美国网络空间安全体系

刘峰 林东纯 等◎著

Overview of the Cybersecurity System in USA

科学出版社

美国网络空间安全体系

刘　峰　林东岱 等　著

中国科学院信息工程研究所

信息安全国家重点实验室

阜阳师范学院图书馆 藏书

科学出版社

北京

内 容 简 介

本书共 9 章，围绕美国的网络空间安全展开。第 1 章介绍了联邦政府相关的组织机构及管理协调机制；第 2 章介绍了法律法规体系；第 3 章介绍了标准体系；第 4 章介绍了四个具有历史意义的技术体系框架；第 5 章介绍了美国多年来在几个重要技术领域的技术发展规划；第 6 章介绍了科研体系；第 7 章介绍了美国的网络空间安全教育体系；第 8 章介绍了美国联邦政府国家级战略和重大计划；最后，作为本书的总结，给出美国所谓的战略优势究竟为何物，分析了我国同美国在安全战略方面的差距，并给出了一些具体的发展建议。

本书可以作为网络空间安全研究人员及政策制定人员的参考书。

图书在版编目(CIP)数据

美国网络空间安全体系/刘峰等著. —北京：科学出版社，2014

ISBN 978-7-03-042629-1

Ⅰ.①美… Ⅱ.①刘… Ⅲ.①互联网络-安全技术-研究-美国 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 277427 号

责任编辑：赵丽欣 / 责任校对：刘玉靖

责任印制：吕春珉 / 封面设计：东方人华平面设计部

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2015 年 1 月第 一 版 开本：787×1092 1/16

2015 年 1 月第一次印刷 印张：22 1/2

字数：560 000

定价：99.00 元

（如有印装质量问题，我社负责调换〈双青〉）

销售部电话 010-62134988 编辑部电话 010-62134021

版权所有，侵权必究

举报电话：010-64030229；010-64034315；13501151303

前　言

网络空间作为继陆、海、空、天之后的第五维空间，它提升了人类的计算能力、存储能力、传输能力，给人们的生产生活带来了革命性的飞跃。网络空间虽然总体上是一个虚拟空间，但是它可以通过影响人类的思想、控制与人类生活息息相关的电子设备和设施，对人类社会和物理世界产生重要影响。因此，各国均试图从网络空间中寻求竞争优势，并试图如在军事、政治、外交、文化等领域争取竞争优势一样，以期能够胜出。

作者在研究过程中深切地感受到，对于一个国家来说，网络空间安全是一个庞杂的体系，涉及组织管理、法律法规、标准技术、科研教育、国家战略等诸多方面，各种因素相互影响、相互制约，是一个系统工程。因此，若想做好我国网络空间安全的工作，需要从全局的角度考虑各种因素，使其服务于国家总体的安全战略，使各个部分相互促进、避免重复和相互制约。

美国作为世界上军事和经济实力最强大的国家，在网络空间安全领域的研究和实力也远远领先于其他国家。美国早在老布什时代就提出了兴建信息高速公路的计划，之后网络渗透到人们生活的方方面面，促成了人类历史上一次伟大的信息革命。但随之而来的信息安全保密问题时时刻刻刺激着人们的神经，一些影响巨大的事件层出不穷。之后的克林顿、小布什和奥巴马政府，通过越来越密集地发布针对性国家政策、组建专门的政府机构，来应对日益严峻和复杂的信息安全挑战。至今，美国在网络空间安全领域的综合实力远远领先于世界上的其他国家。

在复杂的信息社会环境中，摸索一套完善的网络空间安全体系很难。作为当前世界上信息安全研究最早、最先进和最完善的国家，美国的一些做法值得我们借鉴，如明晰联邦政府在网络空间的定位、设立高级别的协调机构、强调国家体系化的危机应对、完善的产学研用创新机制、持续稳定的科研投入、注重信息的共享、汇集全球的智慧、培养全民信息安全意识、利用国家级的战略规划和重大计划引导社会力量的投入等。但是我们也注意到，由于社会结构、国家体制及意识形态上的差异，我们也不能照搬美国的做法，还需要辩证地看待美国的网络空间体系，要结合中国的实际情况制定适合自己的发展策略。

本书由信息安全国家重点实验室组织撰写，由多个作者合作完成。其中，刘峰负责全书的组稿，并主持各个章节的撰写，林东岱负责全书的审校。第 1、2、6、7 章主要由赵倩执笔完成，第 3、4 章主要由皮兰执笔完成，第 5 章主要由王文浩执笔完成，第 8、9 章主要由刘淼执笔完成。

由于时间及水平所限，本书难免有错漏之处，希望读者批评指正。如有机会，我们将在后续的版本中更新，我们也将根据后续的研究补充一些内容。若有任何意见，请发送至 fengliu.cas@gmail.com。如果本书的部分章节有更新，将通过网页 http://www.fengliu.net.cn 发布。

撰写本书得到了中国科学院战略性先导科技专项项目（XDA06010701）及科研项目

BMKY2013A02 的支持。田静所长、朱标明司长、杨芸处长、唐树才处长多次对本书的撰写给予了指导。赵战生老师多次参加我们课题组的研讨班，为作者去疑解惑。实验室武传坤、王雅哲等众多科研人员也贡献了他们的智慧和见解，在此一并向他们表示衷心的感谢。

试读结束：需要全本请在线购买： www.ertongbook.com

目　录

第 1 章　美国网络空间安全组织管理体系

随着网络逐渐渗入金融、交通、通信、军事等各个领域，目前网络已成为一个国家正常运转的“神经系统”，一旦这个“神经系统”出现病变，国家安全也将面临极大的威胁。然而近年来的经验告诉我们，只在技术上寻求突破，无法从根本上解决网络空间安全问题。网络空间安全问题的解决需从管理、技术、法律等多方面统筹规划。美国作为信息技术高速发展的一个国家，十分重视网络空间安全领域的组织管理工作，从最初的没有机构对该领域进行管理，到多个机构的管理，再到多个跨部门机构的协调管理机构的成立，这些变化显示了美国在网络空间安全管理领域做的不断尝试和努力，同时也体现了美国对网络空间安全管理领域工作的重视。

本章主要从四部分介绍美国网络空间安全机构的管理情况，第一部分主要介绍了美国联邦政府在网络空间安全领域设置的主要机构及其职能；第二部分依据美国网络空间安全管理的特点，结合 PDRR 体系模型，从防御（Protection）、监测（Detection）、响应（Response）和恢复（Recovery）四个方面讲述美国网络空间安全在防御、态势感知、应急响应和事件恢复四个方面的管理协调工作；第三部分从法律法规、政策引导、力量整合、经济支持、建设中介平台服务五个方面介绍了美国在网络空间安全领域的产学研协同创新机制；第四部分主要对美国联邦政府在网络空间安全领域的机构设置的特点进行了总结。

1.1　美国网络空间安全机构概述

美国的行政机构是美国管理公共事务的行政组织体系，它是美国政治制度的重要组成部分。美国行政机构的组成包括联邦行政机构和州及地方行政机构。联邦行政机构由内阁各部、总统办公厅和独立机构构成。与网络空间安全相关的机构还包括美国的军事机构、情报机构、立法和司法机构及相应的产学研机构。

奥巴马于 2009 年在美国的国家安全委员会（NSC）和国家经济委员会（NEC）下设了网络空间安全办公室（CSO），先后任命霍华德·施密特（Howard Schmidt）和迈克尔·丹尼尔（Michael Daniel）为 CSO 的协调员。CSO 将负责为政府编纂和综合所有的网络空间安全政策，在整个国家范围内统一协调网络空间安全相关的事务，包括协调国家层面的保护和危机事件的应对，每年定期向美国总统汇报网络空间安全方面的各种情况，并提出发展建议。CSO 是美国政府在网络空间安全方面最高的协调机构。另外，白宫的国家科学与技术委员会（NSTC）下设的网络与信息技术研发子委员会（NITRD Subcommittee）专门设立了网络空间安全研究高级监督小组，专门负责制定美国的网络空间安全研发政策。

在内阁各部中，与美国网络空间安全联系较多的部门是国防部（DoD）和国土安全部（DHS）。其中，DoD 的首席信息官（CIO）担任国家安全系统委员会（CNSS）的主席，该机构负责协调美国政府各个部门和局商讨信息保障政策，设立国家级的信息保障政策、指令、指南、操作规程。美国国家安全局（NSA）作为 DoD 的一部分，拥有非常强的研究能力，

负责美国国家保密系统的安全工作，组织撰写了著名的《信息保障技术框架》（IATF）。DHS主要负责帮助联邦行政部门的文职机构保护他们的非保密网络，并协调对危机事件做出响应，是美国各项信息保障政策和计划的实际执行者。DHS 下包含多个执行机构，如网络空间安全和通信办公室（CS&C）、国家网络空间安全和通信集成中心（NCCIC）、国家协调中心（NCC）和美国计算机应急准备小组（US-CERT）等。

在涉密信息管理方面，美国的主管机构是信息安全监督办公室（ISOO）。该机构隶属于国家档案记录管理局（NARA），全面负责美国政府和各行业中涉密信息和计划的保护、管理和监督。ISOO 每年负责向总统就涉密信息和项目的状态及预算花费等内容做汇报。美国的一些情报部门，如中央情报局（CIA）、国防情报局（DIA）、国家情报总监办公室（ODNI）、国家地理空间情报局（NGA）、国家侦察局（NRO）、NSA 及美国军方等机构涉密较深。这些机构对涉密信息管理较严格，有些部门拥有自己的涉密信息管理制度。对于实施涉密信息保护所造成的花费，ISOO 通常以保密附件的形式呈交给总统。

“维基解密”事件之后，为防止内部人员泄密，并促进涉密信息的共享，美国特别组建了四类机构，包括：高级信息共享和保护指导委员会、涉密信息共享和保护办公室、网络中涉密信息保护执行代理、内部威胁专责小组。

在美国设立的众多网络空间安全管理机构中，有如 DHS 和 DoD 类的管理机构，有负责对各个行政机构的保密制度进行监督和审查，协调行政机构间有关保密制度事项的保密监管机构——ISOO。负责网络空间犯罪的调查和起诉的执法机构 DoJ。作为科技强国，美国拥有为数众多的产学研机构，包括高校、企业和信息安全保密顾问、专家等。美国政府还设有专门的计划来广泛吸取社会上（高校和企业）的科研成果来加强和加速联邦政府在网络空间安全方面的能力建设。此外，美国总统和国务卿等高级官员经常性地就网络空间安全事件发表言论，并制定国家层面的战略和政策，从而影响美国，甚至跨越国界影响这个“平坦的世界”。

图 1-1 是美国联邦政府的网络空间安全组织机构体系。

下面介绍美国的主要网络空间安全机构。

1.1.1　白宫网络空间安全机构

网络空间安全办公室（CSO）于 2009 年成立，隶属于 NSC 和 NEC。2012 年 5 月，迈克尔·丹尼尔接替霍华德·施密特担任现任 CSO 协调员。网络空间安全协调员同时担任总统特别顾问，有权直接接触美国总统，被媒体称为“网络空间沙皇”。CSO 的人员将负责为政府编纂和综合所有的网络空间安全政策。他们将同管理与预算办公室（OMB）密切合作来保证部门预算，而且在重大网络空间事故或攻击情形下协调政府反应。网络空间设施保护不仅仅限于联邦政府，办公室还将同国务院（DoS）、地方政府和其他合作伙伴国家一起防御网络空间攻击，并且同私人部门合作以保证对未来网络事件能够做到及时且有组织的响应。

1.1.2　国家安全局

美国国家安全局（NSA）是一个美国政府的情报机构，作为美国 DoD 的一部分进行管理，1952 年 11 月 4 日由时任总统杜鲁门秘密指挥创建。它领导了美国政府在密码方面的工作，包括负责通信信息保障和信号情报方面的产品与服务（对应有两个理事会），在计算机

试读结束：需要全本请在线购买：　www.ertongbook.com

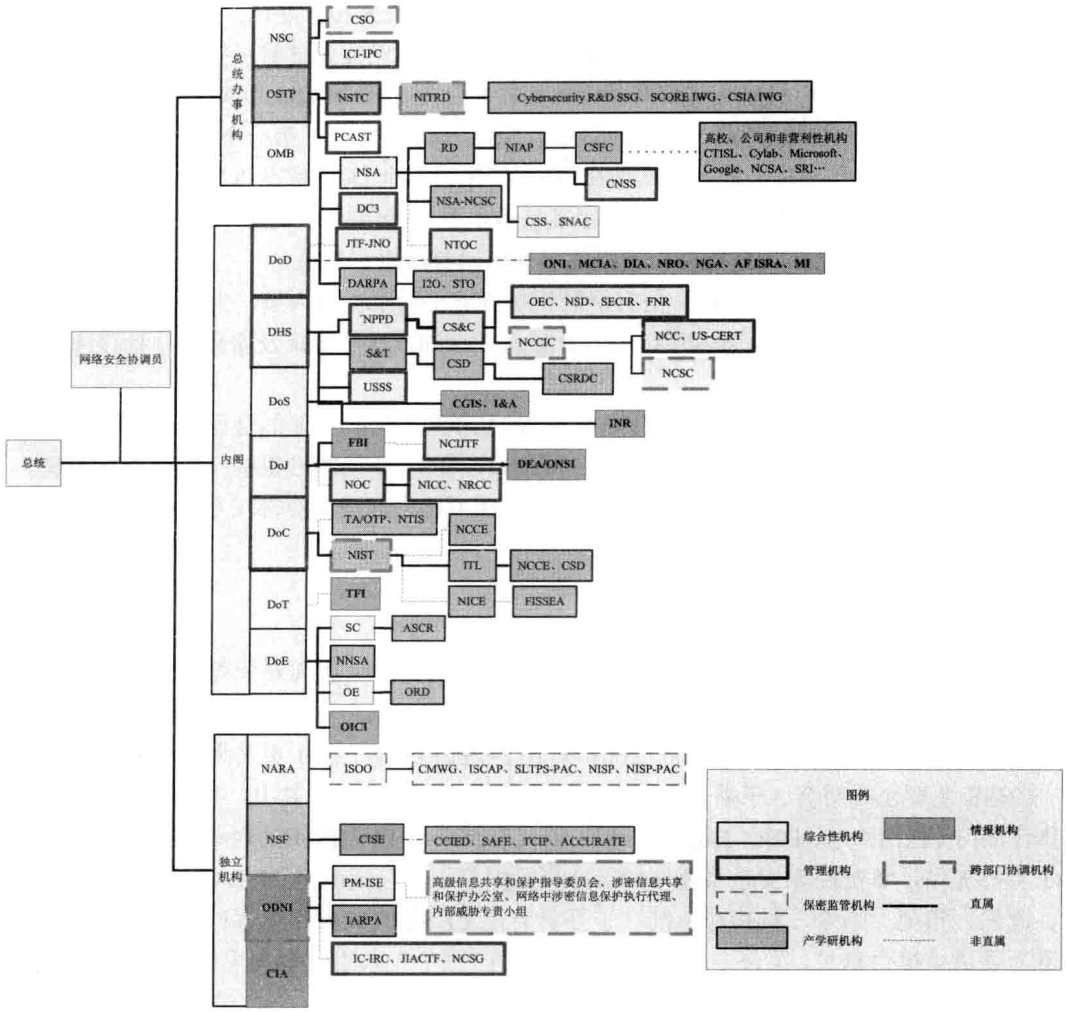

图 1-1　美国联邦政府的网络空间安全组织机构体系

网络空间战中为国家和其同盟国提供政策上的优势。其中，在信息保障方面的职责包括阻止外国敌对势力获取敏感或涉及国家安全的信息；在信号情报方面的职责包括收集、信息处理，以实现国外收集情报和反间谍的目的，并支持军事行动。该局也在美国法律和保护公民隐私与自由的条件下，支持针对恐怖分子及其组织的网络空间战。

早在 1981 年 12 月，12333 号总统令就对 NSA 的角色和职责进行了阐述，即收集、处理、分析、产生和传播关于对外情报和反情报的信号情报信息和数据，以支持国家和部门任务，承担国家安全系统（NSS）的管理者角色，制定关于信号情报和通信安全材料的安全规定。其现任领导人是迈克尔·S. 罗杰斯（Michael S. Rogers）。

NSA 下设国家计算机安全中心和系统与网络攻击中心。

国家计算机安全中心（NCSC）能评估用于高度安全方面的计算机的安全性，以确保设备处理机密或者其他敏感材料的时候使用可信的计算机系统和元件。NCSC 于 1981 年建立，当时它是防御计算机安全中的一个部门，并于 1985 年改名为 NSA-NCSC。NSA-NCSC 与工

业、教育和政府机构人员合作以促进信息安全系统开发的研究和标准化。NSA-NCSC 的教育功能主要体现在通过每年组织国家信息系统安全会议等活动宣传计算机安全方面的信息。NSA-NCSC 的计算机评估程序（可信产品评估程序）是由另一个 NSA 组织设计的，它是一套完整的安全相关标准测试商业产品。1983 年，NSA-NCSC 发行了第一个 DoD 可信计算机系统评估标准，被看作橘皮书的这份文件在 1985 年作为一个 DoD 标准重新发行，它包含了定期提供制定安全相关标准的目标（这些标准包括相关产品特征），还提供了关于评价多种用于处理敏感材料的产品 DoD 组件，该组件可对可信等级进行测量。

系统与网络攻击中心（SNAC）的目标是保护计算机网络免遭入侵，为此它出版全面的配置指南，修改可能被蠕虫病毒利用以侵入计算机系统的默认许可证及密码，并且移除存在潜在威胁的外来数据包。

中央安全署（CSS）成立于 1972 年，负责 NSA 和军方密码方面的合作，是美国所有情报部门的中枢、美国情报界（Intelligence Community，IC）中的核心机构，具有最高密级。CSS 的最高军事长官是 NSA 局长兼 CSS 局长及美国网络空间战司令部司令，NSA 副局长是 CSS 的最高行政长官。

1.1.3　国家安全系统委员会

国家安全系统委员会（CNSS）于 1953 年成立，前身是国家通信安全委员会（USCSB），1990 年依据国家安全第 42 号总统令（NSD-42）作为国家安全通信和信息系统安全委员会（NSTISSC），由 NSA 局长负责领导。2001 年 10 月遵循 E. O. 13231 更名为 CNSS。

CNSS 主要由委员会、子委员会、专家组和不同工作组组成。其中，委员会由 21 个政府执行部门（包括 CIA、DIA、DoD 等）和局的代表及来自 14 个组织的观察员组成，由 DoD CIO 主持工作，负责国家安全系统（NSS）的保护工作，包括制定 NSD-42 所需的运营政策、流程、指南、指令、机构和标准；子委员会由 CNSS 的成员和观察机构的代表组成，负责为委员会提供意见，监督专家组和各工作组的工作；专家组主要为子委员会提供支持，负责协调和监督 CNSS 各工作组之间的工作，并向子委员会汇报；各工作组依据问题而成立，主要由来自 CNSS 成员机构的专家和代表组成，负责指导 NSS 的保护工作和制定 NSS 的最初需求和能力。

CNSS 的职责是为美国政府各个部门和局之间商讨信息保障政策提供一个论坛，设立国家级的信息保障政策、指令、指南、操作规程，并为美国政府执行部门和局提供咨询。CNSS 的目标是保障 NSS 的安全，避免技术开发导致的安全问题。CNSS 主要通过提供可靠而持续的风险和脆弱性评估并实施有效的反制措施，为美国政府内部提供基础技术支持，为私有部门提供所需的基础技术支持，保证 NSS 能够获得所需要的信息系统安全产品。

当今不断变化和日益复杂的网络空间环境使来自网络空间的威胁越来越大，使 CNSS 在 CNSS 成员及在工业界、学术界和国外合作伙伴之间不断提出网络安全日益紧密和持续的协调需求。CNSS 自成立以来，在人员培训、人员培训标准、产品使用、产品管理、卫星及空间系统防护、网络安全防护、密码设备防护、通信安全防护等领域共发布了 70 多项政策、指令和指南性文件，推动了在联邦 NSS、联邦非 NSS 和非联邦体系之间的网络空间安全合作，是美国各机构间信息安全保障合作努力的基石。

1.1.4　网络空间安全和通信办公室

网络空间安全和通信办公室（CS&C）隶属于 DHS 的国家保护和计划理事会（NPPD），负责提升国家网络空间和通信基础设施的安全性、容灾能力和可靠性。CS&C 主动与公共、私有及国际伙伴合作，为可能导致这些战略性资产损失的灾难事件做必要准备，阻止灾难事件发生并在发生灾难时提供应急响应。CS&C 负责协调编写国家级的应急报告，该报告与《国家应急框架》（NRF，旨在全国范围内指导应对自然灾害、恐怖分子攻击及其他破坏性的事件）兼容。

美国国会于 2006 年批准设立 CS&C，并在其下设三个子部门：国家通信系统（NCS）、国家网络空间安全司（NCSD）和应急通信办公室（OEC）。2012 年 10 月，DHS 对 CS&C 做出调整：原 NCSD 下的联邦网络空间安全单元成为独立机构，并按其职能分别成立联邦网络空间弹性恢复司（FNR）和网络空间安全调度司（NSD）。其中，FNR 负责监控《联邦信息安全管理法案》（FISMA）的执行情况，与民用机构合作开发和配置网络空间安全的性能和标准，制定网络空间安全的方案，以及使用自动化工具在联邦网络上审计和测试。NSD 负责支持国家网络空间安全保护体系（NCPS），以增强联邦政府部门及合作者的网络空间安全。NCCIC 整合了多个已有的部门，如原 NCSD 下的 US-CERT、控制系统安全计划（CSSP）、NCC 等，负责执行爱因斯坦 3A 计划。NCCIC 整合了国家网络空间安全中心（NCSC）的工作，在 DHS 的一些执行单元、一些联邦部门、州和地方部门及一些私营部门之间进行信息协调。作为这些部门的信息集成和应急响应中心，NCCIC 提供对网络数据、威胁、脆弱性等的分析和实时的监控、信息共享、应急响应。新成立的网络基础设施恢复能力参与方协调司（SECIR）负责与私营部门合作，参与协调整个国家的安全和应急准备工作。OEC 在原有工作的基础上增加了原 NCS 的职责，负责为增强应急通信能力提供支持，如提供培训和技术支持等，以及协调部门的应急响应活动和增强互操作性。

1.1.5　信息安全监督办公室

信息安全监督办公室（ISOO）成立于 1978 年，是 NARA 的一部分，接受国家安全理事会的政策和计划指导。ISOO 确保政府和行业的发展与应用，保持其风险框架的完整性，平衡国家安全相关信息的公开、共享与保护之间的关系。ISOO 依照 13526 号总统令和 12829 号总统令修正案，监督政府和工业的安全保密计划，同时收集与各部门的安全涉密计划相关的统计数据（包括核算涉密活动所需的成本），进行分析并就其状态每年向总统汇报。ISOO 共监管大约 65 个执行分支部门、独立机构和办公室，以及他们的主要组成机构。除了监管各部门的安全教育与培训计划外，ISOO 还承担政府和行业界的部分安全教育工作。

ISOO 下设三个工作组：保密管理工作组（The Classification Management Staff）、业务工作组（The Operations Staff）和可控非涉密信息工作组（Controlled Unclassified Information Office）。其中，保密管理工作组负责制定用于定密、取消定密及保护政府和行业部门发布的国家安全信息的安全保密政策；业务工作组负责评估政府和行业的安全保密计划的有效性；可控非涉密信息工作组负责制定标准的非涉密信息的政策和规程，通过有效的数据访问控制措施合理地保护敏感信息。除此之外，ISOO 还下设多个计划和职能小组，包括跨部门安全等级上诉委员会（ISCAP）、州、地方、部族和私营部门（SLTPS）政策咨询委员

会（SLTPS-PAC）、国家行业安全计划（NISP）、NISP 政策咨询委员会（NISPPAC）、定密管理工作组（CMWG）。

1.1.6　信息共享和保护机构

2011 年，奥巴马发布了第 13587 号总统令《促进涉密网络安全和责任共享以及保护涉密信息的结构改革》。该总统令在强调信息共享的基础之上，在国家层面建立体系化的机构和协调措施来保证信息的共享和保护。依照该总统令，美国还将在涉密信息保护和共享方面建立一系列机构，包括高级信息共享和保护指导委员会、涉密信息共享和保护办公室、网络中涉密信息保护执行代理、内部威胁专责小组。[①]

这四类机构是美国在吸取“9·11”事件和“维基解密”事件的教训之后做出的重大举措，是美国近年来在保密监管问题上“共享和保护”理念的具体实施。这些措施是美国政府为未来实施进一步保密管理改革所作的组织准备和保障。

1）高级信息共享和保护指导委员会（Senior Information Sharing and Safeguarding Steering Committee）的责任与义务是关于网络中共享和保护涉密信息的政策与标准的跨部门的制定与实施。高级信息共享和保护指导委员会由 OMB 和 NSA 的高级代表主持，成员包括由 DoS、DoD、DoJ、能源部（DoE）、DHS、ODNI、CIA、ISOO 和其他机构的主管任命的美国政府官员。

2）涉密信息共享保护办公室（CISSO）是信息共享环境项目管理（PM-ISE）办公室的下属机构，对涉密网络安全和责任共享及保护涉密信息提供专业的、全时的、持续的关注。涉密信息共享保护办公室的工作人员包括来自高级信息共享和保护指导委员会的代表机构的官员。

3）网络中涉密信息和保护执行代理（Executive Agent for Safeguarding Classified Information on Computer Networks）由 DoD 部长和 NSA 主任共同担任，行使现有的 NSS 的执行代理和主任的职能。除此之外，网络中涉密信息保护执行代理的职责还包括：

① 与 CNSS 协调制定有效的技术保护政策和标准，保护 NSS 及其中的涉密信息。

② 把任何未解决的问题送交高级信息共享和保护指导委员会，并参考该委员会发布技术政策和标准。

③ 至少每年向高级信息共享和保护指导委员会汇报 CNSS 的工作，包括改进工作的时效性和有效性的必要变动的建议。

④ 独立评估与已有保护政策和标准的一致性，并把评估结果向高级信息共享和保护指导委员会报告。

4）内部威胁专责小组（ITTF）负责制定政府范围内的内部威胁计划以检测和缓解内部威胁，包括保护涉密信息的利用、泄漏和其他未授权的暴露，计划需要考虑风险等级和独立机构的不同的需求、使命、系统。计划的内容应该包括制定建立综合安全系统的政策宗旨和优先级、反间谍活动、用户审核和监控及其他机构内部的保护措施。内部威胁专责小组的联合主席应该由 DoJ 部长和 DNI 共同担任，成员应该包括由 DoS、DoD、DoJ、DoE、DHS、ODNI、CIA、ISOO 和其他可能的部门主任指定的美国政府官员，其员工应该是来自联邦调查局（FBI）、国家反间谍办公室（ONCIX）和其他联合主席指定的法律允许的机构和个人。

① 该总统令发布之后立即开始执行，至今，这四个机构应该都已经建成，但由于涉密较深，很难找到公开的研究资料。

在法律允许的范围内，ONCIX 应该对内部威胁专责小组提供工作地点和管理支持。

1.1.7　网络空间战司令部

美国 DoD 于 2009 年 6 月 23 日宣布成立网络空间战司令部（USCYBERCOM），隶属国家战略司令部（USSTRATCOM）。陆军、海军、空军和海岸警备队均设有各自的网络空间战司令部。网络空间战司令部由原网络攻击部队和网络防御部合并而成，2010 年 10 月开始全面运作，总部位于马里兰州米德堡陆军基地。美国为网络空间战司令部投入了大笔资金，其中 2013 年经费预算 34 亿美元，2013～2017 年共计 180 亿美元。网络空间战司令部编配了 464 名现役军人和 476 名文职人员，其现任司令是海军上将迈克尔·S. 罗杰斯。

网络空间战司令部负责领导国防部信息网络的行动和防卫工作；执行全面的军事网络空间行动，以确保美国和盟友在网络空间上的活动自由，并阻止敌方的相同行动；具体指挥美军的“黑客”部队。据悉，这支部队具备摧毁敌方网络、进入敌方计算机窃取或伪造数据的作战能力，他们可以释放蠕虫病毒致瘫敌方的指挥和控制系统，使敌方无法指挥地面部队或发射地对空导弹。同时，该部队还能保护美国国防部的所有网络免受攻击。为了强化美军网络空间战部队的行动能力，美军每年进行一次被称作“网络空间防御”项目的演习，以研究美军网络空间安全可能存在的漏洞。

1.1.8　美国的情报机构

1981 年，里根政府签署了第 12333 号总统令，对美国情报界的职责进行了明确的界定，后期几届政府也分别对美国的情报界进行了调整。根据第 12333 号总统令，美国的情报界具有六大目标：为美国总统、国家情报委员会（National Intelligence Council，NIC）、DoS、DoD 及其他行政部门官员所在职责范围内提供情报服务；产生并传播情报；收集有关外国势力、组织、个人及其代理人所施行的针对美国的国际恐怖活动、贩毒活动和其他破坏活动等相关信息，并开展相关的保护活动；特殊行动；管理并支持美国在境内和境外的活动，保证美国授权活动的圆满完成；完成美国总统提出的其他情报相关任务。

事实上，美国情报界的工作并不是完全保密的，需要接受美国行政与立法机构的监督。其中，主要的行政监督部门有总统的对外情报顾问委员会（PIAB）、联合情报体系委员会（JICC）、总监察长办公室（OIG）、OMB；主要的国会监督部门有众议院特别情报委员会和参议院情报委员会。

最初美国的情报机构主要由中央情报总监（通常是 CIA 局长）负责统一协调美国的情报工作。“9·11”事件以后，美国为适应新的反恐形势，设立了国家情报总监（DNI）一职，作为美国情报界的总负责人，其所在机构是美国国家情报总监办公室（ODNI）。ODNI 负责协调其他情报机构的工作，施行国家情报计划。DNI 直接受美国总统的任命和领导，是美国总统和 NSC 在国家安全情报问题上的首席顾问。现任的 DNI 是丹尼斯·C. 布莱尔（Dennis C. Blair）。

美国的情报机构涉及七个独立的机构共 16 个部门，分别是中央情报局（CIA）、国防部（DoD）、能源部（DoE）、国土安全部（DHS）、司法部（DoJ）、国务院（DoS）、财政部（DoT）。其中，CIA 是美国最大的，同时也是唯一一个独立的情报机构，主要负责收集和分析国内外政府、企业和个人的信息；DoD 是包含情报机构最多的一个部门，共有八个，分别是空军情报

监视及侦察局（AF ISRA）、陆军军事情报队（MI）、国防情报局（DIA）、海军陆战队情报部（MCIA）、国家地理空间情报局（NGA）、国家侦察局（NRO）、国家安全局（NSA）和海军情报办公室（ONI）；DoE 下设有情报及反情报办公室（OICI）；DHS 下设情报分析办公室（I&A）和海岸警卫队调查处（CGIS）两个部门；DoJ 下设著名的 FBI 和美国缉毒局/国家安全情报办公室（DEA/ONSI）两个机构；DoS 下设情报研究局（INR）；DoT 下设恐怖主义及金融情报办公室（TFI）。

美国情报体系的组织结构如图 1-2 所示（各机构详细介绍见附录 11）。

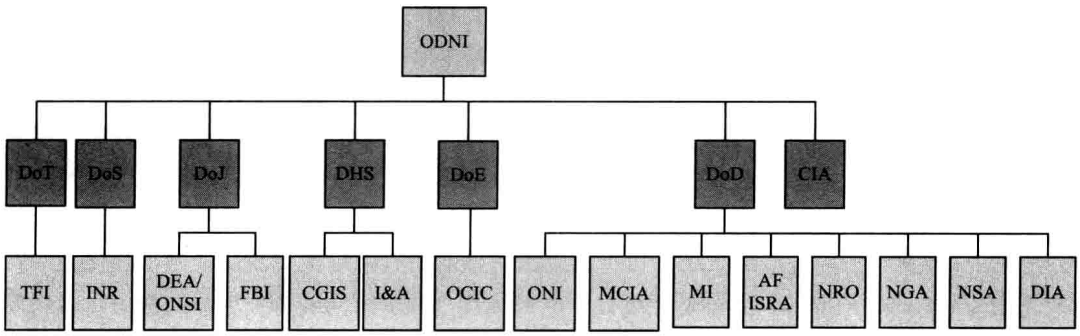

图 1-2　美国情报体系组织结构

1.1.9　产学研机构

美国的产学研合作模式产生于 20 世纪 50 年代，是世界上最早进行产学研相结合的国家之一。作为世界上科技最发达的国家，美国拥有世界上最多、最先进的网络空间安全的科研教育机构，且机构种类繁多、分工明确；不仅具有管理机构，还有资助、监督和咨询机构。例如，由 NSTC 下的技术委员会组织《NITRD 计划》负责协调联邦政府在计算机和网络空间安全方面的研究和开发（R&D）活动；商务部（DoC）下属的国家标准和技术研究院（NIST）负责通过美国的《国家网络空间安全教育（NICE）计划》整体协调和规划美国网络空间安全教育活动；NIST、国家科学基金会（NSF）、国防高级研究计划局（DARPA）、DoE、DHS 等都对网络空间安全的科研和教育工作提供资金资助。此外，美国联邦政府中几乎在所有从事科研的机构中都设立了专门的技术转让办公室或单独的部门，专门负责科研成果的技术转让工作。详情参见第 6 章和第 7 章。

到目前为止，美国已经形成了以政府部门为主，以企业、高校、非营利机构等为辅，利用各机构的优势资源进行优势互补的局面，构建了体系较为健全的产学研协同创新模式，从而促进了美国经济的快速发展。美国网络空间安全领域的产学研协同创新机制将在 1.3 节中进行介绍。

1.2　美国国家网络空间安全管理协调机制

虽然美国拥有庞大的网络空间安全管理机构，但奥巴马认为：美国的网络空间安全管理权力较为分散，没有一个统一的部门负责制定网络空间安全政策，没有一个委员会去监控网络空间安全威胁等级和范围，需要建立一个能够统一协调所有网络空间安全政策和行

试读结束：需要全本请在线购买：　www.ertongbook.com