联网的运行。

（七） 印度完善《信息技术法》 从立法层面规范网站

2011 年，印度继续修订《信息技术法》，旨在从立法层面进一步规范网站。新法案规定：印度通信与信息技术部有权查封网站和删除内容，网站运营商须告知用户不得在网站发表有关煽动民族仇恨、威胁印度团结与公共秩序的内容；网站在接到当局通知后应该在 36 小时内删除不良内容，否则网站所有者将面临长达三年的监禁。新法案还对网吧经营活动作出了具体规定，网吧业主须保留客户所访问的所有网站为期一年的日志，并要求客户在上网前出示身份证。网吧的所有电脑应配备安全与过滤软件，以避免用户对淫秽、色情、恐怖主义等网站的访问。

（八） 伊朗启动互联网警察部门以打击网络间谍和破坏行为

伊朗官员 2011 年 1 月 23 日宣布，伊朗首批互联网警察开始执行“网络巡逻”任务，以打击针对本国的网络间谍和破坏行为。到 2012 年初，全国所有警察局将配设网络警察。伊朗警方信息生产与交换部门负责人赛义德•卡迈勒•哈迪安法尔说，互联网警察将“抵御利用信息技术工具发起的间谍与破坏活动”。

（九） 哈萨克斯坦《国家安全法修正案》明确国家信息安全工作

哈萨克斯坦参议院 2011 年 12 月 14 日在全体会议上通过了《国家安全法修正案》。哈萨克斯坦国家安全委员会副主席阿姆林表示，《国家安全法修正案》旨在进一步完善国家安全体系，把国家应对安全威胁的能力提升到一个全新水平。据了解，哈萨克斯坦《国家安全法修正案》对保障国家信息安全工作的优先方向做出了明确规定，把金融体系的不稳定列为国家经济安全的主要威胁。

（十） 澳大利亚安全情报局成立新的网络间谍部门应对网络攻击

2011 年 3 月 10 日消息称，澳大利亚安全情报局（ASIO）新成立的网络间谍部门即将揭开面纱，将保护澳大利亚国家网络避免受电子间谍活动的侵害。澳大利亚司法部长麦克莱兰德称，“这个专门的网络调查部门将调查由别国政府资助的、针对或涉及澳大利亚利益的网络攻击行为并提供建议。ASIO 将会与澳大利亚计算机应急响应小组（CERT Australia）、澳大利亚国防信号局下属的网络安全行动中心紧密合作，以识别不断发展中的威胁，并确定合适的反制措施”。他还援引了“Stuxnet”蠕虫病毒的例子，这一病毒击垮了伊朗的核电站，而爱沙尼亚因遭受拒绝服务式攻击，网络几乎瘫痪。他表示，“我们必须不断投入，以增强我们抵御类似威胁的能力。”

（十一） 澳大利亚公布网络犯罪法以应对全球黑客攻击威胁

澳大利亚政府 6 月 22 日公布法律，打击网络犯罪。在新颁布的法律下，澳大利亚警察和情报人员将有权要求网络服务提供商给出正在接受调查的网络犯

罪嫌疑人的信息。此前不久，多个跨国公司和机构遭受网络攻击，谷歌、国际货币基金组织以及美国参议院亦在此列。本月早些时候，基辛格亦呼吁美国和中国就限制网络攻击以及设置一些网络行为禁区达成协议。澳大利亚已经遭受了一轮网络攻击，有 4000 多家企业被攻击，来自海外的黑客还搞垮了澳大利亚议会的电脑网络。不过澳大利亚正在开发了一套对抗黑客和电子间谍活动，尤其是由国家自主的网络攻击行为的网络防护机制。这套机制的蓝图将于明年发布。

（十二） 新西兰国家网络安全中心正式成立运行

2011 年 9 月 27 日新西兰国家网络安全中心（NCSC）正式成立，旨在帮助政府各机构和关键基础设施供应商抵御网络威胁。报道称，新西兰政府曾于 2011 年 6 月发布《新西兰网络安全战略》，概括了一些有针对性的举措，以促进新西兰的网络安全。其战略重点是增强网络安全意识，提高网络安全水平，保护政府体系和信息，并加强对突发事件应对和策划能力。NCSC 是《新西兰网络安全战略》的一个关键部分，将以现有网络安全和信息安全保障为基础，对政府各机构加强保护。NCSC 有三个主要的基本功能：对开发安全网络提供咨询和支持；对复杂的网络威胁进行监测和响应；协调、协助采取响应措施，以应对危及国家安全的重大网络安全事件。NCSC 还将承担关键基础设施保护中心（CCIP）的现有功能。政府通信安全局将主持 NCSC 的工作。

8.3分布式拒绝服务攻击趋势分析

拒绝服务（DoS: Denial of Service）攻击是指攻击者向受害机器发送大量数据包，或无限制访问受害机器，消耗关键资源，从而使目标机器无法处理正常用户的请求，达到停止服务的效果。而分布式拒绝服务（DDoS: Distributed Denial of Service）攻击，是指攻击者利用众多攻击源向受害机器同时发动 DoS 攻击，是 DoS 攻击中最常用的一种方式，如图 8-1 所示。

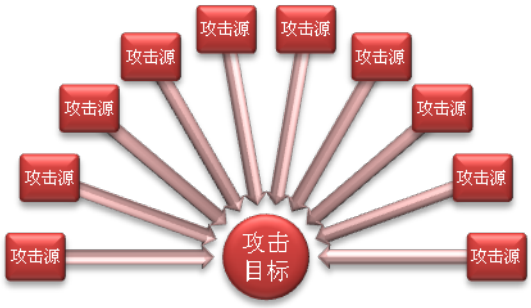

图 8-1 DDOS 攻击示意图

■ DDoS 攻击分类

根据 DDoS 攻击使用协议的不同，DDoS 攻击主要可分为以下几类：

- ICMP 洪水攻击（ICMP FLOOD）

向攻击目标发送大量 ICMP 数据包，消耗攻击目标带宽资源

- UDP 洪水攻击（UDP FLOOD）

向攻击目标发送大量 UDP 数据包，消耗攻击目标带宽资源

- TCP SYN 洪水攻击（TCP SYN FLOOD）

向攻击目标发送大量 TCP SYN 标志数据包，消耗攻击目标主机资源

- HTTP 洪水攻击（HTTP FLOOD）

向攻击目标（通常是网站服务器）发送大量 HTTP 连接请求，消耗攻击目标带宽资源及主机资源

由于网络协议自身存在的弱点，DDoS 攻击一直以来都是网络安全防护的一个难点。而且，ICMP FLOOD、UDP FLOOD 以及 TCP SYN FLOOD 通常采用的是虚假源 IP 地址，给 DDoS 攻击事件的追溯和处置带来巨大挑战。

■ DDoS 攻击特点

2011 年，DDoS 攻击仍然对我国互联网网络安全带来了巨大挑战，主要呈现出以下几个特点：一是 DDoS 攻击事件发生频率高，且虚假源 IP 地址成为主要攻击方式。据 CNCERT 抽样监测发现，我国境内日均发生攻击总流量超过 1GB 的较大规模的 DDoS 攻击事件 365 起。同时，TCP SYN FLOOD 和 UDP FLOOD 等常见虚假源 IP 地址攻击事件约占 70%，如图 8-2 所示。DDoS 攻击事件的频繁发生，反映出我国互联网网络安全面临的严峻形势，而虚假源 IP 地址成为主流，则进一步加大了相关部门对 DDoS 攻击事件的追溯和处置难度。

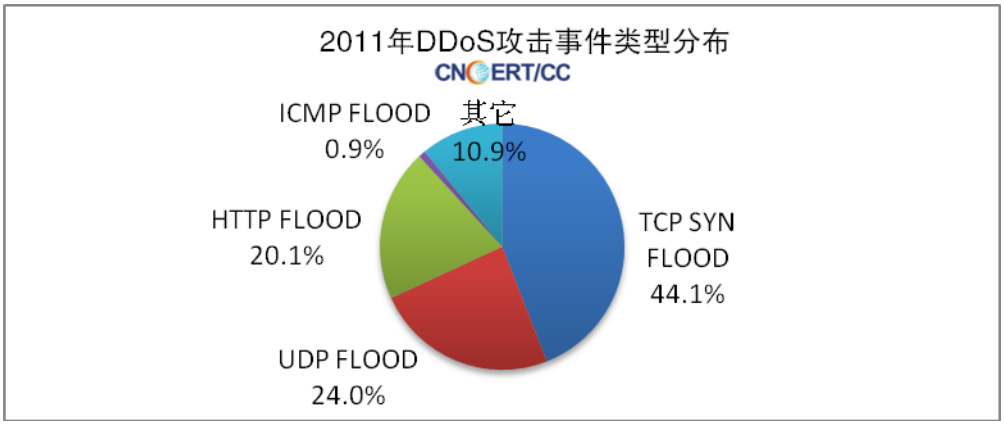

图 8-2　DDOS 攻击事件类型分布

二是流量转嫁事件屡见不鲜。所谓流量转嫁，是指受攻击目标（一般是网站）在遭受 DDoS 攻击时通过修改域名指向，将自身域名指向到其他网站域名或服务

器 IP 地址，从而将攻击流量转移到其他网站服务器。一般而言，流量转嫁对受攻击目标来说，并没有达到消除攻击影响的目的，在流量转嫁期间由于需要修改域名指向，其网站本身依旧不能提供正常服务。通常情况下，流量转嫁的目的主要是想引起相关政府管理部门对攻击者的调查和处置，因此相关政府管理部门网站成为流量转嫁的主要受害者。2011 年，工信部、北京市公安局等多家政府网站都遭受到过流量转嫁攻击，且这些流量转嫁事件多数是由游戏私服网站争斗引起。这也说明另外一个问题，意图采取流量转嫁而非通过正常渠道报告来引起相关政府管理部门对攻击事件调查和处置的网站一般提供的是非正规业务。

三是 DDoS 攻击日益规模化、组织化和经济利益化。随着黑客地下产业链的日益蔓延， DDoS 攻击已经成为黑客谋取利益的一个主要工具。在黑客地下产业链中，DDoS 攻击服务已经成为一个商品，任何个人和组织只要支付一定额度的金钱就可以获得相应流量大小和时间长度的针对特定目标的 DDoS 攻击服务。伴随着 DDoS 攻击经济利益化的同时，DDoS 攻击也呈现出规模化和组织化。为达到 DDoS 攻击的效果，黑客有组织地对攻击目标发动长期攻击，且随着受攻击目标防护措施的加强而不断调整攻击规模和攻击方式。例如，2011 年针对浙江某游戏网站等多家网站的攻击，时间上持续数月，攻击方式变化多种，包括 DNS 请求攻击、UDP FLOOD、TCP SYN FLOOD、HTTP 请求攻击等，攻击峰值流量达数十个 Gbps。

四是域名解析系统成为 DDoS 攻击的主要目标。以往，针对网站的 DDoS 攻击一般是直接向被攻击网站服务器发动攻击，但随着网站服务器安全防护手段和设备的不断完善，这类 DDoS 攻击往往难以真正达到拒绝服务的目的。因而，通过攻击其他与网站相关的薄弱环节以达到拒绝服务目的的攻击应运而生。域名解析系统由于其自身存在的弱点，包括使用 UDP 协议、固定端口等，成为黑客为达到攻击目的而选择进行间接攻击的主要目标。根据 CNCERT 抽样监测发现，每天发生的 DDoS 攻击事件中，约 7%的事件与域名系统相关。

■ 针对域名系统的 DDoS 攻击

针对域名系统的 DDoS 攻击主要分为两类：

一类是针对权威域名解析服务器的攻击。权威域名解析服务器直接负责域名对应 IP 地址的解析，一旦被 DDoS 攻击，将无法响应其负责解析域名的正常请求，同时，权威域名解析服务器可以租用域名服务商的服务，也可以是自建，防护手段参差不齐，因此成为黑客攻击的重点。

一般情况下，针对权威域名服务器的攻击可以分为两种：一种是大流量攻击。

由于域名解析服务使用 UDP 53 固定端口，黑客可利用此向权威域名解析服务器 UDP 53 端口直接发送大量 UDP 数据包，以达到拥塞服务器网络的目的。同时，由于使用的是 UDP 协议，攻击源 IP 地址往往是虚假地址。另一种是大量域名解析请求攻击。通过构造大量域名解析请求到被攻击权威域名解析服务器，以达到占用服务器资源的目的。构造的域名解析请求中请求的域名一般是随机生成的三级域名，而且其二级域名的解析是被攻击权威域名解析服务器负责解析，这样大量构造的域名解析请求就被发送到了被攻击权威域名解析服务器上。同时，由于此类攻击需要通过递归域名解析服务器，因此攻击会间接对递归域名解析服务器造成压力。

另外，针对权威域名解析服务器的攻击目的往往是企图使某一个或某些在该服务器上解析的网站域名无法解析，但是一旦攻击得逞，该权威域名解析服务器负责解析的所有域名的请求将都无法得到正常应答，造成牵连效果。例如 2011 年 7 月份，深圳大运会官网在部分地区无法解析，就是因为负责为其提供域名解析的权威域名解析服务器受到攻击，牵连到大运会官网域名的正常解析。

第二类是直接针对递归域名解析服务器的攻击。攻击方式同样可分为大流量攻击和大量域名解析请求攻击。其中，大量域名解析请求攻击构造的域名解析请求中请求的域名一般是随机生成的。由于递归域名解析服务器一般是基础电信运营企业构建，属于基础网络设施，一方面安全防护手段和设备较为齐全，不易被攻击；另一方面，一旦攻击得逞，将对普通用户网站访问造成直接影响。例如，2011 年 8 月份，新疆部分用户网站访问受到影响，就是由于新疆某运营商部分递归域名解析服务器受到大量随机生成的 DNS 请求攻击导致。

另外，值得提起的另一类攻击是 DNS 放大攻击。这类攻击通过伪造被攻击目标 IP 地址，向第三方 DNS 服务器发送大量的查询请求，DNS 服务器将大量的查询结果发送给被攻击目标，从而造成被攻击目标的网络拥塞。由于域名解析请求包往往远小于应答包，尤其是请求类型为 ANY 等类型时，因此黑客可利用此来达到放大攻击流量的目的。例如，2011 年 12 月份，大量 DNS ANY 请求被发往 NEUSTAR 等境外知名 DNS 服务商，其源 IP 系伪造的一些游戏私服网站 IP 地址，目的就在于利用 DNS 放大攻击来攻击这些游戏私服网站。

■ 防范 DDoS 攻击的建议

由于 DDoS 攻击呈现出越来越多的新特点，以及 DDoS 攻击和防护本身的不对等性，DDoS 攻击的防护面临越来越大的挑战。而有效对抗 DDoS 攻击，需要各方面共同努力，在以下几个方面加强工作：

1、相关单位和企业要加强自身网络安全防护措施。要配备专门的网络安全防护人员；重要信息系统要部署在防火墙后端，并配置适当的防 DDoS 攻击设备或软件；发生 DDoS 攻击事件时注意留存相关日志，必要时及时向公安机关报警。

2、相关政府管理机构、基础电信运营企业、域名注册和服务机构以及网络安全厂商要协同联动，共同清除 DDoS 攻击来源，让 DDoS 攻击成为“无源之水”。一般情况下，DDoS 攻击源头主要有两类，一类是黑客控制的“肉鸡（肉机）”。由于黑客控制肉机一般是通过木马、僵尸等恶意程序来实现的，因此打击木马和僵尸网络成为 DDoS 攻击防护的一个重要手段。由于需要对木马和僵尸程序进行监测、分析，对传播木马和僵尸程序的域名和服务器进行清理，因此相关政府管理机构、基础电信运营企业、域名注册和服务机构以及网络安全厂商需要共同行动，才能在这一环节进行有效的遏制。第二类源头是黑客租用或自有服务器。这类服务器往往分布在 IDC 机房或网吧中，往往有较大的网络带宽，能够在短时间内集中发出巨大的攻击流量，甚至可以对整个互联网流量造成影响；而且随时随地受黑客控制，可以长时间持续发出攻击流量，攻击方式也可以随时改变，对攻击的目标造成巨大损失。对于此，相关政府管理机构和基础电信运营企业要加强管理、监督和检查，避免 IDC 机房以及网吧成为 DDoS 攻击的“利器”。

3、基础电信运营企业应尽快全面启用路由器源地址认证功能，遏制使用虚假源 IP 地址发起的 DDoS 攻击。使用虚假源 IP 地址的 DDoS 攻击的泛滥不仅让许多安全防护措施失效，更增加了对 DDoS 攻击事件追溯和处置的难度。

4、广大网民也要积极行动起来，安装必要的杀毒软件和安全防护软件，加强自身电脑的安全保护，必要时定期重装系统，避免成为黑客发动 DDoS 攻击的肉机。

8.4用户个人信息泄漏事件分析

2011 年 12 月 21 日，中国互联网遭遇了一次强大的“地震”，从国内最大的中文技术社区 CSDN 用户数据库被泄漏开始，几天时间内，国内多家大型网站用户数据库被陆续曝光，在互联网上广泛流传。更为严重的是，被泄漏的用户数据库大多数包含明文保存的用户密码，受影响用户数以亿计。

■ 信息泄露情况

截至 2011 年 12 月 29 日，CNCERT 通过公开渠道获得疑似泄露的数据库有 26 个，涉及帐号、密码 2.78 亿条。其中，具有与网站、论坛相关联信息的（例

如，被声称属于某个网站的数据）数据库有 12 个，涉及数据 1.36 亿条；无法判断网站、论坛关联性的数据库有 14 个，涉及数据 1.42 亿条。

由于部分互联网用户在不同网站注册帐号时习惯使用相同用户名和密码，因此一旦在某个网站注册的帐号、密码等信息被泄漏，该用户在其他网站注册的帐号和密码也面临被泄漏的风险；此外，部分用户设置的密码比较简单（例如，使用用户名拼音、电话号码等），容易被黑客猜解。因此，部分黑客利用上述隐患，大肆对各个网站的用户注册信息进行探测猜解，甚至利用个别网站泄漏的用户数据作为“字典”，在其他网站上做恶意尝试，这两种被形象地称为“暴力破解”和“撞库”的恶意行为，极大地威胁到互联网用户的信息安全。根据各网站的验证结果，目前网上流传的泄漏库中，部分数据是有效的，但也有大量的数据是虚假的、无效的。例如，根据 CSDN 和天涯的测试结果，网上曝光的相关数据库中有一部分并不是其用户的数据。

尽管曝光的数据有真有假，但是不可否认的是此次事件的确给互联网用户带来了严重的个人信息安全威胁。被泄漏真实信息的用户，其网站个人账户中的信息可能会被窃取，甚至帐号被盗用；很多用户注册帐号时留下了电子邮件帐号，如果泄漏的密码与电子邮件密码相同，则会带来个人邮件的泄漏风险；黑客甚至可以利用这些邮件帐号冒用用户名义，在其他网站上利用密码重置功能进一步窃取更多帐号。此外，这些大量被泄漏的帐号也可能被黑客用于发送虚假、欺诈信息，危害其他用户安全和社会稳定。

事件发生以来，CNCERT 在工业和信息化部的指导下，紧急联系各个网站、论坛开展应急处置，并组织召开专家研判会议。CSDN 社区和天涯社区分别在各自网站发布公告，确认事件并提醒用户采取应对措施，对泄露账户密码进行有效性测试、临时锁定账号并通知用户修改密码。其他网站、论坛也分别对网上泄漏数据进行比对测试，通知受影响用户采取应对措施。各个网站、论坛也根据专家建议，着手采取系统安全防护工作，提高用户信息保密强度、用户登录验证难度等。

这次“地震”过去仅仅一个月时间，2012 年 1 月 25 日，新浪微博中再次爆出 Putty、WinSCP 等 SSH 管理软件中文版本（另称汉化版）存在后门程序导致用户信息泄露的事件情况。至 1 月 30 日、31 日，网络安全企业、相关博客论坛以及业内人士等纷纷披露并确认后门程序存在的情况，同时还披露了黑客通过后门程序窃取大量 SSH 管理软件用户信息系统相关的账号和口令信息、存储在后门程序服务器的情况。随后，由于黑客的后门程序服务器存在 SQL 注入漏洞以及目录权限漏洞，导致其存储的窃取信息被更多的人获得。

至 2 月 2 日，ANVA 成员单位通过公开渠道获得的存在后门程序的 SSH 管理软件样本涉及 Putty、Winscp、SSHSecure、Psftp 等多款软件产品中文版本，主要来源于 putty.org.cn、putty.ws、winscp.cc 和 sshsecure.com 等站点提供的下载点，而对应的非中文版本未发现存在后门程序。分析结果表明，黑客植入的后门程序具备记录用户输入和通讯、发送记录信息至指定服务器的功能。目前，暂未发现后门程序常驻系统内存或文件系统的情况，窃取信息行为发生在使用 SSH 管理软件过程中。

值得注意的是，黑客用作窃取信息管理的后门程序服务器域名为 l.ip-163.com。经验证，l.ip-163.com 与 www.putty.org.cn（Putty 中文站）位于同一 IP 服务器。至 2 月 2 日，后门程序服务器和 Putty 中文站已经不可访问。

ANVA 成员单位获得了记录窃取信息相关的多个数据文件，共得到 27261 条信息记录。这些记录包含受害信息系统 IP 或域名、连接账号、连接密码、连接时间、通讯端口、对应 SSH 管理软件产品等信息，可直接用于发起指定信息系统主机的攻击，获得系统管理权限。根据知道创宇公司提供的信息，去除无效、重复信息后，得到受害信息系统 IP 或域名共 1512 个，当中涉及 64 个政府网站域名（.gov.cn）。此外，统计得到受害用户使用的 SSH 管理软件的分布情况如图 8-3 所示，使用 Putty 和 Winscp 的受害用户占大部分。

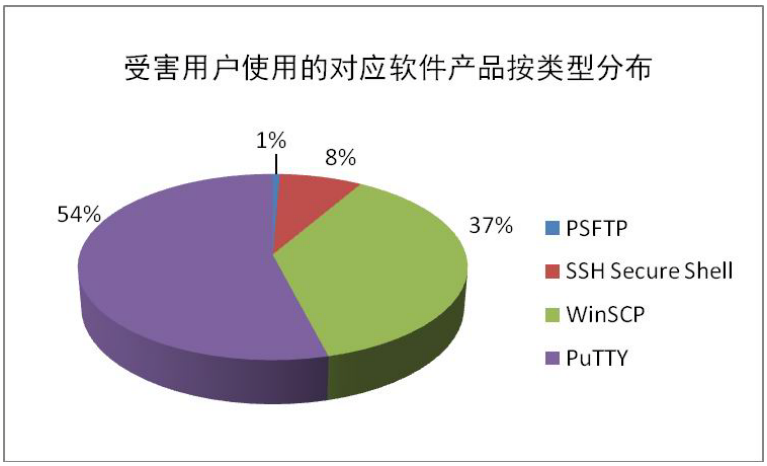

图 8-3　受害用户使用的对应软件产品按类型分布（来源：知道创宇公司）

■ 防范措施建议

CSDN 和天涯社区用户数据泄漏、部分 SSH 管理软件中文版本存在后门程序导致用户信息泄露等安全事件带来了广泛的社会影响，再一次对互联网企业和互联网用户敲响了安全警钟。针对此类事件反应出的问题，CNCERT 提出如下安全防范措施建议，供各互联网企业和广大用户参考。

1. 建议各互联网企业认真看待网络安全防护工作，加强联网系统的安全漏洞检查和修补，部署安全防护设施，不给黑客渗透入侵的机会。

2. 建议各互联网企业加强对用户信息的保护，采用强加密的方式保存用户密码等关键数据，采用严格、多重的用户认证程序，一旦发现帐号出现异常，应立即通知用户，对于重要业务，应建立强制性密码定期更新机制，以及采取 U 盾等其他身份识别技术。

3. 建议各互联网企业加强内部管理，建立有效可行的管理机制和操作规程，避免内部人员窃取并故意泄漏用户数据；此外，还应设置专门岗位负责日常网络安全保障工作，并与 CNCERT 或其他国家相关部门建立工作联系机制，及时报告和处置安全事件。

4. 建议广大互联网用户养成良好的安全意识和上网习惯。避免在不同网站注册时使用同一套账号和密码，应采用数字、字母、符号相结合的 8 位以上长度的密码，并定期更换；从事重要工作的用户尤其要注意避免使用工作邮箱作为注册其他网站帐号时填写的联系邮箱；平时要注意对个人电脑的安全防护，及时升级补丁并安装安全软件，避免因感染木马而导致个人信息被盗。

5. 建议各互联网网站、论坛应坚决抵制网上散播用户个人信息的行为，不提供、不转发相关下载链接；互联网用户一旦发现存在数据泄漏隐患的网站、论坛，应及时向当事方发出提醒，或者通报并委托 CNCERT 等国家相关机构联系当事方处置。

6. 建议国家有关部门积极介入事件的调查，严惩造成严重危害或造成恶劣影响的行为。建议互联网行业主管部门加强对软件下载站特别是开源软件下载站的安全监管，对传播恶意程序、危害用户利益和行业秩序的进行严厉打击。

7. 涉事厂商应及时发布安全公告，积极做好用户的应急处置工作。此前也出现过一些应用广泛的操作系统软件、应用软件官方下载文件特别是一些重新编译或汉化的开源软件被植入后门的情况，对开源软件的推广应用造成了负面影响。相关生产者（厂商）应以此为鉴，严格自律，同时要加强下载站的安全管理。

8. 建议使用了上述 SSH 管理软件产品的用户及时更换所管理信息系统的账号和口令，同时对系统进行安全审计，以免被黑客控制。同时，提醒广大用户注意软件应用安全问题，注意加强主机的安全防护，对下载文件进行查杀，更不要去下载来源不明的软件。

9. 呼吁掌握后门程序服务器存储数据信息的安全企业、业内人士不要擅自传播相关信息，以免造成更严重的后果。同时，呼吁安全企业加强技术分析和跟踪，在终端防护产品中加强对此类后门程序的识别查杀力度。