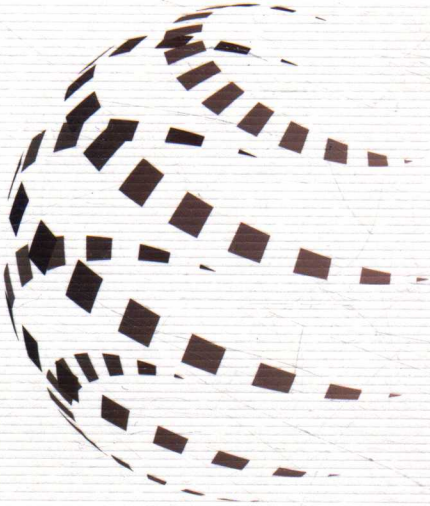
工业和信息产业科技与教育专著出版资金
cbjj.phei.com.cn

宽带中国出版工程

网络空间安全

魏亮　魏薇　等编著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

宽带中国出版工程

工业和信息产业科技与教育专著出版资金资助出版

网络空间安全

魏 亮 魏 薇 卜 哲 马志刚 王亦澎 王 昕
王秋野 田慧蓉 宁 华 许子先 杜 伟 李 强
张彦超 陈吉学 陈其云 陈 湉 汪 坤 杨丁宁
杨剑锋 孟 楠 封 莎 柳 青 郭 丰 崔 涛
落红卫 谢智刚 廖 璇 潘 娟 魏 翔 编 著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

网络空间是继陆、海、空、天之后的第五疆域。网络空间安全是全球共同关注的热点话题，受到广泛关注，包括美国在内的西方发达国家已经在网络空间安全方面积极部署，我国对此也有相应动作。近年来在网络空间安全方面出现了新威胁、新技术及新动态。本书主要内容包括：美国等发达国家在网络空间安全方面的新动向、网络空间安全所面临的新形势、网络空间所面对的种种安全威胁、当前网络空间安全涉及的技术手段、我国在网络空间安全方面的部署、现阶段我国网络空间安全存在的问题、对我国网络空间安全的相关建议等。

本书的主要读者对象是各级政府和行业主管部门、国内外电信运营商、设备制造商，以及相关行业协会和研究机构的专业人士和相关高等院校的师生。

图书在版编目（CIP）数据

网络空间安全 / 魏亮等编著. —北京：电子工业出版社，2016.1
（宽带中国出版工程）

ISBN 978-7-121-27615-6

Ⅰ. ①网… Ⅱ. ①魏… Ⅲ. ①互联网络—安全技术—研究—中国 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 277735 号

策划编辑：宋 梅
责任编辑：谭丽莎
印 刷：三河市双峰印刷装订有限公司
装 订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：720×1 000 1/16 印张：19.5 字数：416 千字
版 次：2016 年 1 月第 1 版
印 次：2016 年 1 月第 1 次印刷
印 数：3 000 册 定价：68.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

宽带中国出版工程

总序 1

宽带网络是新时期我国经济社会发展的战略性公共基础设施，是推进国家治理能力现代化和公共服务均等化的重要手段，是推动工业强国建设、促进农村经济发展和新型城镇化建设的重要途径。发展宽带网络对于促进信息消费、推动经济发展方式转变、全面建成小康社会具有重要支撑作用。加快宽带网络建设、增强技术创新能力、丰富信息服务应用、繁荣网络文化发展、保障网络安全，利在当前惠及长远。

当前，我国已建成覆盖全国、连接世界、技术先进、全球最大的宽带网络，网民数量、移动智能手机用户规模全球领先，相关产业能力持续提升，已经成为名副其实的网络大国。但同时，我国宽带领域的自主创新能力相对落后，区域和城乡普及差异比较明显，平均带宽与国际先进水平差距较大，网络安全形势日益严峻，总体上看国内宽带网络发展仍存在诸多瓶颈。在全球各国加强宽带战略部署、ICT 产业变革发展日新月异的形势下，要实现工业化、信息化、城镇化、农业现代化四化同步发展、建成网络强国仍然任重道远。

党中央、国务院高度重视宽带网络发展和管理，2013 年国务院先后出台了《“宽带中国”战略及实施方案》和《关于促进信息消费扩大内需的若干意见》。2013 年年底，中央网络安全和信息化领导小组成立，习近平总书记亲自担任组长，提出努力把我国建设成为网络强国，战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。这是党中央在新时期对我宽带网络发展提出的新目标和新要求，需要我们以改革创新精神，通过政策推动、技术驱动、产业带动、应用拉动促发展保安全；需要我们着眼长远、统筹谋划，积跬步、行千里，不断推动网络大国向网络强国迈进。

工业和信息化部电信研究院是我国在 ICT 领域权威的研究机构，多年来在重大决策支撑、行业发展规划、技术标准引领、产业创新推动和监管支撑服务中发挥了重要作用。“宽带中国出版工程”系列丛书，是该院及业界多位专家学者知识和智慧的结晶，是多专业科研成果的集中展现，更是多年理论与实践经验的综合集成，该系列丛书的出版有助于读者系统学习宽带网络最新技术，准确把握宽带应用和相关产业的最新趋势，从而提升对宽带网络的研究、规划、管理、运营水平。希望我国政产学研用各界齐心协力，共同为宽带中国发展、网络强国建设事业贡献力量！

工业和信息化部

总序 2

市场牵引是通信发展的动力，通信业务从语音为主到数据和视频为主，对带宽的需求与日俱增。思科公司 2014 年 6 月发布的报告指出，2013 年全球互联网忙时流量是平均值的 2.66 倍，与 2012 年相比，平均流量和忙时流量分别增长了 25%和 32%，思科公司还预测从 2013 年到 2018 年，全球互联网流量忙时是平均值的 3.22 倍，平均流量和忙时流量分别年增 23%和 28%。在互联网流量中视频已成主流，全球互联网视频流量占总量之比从 2013 年的 57%将增长到 2018 年的 75%。全球移动数据流量增长更快，2013 年一年就增加 81%，到 2018 年还将保持平均年增 61%的速度，届时移动数据流量将占全部 IP 流量的 12%。美国 Telegeography 公司给出的国际互联网干线流量 2009－2013 年平均年增 45%，2013 年相比 2012 年增加了 38%。我国国际互联网干线带宽从 2009 年到 2013 年平均年增 39.6%，2013 年相对 2012 年增 79%，增长的后劲更明显。

通信业务与技术的发展总是市场牵引与技术驱动相辅相成，市场催生了技术，技术支撑了市场。集成电路继续遵循摩尔定律，单位面积的晶体管数年增 40%，强大的计算和处理能力改进了频谱效率与信噪比，提升了通信流量，比较好地适应了互联网流量的增长。光器件的技术进步加上电域的信号处理，使光纤通信干线商用容量水平基本按照十年千倍提升。2009 年起我国移动通信从 2G 经 3G 跨越到 4G，借助先进的多址复用技术和频谱的扩展技术等，峰值速率增加数百倍。

近年通信技术与业务发展一个值得注意的趋势是从消费者的应用向企事业应用扩展，2013 年全球企事业单位互联网流量较 2012 年增 21%，到 2018 年还将达到 2013 年的 2.6 倍，将占全球互联网流量的 14%，而且全球企事业单位互联网流量中的 14%将是移动流量。随着物联网发展及信息化与工业化深度融合，企事业单位的互联网应用还将有更大的发展。

互联网的渗透促进了经济的复兴，2013 年发布的《OECD 互联网经济展望 2012》分析了互联网对所有行业经济的影响，得出如果宽带普及率增长 1%，GDP 将增长 0.025%，并且通过模拟得出互联网的贡献占 2010 年美国 GDP 的 4.65%～7.21%，占企业增加值的 3%～13%。波士顿咨询公司 2012 年发表的《连接世界》报告分析 2010－2016 年互联网经济对 GDP 的贡献，中国仅次于英国和韩国为第三位，占 GDP 的比例从 2010 年的 5.5%增加到 2016 年的 6.9%。IDC 公司提出信息技术已从计算机和互联网这两个平台发展到移动宽带、云服务、社交应用和大数据为标志的第三平台，即宽带化平台，并预测到 2020 年信息产业收入的 40%和增长的 98%将由第三平台的技术所驱动。世界银行的研究报告表明，对制造业的海外销售额和服务业的销售额来说，使用宽带的企业与其他企业相比分别高出 6%和 7.5%～10%，中低收入

国家的宽带普及率每增加 10 个百分点，GDP 将会增长 1.38 个百分点。美国认为宽带的发展对上下游产业就业的拉动作用是传统产业的 1.7 倍。GSM 协会和德勤咨询机构 2012 年发表的研究报告指出，3G 移动数据应用增加 100%，人均 GDP 增速提升 1.4 个百分点。

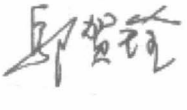
为了抢占信息技术新的制高点并获得宽带化的红利，一些国家纷纷出台国家宽带战略，最近两三年来美国出台了《国家宽带计划》和《大数据研究和发展倡议》等，全球有 146 个国家都制定了加速发展宽带的国家战略或规划，不少国家建立了宽带普遍服务基金。

我国网民数量世界第一，但按网民平均的国际互联网干线带宽、固网平均接入速率和移动互联网下载速率仍低于世界平均水平，这几年有了显著改进，但与互联网高速发展和社会大众的期望相比总是恨铁不成钢。国务院在 2013 年 8 月发布了《“宽带中国”战略及实施方案》，提出到 2015 年要初步建成宽带、融合、安全、泛在的下一代国家信息基础设施，到 2020 年我国下一代信息基础设施基本接近发达国家水平，技术创新和产业竞争力达到国际先进水平。该方案对宽带网络覆盖、网络能力、应用水平、产业链发展和网络信息安全保障五方面提出了具体发展目标、重大任务和保障举措等。可以预期“宽带中国”战略的实施，必将为我国经济和社会的发展奠定坚实的网络基础，并惠及大众。

工业和信息化部电信研究院作为“宽带中国”战略的起草支撑单位之一，为“宽带中国”战略的制定做了深入的调查研究，现在与电子工业出版社联袂推出“宽带中国出版工程”系列丛书。该丛书串起终端、接入、传送、网络和云端各环节，涉及研究、制造、运营与服务各方面，涵盖宽带化技术、业务、应用、安全与管理各领域，解读“宽带中国”战略制定的背景，分析宽带化的解决方案，展望宽带化发展的前景。本套丛书内容全面，系统性强，既反映了宽带网最新的技术及国际标准化进展，又有国内实践经验的总结，兼具前瞻性与实用性。在此，衷心感谢工业和信息化部电信研究院和电子工业出版社及众多的作者所付出的辛勤劳动，希望本套丛书能够有助于业内外人士加深对宽带化的意义和内涵及难度的理解，相信本套丛书能够对行业发展和政府决策起到积极作用，为“宽带中国”战略的实施贡献正能量。

工业和信息化部通信科学技术委员会主任

中国互联网协会理事长



前　言

随着信息通信技术（ICT）的飞速发展及其向经济和社会的全方位渗透，云计算、大数据、4G 时代扑面而来，一方面对世界范围的经济社会发展产生了巨大的正面影响，另一方面则给网络空间安全带来了无法回避的更大威胁和挑战。网络空间安全涉及经济安全、国防安全、政治安全和文化安全，是影响国家安全和公民权益保障的极重要因素。如今，网络空间已被视为继陆、海、空、天之后的第五疆域，是一个国家主权的象征，也是大国地缘政治竞争的重要场所。网络空间的安全威胁对任何一个现代国家的潜在破坏性已经不亚于核武器。

本书对网络空间安全概念及形势、网络空间现状及发展、网络空间安全技术、网络空间安全热点、网络空间安全基线等内容进行了深入阐述。第 1 章概述网络空间、网络空间安全基本概念及世界各主要国家的网络空间安全目标；第 2 章分析当前我国网络空间安全现状，包括网络空间安全发展阶段、取得的成绩及不足；第 3 章从政策法规、安全管理、国际合作、文化建设等层面给出网络空间安全现状及发展；第 4 章试图将网络空间安全分层，按层描述网络空间的相关技术，包括认证、加密、备份、攻击、保障等；第 5 章给出当前网络空间安全热点问题与研究重点；第 6 章分析网络空间安全热点事件和相关技术；第 7 章描述网络空间安全的一些基线要求。

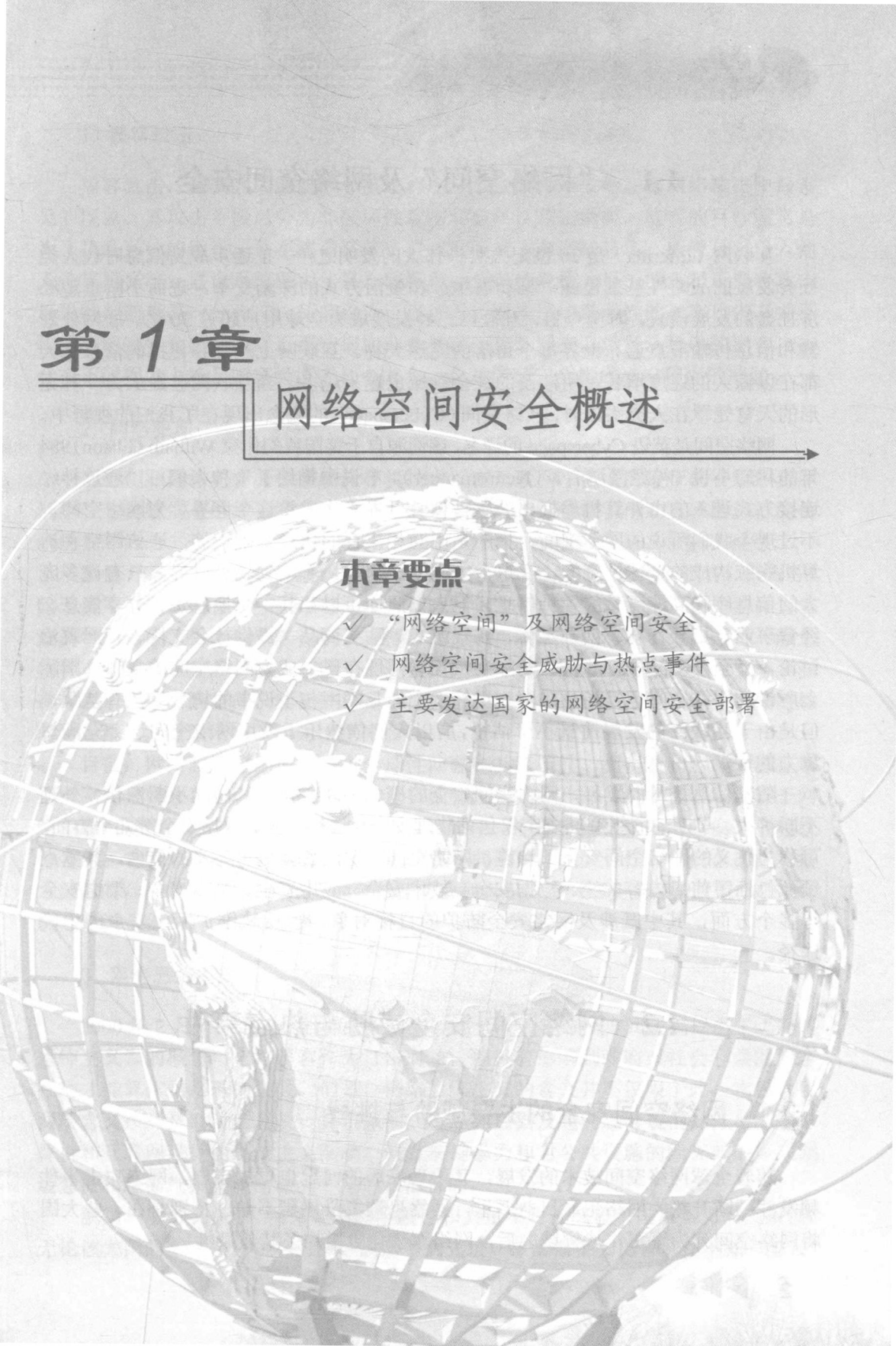
本书属于“宽带中国出版工程”系列丛书之一，通过对网络空间概念、管理、技术及热点等的描述，以期给我国网络空间安全管理人员、专业技术人员及广大读者关于网络空间安全方面的基本知识。此外，本书还给出了一些网络空间安全基线的描述，可使读者明确了解如何保护网络空间安全。

编著者

2015 年 9 月

目　录

第 1 章 网络空间安全概述



本章要点

- ✓ “网络空间”及网络空间安全
- ✓ 网络空间安全威胁与热点事件
- ✓ 主要发达国家的网络空间安全部署

1.1 “网络空间”及网络空间安全

互联网（Internet）是20世纪人类最伟大的发明之一，正逐步成为信息时代人类社会发展的战略性基础设施，推动着生产和生活方式的深刻变革，进而不断重塑经济社会的发展模式。时至今日，互联网已经发展成为全球用户超过30亿、联网处理器和信息传输节点遍布世界每个角落的庞然大物。互联网上产生和传播的信息每天都在以惊人的速度增长，所涉及的社会领域也越来越多。当互联网已经成为一种无形的天穹笼罩在人类头顶时，网络空间（Cyberspace）的概念出现在了我们的视野中。

网络空间是英语Cyberspace的译名，该词源自于美国科幻作家William Gibson1984年的科幻小说《神经漫游者》（Neuromancer）。小说中描绘了一种人们可以通过神经连接方式进入的由计算机虚拟出的感官体验世界，作者将这个世界称为网络空间。不过现今我们所说的网络空间，指的是由互相依存的信息基础设施、通信网络和计算机系统构成的全球性空间。在这个广袤的空间里，看不到物理世界，只有许多庞大的信息库和高速流动的各种信息，但人们照样可以在其中交换思想、分享信息、经营事业、指导行动、创办媒体、畅玩游戏、购买商品、提供社会支持、开展政治讨论，甚至发动战争，等等。实际上，互联网现在已经成为网络空间的主体。国际上所说的网络空间也是指互联网。虽然现今的互联网与小说中的构想依然有差距，但是由于互联网的发展前景不可估量，所以人们依然乐于使用网络空间这个充满想象力的词汇。

随着信息技术的发展，网络空间安全的概念不断变化，其内涵不断深化、外延不断扩大。早期的网络空间安全仅包括物理安全、运行安全、数据安全等几个方面，可称为狭义的网络空间安全。当前，网络空间安全演变为更为广义的概念，其重点领域包括了信息内容安全、数据安全、技术安全、应用安全、资本安全、渠道安全等多个方面，其中既涉及网络安全防护的目标对象，也反映维护网络安全的手段途径。

1.2 网络空间安全威胁与热点事件

1.2.1 网络空间安全的主要威胁与挑战

随着全球网络空间技术的发展，其治理滞后的问题也更加突出。网络攻击事件频发并不断升级，网络犯罪日益严重，网络恐怖主义屡剿不绝，特别是在一些大国将网络空间列为军事作战领域之后，网络军事化更增加了其复杂性。

1. 黑客攻击

黑客攻击，即黑客破解或破坏某个程序、系统及网络安全，是网络攻击中最常见的现象。其攻击手段可分为非破坏性攻击和破坏性攻击两类，前者的目标通常是为了扰乱系统的运行，并不盗窃系统资料或对系统本身造成破坏；后者是以侵入他人计算机系统、盗窃系统保密信息、破坏目标系统的数据为目的的。对于黑客攻击后果的判断尚需一分为二：那些仅为了表达不满而未造成破坏性的黑客攻击，并不构成对国家安全的威胁；而那些窃取商业机密、扰乱国家政治经济秩序的黑客攻击会在不同程度上涉及国家经济或社会安全，会对国家安全构成一定程度的威胁。

2. 网络犯罪

网络犯罪是指犯罪分子借助计算机技术，在互联网平台上所进行的有组织犯罪活动。与传统的有组织犯罪有所不同，网络犯罪活动既包含了借助互联网进行的传统的犯罪活动，也包含了互联网所独有的犯罪行为，如窃取信息、金融诈骗等。

2011 年 5 月，欧盟刑警组织发布了《有组织犯罪威胁评估》半年报告。报告称，除了信用卡欺诈、音视频盗版等高技术互联网犯罪外，互联网的广泛使用同样为非法药物的合成、提取和流转提供了支持。此外，互联网被广泛用于人口贩卖、濒危物种走私等非法交易，成为犯罪人员洗钱的通信工具。欧盟刑警组织主管罗布·温赖特表示，过去两年间，相比纯粹基于计算机的犯罪，有组织犯罪“转战”互联网的数量激增，互联网犯罪成为“主流”。

目前，网络犯罪已经成为一个全球性问题，其跨国性、高科技和隐蔽性特征都给国家安全带来了前所未有的挑战，这些威胁主要集中在非传统安全领域。鉴于网络犯罪可能给国家带来的巨大潜在损失，打击网络犯罪应该被纳入国家安全战略统筹考虑。它既需要国家之间的合作，也需要不同部门之间的合作，如安全部门与技术部门的合作。2011 年 7 月成立的全球性非营利组织国际网络安全保护联盟（ICSPA）就是跨国合作的一个很好尝试。

3. 网络恐怖主义

2000 年 2 月，英国《反恐怖主义法案》第一次以官方的方式明确提出了“网络恐怖主义”的概念，它将黑客作为打击对象，但只有影响到政府或社会利益的黑客行动才能算作网络恐怖主义。但是，网络恐怖主义的含义并不仅限于此，它包含了两层含义：一是针对信息及计算机系统、程序和数据发起的恐怖袭击；二是利用计算机和互联网进行的恐怖主义活动，通过实施暴力和对公共设施的毁灭或破坏来制造恐慌和恐怖气氛，从而达到一定的政治目的。

就第一层含义而言，网络攻击的隐蔽性和力量不对称凸显了国家实力的局限性，无论该大国的军事实力多么强大、武器多么先进、核武器多么厉害，在不知“敌人”

在哪里的情况下，也只能被动防御。从这个角度来说，网络攻击无疑先天就具备了恐怖主义的特质。不过，目前的网络恐怖主义活动主要集中在第二个层面。通过黑客攻击和低级别犯罪等手段，借助互联网组织发起恐怖主义活动，互联网已经成为恐怖主义分子互通有无、相互交流的最重要的场所。除了将网络空间作为通信和交流的媒介之外，恐怖组织还利用网络空间进行理念宣讲、人员招募和激进化培训。目前，恐怖主义的网络攻击还未出现，但是，一旦恐怖组织通过互联网完成了培训和自我激进化，就很有可能将网络空间当作未来的一个新战场。

4. 网络战

网络战的主体既包括国家行为体，也包括以不同方式参与其中的非国家行为体。国家参与的网络战对国家安全威胁的程度最高，涉及传统的军事安全领域，它既可以独立存在，也可以是战争中的一部分。网络战的攻击目标既可以是军事、工业或民用设施，也可以是机房里的某一台服务器。

网络战最大的威胁是对军事设施的直接打击。由于网络技术被广泛应用于军事领域，从军事装备和武器系统、卫星到通信网络及情报数据，所以一个国家的军事能力高度依赖信息和网络通信技术的发展。但这无疑也让它更加脆弱，一旦这些军事领域的网络系统遭到攻击，国家的军事力量就可能直接被削弱，甚至面临着部分或全部瘫痪的风险。在 2008 年的格鲁吉亚战争中，俄罗斯就被认为是配合其军事攻势发动了一场网络战。

通过攻击金融系统、能源和交通这些重要的民用部门，网络战同样可以对国家安全带来间接的冲击和破坏。1982 年，里根政府批准了一项针对苏联西伯利亚输油管线数据采集和监视控制系统的网络攻击，这是有记载的最早的一次网络战，它不仅破坏了苏联的军事工业基础，而且间接地削弱了苏联的军事实力。2010 年伊朗所遭受的“震网”病毒攻击也被认为是美国或以色列对伊朗军事实力的一次间接打击。

网络间谍是国家所从事的最常见的一种网络战，一国利用互联网在有价值的网络系统中植入恶意软件，从而以最小的成本从敌方获取所需要的信息和情报。一旦植入目标系统的“木马”或“后门”在某个特殊的时期同时被激活，例如，政治局势紧张或常规战争爆发，这些情报会给国家安全带来巨大的威胁。2013 年 6 月，前美国中央情报局人员斯诺登将两份关于美国国家安全局“棱镜项目”的绝密资料交给了英美两国的一些媒体，从而爆发“棱镜门”事件，美国政府授权情报系统侵入他国公民邮件、通过技术手段全面监控互联网的行为引发国际的广泛关注。

信息战是基于信息操控的一种软网络战，也是心理战的重要组成部分，它旨在通过信息披露来影响敌方的思想和行为，在外交领域也被称为公共外交。20 世纪 90 年代，随着网络媒体的逐渐增多，信息战的使用也越来越多。美国对信息战非常重视，如在伊拉克战争中对基地组织的信息战；在伊朗、巴基斯坦、阿富汗和中东地区，为了扭转在伊斯兰世界的不佳形象，美国也开始越来越多地使用了信息战。