国内外互联网研究系列丛书

美国国家网络安全战略研究

Information Studies Institute

程工 孙小宁 张丽 石瑾 / 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

国内外互联网研究系列丛书

美国国家网络安全战略研究

程 工 孙小宁 张 丽 石 瑾 编著

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

内 容 简 介

随着各国在互联网安全领域的交流与对话日益深入，制定网络安全的国家安全战略，对于有效调动协调各方力量，更好地保护国家利益，显得至关重要。作为互联网大国，美国拥有最先进的互联网技术，同时也面临着来自网络的严峻威胁与挑战，因此一直以来美国对于互联网安全给予了高度重视。本书通过重点研究美国近年来的网络安全战略走向，分析美国网络安全战略的制定与不断演进过程中的有益经验与做法，希望为我国制定国家层面的网络安全战略提供借鉴和参考。

本书理论与实际相结合，对于各级党政机关和企业开展网络舆情的监测和分析工作，充分发挥其在信息决策中的作用，具有重要的参考意义。也可供网络舆情研究领域的各类学术机构的工作人员和学生阅读参考。

图书在版编目（CIP）数据

美国国家网络安全战略研究 / 程工等编著. —北京：电子工业出版社，2015.11
（国内外互联网研究系列丛书）
ISBN 978-7-121-27472-5

Ⅰ. ①美… Ⅱ. ①程… Ⅲ. ①计算机网络－国家安全－国家战略－研究－美国 Ⅳ. ①D771.235 ②TP393.08

中国版本图书馆 CIP 数据核字（2015）第 258099 号

责任编辑：徐蔷薇　　特约编辑：王　纲
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
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：787×1092　1/16　　印张：16.5　字数：412 千字
版　　次：2015 年 11 月第 1 版
印　　次：2015 年 11 月第 1 次印刷
定　　价：49.00 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。

前　言

2015 年 7 月 6 日，《网络安全法》（草案）经十二届全国人大常委会第十五次会议初次审议后，正式全文发布并向全社会公开征求意见。这是我国网络安全工作的一件大事，彰显了国家对于网络安全问题的高度重视，同时也标志着网络安全被提升到国家安全与发展层面，为建设“网络强国”的战略部署提供了法律支撑和保障。事实上，各国政府对于网络攻击的威胁，对于网络关键基础设施的保护，对于统筹国家和民间力量，从宏观和微观两个层面建设本国的网络安全体系框架，早已有了共识。至少有 41 个国家颁布了各种形式的网络空间安全的国家战略，旨在加强本国网络安全方面的攻防能力。而其中，作为世界上互联网最发达的国家，同时也是走在网络安全技术最前沿的国家，美国对于网络安全的重视程度，也是各国之中最为突出的。从 20 世纪 80 年代起，至 2015 年 6 月底，美国以战略、计划、总统令等多种形式，先后颁布了 40 多份与网络安全相关的文件，构成了一个较为完备的网络安全战略体系。本书重点选取了克林顿、布什和奥巴马三位最近的美国总统执政期间推出的相关战略文件，对其战略的演变脉络以及相关举措进行了梳理和分析。

本书与 2014 年出版的《国外网络与信息安全战略研究》是姊妹篇，所有内容都围绕美国的网络安全战略体系，分为三章：第一章为美国网络安全战略分析，第二章为美国网络安全战略概要，第三章为美国网络安全战略译文。希望本书能够为关注网络安全战略问题的读者提供借鉴和参考。

编　者

2015 年 7 月

目　录

第一章　美国网络安全战略分析

美国政府历年重要网络与信息安全文件概述

作为世界上互联网最发达的国家之一，美国对互联网的应用程度和依赖程度远高于大多数国家，因而面临更大的网络和信息安全威胁。20 世纪 80 年代以来，美国政府对网络安全的重视程度不断提升，并视之为国家安全的重要组成部分。截至 2015 年，美国先后颁布了 40 多份与网络安全有关的文件，形式包括战略、计划、行政令、总统令等。本书重点研究克林顿、布什和奥巴马三届美国总统执政期间所推出的与网络和信息安全相关的战略文件。

一、克林顿政府时代（1992—2001 年）

美国的网络安全政策产生于克林顿政府时期保护关键基础设施的行动。克林顿总统在 1996 年签发了第 13010 号行政命令，创立了总统关键基础设施保护委员会，并强调了网络攻击对国家的经济和国防安全的威胁。在该委员会的建议下，克林顿总统在 1998 年 5 月签发了第 63 号总统决策令。

（一）第 63 号总统决策令：《克林顿政府对关键基础设施保护的政策》（Presidential Decision Directive 63：The Clinton Administration's Policy on Critical Infrastructure Protection）

1998 年 5 月 22 日，克林顿政府发布了第 63 号总统决策令（PDD63）：《克林顿政府对关键基础设施保护的政策》，第一次就美国信息安全的概念、意义、长期与短期目标等做出了明确的说明，并针对下一步的行动做了指示。克林顿政府在 PDD63 中指出，“我们的经济越来越依靠那些相互依赖的、由计算机和网络支持的基础设施，对我们的基础设施和信息系统的非常规攻击有可能使我们的军事和经济力量遭到巨大伤害。”

PDD63 提出，最迟不晚于 2000 年，美国应当实现初步的信息保障能力。PDD63 要求从总统令发布之日起，五年后美国将获得并保持对国家的关键基础设施进行保护的能力，以防止可能严重危害到下述职能的有预谋的行为：联邦政府履行其重要的国家安全责任并确保公众健康和安全；州和地方政府维持有序运转，提供最起码的重要公共服务；民营部门确保经济有序运行以及重要电信、能源、金融和运输服务的正常提供。这些关键职能遭到的任何破坏或操纵必须控制在短时、低频、可控、地域上可隔离且对美国的利益损害最小的规模。

（二）《信息系统保护国家计划（V1.0）》（National Plan for Information Systems Protection Version 1.0）

2000 年 1 月 5 日，克林顿政府发布了《信息系统保护国家计划（V1.0）》，提出了美国政府在 21 世纪之初若干年的网络空间安全发展规划。克林顿表示，“信息系统保护国家计划是一系列更为复杂的工作的第一步。随着我们对正在出现的威胁和脆弱性的认识不断深入，我们的计算机保护计划将持续发展和更新。它向我们展示了一个综合的方案，为我们的经济、国家安全、公共健康和安全中的关键部门提供了保护措施。为成功实施这个计划，政府和私人业主必须齐心协力，建立一种前所未有的合作关系。只有举国上下团结应战，我们才能达到我们的目标。我们不能指望只依赖政府法令来实现我们的目标，每个部门必须自己决定保护其关键系统所必需的方法、步骤和标准。作为合作关系中的一方，联邦政府随时准备提供帮助。”

（三）《全球时代的国家安全战略》（A National Security Strategy For A Global Age）

2000 年 12 月 1 日，克林顿总统签署了《全球时代的国家安全战略》。签署该文件是美国国家信息与网络安全政策的重大事件。文件将信息安全与网络安全列入国家安全战略，成为国家安全战略的重要组成部分。这标志着网络安全正式进入了国家安全战略框架，并具有了独立地位。

二、布什政府时代（2001—2009 年）

布什总统上台不久，美国便发生了举世瞩目的“9 • 11”事件，布什政府深刻认识到反恐必须切实加强对国家关键基础设施与资产的保护。因此，布什执政期间对关键基础设施保护的重视程度达到了空前的高度，出台了一系列相关战略文件。此外，分别于 2003 年和 2008 年出台的两份重要文件：《确保网络空间安全的国家战略》和《国家网络安全综合计划》（CNCI），强调了发展保卫国家网络安全的能力。

（一）第 13231 号行政令：《信息时代的关键基础设施保护》（Executive Order 13231：Critical Infrastructure Protection in the Information Age）

2001 年 10 月 16 日，布什政府意识到了“9 • 11”事件之后信息安全的严峻性，发布了第 13231 号行政令：《信息时代的关键基础设施保护》，宣布成立“总统关键基础设施保护委员会”（PCIPB），代表政府全面负责国家的网络空间安全工作。委员会成立以后，为制定布什政府的国家网络空间安全战略，2002 年 3 月 20 日向美国民众公布了国家战略中可能会涉及的 53 个重点问题并广泛听取了国民的意见和建议。2002 年 9 月 18 日，“9 • 11”事件一周年纪念日之后，在整理国民对 53 个问题的反馈意见的基础上，发布了《确保网络空间安全的国家战略》（草案）。

（二）《确保网络空间安全的国家战略》（The National Strategy to Secure Cyberspace）

2003 年 2 月 14 日，美国公布了《确保网络空间安全的国家战略》（正式版）。该战略是

布什政府对《美国国土安全的国家战略》（2002 年 7 月公布）的补充，并以《保护至关重要的基础设施和关键资产的国家战略》（2003 年 2 月 14 日公布）作为其补充文件。该战略明确界定了关键基础设施，是指“那些维持经济和政府最低限度的运作所需要的物理和网络系统，包括信息和通信系统、能源、银行与金融、交通运输、水利系统、应急服务、公共安全等部门以及保证联邦、州和地方政府连续运作的领导机构”。

该战略确定了在网络安全方面的三项总体战略目标和五项具体的优先目标。发生网络攻击时，使损害程度最小化、恢复时间最短化。五项优先目标如下。

（1）建立国家网络安全响应系统。

（2）建立一个减少网络安全威胁和脆弱性的国家项目。

（3）建立一个网络安全预警和培训的国家项目。

（4）确保政府各部门的网络安全。

（5）国家安全与国际网络安全合作。

（三）《关键基础设施和重要资产物理保护国家战略》（The National Stategy for The Physical Protection of Critical Infrastructures and Key Assets）

2003 年 2 月 14 日，美国发布了《关键基础设施和重要资产物理保护国家战略》，标志着美国从国家安全的高度全面推行关键基础设施与资产保护计划。该战略将美国的关键基础设施分为 11 项，包括：农业与食品、水、公共卫生、应急服务、国防工业基地、通信、能源、交通运输、金融、化学工业与有害物质、邮政与货运。关键资产则包括核电站、水坝、有害物质存储设备，以及代表国家形象的肖像、纪念馆、政府与商务中心等。

（四）《网络空间安全：迫在眉睫的危机》（Cyber Security: A Crisis of Prioritization）

2005 年 4 月 14 日，美国政府公布了美国总统 IT 咨询委员会 2 月 14 日向总统布什提交的《网络空间安全：迫在眉睫的危机》紧急报告，该报告对美国 2003 年的信息安全战略提出了不同看法，指出过去十年里美国保护国家信息技术基础建设工作是失败的，短期弥补修复不能解决根本问题。全球信息栅格（GIG）耗资 1000 亿美元，仍然漏洞百出，没有解决安全问题。该报告提出了以下问题和建议。

（1）政府对民间网络空间安全研究的资助不足，建议每年向美国国家科学基金会（NSF）增加 9000 万美元的预算支出；

（2）网络空间安全基础性研究团体规模小，建议用七年时间将团体规模扩大一倍；

（3）安全研究成果的成功转化不够，政府应加强在技术转让方面与企业的合作；

（4）政府部门间协作与监管缺乏是安全对策无重点和无效率的根源，建议成立“重要信息基础设施保护的跨部门工作组”。

（五）《国家网络安全综合计划》（The Comprehensive National Cybersecurity Initiative，CNCI）

2008 年 1 月 8 日，美国总统布什签署发布了第 54 号国家安全总统令暨第 23 号国土安全总统令（NSPD54/HSPD2），要求保护美国的网络安全，防止美国遭受敌对的电子攻击，

并能对敌方展开在线攻击。

在布什签署该项总统令后，美国有关部门制定了《国家网络安全综合计划》（CNCI）。该计划的预算至今未公布，据《纽约时报》估计有 400 亿美元，而《华盛顿邮报》声称是数十亿美元。由于是密令，其一直对外保密。2010 年 3 月 20 日，经多方呼吁，美国总统奥巴马高调宣布解密其部分内容，旨在提高透明度以争取民心。部分解密的内容显示，CNCI 有三个重要目标。

（1）通过在联邦政府（最终将在州、地方和部族政府以及民营领域合作者）内部创建和加强对网络漏洞、威胁和事件的共享态势感知能力和对减少当前漏洞和防止入侵的快速反应能力，进而建立一个防御前线以抵御当前面临的迫切威胁。

（2）通过加强美国的反情报能力和增进关键信息技术供应链的安全，进而实现应对全方位威胁的防御能力。

（3）通过扩大网络教育、全面协调和重新定位联邦政府内的研发工作、致力于明确和制定相关战略以阻止敌对和恶意的网络空间行动等措施，进而巩固未来的网络空间环境安全。

（六）《提交第 44 届总统的保护网络空间安全的报告》（Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency）

2008 年 12 月，布什政府成立的“第 44 届总统网络空间安全委员会”经过一年半的工作，形成了《提交第 44 届总统的保护网络空间安全的报告》。随着任期将满，第 43 届美国总统布什希望下一届总统能够解决网络信息安全问题。报告提出网络安全是美国在竞争更加激烈的新国际环境中面临的最大安全挑战之一。报告认为，过去 20 年来，美国一直在努力设计一种战略来应对这些新型威胁并保护自身利益，但始终都不算成功。无效的网络安全以及信息基础设施在激烈竞争中受到攻击，削弱了美国的力量，使国家处于风险之中。该报告建议，在布什时期的网络安全战略基础之上建立一个包括外交、情报、军事、经济的综合性网络安全战略。

报告提出了 12 项、25 条建议，分别从制定战略、设立部门、制定法律法规、身份管理、技术研发等方面进行了阐述。报告指出，网络不仅是一种企业资产，还应作为一种武装系统加以保护，如同国家其他的关键基础设施那样受到保护。针对当前和未来可能的网络攻击，报告重点提出了“设计、运行和保护网络”，确保联合作战的需求。

三、奥巴马政府时代（2009 年至今）

奥巴马在竞选期间就一直强调网络安全对美国的重要性。2009 年 2 月，他在就职后不久即要求对美国的网络安全状况展开为期 60 天的全面评估，检查联邦政府部门保护机密信息和数据的措施。此后，奥巴马政府将制定网络空间战略列为重中之重，先后出台了《网络空间可信身份国家战略》、《网络空间国际战略》、《网络空间行动战略》、《国土安全相关实体网络安全战略》、《网络安全框架》等一系列重要战略文件，构建了一个包含网络安全、网络经济、网络监控、网络自由、网络威慑等在内的全方位战略体系，从战略层面确立美国在网络空间的主导地位，帮助美国实现制网权。

（一）《国家网络安全战略：需要进行的关键改进》（National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture）

2009 年 3 月 10 日，美国联邦审计署发布了《国家网络安全战略：需要进行的关键改进》报告，对需要进一步加强的网络安全关键领域和改进美国国家网络安全战略提出了建议。报告要求采取积极措施，进一步加强五个领域的网络安全，即支持网络分析和预警能力，完成网络安全实践提出的行动，增强基础设施控制系统的网络安全性，加强国土安全部对网络攻击的恢复能力，解决网络犯罪问题。

（二）《网络空间政策评估：保障可信和强健的信息和通信基础设施》（Cyberspace Policy Review：Assuring a Trusted and Resilient Information and Communications Infrastructure）

2009 年 5 月 29 日，奥巴马总统公布了由安全部门官员起草的题为《网络空间政策评估：保障可信和强健的信息和通信基础设施》的报告。报告认为美国的数字基础设施主要建立在互联网基础上，目前并不安全，现状“不可接受”，来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一。报告共 76 页，正文包括 6 章，分别如下。

（1）加强顶层领导。通过以下事项来加强对网络空间安全的领导：设立总统网络空间安全政策官及支撑机构，审查法律和政策，加强联邦对网络空间安全的领导。

（2）建立数字国家。提升公众的网络安全意识；加强网络安全教育，扩大联邦信息技术队伍，使网络安全成为各级政府领导人的一种责任。

（3）共担网络安全责任。改进民营部门和政府的合作关系，评估公私合作中存在的潜在障碍，与国际社会有效合作。

（4）建立有效的信息共享和应急响应机制。建立事件响应框架，加强事件响应方面的信息共享，提高所有基础设施的安全性。

（5）鼓励创新。通过创新来解决网络空间安全问题；制定全面、协调并面向新一代技术的研发框架，建立国家的身份管理战略；将全球化政策与供应链安全综合考虑；保持国家安全暨应急战备能力。

（6）行动计划。提出了近期行动计划 10 项和中期行动计划 14 项。

（三）《网络空间可信身份国家战略——增强在线选择、效率、安全与隐私保护》（National Strategy for Trusted Identities in Cyberspace——Enhancing Online Choice, Efficiency, Security and Privacy, NSTIC）

2011 年 4 月 15 日，美国白宫发布了《网络空间可信身份国家战略——增强在线选择、效率、安全与隐私保护》（NSTIC），旨在通过政府和企业的共同努力，建立一个以用户为中心的身份生态系统，促使个人和组织遵循协商一致的标准和流程来鉴别和认证数字身份，从而实现相互信任。计划用 10 年左右的时间，构建一个网络身份生态体系，推动个人和组织在网络上使用安全、高效、易用的身份解决方案。为此，美国成立了专门的主管办公室（NPO），负责协调政府和私人部门的活动，并牵头制定实施路线图。NSTIC 将是美国信息高速公路建设后，又一项涉及全球的巨大信息技术工程，美国政府希望借此再次引领世界经济新潮流，

占领未来全球经济的制高点。

（四）《网络空间国际战略——互连世界的繁荣、安全与开放》（International Strategy for Cyberspace——Prosperity, Security and Openness in a Networked World）

2011 年 5 月 16 日，美国联邦政府六大部门——白宫、国务院、司法部、商务部、国土安全局和国防部共同宣布了《网络空间国际战略——互连世界的繁荣、安全与开放》。奥巴马总统在前言当中指出，这是美国第一次针对网络空间设定全盘计划，并且结合政府部门与民间，以及国际盟友来共同实施。战略宣称要建立一个“开放、互通、安全和可靠”的网络空间，并为实现这一构想勾勒出了政策路线图，内容涵盖经济、国防、执法和外交等多个领域，“基本概括了美国所追求的目标”。

该战略列出了七个政策重点：通过制定国际标准、鼓励创新和开放市场，加强知识产权保护；确保网络的安全、可靠和韧性；深化执法合作并积极推出国际规则；强化“网军”以应对 21 世纪的安全挑战；建立有效且多方参与的国际互联网治理架构；展开“网络援外”；保障互联网自由。战略中还提出了网络空间十大“基本原则”，即维护基本自由、尊重知识产权、重视隐私、打击犯罪、维护自卫权、确保网络全球互通、确保网络稳定、确保人人能上网、多方参与的互联网治理，以及给予网络安全应有的重视。

（五）《网络空间行动战略》（Department of Defense Strategy for Operating in Cyberspace）

2011 年 7 月 14 日，美国国防部发布了首份《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。根据美国国防部网站公开的部分文件内容，该战略包括五大支柱。

（1）将网络空间作为与陆、海、空、外太空并列的“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。

（2）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。

（3）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。

（4）加强与美国的盟友及伙伴在网络空间领域的国际合作。

（5）重视高科技人才队伍建设并提升技术创新能力。

（六）《可信网络空间：联邦网络安全研究与发展项目战略计划》（Trustworthy Cyberspace: Strategic Plan for The Federal Cybersecurity Research and Development Program）

2011 年 12 月 6 日，美国白宫发布了路线图，公布了网络安全的研究与发展重点，以确保美国网络基础设施的安全，并改变人们处理网络安全问题的方式。美国首席技术官安尼什·乔普拉与白宫网络安全负责人霍华德·施密特发表博文称，《可信网络空间：联邦网络安全研究与发展项目战略计划》源于 2009 年年初美国总统奥巴马下令开展的一次为期 60 天的国家网络安全状态评估。该评估报告呼吁政府采取紧急行动，以确保美国计算机网络基础

设施的安全。为响应此号召，美国白宫科学和技术政策办公室制订了该研究与发展计划，旨在帮助美国应对网络安全的挑战，并更有效地保护网络空间的安全。

经过全面评估以及公共与民营部门网络安全专家的论证，该计划确定了保护美国网络基础设施的四个战略重点。

（1）运用“改变游戏规则（game-changing）”的思维来理解网络安全目前的缺陷根源，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“动态目标”，使黑客难以渗透到计算机网络。静态、链式的网络更容易招致攻击，因为黑客有更多的时间来计划并执行攻击。

（2）像所有科学实践一样，为网络安全构建科学基础，诸如法律、假设检验、重复实验设计、数据收集方法与指标标准化、常用术语等。

（3）与研究机构合作，协调和整合相关技术，最大限度地发挥研究影响，确保网络安全的研究方向与研究机构的目标相一致。

（4）缩短网络安全从研究到投入实践阶段的时间。

（七）《实现能源输送系统网络安全路线图》（Roadmap to Achieve Energy Delivery Systems Cybersecurity）

2011 年 9 月 15 日，美国能源部发布了《实现能源输送系统网络安全路线图》，确定了 2020 年前美国能源输送系统网络安全目标，并给出了应对网络攻击的策略。这份路线图向拥有和控制重要能源基础设施的政府部门和民营企业提出了 5 项战略，呼吁它们精诚合作，为美国打造安全可靠和恢复力强的能源输送系统。

路线图要求：公共和私企的利益相关方应当对风险进行评估和监控，这样才能针对不断演进的网络威胁和漏洞做出快速响应。路线图要求能源领域继续改进安全，并确保公共和私有利益相关方的合作顺利进行。路线图还指出了实现这些目标可能遇到的障碍，其中包括：在能源行业里，技能熟练的工程师和工人不足；在能源输送系统安全风险方面的知识有限、理解不到位、评估不足；安全风险环境迅速变化。

（八）《确保未来网络安全的蓝图：国土安全相关实体网络安全战略》（Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise）

2011 年 12 月 12 日，美国国土安全部网站发表了 2011 年网络安全战略报告，题为《确保未来网络安全的蓝图：国土安全相关实体网络安全战略》。该报告在《四年国土安全评估报告》的基础上撰写，意图是呼吁保护对美国至关重要的关键基础设施，并在不久后开发出更强大的信息和通信技术，使政府、企业和个人更安全地使用互联网。

报告列出了两大行动领域：一是保护当前的关键信息基础设施，二是建设未来的网络生态系统。其中，保护关键信息基础设施的四项目标是：降低网络安全风险；快速应对网络安全事件，提高网络恢复能力；共享网络安全信息；增强网络抗压能力。加强网络生态系统建设的四项目标是：提高个人和组织安全使用网络的能力；研发和应用更可信的网络协议、产品、服务、配置和架构；构建合作型网络社区；建立透明的安全流程。

（九）《国家信息共享及保护战略》（National Strategy For Information Sharing and Safeguarding）

2012 年 12 月 19 日，美国白宫发布了《国家信息共享及保护战略》，允许政府部门间共享信息，建立政府机构间数据共享机制。此举有助于增强打击和防御国外黑客攻击及其他犯罪的能力。该战略的主要目标是：推进网络的互联互通和共享服务数据，通过体制改革以及政策技术方案的支持，建立安全机制。战略还强调网络安全保障不能侵犯公民的隐私和权利。

《国家信息共享及保护战略》全面概括地强调了数据共享的重要性。该战略指出，美国的国家安全在很大程度上取决于信息分享的天时、地利、人和。信息共享的管理工作，需要各联邦州政府、各地方、各民营部门以及国外合作伙伴间长期不懈的合作。此外，奥巴马政府将“信息”视为保障国家基础设施安全的重要“国家资产”，同时也强调保护情报和知识产权的重要性。

（十）第 13636 号行政令：《增强关键基础设施网络安全》（Executive Order 13636：Improving Critical Infrastructure Cybersecurity）

2013 年 2 月 12 日，美国总统奥巴马签署了名为《增强关键基础设施网络安全》的第 13636 号行政令，旨在保护国家基础设施免受网络攻击。该行政令的主要内容包括：在国家层面上，美国总统正式认定“信息战”会一直持续下去，是目前显而易见的威胁。政府将与民营部门合作建立“网络安全框架”（Cybersecurity Framework），实现网络攻击与威胁的信息共享，从而降低针对关键基础设施的网络安全风险。

行政令指出，网络安全基本框架将由美国国家标准与技术研究所（NIST）制定。该框架包含一套标准、方法、步骤、流程以及应对网络安全风险的非指定的技术手段。“网络安全框架”的建立有助于将现有的政府项目向民营部门扩展，从而让更多的民营部门的专家在一段时间内为政府服务。行政令中还规定了建立“网络安全框架”的具体时间表，以及“网络安全框架”对隐私状况的影响的评估报告。行政令呼吁政府和机构加强政策协调，实现更广泛的信息共享，但是该行政令并不具有和法律同等的效力，白宫期望能借此引入立法机制。

（十一）《网络安全框架》（Framework for Improving Critical Infrastructure Cybersecurity V1.0）

2014 年 2 月 12 日，美国政府公布了最新《网络安全框架》，用于协助关键基础设施经营者制定网络安全总体方案。该框架是根据一年前发布的第 13636 号行政令《增强关键基础设施网络安全》的要求制定的。该框架由美国企业与政府历时一年共同完成，由隶属于美国商务部的美国国家标准与技术研究所（NIST）发布。框架搜集了全球现有的标准与做法，采用了风险管理的方法，以便于各机构适应“不断变化的网络安全环境，并对变化中的复杂威胁及时做出响应”。企业可以利用该框架制定一个“可信的”网络安全方案。

《网络安全框架》包括三部分内容。

（1）核心。框架核心（Framework Core）描述了企业在确认网络安全风险、保护企业免遭攻击、如有事故发生开展检测、响应，并从可能造成的任何损害中恢复的整个过程中的高级活动。

（2）概况。框架概况（Framework Profiles）用来描述一个企业安全做法的现状。将一个企业的现状与目标相比，可以衡量该企业与其安全项目目标的差距。

（3）实施层级。框架实施层级（Framework Implementation Tiers）描述随着严密性的提升，具体的过程分为四级，从“部分（partial）”（1 级）到“适应（adaptive）”（4 级）。企业可以根据其商业目标、法律以及监管要求和其他限制条件，自行选择最适合的层级。

美国政府官员表示，他们希望该框架能推动改变企业处理网络安全的方式。虽然是否采纳该框架是自愿行为，不过，美国国土安全部已成立关键基础设施网络社区（C3）志愿项目来提升企业对该框架的认识，协助它们管理风险。

（十二）总统行政令：《促进民营部门网络安全信息共享》（Executive Order: Promoting Private Sector Cybersecurity Information Sharing）

2015 年 2 月 12 日，美国总统奥巴马签署了一项旨在提高关键性基础设施网络安全的行政命令，要求美国政府与运营关键性基础设施的合作伙伴加强信息共享，共同建立和发展一个推动网络安全的实践框架。行政命令要求联邦机构“及时”向运营商提供非保密的网络威胁信息。同时，行政命令还扩大了“强化网络安全服务项目”的覆盖范围，国防基础工业之外的关键性基础设施也可以参与该项目，获得近乎同步的信息共享以提高网络安全防御能力。美国国家标准与技术研究所（NIST）将负责提供技术标准和指导，与关键性基础设施行业共同发展网络安全的实践框架。

奥巴马表示，要确保网络安全，私人企业之间，以及私企同政府之间必须更快速地分享情报。“我们的许多电脑网络和关键基础设施都由私人企业界控制，这意味着政府不能孤军作战。事实是私人企业界本身也无法单独行事，因为最快截获威胁情报的向来是政府。”根据奥巴马的行政命令，国土安全部将拨款设立一个机构，制定有关自愿分享信息的标准。

（十三）《美国国防部网络战略》（the Department of Defense Cyber Strategy）

2015 年 4 月 23 日，美国国防部发布了《美国国防部网络战略》，这是 2011 年 12 月 12 日发布的《国土安全相关实体网络安全战略》的升级版。新战略明确了三大任务：一是保护国防部的网络、系统和信息；二是保卫美国国土及国家利益不受重大网络袭击活动的侵犯；三是集中网络军事力量支持军事行动和应急计划。战略提出了五大目标。

（1）建立和维持网络力量和能力以进行网络空间作战。

（2）保护国防部信息网络、确保国防部数据安全和减轻国防部任务风险。

（3）保护美国本土和美国切身利益免受具有严重后果的破坏性网络攻击。

（4）建立和维护可行的网络方案并在各阶段控制冲突升级以及塑造冲突环境。

（5）建立和维护强大的国际联盟以阻止威胁蔓延并增强国际安全与稳定。

奥巴马政府网络安全相关举措及行动路线图

美国历来十分重视网络安全，也是最早制定和实施网络安全战略的国家。从克林顿时代起，美国政府就将网络安全视为国家安全战略的重要组成部分。美国网络安全战略演变的实质，就是逐步确立美国的制网权战略。为保证网络安全战略的实施，美国形成了组织管理保障、技术保障、法律法规保障和执行保障等体系。经过克林顿和小布什两届政府，在国务院、国防部、情报部门、国土安全部等各部门的积极配合下，一个集战略思想、政策举措和行动策略三位一体的网络空间战略逐渐浮出水面。

奥巴马自 2009 年上任以来，比其前任更加强调网络空间安全的重要性，陆续发布了《网络空间政策评估》、《网络空间国际战略》、《网络空间行动战略》等一系列重要战略文件，为美国构建了一个立体的网络安全战略体系，也使网络安全成为美国国家安全战略的核心部分之一。在此框架下，美国政府相关部门采取了多项举措，重新安排网络空间的权力和规范，谋求更高程度的网络空间霸权，以确保美国政府所确定的繁荣、安全、价值观三大核心利益。

一、奥巴马政府对网络安全问题的整体判断和战略定位

（一）“最迫切的问题”、“最优先的事项”和“最严重的挑战”——进一步提升网络安全的国家战略地位

在竞选总统期间，奥巴马就表示要高度重视网络安全。2008 年 12 月，美国“第 44 届总统网络空间安全委员会”向当选总统奥巴马提交了《提交第 44 届总统的保护网络空间安全的报告》。报告指出，过去 20 年来，美国一直致力于设计一种战略，以应对网络安全挑战，保护美国利益，但始终都不算成功。网络安全以及信息基础设施在激烈竞争中受到攻击，削弱了美国的力量，使国家处于风险之中。报告明确表示：“美国不能保护网络空间，是新政府所面临的最迫切的国家安全问题之一”。奥巴马本人在竞选时，也曾批评小布什政府在解决网络威胁方面过于缓慢，并在 2008 年 7 月的一次讲话中称：“作为总统，我要让网络安全成为 21 世纪的最优先事项。”就任总统后，奥巴马仍高度重视网络安全在国家安全战略中的作用，将其列为执政的首要任务之一。2009 年 5 月 29 日，奥巴马在公布网络安全审查和评估报告的演讲中称：“现在已经很清楚，网络威胁是我们国家所面临的最严重的经济和国家安全挑战之一。”并宣布“数字基础设施将被视为国家战略资产，保护这一基础设施将成为国家安全的优先事项”。

事实上，奥巴马上任以来推行的一系列网络安全举措，都可以从其上任之初的判断和表述中得到印证。结合其竞选期间的施政理念，奥巴马政府推行网络空间安全政策的动因可以概括为：适应国际环境变化，确保美国安全利益；维持信息技术优势，促进美国持续繁荣；运用新型网络力量，扩展美国价值观念。

（二）从网络防御、攻防结合到全球威慑——美国网络安全战略的“扩张性”演变

美国政府的网络安全战略，经历了从重视网络防御、网络攻防结合到全球网络威慑的演变。奥巴马执政以来，美国政府以《网络空间政策评估》和《网络空间可信身份国家战略》等文件为铺垫，以《网络空间国际战略》为典型代表，加上2010年2月的《四年防务评估报告》、同年5月的《美国国家安全战略》和2011年2月的《美国国家军事战略》等文件对网络安全及网络空间行动的指导与补充，奥巴马政府的网络安全政策体系日臻成熟。

奥巴马政府一系列网络安全举措的核心原则，体现在《网络空间国际战略》之中，即“基本自由、隐私和信息自由流动”。具体而言，主要表现为经济、网络安全、司法、军事、网络管理、国际发展及网络自由七个领域的政策优先。纵观美国近三届政府的网络安全战略，先后经历了从保护美国关键基础设施到扩展先发制人的网络打击，再到谋取全球制网权的演变，明显体现出该战略的“扩张性”特征。

二、奥巴马政府推行的网络安全举措及行动路线图

鉴于美国垄断负责互联网运营的国际机构和企业这一现状，美国政府网络空间政策主要通过国际和国内两种行动策略来实施。

在国际层面，美国主要是推动一种“去政府化”的网络空间治理模式，一方面，从理论上把网络空间描述为“全球公域”，否认网络主权；另一方面，推动“多利益攸关方”治理模式，以企业、非政府组织、公民社会为网络空间治理的主体，限制国家及政府间组织在网络空间治理中发挥作用。此外，为进一步抢占网络空间治理领域的话语权，美国国务院牵头搭建“伦敦议程”（London Agenda）的网络空间治理平台，向其他国家兜售美国的思想和价值观。

在国内层面，奥巴马政府积极推动公私合作。美国的网络资源大多分布在政府之外的企业、非政府组织和社会当中，推动公私合作是为了整合这些资源，并将其转化为美国的网络权力。奥巴马政府还积极推动对于美国具有战略意义的网络技术发展，如大数据和云计算技术。对此，奥巴马政府特别责成白宫科技政策委员会成立大数据高层指导小组，要求联邦政府各部门积极支持“大数据研发计划”。美国政府不仅在每年庞大的IT采购预算中优先采购云计算服务，还建立联邦云计算示范工程，并通过一揽子计划鼓励亚马逊、谷歌、微软、IBM等企业在全球获得领先地位，把美国打造成全球数据的存储、交换中心。这样一来，美国政府无须进入他国即可获得网络数据的“全球介入”能力。

具体到网络安全直接举措层面，奥巴马同样有着国内和国际的双重考量。对内，奥巴马确立了对网络安全问题的最高领导权，坚持推进美国数字化基础设施建设，呼吁政府和企业间的责任分享和有效响应，并加强了对网络行为的安全和隐私的保护。对外，奥巴马政府不断实行网络干涉，推行美国式的“互联网自由”，以互联网为工具直接干涉他国内政，并企图主导网络空间国际规则制定，从而确立其在网络空间的霸权地位。

（一）以国内为主线，巩固美国网络安全根基

为检验小布什政府的网络安全计划是否奏效，2009年2月9日，奥巴马要求对美国网