DETT 国防电子智库
Defense Electronic Think Tank

世界主要国家网络空间发展年度报告 2016

主　编　黄　锋
副主编　郭　海　　颉　靖

国防工业出版社
National Defense Industry Press

世界主要国家网络空间发展年度报告 2016

主　编　黄　锋
副主编　郭　海　颉　靖

国防工业出版社
·北京·

内容简介

本书跟踪研究了2016年世界网络空间重大动向，分为战略政策篇、组织体系和专业队伍建设篇、网络安全演习演练篇、网络安全技术篇和2016年度大事记五部分。该书可为领导机关决策提供支撑，还可为相关科技人员及时了解国外网络空间领域发展动向提供全面的参考信息。

图书在版编目(CIP)数据

世界主要国家网络空间发展年度报告. 2016 / 黄锋主编. —北京：国防工业出版社，2017. 1

ISBN 978-7-118-11521-5

Ⅰ. ①世… Ⅱ. ①黄… Ⅲ. ①互联网络—发展—研究报告—世界—2016 Ⅳ. ①TP393. 4

中国版本图书馆CIP数据核字(2017)第301117号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路23号 邮政编码100048)

三河市众誉天成印务有限公司印刷

新华书店经售

*

开本 710×1000 1/16 **印张** 11¼ **字数** 162千字

2017年1月第1版第1次印刷 **印数** 1—2000册 **定价** 168.00元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

PREFACE 前言

网络空间是继陆、海、空、天后的“第五维作战空间”，它是由包括互联网、电信网、计算机系统，以及嵌入式处理器和控制器在内的相互依赖的信息技术基础设施网络和其中的数据组成的，是信息环境中的一个全球域。

2016 年，美国、日本继续深化和落实网络安全建设的相关战略目标，俄罗斯、欧洲等国家和地区也相继新出台了本国网络安全建设战略文件；美国网络任务部队达到初始作战能力，英国、德国、法国、乌克兰、芬兰、日本、以色列、韩国、澳大利亚等国家持续加强机构建设，已成立或计划成立新的网络空间专业机构；同时，美国、日本、北约、欧盟等世界主要国家和组织在网络安全演习演练方面活动频繁；在技术领域，攻击、防御、测评等技术方向都出现了大量新进展。

为使大家深入了解 2016 年世界网络空间发展态势，工业和信息化部电子第一研究所国防电子科技研究中心对该领域进行了持续的跟踪研究，并从网络空间战略政策、组织体系和专业队伍建设、演习演练、技术等方面出发，系统梳理和分析了 2016 年网络空间领域最新发展动向，编撰成书。

网络空间属于新兴研究领域，涵盖内容广泛，对报告撰写者的知识储备和研究积累具有较高要求。由于我们的能力和水平有限，加之经验不足，纰漏在所难免，衷心恳请广大读者批评指正。

工业和信息化部电子第一研究所
军工电子研究部
2016 年 12 月

CONTENTS 目录

>> 战略政策篇

>>组织体系和专业队伍建设篇

>>网络安全演习演练篇

>> 网络安全技术篇

战略政策篇

一、美国

二、日本

三、其他国家和组织

网络空间的快速发展正在塑造全新的社会系统、权力结构、生活方式和价值观念，推进了经济发展全球化、政治权力分散化和军队建设信息化的进程。近年来，世界主要国家纷纷出台或更新其网络空间战略和政策，明确本国网络空间发展方向和建设目标，从顶层统筹和指导网络空间更快、更健康地发展。2016 年，美国、日本继续深化和落实网络安全建设的相关战略目标。俄罗斯、欧洲等国家和地区也相继新出台了本国网络安全建设战略文件，指导本国未来几年的网络空间安全建设工作。

一、美国

2016 年，美国网络空间建设全面进入战略体系深化和战略目标落实阶段，白宫、国防部密集出台《网络空间安全国家行动计划》《2016 年联邦网络空间安全研发战略规划》《国防部网络安全规程实施计划》《美国网络事件协调》等重要文件，与先前出台的文件相比，这些文件更加细化、更具操作性，从多角度提出了具体的落实措施，将有力地推动美国网络空间能力建设。

（一）政府换届与美国网络空间整体战略走向

2016 年恰逢美国政府换届之际，有着“网络总统”之称的奥巴马期满卸任，特朗普当选为下一届美国总统。在这一年中，奥巴马政府对其执政期间的网络空间安全建设实践经验进行了总结，候任总统特朗普延续了奥巴马对于网络空间的重视，也多次发表讲话阐述其在网络空间领域的主要政策和关注重点。

1. 奥巴马政府在网络空间领域的“政治遗产”

纵观奥巴马执政期间，美国网络空间能力建设取得了重大成就，构建了由《网络空间国际战略》《网络空间可信身份识别国家战略》和《网络空间行动战略》三大战略为核心的战略体系，建立了集中统一、军民

协同的管理体制与运行机制，形成了由网络司令部和各军种网络作战部队组成的作战体系，并积极探索“改变游戏规则”的网络攻防技术。随着奥巴马政府任期将至，美国于2016年初出台《网络空间安全国家行动计划》，该文件凝聚了美国网络空间安全建设的实践经验，是奥巴马政府在网络空间领域的“政治遗产”，对确保美网络空间在“后奥巴马时代”继承现有战略思想、有效落实网络空间安全战略目标具有重要意义，同时也彰显了美国在未来解决本国网络空间安全问题的决心。

美国将从军民两个层面统筹协调并推进该行动计划落实。国防部、国土安全部、商务部、财政部、能源部、司法部等机构将共同参与，并从建设网络任务部队、设立“国家网络空间安全促进委员会”、强化网络安全管理与保护、提升基础设施安全、推动“网络威慑”技术发展等方面具体落实行动计划。为了推动相关计划落实，2017财年美国拟为网络空间安全领域投资190亿美元，较2016财年增长35%，其中司法部、联邦调查局网络空间安全活动经费的增涨幅度超过23%，31亿美元用于设立“信息技术现代化基金”，以升级国防部老旧信息系统，6200万美元用于网络空间安全专业人员培养。

2. 特朗普政府最新的网络空间安全理念

总体来看，特朗普政府延续了奥巴马政府在网络空间领域的主要政策，并将对某些重点领域进行深化，预计在2017年将会陆续出台相关落实计划。目前，特朗普政府虽没有提出明确计划，但通过分析特朗普有关网络空间方面的言论，可以得出其关注和发展重点：

一是网络安全漏洞检测。特朗普在一次讲话中表示，要求军方、执法机构和私营部门组成网络审查小组，立即审查包括关键基础设施在内的网络安全漏洞。该小组还将为不同的实体提供具体建议，以便实体采用最佳防御技术保护网络安全。同时，特朗普还计划在未来公开所有的网络安全漏洞。

二是网络控制权。对于ICANN移交互联网基础资源管理权一事，特朗普明确提出美国不应该放弃美国运营互联网的一些核心功能，认

为国会应该阻止政府移交互联网域名管理权，否则美国将失去互联网自由。

三是打击网络恐怖主义。在2016年9月的一次采访中，特朗普指出，应该特别重视网络安全对于打败“伊斯兰国”组织（ISIS）发挥的核心作用，政府需要借助社交媒体平台打击网络恐怖主义的传播。

四是发展网络进攻能力。特朗普提出，要建立先进的网络防御和攻击系统，以抵制国家和非国家层面的网络攻击。同时，他还要求国防部长和参谋长联席会议提出加强美国网络司令部的建议，特别是在网络攻防方面。

（二）进一步落实网络威慑战略思想

网络威慑是指向敌方展示己方应对网络攻击的能力和决心，加大敌方网络攻击成本和承担后果，从而影响敌方决策，降低攻击意愿，最终实现国家安全。2015年12月，美国白宫向国会提交《网络威慑战略》，将网络威慑思想提升为国家顶层战略，初步规划了美国“网络威慑”战略的实施路线图，强调以多元化手段威慑网络威胁，以降低网络攻击者的攻击意愿。2016年，美国国逐渐明确了网络威慑能力主要构建途径：

一是加强网络威慑技术发展。2月，美国国家科学技术委员会（NSTC）发布《2016年联邦网络空间安全研发战略规划》，进一步明确了未来15年联邦网络安全技术研发方向，以期保持并扩大美国在网络空间领域的技术优势。规划强调未来要重点开展可提升网络空间威慑、防护、检测、适应能力的技术研发，明确了未来7年削弱敌人非对称优势的目标，以及未来15年实现威慑恶意网络行为的目标，重点发展拒止与溯源技术，为美国实现“网络威慑”战略目标奠定技术基础。

二是部署具有强大网络防御和恢复能力的系统。如进一步拓展可增强终端防护的“爱因斯坦”系统，增强联邦政府网络安全防御能力，加快部署“联合区域安全堆栈”，强化对国防部信息网络及相关网络资

源的集中管理与控制，提升其安全性等。

三是综合利用多元化手段。提出要综合利用政治、经济、法律、军事等多元化手段，增加敌方攻击成本，如以经济和法律手段制裁网络攻击者，依法查处从私营部门或政府窃取信息及危害、扰乱、破坏计算机和网络的网络犯罪行为，同时加强网络任务部队建设，开展进攻性和防御性网络空间行动，必要时动用军事力量。

四是强化战略和政策宣示。建立网络空间国家行为规范，在针对关键基础设施受到网络攻击时所采取的响应方面建立共识，进一步发展情报能力，积极开展国际合作，加强网络威胁信息共享。

作为在网络空间领域处于绝对优势地位的美国，其采取的是“积极防御、主动进攻、全面威慑”的发展战略。可以预见，未来美国还将根据威胁的变化和国家战略需要，进一步调整“网络威慑”战略，这将对全球网络空间的安全与稳定产生重大影响，引发网络空间作战力量、装备技术等领域的全面竞争。

（三）建立国家网络事件应急响应体系

7月26日，美国白宫出台一项新的总统政策指令PPD－41——《美国网络事件协调》，旨在明确联邦政府相关机构在遭受网络攻击时的职责，为其实施网络事件响应提供指导原则。2016年初，美国出台《网络空间安全国家行动计划》，强调要加强政府对网络事件的协调与响应能力，提升联邦政府的网络安全管理。此次出台的总统政策指令，继承了该行动计划的思想，明确了联邦政府机构在遭受网络攻击时的职责，建立了政府应对重大网络事件的协调体系和响应机制，是全面落实提升联邦政府网络空间安全能力的重要举措，具体内容如下：

一是确立网络事件响应的指导原则。强调政府机构在应对网络攻击时，应遵循“共同承担责任”“基于风险评估进行响应”“尊重受影响实体的隐私”“保证政府努力的统一性”“修复和恢复受影响实体”5项原则。

二是明确联邦政府相关机构职责。指出为应对各类网络事件，联邦政府应开展以下三方面工作：①威胁响应；②资产响应；③情报支持和相关活动。司法部是威胁响应的领导机构，将通过联邦调查局、国家网络调查联合特遣部队开展工作，主要负责协调应对“直接”威胁，促进攻击溯源、收集证据和执法行动；国土安全部是资产响应的领导机构，将通过国家网络安全和通信集成中心开展工作，主要负责协调处理网络攻击产生的影响，为攻击溯源提供技术支持；国家情报总监办公室是情报支持和相关活动的领导机构，将通过网络威胁情报集成中心开展工作，主要负责整合情报并对网络威胁进行分析。

三是建立国家网络安全事件应急协调体系。将国家网络安全事件应急协调体系分为三层：第一层是“网络响应小组”，由国务院、财政部、国防部、司法部、能源部、国土安全部、国家情报总监办公室等十几个机构的高级代表组成，负责协调各机构制定“重大网络事件”响应政策。第二层是“网络统一协调小组”，由国土安全部和司法部联合建立，负责协调网络安全相关机构联合应对重大网络安全事件，协同制定和实施响应方案，确保情报快速、准确共享。第三层是核心执行机构，国家情报总监办公室负责整合情报并分析网络威胁；司法部负责协调应对“直接”威胁，促进攻击溯源、收集证据和执法行动；国土安全部负责提供攻击溯源技术支持，保护网络资产安全，修补漏洞和恢复系统。

四是明确网络事件响应办法。规定在地方政府在其网络受到攻击时，应根据总统政策指令中的适应性政策与规程，对“重大网络事件”做出响应，并向国土安全部报告相关事件。对于国防部信息网络，国防部长应当负责对影响到国防部信息网络的网络事件进行威胁响应与资产响应，同时接受来自其他政府机构的必要支持。对于情报部门网络，国家情报总监应当负责通过情报界、安全协调中心，对情报部门信息环境面临的威胁进行威胁响应与资产响应，同时接受来自其他政府机构的必要支持。

五是强调对政策指令的实施与评估。规定要从以下 6 个方面开展

工作:①国家安全委员会应当自该指令发布后90日内,更新网络响应小组章程,以涵盖并支持上述指导意见。②各政府机构应当自该指令发布后90日内,建立强化协调规程,确定专项领导、支持人员、设施和内部流程方案,保证相关机构在实际需求超出自身条件的情况下,能够以协调方式管理"重大网络事件"。③各政府机构应当自该指令发布后150日内,要更新网络事件协调培训项目。根据国家事件管理系统和统一协调政策,建立并维持一套具体的人员考核与培训办法。④各政府机构应当自该指令发布后180日内,将相关原则纳入网络事件响应演习中。⑤在每一次网络统一协调小组使命任务结束后,网络响应小组主席应对该小组所响应的"重大网络事件"进行审查并出具报告,并在30日内提交。⑥国土安全部与司法部应当在指令发布后180日内,协同有关机构向总统提交网络统一协调小组运行情况报告,其内容主要包括各政府机构间如何协同管理网络事件以避免其对实物产生影响的措施,以及如何同私营部门在合适时机共同做出响应。

总体来讲,该总统政策指令补充和完善了2011年3月出台的总统政策指令《国家准备》(PPD-8)的相关内容,标志着美国已将网络准备工作融入了传统的准备工作之中,此举对于强化联邦政府的网络安全管理、提升网络攻击响应能力意义重大。

(四)加强军事网络设施安全战备与防御能力

美国国防部《网络安全规程实施计划》(以下简称"《实施计划》")于2015年10月发布,2016年2月修订后,3月正式对外公布。该计划是美军加强军用网络安全战备、提高网络防御能力的执行手册,明确了美军各级指挥官和主管人员必须遵守的规则。

美军认为,当前美军事网络面临很多安全问题,其原因并非攻击者拥有非常先进的攻击方法和技术,而是由于其成功利用了一些常见漏洞。贯彻落实基本的网络安全要求,需要各级指挥官和主管人员,以及其他人员从微观层面理解自己在网络安全战略中的角色、责任和行动,

这需要一个规定明确、措施具体的网络安全实施规程。美国国防部开展的“国防部网络安全行动”，是对《国防部网络战略》和《网络空间安全国家行动计划》的重要支持。而《实施计划》则是“国防部网络安全行动”的重要组成，是强调执行性、操作性、强制性的具体落实措施。《实施计划》对实现《国防部网络战略》提出的“防卫国防部信息网络、保证国防部数据安全、降低国防部任务风险”战略目标至关重要。同时，《实施计划》也呼应了《网络空间安全国家行动计划》中关于提高关键信息基础设施安全、加强个人身份验证等内容。

《实施计划》强调要采取4类措施，并对指挥官和主管人员提出了17项具体执行规程，旨在提升美国国防部的网络安全水平。

一是加强身份认证，实施严格的访问控制程序。确保美国国防部网络中的每个Web服务器和Web应用程序必须使用国防部批准的基于公钥基础设施（PKI）的用户认证；确保每个系统管理员必须100%使用单独的PKI认证，禁止以用户名/密码认证方式登录；确保每个用户登录任何网络基础设施设备都要使用PKI认证。通过全面执行强身份验证，减少网络匿名，以提高国防部对非法访问的态势感知能力。

二是加固设备，确保设备正确配置并安装最新补丁。完成国防部网络中的Windows XP和Windows Server 2003操作系统的升级或移除；确保国防部每台计算机必须按照安全技术实施指南（STIG）进行正确配置；确保计算机符合“基于主机的安全系统”的安装要求；确保Outlook电子邮件客户端禁用超文本标记语言（HTML）、富文本格式（RTF）、活动链接；确保HTML和RTF对由政府提供电子邮件服务的商用移动设备禁用；确保所有服务器和网络基础设施设备都已及时更新补丁。通过对老旧操作系统进行升级和移除、正确配置系统、及时更新补丁，可以有效减少国防部系统设备漏洞，提高网络安全性。

三是减少攻击面，减少进入国防部信息网络的人员数量和网络访问点数量。审查并确保所有面向互联网的资产均列入国防部非军事网络管辖范围内，在没有使用需求时，断开所有面向互联网的Web服务