美国网络安全战略与政策二十年

左晓栋　等 编译

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

美国网络安全战略与政策二十年

左晓栋　等 编译

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

内 容 简 介

本书收录了自 1998 年至今克林顿、小布什、奥巴马和特朗普共四任总统任期内，美国政府、军方、国会和有关部门发布的主要网络安全战略、法律、规划、行政令、总统令，以及根据美国网络安全战略要求，各关键基础设施部门发布的本行业网络安全战略和规划，共计 36 篇，并以时间顺序排列。附录 I 还摘要介绍了美国重要智库战略与国际研究中心（CSIS）对特朗普政府的网络安全政策给出的建议。为了更全面地反映美国网络安全政策制定过程，本书收录的文件包括一些过程稿或征求意见稿。

考虑到篇幅等因素，本书对各行业的网络安全战略和规划进行了摘要介绍，全部详细内容可通过扫描书中给出的二维码免费阅读。

本书可供各级网络安全和信息化领导机构以及各网络安全主管部门、各关键信息基础设施主管或监管部门在制定网络安全政策时参考，也可供各类网络安全管理和技术人员在实际工作中参考，还可用作高等院校和科研机构在网络安全、国际关系等专业方向的教学或研究参考资料。

图书在版编目（CIP）数据

美国网络安全战略与政策二十年 / 左晓栋等编译. —北京：电子工业出版社，2017.12
ISBN 978-7-121-33159-6

Ⅰ. ①美… Ⅱ. ①左… Ⅲ. ①计算机网络—国家安全—国家战略—研究—美国 Ⅳ. ①D771.236 ②TP393.08

中国版本图书馆 CIP 数据核字（2017）第 316673 号

策划编辑：齐 岳
责任编辑：苏颖杰
印 刷：北京画中画印刷有限公司
装 订：北京画中画印刷有限公司
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：787×1092 1/16 印张：49.25 字数：1261 千字
版 次：2017 年 12 月第 1 版
印 次：2017 年 12 月第 1 次印刷
定 价：298.00 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）88254888，88258888。

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。

本书咨询联系方式：（010）88254473、qiyue@phei.com.cn。

前　言

习近平总书记指出，没有网络安全就没有国家安全。中央网络安全和信息化领导小组成立以来，特别是“4·19”网络安全和信息化工作座谈会召开后，在习总书记“网络强国”战略思想指引下，我国网络安全工作进入了加速发展的崭新阶段，《网络安全法》、《国家网络空间安全战略》的出台推动网络安全顶层设计趋于完善，关键信息基础设施安全保护等重要制度相继建立，国家网络安全保障体系日益健全，维护国家空间、主权和国家安全的能力显著增强。

与此同时，网络安全形势仍十分严峻，各国在网络空间展开激烈博弈，围绕网络空间发展权、主导权、控制权的竞争愈演愈烈。知彼知己，百战不殆。做好自己的事情重要，了解别人也同样重要。加之网络安全是开放而不是封闭的，维护国家网络安全要有全球视野和开放心态，因此更有必要关注其他国家的做法。

美国全面加强网络安全工作已有二十年的历史，是值得我们关注的重点对象。1996 年，美国国防授权令要求美国总统从防止战略攻击的角度向国会报告联邦政府的网络安全政策。为此，经过一系列国家安全会议的讨论，当时的美国总统克林顿发布了第 63 号总统决定令（PDD63）《对关键基础设施保护的政策》，从此拉开了美国以关键基础设施保护为重点的网络安全工作历史大幕。二十年间，美国历经四任总统，围绕网络安全先后发布了一系列战略、法律、规划、行政令、总统令。

在中央网络安全和信息化领导小组办公室的关心、支持和指导下，我们对美国的这些文件进行了全面回顾、翻译和研究，并编译成本书。前事不忘，后事之师。我们不但关注特朗普政府的最新网络安全政策，而且重视早期的美国网络安全战略部署，甚至是一些战略的过程稿。正是这些文件，使我们得以完整地看到美国网络安全机构演变过程和网络安全思路调整脉络，这是重要的他山之石，希望能为我国网络安全工作提供参考。

左晓栋

2017 年 12 月

目　录

一、第 63 号总统决定令：克林顿政府对关键基础设施保护的政策

1998 年 5 月 22 日

本白皮书解释了克林顿政府对关键基础设施保护的政策。我们希望它能够在私营部门和公共部门所有感兴趣的团体中得到传播。我们还希望它能够应用于美国政府专业教育机构，如国防大学和国家外事培训中心，使它们在跨机构的操作及规程上得到课程学习和锻炼。美国政府的所有机构都支持这一非涉密性质的白皮书广为传播。

1. 日益增长的潜在脆弱性

美国同时拥有世界最强大的军队以及最强盛的国家经济，我们国力的这两个方面互为补充并互相依赖。而且，它们越来越依靠某些关键基础设施以及基于计算机和网络的信息系统。

关键基础设施是那些物理系统和以计算机和网络为基础的系统，它们对于最基本的经济运行和政府运转非常关键。这些关键基础设施包括但不限于政府和私营部门拥有的电信、能源、银行与金融、运输、供水系统和应急服务。在历史上，国家的很多关键基础设施都是物理和逻辑上分离的系统，彼此之间依赖性不强。然而，随着信息技术的发展以及对提高效率的要求，这些基础设施逐渐变得自动化和互联。这种进步产生了一些新的脆弱性，这些脆弱性将导致设备故障、人为错误、天气和其他自然灾难以及物理和信息攻击。解决这些脆弱性离不开灵活、渐进的方法，以横跨公共和私营部门，对国内和国际安全提供保护。

由于我们的军事力量（强大），未来的敌人——国家、集团或者个人将有可能通过非常规的手段对我们造成伤害，包括在美国本土发动攻击。我们的经济越来越依靠那些互依赖的、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。

2. 总统的意愿

长久以来，保障关键基础设施的连续性和生存力一直是美国政府的政策。我希望，美国政府要采取所有必要的措施来迅速减弱我们的关键基础设施，尤其包括我们的信息系统在面临物理和信息攻击时的任何重大脆弱性。

3. 国家目标

最迟不晚于 2000 年，美国应当实现初步的信息保障能力；从这份总统令发布之日起，五年后美国将已经获得并保持对我国的关键基础设施进行保护的能力，以防止可能会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。
- 私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。

这些关键功能遭到的任何破坏或操纵必须控制在历时短、频率小、可控、地域上可隔离以及对美国的利益损害最小的规模上。

4. 公共–私营合作联盟以减少脆弱性

对我们的关键基础设施的攻击目标将很可能包括经济以及政府部门中的设施，因此需要密切协调公共和私营部门的工作来消除潜在的脆弱性。为取得成功，这一合作联盟必须是真正的、相互的和协作的。为了达到我们的国家目标，消除我们关键基础设施中的脆弱性，美国政府应该在最大可能的程度上努力避免造成政府法规的增多，尽量避免对私营部门发放没有资金支持的政府训令。

对于我们经济中的每个易于受到基础设施攻击的大型部门来说，联邦政府将从指定的领导机构中指派一名高级官员，作为部门联络官来与私营部门合作。经过与他们所负责的基础设施领域内的私营部门实体的交流和合作，部门联络官将确定一个私营部门内代表该部门的合作者（部门协调员）。

部门联络官、部门协调员以及他们所代表的政府机构和公司应该完成下列工作，以促成各自部门级“国家基础设施保障计划”的制定：

- 评估该部门对计算机或物理攻击的脆弱性。
- 推荐用以消除重大脆弱性的计划。
- 提出用来标识并预防大规模攻击的系统。
- 制定下列行动计划：在受到攻击的过程中对该攻击进行报警，控制并切断攻击，随后，在攻击的余波之中，必要时与 FEMA（联邦应急管理局）协商，迅速重建最基本的重要职能。

在每篇部门级计划的准备过程中，国家协调员（见 VI）应该与领导机构的部门联络官、国家经济委员会的代表一起确保各计划的全面协调及整合，尤其要注意其中的相互依赖性。

5. 方针

为了消除这些潜在的脆弱性，并阐明消除这些脆弱性的手段，我希望有关人员能够在头脑中牢记如下的普遍原则和事项：

- 针对那些旨在满足总统令目标的方法和项目，我们必须向国会咨询，并努力寻求国会的参与。
- 对我们的关键基础设施的保护必须是一种在关键基础设施所有者、运营者和政府之间共同承担的责任以及一种合作性质的关系。
- 应该时常评估我们的关键基础设施的现有依赖性、脆弱性和威胁环境，因为我们的关键基础设施所面临的威胁的性质一直在迅速地变化着，因此我们的保护措施和响应必须具有充分的适应性。
- 市场诱因是解决关键基础设施保护问题的首选，只有在市场无法为保护美国人民的健康、劳动安全和福利而提供足够资源的时候，才可以诉诸法规。此时，各机构应该确定并评估可行的替代方案，以指导法规的执行，包括提供经济刺激以促进预期行为的实现，或对私营部门的备选方案提供有关信息。这些刺激以及其他的有关行

动应当有助于与最新的技术保持协调，应当引入对国际问题的全局性解决方案，应当使私营部门的所有者和运营者可以获取并维持最大可能的安全性。

- 政府的各级机构、政府的所有功能以及资源，包括执法、法规条例、国外情报和国防战备等功能应在必要的时候使用，以确保关键基础设施得到保护，并维持这种保护状态。
- 必须对私有权给予认真的尊重。必须使消费者和运营者有这样的信心：他们的信息得到了正确、安全和可靠的处理。
- 通过研究、开发和采购，联邦政府应当鼓励对有效的基础设施保护方法进行引进。
- 在如何最佳地实现基础设施保障这一问题上，联邦政府应当成为私营部门的楷模，并且，联邦政府应当使其工作的成果在最大范围内得到传播。
- 我们必须关注预防性措施以及威胁和风险管理。为此，应当鼓励私营部门的所有者和运营者为他们所控制的基础设施提供最大可能的安全性，并鼓励他们向政府提供必要的信息，以利于政府协助他们实现这个目标。为了使私营部门能全面投入，私营部门所有者和运营者对于是否参与国家基础设施保护系统是自愿的。
- 对于一个稳健、灵活的基础设施保护项目来说，同州政府、地方政府以及第一时间响应人员的密切合作与协调是非常重要的。所有的关键基础设施保护计划和行动应当将州、地方政府和第一时间响应人员的需求、活动和责任考虑进去。

6. 结构和组织

为了达到我们的目标，联邦政府应当围绕四个部分进行组织（附录 A 详述）。

（1）作为部门联络的领导机构：对每个有可能成为信息或物理攻击目标的基础设施部门来说，将唯一的联邦部局作为联络时的领导机构。每个领导机构将指派一名相当于助理部长或更高级别的人来担任该基础设施领域内的部门联络官，他应与私营部门的代表（部门协调员）一起解决与关键基础设施保护有关的问题，尤其是一起为国家基础设施保障计划添砖加瓦。领导机构和相对应的私营部门将制定并执行该部门的脆弱性意识和教育项目。

（2）特殊职能的领导机构：除上述之外，某些关键基础设施保护职能必须主要由联邦政府执行（国防、外事、情报、执法），对其中的每项特殊职能，都应有一个领导机构负责协调美国政府在该领域内的活动。每个领导机构将指派一名助理部长和更高级别的高级官员来担任联邦政府的职能协调员。

（3）跨机构协调：领导机构的部门联络官、功能协调员以及来自其他相关机构和部局，包括国家经济委员会的代表，需要在关键基础设施协调组（CICG）的帮助下，一起协调本总统令的执行。CICG 由安全、基础设施保护和反恐怖主义国家协调员领导。国家协调员将由总统指派并通过总统国家安全事务助理向总统汇报，国家安全事务助理则应当确保与总统经济事务助理的协调。CICG 内各机构的代表应当具有较高级别（助理部长和更高）。在必要的时候，CICG 将得到外部政策组织的协助，比如安全政策委员会、安全政策论坛、国家安全和电信委员会以及信息系统安全委员会。

（4）国家基础设施保障委员会：由领导机构、国家经济委员会和国家协调员推荐，总统将指派一个由大型基础设施提供商和州及地方官员组成的小组组成国家基础设施保障委员