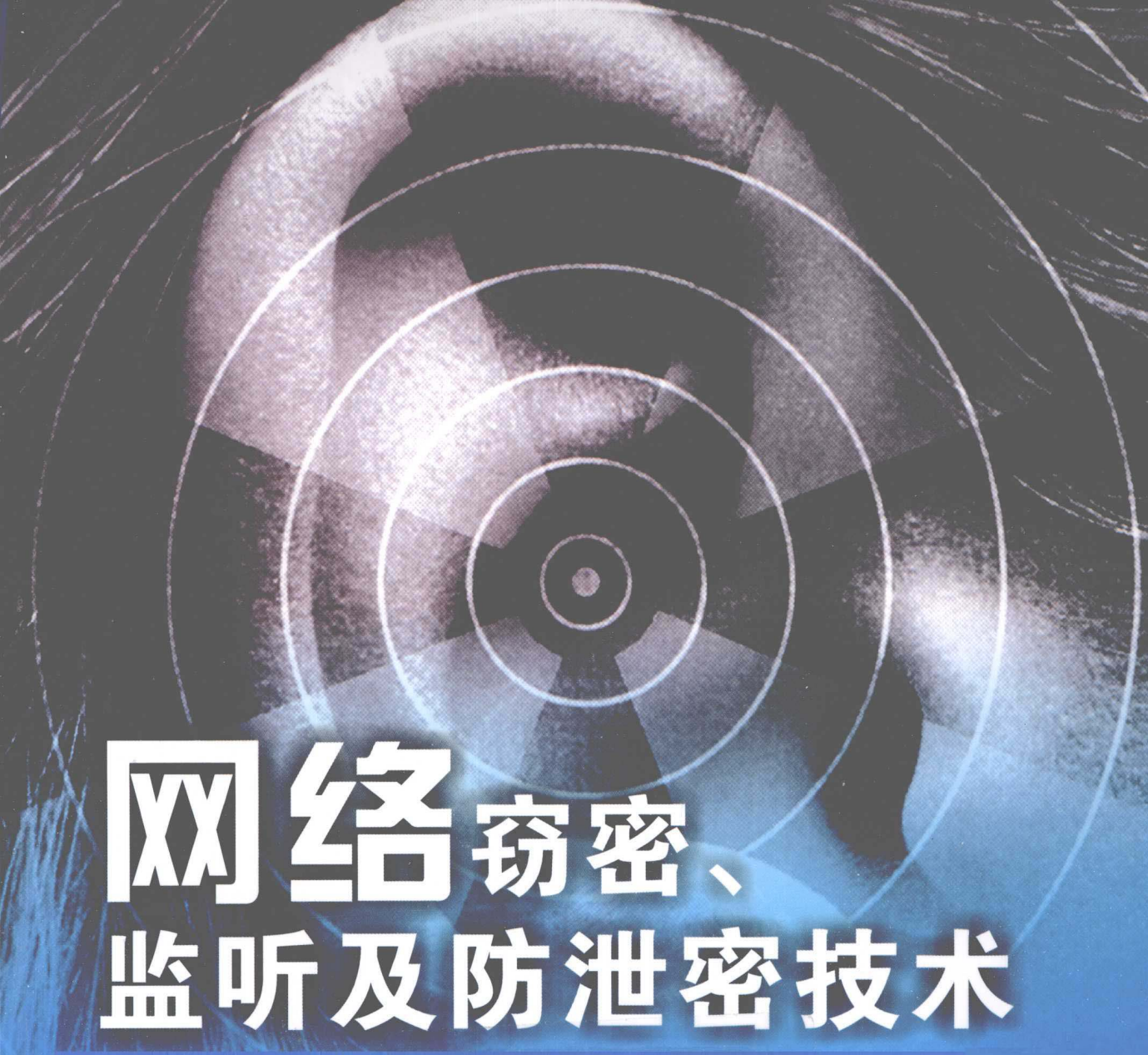

网络窃密、监听及防泄密技术

孙继银　张宇翔　申巍葳　编著◎

西安电子科技大学出版社
http://www.xduph.com

网络窃密、监听及防泄密技术

孙继银　张宇翔　申巍葳　编著

西安电子科技大学出版社

内 容 简 介

本书按照“了解和分析新形势下的网络攻击窃密威胁，有针对性地引入安全防御和网络监控新技术，逐步完成核心内网安全防御与防泄密体系构建”的思路进行阐述。第一部分重点介绍了新形势下“重点强化应用渗透、利用僵尸网络攻击、针对用户人性弱点攻击、内部攻击”的网络攻击窃密思路和技术手段。第二部分给出了网络监听的原理和关键技术、具体实施方案，国内外典型产品，以及监听技术在监控和防御领域的应用。第三部分在“构建核心内网安全防御与防泄密体系”的背景下着重探讨了其建设的指导思想和安全防御技术，以及具体设计方案和风险评估方法。

本书主要面向银行、证券、保险、政府机关、军队、国家安全、国防科研等重点单位从事网络安全工作的人员，以及对信息安全领域感兴趣的学生、教师或技术人员。书中部分内容，包括“高可靠性僵尸网络设计”、“面向核心内网的网络风险评估模型”、“网络监听实施方案”、“网络监听技术应用”、“面向核心内部网络的安全解决方案”等，融合了信息安全领域的最新技术和作者近年来的研究成果，对业内人士具有重要的参考价值和实用价值。

图书在版编目(CIP)数据

网络窃密、监听及防泄密技术 / 孙继银，张宇翔，申巍葳编著 —西安：西安电子科技大学出版社，2011 3

ISBN 978-7-5606-2529-4

Ⅰ. ① 网… Ⅱ. ① 孙… ② 张… ③ 申… Ⅲ ① 计算机网络—安全技术

Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字(2010)第 249952 号

策　　划　臧延新

责任编辑　樊新玲　臧延新

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　　编　710071

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西天意印务有限责任公司

版　　次　2011 年 3 月第 1 版　　2011 年 3 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印　张　19

字　　数　441 千字

印　　数　1～3000 册

定　　价　35.00 元

ISBN 978-7-5606-2529-4/TP • 1259

XDUP 2821001-1

前　言

这是一个 Web 2.0 的时代。IT 巨头们铆足了劲，为我们带来了更大的带宽、更便捷的入网方式、移动化的网络生活和“人人都能做老板”的电子商务梦想。“谁控制了信息，谁就拥有了未来”，这是永恒的真理。越来越多的企业、政府和机构不断加大投入，期望能掌握最先进的技术和最现代化的管理手段，从而获得生产力、工作效率和投资回报的最大提升。如今，无论是专家、领导还是“草根阶层”，每个人都可以享受社交网络带来的便利：每个人都可以“拥有属于自己的个性空间”，每个人都可以“参与没有国界的交际圈”；无论你是梅德韦杰夫还是安妮·海瑟威，不管你正遨游太空，还是正进行远洋勘探，处于不同社会阶层却拥有“相同属性”的一群人，无论千里之外还是近在咫尺，都能通过“好友圈子”、微博、个人视频空间，以最易于接受的方式，完成知识共享、近况告知和感情交流。网民，不再是网络中单纯的受益者和附庸物，而可以成为积极的“内容创造者和概念创新者”。在 Web 2.0 时代，网民将成为网络中最有价值、最富活力的元素。

这是一个全球网络战的时代。2010 年 5 月 21 日，美国国家安全局局长亚历山大晋升四星上将，并出任美军网络司令部司令，标志着网络空间已正式成为与陆、海、空、天同等重要的第五大战略空间，这也意味着原本无限神秘的网络攻防“国家队”将从幕后走向前台，开始公开地、不择手段地追求“制网权”。未来，围绕其中的资源、人才、战略、战术等等，将更加丰富和系统化。

这是一个黑客尽显风流的时代。黑客，也许是这个世界上智商最高、破坏力最大的一群人，他们能够利用所掌握的顶尖技术，为网络带来各种各样的“Surprise”，也许是善意的提醒，也可能是恶意的攻击；可能是有组织的、有目标的大规模侵袭，也可能是非理智的、纯报复或娱乐性质的网站页面涂鸦。黑客一直坚信“自由和共享”的信念：“所有数据应该免费并且全人类共享。但如果前者不能实现，那么网络就一定会受到攻击。”在这样的时代，不管数据是敏感的，还是无关紧要的；是属于政府机构、团体、企业，还是个人；是存储在磁盘、光盘、磁带中，还是在 SAN(存储区域网络)或集群存储系统中；是通过明码传输，还是通过加密传输，都存在被监听、截获、破译、阅读和利用的可能。

这是一个以核心敏感数据为目标，攻防双方激烈斗争的时代。近年来，网络攻击已不再局限于“沽名钓誉”的 DDoS 或者政府网站主页的修改。在利益的驱动下，攻击方逐渐把目光集中在敏感数据上，行动越来越隐秘，方法无所不用其极；防御方空前重视，投入巨资展开研究，推出种类繁多的新概念和新技术，当昨日的“防水墙”、“内容墙”、“UTM”、“版权保护系统”、“加密密盘”尚余音绕梁时，今日“云安全”、“DLP”、“企业内控”已粉墨登场。不可否认，开发商水平参差不齐，黑客技术飞速发展，用户背景千差万别，加上某些心存侥幸或心怀不轨的内部人员，所有这些因素都可能造成核心内网安全态势空前动荡，敏感数据不断泄露，一个又一个曾经光芒四射的“Somebody”身陷囹圄。

当狄更斯在《双城记》里沉吟着“这是一个……的时代”的时候，他如何能想到如今

的网络安全领域会呈现如此纷繁复杂的特征。网络攻击、窃密和监听与网络防御和反泄密，这一对“矛”与“盾”正你追我赶，日新月异。“黑客”这个原本神秘，代表着顶尖的计算机人才和破坏者的词汇，已经延伸出新的含义：“黑色产业链从业者”、充满好奇心的网络爱好者、网络间谍和网络安全专家。这些具有鲜明特色的不同人群，在研究和实践中不断进化发展，彼此间既竞争又相互学习，构成了一幅奇特而壮丽的生态图景。

就像那首曾唱响80后童年的歌谣：“昨天的红领巾，今天的特种兵”。如今，网络新技术和新应用层出不穷，网络安全也从一个原本相对简单的概念变得越来越丰富多彩。CCIE Security、CISSP、CWNE，国际网络安全领域精英辈出，各类教材浩若烟海。期望这本书能够涵盖网络窃密、监听和防泄密的所有内涵，那是“绝不可能完成的任务”。在这里，我们唯有穷竭才智，从浩瀚无垠的网络攻防海洋中挑选出自己认为最具时代性、创新性、代表性、启发性、针对性的观点或者有一定研究深度的知识点加以介绍和分析，一得之愚，希望能够引起读者的共鸣。

作为一本专注于“企业/机构核心内网窃密与反泄密斗争”的信息安全类书籍，本书内容分为三大部分：

第一部分为“网络战时代的网络窃密”。首先介绍“全球网络战时代”这个大的背景，分析Web 2.0、社交网络、无线移动网络和P2P技术所带来的机遇与挑战。其次，从一名黑客的角度，阐述新的安全形势下展开网络攻击窃密行动的总体战术思维和技巧，引出“应用层、数据、终端和人已经成为新的攻击焦点”这一思想。最后，按照从物理层到应用层、直至员工和管理的顺序，分别介绍了针对网络基础设施、应用层、内部用户等的攻击技术，并根据作者长期的跟踪研究，重点阐述了“僵尸网络”和“内部破坏”这两个影响力越来越大的安全威胁。

第二部分为“监听与控制”。首先对网络监听的原理和关键技术进行了介绍。其次针对子网、企业网、互联网监听等不同的需求，基于各种设备和手段，提出了十余种监听方案。然后，对国内外先进的网络监听和协议分析解决方案进行了介绍。最后介绍了监听技术在网络监控和安全防御中的应用。

第三部分为“构筑网络防泄密安全体系”。面对本书第一部分提到的各种新型安全威胁，针锋相对地引入相应的安全防御技术，包括安全接入和身份认证、应用层防御、云计算和虚拟化技术安全应用、网络安全隔离和数据防护等，着重解决“应用层安全、桌面安全、数据安全和人员管控”这几个近年来最为突出的安全隐患。在实践方面，阐述了网络安全防御与防泄密体系建设的指导思想，并根据重点核心内网在防泄密方面的特殊需求，给出并详细介绍了一种基于虚拟化技术、分布式监听与分析技术和隔离技术的整体解决方案。最后，将本书的精髓凝聚为一章，介绍了一种蕴涵作者独特思维的新型网络风险评估模型。

本书内容由孙继银总体规划和设计。其中，第1～11章由张宇翔编写，第12～19章由孙继银和申巍葳协作编写。因时间仓促，书中难免存在疏漏，敬请读者指正。

作　者

2010年9月

作 者 简 介

孙继银，山东省单县人，1952 年 4 月出生，毕业于国防科技大学计算机专业。教授、博士生导师，国家 863 计划评审专家，全军先进教育工作者，享受国务院特殊津贴，中国计算机学会高级会员，中国计算机用户协会理事。主要研究方向是 C4ISR、数据链技术、网络信息对抗技术、虚拟现实技术和硬件故障诊断技术。先后完成科研课题 30 余项，获国家科技进步二等奖 1 项，军队科技进步二等奖 9 项、三等奖 16 项。在国际会议及国内核心期刊发表学术论文 100 余篇，已出版专著 6 部。

张宇翔，湖南省长沙人，“80 后”，博士研究生，某部助理工程师，获第三届“学习成才先进个人”，Network General SCM，Cisco CCDP，软件设计师。12 岁起学习编程，从小爱好计算机病毒分析与设计。曾获国家级外语竞赛奖励 6 项，目前主要研究方向是数据链技术、网络信息对抗技术。先后参与完成课题 8 项，获军队科技进步三等奖 1 项，已参与出版专著 1 部。

关于作者

撰写本书的三位作者，多年来默默在网络对抗的不同领域潜心耕耘，他们坚持着共同的信念和目标：维护我国的网络安全和稳定发展，决不将“制信息权”拱手让人。

三位作者中，有一名年轻的“鹰派红客”，从 DOS 时代起就与计算机病毒结下了不解之缘，在网络攻击战术、僵尸网络改进、心理战和内网攻击破坏方面兴趣浓厚。他还是一名 Sniffer Certified Master，几年来潜心钻研网络监听技术在黑客行为分析与网络舆论战领域的实践应用。来自我军 C4ISR 领域的两位资深专家的加入使本书份量陡增，他们在指挥自动化、网络对抗和通信网络技术保障方面有着数十年的宝贵经验。

致 读 者

兵书有云，为将者须攻防兼备、知己知彼方可百战百胜。无论是黑客还是安全专家，只有具备对手的领域知识，了解敌方发展动态和思维方法，能够从他们的角度来审视自己，才能高屋建瓴地分析问题，有的放矢地做出应对。网络攻防，是一种要求知识全面、思维缜密的综合对抗。

也许有人担心，本书将网络攻击窃密技术和方法讲得过于透彻，会不会导致“教唆犯罪、泄露机密”等不良后果？作者认为，这种担心是多余的。学习敌人是为了锻炼自己，必须打破那种“害怕挑战、闭门造车、坐井观天、夜郎自大”的传统思维。核心网络安全与防泄密体系的建设和完善过程，就像如今 Linux、Apache、Emule 等开源软件的协作开发模式一样，需要有开放的胸襟、包容的心态，博采众长，勇于培养对手，勇于接受各种质疑、评估和挑战，在反复多次“提出方案—质疑/驳斥/破坏/推翻—改进完善”的迭代过程之后，大浪淘沙，才能最终诞生可靠的设计方案。本书是写给国人看的，只有培养出足够数量的“红色攻击者”，在和平时期不断检验我们自己网络的安全性，提出合理化建议，不断优化我们的系统，才能使我们在未来可能的全球网络战中立于不败之地。

本书汇集了网络攻击窃密、网络监听分析和网络安全防御体系设计三个领域的专业知识。在写作风格上，力图体现前后统一和通俗化；在内容选择上，强调“时代感和对抗性”；在章节编排上，根据网络逻辑模型采用“自下而上”的顺序；在技术分析上，引入国内外权威理论或资料的同时，更注重于阐述作者自己的想法。因此，它不仅是一本教科书，更希望成为一个与同行沟通的平台、一本工程技术资料、一部解决方案大全和攻防策略发展启示录。

本书主要面向以下类型的读者：

(1) 银行、证券、保险等客户信息敏感度高的企事业单位员工；

(2) 政府机关、军队、国防、军工等国家内部单位或组织的人员；

(3) 软件开发、图纸设计、投资机构、会计事务所、咨询公司等知识密集型机构的员工；

(4) 对信息安全研究有兴趣的个人。

如果读者是政府、军队信息化建设工作人员，或者是企业网络使用、管理和维护人员，本书将能帮助他们消除对网络攻击窃密的误解和恐惧，加深他们对内网信息安全防护重要性的理解，并为其提供一些有益的安全思维、理念和解决方案。方案可被直接应用，或根据实际情况进行适当的变更，可为现有的及设计中的内部信息网络提供具有高可靠性、高安全性、极强的灾难恢复和审计与追踪能力的信息安全屏障。

如果读者是头痛于传统教材的“算法和公式之海”，渴望刺激和挑战的计算机科学、信息对抗乃至管理专业的在校大学生，本书将是一本极富价值的攻防实践指导。已经具有一定网络基础知识的学生也会发现本书提供了面向网络对抗前沿、面向领域应用的对抗性极强的分析和解决问题的思路，可帮助他们理解教科书中所涉及的相关概念，激发创新思维

的火花，而不是机械地阐述难懂的安全理论，更不是无耻地“转载”前人的智慧精华。

值得一提的是，本书涉及的部分理论、技术和方案，包括“高可靠性僵尸网络设计”、“面向核心内网的网络风险评估模型”、“网络监听实施”、“网络监听技术应用”、“面向核心内部网络的安全解决方案”等，既反映了世界信息安全领域的前沿，又引入了作者长期的研究实践经验和成果。也许它们仍然面临较大的争议，但对于开阔读者的眼界将大有裨益。作者更希望能抛砖引玉，借此引起国内同行的关注和深入研究，实现我国在关键领域的重大突破。

目　录

第一部分　网络战时代的网络窃密

第二部分 监听与控制

第三部分　构筑网络防泄密安全体系

第一部分 网络战时代的网络窃密

如今，网络应用正空前地融入人类社会生活的各个领域，从政府办公、企业运作、商业交流到人们的日常生活，Web 2.0、社交网络、云计算、移动互联网和 P2P 等，将人、信息和资源越来越紧密地关联在一起。而与此同时，2010 年 5 月 21 日，美国国家安全局局长亚历山大晋升四星上将，并出任美军网络司令部司令，标志着全球网络战时代的正式到来，网络空间将成为与陆、海、空、天同等重要的第五大战略空间。这也意味着，从 2010 年开始，各军事强国将公开地、大规模地、不遗余力地追求“制网权”，更多的网络精英、研究机构和最新成果将投入到网络战中来，与越来越专业化、集团化的黑客群体一道，给网络世界带来不可预知的机遇与挑战。

秘密，按照定义，是指关系国家、机构、企业或个人的，依据规定权限和程序确定的，在一定时间内只限一定范围的人员知悉的事项。窃密，就是试图破坏对方对于秘密的严格规定和控制，在秘密处于有效状态的时间内，超越权限、知悉其内容的行为。从近年来窃密事件的案例中，可以发现这样的趋势：随着各类先进网络防御系统的部署运行，单纯的外部网络层或系统层次的攻击渗透已经变得越来越困难，而利用管理或人性的弱点，直接针对目标网络内部及其合法用户入手展开各类攻击渗透行为，成功的概率和获得的成果要大得多。当然，网络中运行着的数以万计的各类应用，也为攻击者提供了绝好的施展平台。

从战争中来，到战争中去。人类文明数千年发展的精华，在瀚如繁星的战争理论和军事思想中得到了最佳的体现。在人与工具、思维与技术的碰撞过程中，网络攻击窃密的艺术性和创造性被发挥到了极致。“体系作战”、“心理战”、“联合作战”、“点穴战”、“不对称作战”和“间谍战”等等现代战争的理论和思想，正被迅速融入到网络窃密的实践中来，在网络各个逻辑层次的斗争中激荡闪现，迸发出夺目的光彩。

在本部分各章节内容的介绍中，读者将逐步领略到战争艺术与网络窃密技术的结合是如何完美体现的。

第 1 章 网络窃密的新时代

2010 年，网络窃密应该说开始进入一个新的时代。这个时代有三个特点，第一，“网络攻击与防御”由过去遮遮掩掩的隐秘行动，正式成为公开的、国家层次的战略竞争点，作为与陆、海、空、天同等重要的、需要各国维持决定性优势的第五大空间，未来围绕其中的资源、人才、战略、战术等等将更加丰富和系统化。第二，虚拟化技术和“云计算”已经逐渐走向成熟，各种解决方案开始投入到各行各业。与此同时，高速无线网络和智能手持设备从神坛迈入普通老百姓的视野，随时随地通过网络进行社交与沟通已经开始成为普通人生活的一部分。当然，关于 P2P 禁与不禁的问题尽管仍在继续，但不可否认，通过 P2P 下载音乐、视频、资料和软件能够极大地丰富中国老百姓的互联网生活。第三，各类黑客群体也在不断地进化和发展，他们的专业水平更加精湛，攻击效率愈来愈高，从单打独斗的“骑士”逐渐走向以赚取经济利益、政治利益或者情报信息为目的的专业化黑客集团。

1.1 时 代 背 景

1.1.1 全球网络战时代强势来临

从 2008 年开始，俄罗斯黑客对爱沙尼亚和格鲁吉亚政府、商会、银行和媒体网站所展开的网络攻击，其攻击规模广泛而影响巨大，引起了美军的高度关注，并普遍被美国军事专家视为第一场国家层面的网络战。

按照美军的定义，所谓的网络战，即为攻击、干扰和破坏敌方网络信息系统，并保证己方网络信息系统的正常运行而采取的系列网络攻防行动，而“攻防兼备、侧重进攻”也成为美国网络战的核心理念，其典型战法是利用敌方通信系统和各种软硬件所存在的漏洞，将病毒植入目标计算机芯片或核心软件系统，让黑客利用计算机开放结构的缺陷和计算操作程序中的漏洞，使用专门的破译软件，破译超级用户的口令，窃取敌方金融信息系统、交通信息系统和电力信息系统等民用核心网络信息设施以及军事信息系统的核心机密，或在需要时利用无线遥控等手段将病毒激活，对敌方核心的军民网络信息系统实施“软破坏”和“硬摧毁”，使其陷入瘫痪，并释放虚假信息，扰乱敌方的心理等。正如美军网络战的鼻祖，兰德公司的阿尔奎拉和伦费尔特所指出的那样，网络战已成为“21 世纪的闪电战”。

美国国防部在全球 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。2009 年，美国总统奥巴马上任伊始，便将网络安全列为美国所面临的最为严重的经济和军事挑战，并在同年 5 月公布的《网络安全评估报告》中宣布美国将成立白宫网络安全办公室，负责协调美国网络安全政策与行动。之前，美国国家安全局、国防信息系统局、

战略司令部，以及各军种都有专门从事网络攻防的力量，但其资源分散，难以形成合力。为统一协调保障美军网络安全和开展网络战等与网络有关的军事行动，2010 年 5 月 21 日，美国国家安全局局长亚历山大晋升四星上将，并出任美军网络司令部司令。网络空间已被列为与陆、海、空、天同等重要的、需要美国维持决定性优势的第五大战略空间，这意味着美军将追求“制网权”。

根据美军作战指挥序列，网络司令部为美军战略司令部领导下的二级司令部。网络司令部成立后，将对全军网络战力量实施统一管理和运用，其编制不仅包括主要负责保护五角大楼在美国本土和全球范围内网络系统安全的“全球网络联合部队”，而且还包括主要负责对敌人发动网络攻击的“网络战联合功能司令部”，下辖陆军第 9 信号司令部、空军第 24 航空队和海军第 10 舰队三大军种司令部。全美军从事专业网络攻防的人员达 2.1 万人。

1.1.2　新型网络应用如潮涌现

最近几年，网络应用领域涌现出很多以“让人与人协作更紧密”和“让人们获取、处理信息更快捷”为特点的新成员，包括统一通信、Web 业务服务、Web 2.0 与社交网络应用、云计算与移动互联网应用、P2P 应用等。这些应用一方面给人们的工作和生活带来了新的色彩，另一方面也给网络安全增加了新的不确定因素。

1．统一通信

统一通信解决方案部署了很多统一通信应用程序，而这些应用程序通常是用来进行语音、视频、即时通信、文件传输以及应用程序共享的，其中包括企业级 VoIP、多方即时通信、视频会议等，能够向没有企业认证的外部用户授权参与内部网络会议。员工几乎在所有的日常生活中都使用即时通信工具完成与同事及商业合作伙伴之间的通信。IP 通信解决方案已经证明，它们能帮助机构解决这些问题，简化业务流程并降低成本。通过在通用 IP 基础设施上传输语音、数据和视频通信，企业可从一个集成、易用的界面，利用视频会议、语音和 Web 集成会议、移动 IP 软电话、语音留言等高级应用，进行实时协作。

2．基于 Web 的业务服务

基于 Web 的业务服务是指由企业发布的完成其特别商务需求的在线应用服务，其他公司或应用软件能够通过 Internet 来访问并使用这项应用服务。Web 业务采用基本的 Internet 协议“松”连接网络上的服务节点，并将业务“过程”定义在 Web 应用程序中，利用标准的存取协议(XML)为客户端节点提供服务。Web 业务主要解决基于分布在网络上不同服务器或终端之间的业务集成，面对海量的外部信息资源和应用资源，提供一种中间的服务，使得所有用户可以得到方便的信息共享和应用共享。Web 业务平台已经在电子商务、企业信息化中得到广泛的应用，很多企业都将应用架设在 Web 平台上，并不断完善和提高其功能和性能，为客户提供更为方便、快捷的服务支持。

3．Web 2.0 与社交网络应用

蔓生的社会关系网络，来自草根阶层的内容创建以及广泛的交互和协作等等，所有这些构成了精彩的 Web 2.0 世界。HTTP 正迅速成为 Web 2.0 世界的默认传输器。随着网络服务和以服务为标准的结构体系的出现，XML 已经成为一个融合体，它将完全不同的应用程序和数据类型结合到一起。网络门户、内容管理系统甚至企业博客和 Wiki 正成为首选的沟