信息基础设施安全保护丛书

国家信息基础设施的安全保护

Cyber Attacks
Protecting National Infrastructure

〔美〕Edward G. Amoroso 著
郭世泽 陈 哲 冯冬芹 等 译

科学出版社

国家信息基础设施的安全保护

Cyber Attacks
Protecting National Infrastructure

〔美〕 Edward G. Amoroso 著
郭世泽 陈 哲 冯冬芹 等 译

科学出版社
北 京

图字：01-2015-0468 号

内 容 简 介

本书分析国家信息基础设施保护中遇到的各种问题，总结阐述成“欺骗、隔离、多样化、通用性、纵深、慎重、采集、关联、感知、响应”10 项保护原则，分别从第2 ～第11章加以诠释，同时附录中还给出了 10 项原则的需求描述示例和 5 个具体案例。值得注意的是，书中提出的针对国家信息基础设施的全面、系统的保护理念和一些有别于传统计算机安全的具体作法，突破了传统思维定式，创新性明显。

本书可作为从事网络空间战略决策、网络安全工程设计、网络运营、软件设计、网络技术管理、网络应用和法律法规制定等方面研究人员的重要参考资料，也可作为信息安全、计算机科学与技术、通信工程等专业博士生、硕士生和高年级本科生相关课程的辅助教材。

图书在版编目(CIP)数据

国家信息基础设施的安全保护 /(美)阿莫罗索(Amoroso, E. G.)著；郭世泽等译. —北京：科学出版社，2015.4
(信息基础设施安全保护丛书)
书名原文：Cyber attacks: protecting national infrastructure
ISBN 978-7-03-044055-6

Ⅰ.①国… Ⅱ.①阿… ②郭… Ⅲ.①信息安全-国家安全-研究 Ⅳ.①D035

中国版本图书馆CIP数据核字(2015)第069040号

策划编辑：陈 静 / 责任编辑：陈 静 邢宝钦 / 责任校对：张怡君
责任印制：张 倩 / 封面设计：迷底书装

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

新科印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2015年4月第 一 版 开本：720×1000 1/16
2015年4月第一次印刷 印张：15 3/4
字数：332 000

定价：80.00元

（如有印装质量问题，我社负责调换）

编译委员会

丛 书 序

“没有网络安全，就没有国家安全”，没有信息基础设施安全就没有网络安全。信息基础设施是指为社会生产和生活提供公共信息服务的工程设施，是用于保证社会活动和关键基础设施正常运行的信息服务系统。它们支撑着政府、金融、能源、交通、电信、医疗卫生、教育、科技、公用设施等关键业务，其安全保护问题成为国家安全的重中之重。为了更好地对信息基础设施安全保护进行研究，编译委员会对国外相关论著进行了系统梳理，挑选了几本有影响的力作，既涉及传统信息基础设施（如传统IT基础设施和工业控制系统等的保护），也涉及一些新型信息基础设施（如云计算和移动互联网等的保护）；不仅涉及信息基础设施的保护理论、技术和具体作法，还包括具体的实践案例和解决方案。相信本丛书将成为当今开展网络安全研究的重要参考资料。

编译委员会

2015 年 1 月

译 者 序

随着云计算、大数据、物联网、移动互联网、工业控制网络等时髦词汇的普及和深入，这些概念共同指涉的网络空间越来越得到人们的高度关注。甚至类似于马汉的海权论、麦金德的陆权论和杜黑的空权论，有人提出了网权论，即“谁控制了网络，谁就控制了世界”。整体而言，网络空间以前所未见的高速度在全球扩散，来得太急，变化太快，一时间“乱花渐欲迷人眼”，但无论如何，网络空间的极端重要性已是毋庸置疑的事实。译者一直认为，网络空间并不是人们常提到的“第五维空间”，而应该是贯穿物理域、信息域、认知域和社会域的支撑当今人类社会生活的“第二类空间”，并由此产生新的“网络宇宙观”。

爱因斯坦说过：“提出新的问题、新的可能性，从新的方向看旧问题，则需要创造性的想象力，而且标志着科学的真正进步”。网络空间是如此重要，让我们不得不提出两个新问题，一是网络空间中最重要、最核心的组成部分是什么？二是它们安全吗？

关于第一个问题，我们认为，网络空间最重要、最核心的组成应该是国家信息基础设施。“国家信息基础设施”的概念包括两方面，一个是“信息基础设施”，另一个是“国家”。

首先，看一下什么是信息基础设施。信息基础设施是指为社会生产和生活提供公共信息服务的工程设施，是用于保证社会活动和关键基础设施正常运行的信息服务系统。在当今的网络时代，信息基础设施不仅包括支持社会生活的国际互联网、电信网和广播电视网等网络基础设施，还包括支持政府、金融、能源、交通、医疗卫生、教育、科技、公用设施等关键基础设施运行的网络化信息系统。信息基础设施不仅是信息传输的物理–逻辑载体，也是网络空间的物理–逻辑基础，失去信息基础设施的支撑，网络空间无从谈起，因此可以将其称为网络空间最重要的组成部分。

其次，再看一下什么是国家信息基础设施。国家信息基础设施是由国家宏观筹划的，由政府部门、运营商和行业共同建设的，为一个国家和地区提供信息服务的信息基础设施，是国家主权的重要组成部分。一般来说，根据地理位置分布、主权管辖效用和建设主体的不同，可以将信息基础设施分为三类：一是全球信息基础设施（Global Information Infrastructure，GII）；二是国家信息基础设施（National Information

Infrastructure，NII）；三是国防信息基础设施（Defense Information Infrastructure，DII）。从构成和作用来看，全球信息基础设施的主要作用是支撑跨越国家疆域和自然地理疆界的网络互连，是支撑起国际互联网的关键设施，其主要物理表现形态包括海底光纤、陆地光纤和国际卫星等有线-无线信号传输系统，旨在实现洲际和国家间的互通互联，一般由某个国家或者跨国公司和国际银团共同投资建设。与国家信息基础设施相比，全球信息基础设施功能相对集中，构架相对比较简单。国防信息基础设施一般由国防工业部门和军队建设，可以将其理解为裁剪版或缩微版的国家信息基础设施，其规模和复杂度远小于国家信息基础设施。另外，从面临的威胁来看，就如同太空和公海一样，全球信息基础设施在某种程度上具有“全球公域”的基本特征，是全球各国家和所有人共同使用的信息通道。当和平与发展仍然是世界主要潮流时，很少有人会直接攻击和破坏全球信息基础设施，其面临的风险和挑战相对有限；国防信息基础设施是关系“国之大事”的重器，各个国家都自然采取严防死守的态度来保障国防信息网络的安全，甚至很多采取物理隔离的方式，其面临的威胁相对较少。而相比上述两者，国家信息基础设施有更长的战线，更复杂的应用，更多容易遭遇的弱点和脆弱性，同时还必须考虑国家经济利益，选择最具性价比的方式加以保护。因此，无论是从构成和作用还是从保护需要来说，国家信息基础设施都是信息基础设施的核心，是网络空间最重要、最核心的组成部分。

关于第二个问题，我们认为，现在的国家信息基础设施很不安全。无论是美国等发达国家和地区还是中国，都深刻认识到：国家信息基础设施的安全状况堪忧。在奥巴马上任伊始，美国进行了 60 天的信息安全评估，特别是对美国国家信息基础设施的安全状况进行了分析。在 2009 年 5 月 29 日公布的《美国网络空间政策评估报告》中指出：“信息系统、互联网和其他基础设施之间越来越多地连接在一起，为攻击者破坏电信、电力、能源管道、炼油厂、金融网和其他关键基础设施创造了机会”，“一些国家早已拥有了实施这种攻击的技术能力”；报告最后得出了“再也不能容忍目前的状况”的结论。对于中国而言，由于核心信息技术长期受制于国外，信息基础设施主要产品依赖进口，主要技术标准均由国外制定，这些情况在近期难以改变，因此国家信息基础设施面临重大的风险。“棱镜门”历历在目，“震网”病毒不知何时将落在我们的身边。

“没有网络安全就没有国家安全”，若这样的论断出现在几年前，肯定有人会说是一种炒作，而现在谁也不再怀疑网络安全与国家安全的密切相关性了。那我们怎么办？首先应该从借鉴别人的成功经验开始。古语讲“他山之石，可以攻玉”，毛泽东主席也说过“把别人的经验变成自己的，他的本事就大了”。对于同样面临国家信息基础设施安全保护难题的美国，他们在安全保护体系设计和实践方面已经做了几十年尝试，取得了一定的经验。其中的一些内容已经反映在爱德华·阿莫罗索（Edward G. Amoroso）所著的《国家信息基础设施的安全保护》一书中。

爱德华·阿莫罗索是美国电话电报（AT&T）公司的高级副总裁兼首席安全官，他

所供职的AT&T公司秉承着贝尔的创新传统，曾经垄断着美国的全部电信业务，虽然几经反垄断拆分，仍然保持着电信界龙头老大的地位，目前是美国最大的本地与长途电话公司和无线运营商，它所运营的信息基础设施可以称为国家信息基础设施。

作为《国家信息基础设施的安全保护》的作者和当今美国网络安全领域的顶级专家，爱德华·阿莫罗索凭借在电话电报公司工作的亲身实践经验，针对极为复杂的国家信息基础设施，为网络安全工程、网络运营、软件设计、网络技术管理和应用等行业的工作人员提出了国家信息基础设施保护中所遇到的各种问题，从技术、架构和管理层面给出了解决方案，并总结阐述成“欺骗、隔离、多样化、通用性、纵深、慎重、采集、关联、感知、响应”10项保护原则。他所介绍的每种原则都是一项单独的安全战略，所给出的诠释和示例在展示原则运用方面都颇具说服力，特别是他所提出的针对国家信息基础设施的全面、系统的保护理念和一些有别于传统计算机安全的具体作法，突破了传统思维定式，具有创新性。

美国前国防部副部长，现任战略与国际研究中心主席的约翰·哈姆雷先生评价说：“爱德华·阿莫罗索再一次为政策界提供了一幅经过深思熟虑的路线图。现在，网络威胁变得越来越复杂。谢天谢地！爱德华很熟悉这一问题并率先提出了解决方案。”

全球知名的网络安全设备供应商，也是统一威胁管理（United Threat Management，UTM）市场领导者的飞塔（Fortinet）公司总裁谢青对爱德华·阿莫罗索的论著做出了评论：“《国家信息基础设施的安全保护》是一次针对复杂信息基础设施制定网络安全策略的迷人之旅，它的作者是当今大规模网络安全领域的顶级专家之一。如何增强我们国家的网络安全系统？就那些对此感兴趣的人来说，本书是一幅技术路线图。”

本书引起了美国政界和商界的高度关注，一些政府高官和商业巨子称其为私营企业和政府部门从事安全工作的人员的“必读书”。正如爱德华·阿莫罗索自己所说的：“没有哪个国家拥有条分缕析的技术和架构策略来防止网络攻击所造成的关键信息基础设施服务瘫痪。本书围绕全面的技术领域开展了讨论，涉及的是减少国家风险的正确方法，可充当网络安全新型战略的诱人框架，这正是数届美国政府试图创建却没有成功的地方。”

“他山之石借为琛，磨琢良锋利断金。尝胆卧薪凭庙算，楚番震慑宋聋擒。”当然，每个国家面临的安全风险均不会完全相同，需要根据自己国家的具体需要进行本地化筹划和设计。本书不仅说明了怎样做，而且系统阐述了为什么这样做，正因为如此，它对我们研究国家信息基础设施保护问题具有重要的参考价值，是一本值得读一读的好书。

在本译本即将出版之际，国外又出版了学习版，主要是由John R. Vacca先生补充了新的材料，包括章节总结、学习要点、课后习题、案例分析等，可以看出，本书已经成为了国外网络安全教学的重要资料。本译本已经将更新的内容增加进来。

本书得到国家自然科学基金资助项目“工业控制系统安全脆弱性分析与建模的理论

与应用研究（61223004）”资助。

限于水平，书中难免有理解不准和表述不妥之处，恳请读者批准指正。

工业控制系统安全技术国家工程实验室

2015 年 1 月

前　言

人进入社会后，状况不会变得比之前糟糕，其自身权利亦不会变少，而且这些权利还会得到更好的保障。

——《常识》，托马斯·潘恩

在花时间阅读本书之前，请先稍候片刻，浏览以下几个要点，因为它们勾勒出了我在国家信息基础设施安全方面的一些基本理念。我想，对这些要点的认知能够帮助您更好地理解本书内容。

（1）若缺乏基本的安全保护，自由国家的民众就无法充分表达或享受自由。可以说，安全并不是压制自由，而是使自由成为可能。

（2）在几乎所有现代国家里，计算机和网络支撑着关键信息基础设施的方方面面。而网络攻击者可以使用计算机和网络对民众所依赖的信息基础设施加以破坏或毁灭。

（3）诸多安全类书籍中介绍的那些安全保护手段主要是用于企业计算等小规模环境，而对于大规模、复杂的信息基础设施，这些手段就难以胜任了。

（4）国家网络保护要想行之有效，在很大程度上取决于商界、业界和政府组织机构间的合作与协调。因此，对于网络国防而言，组织管理问题与技术问题同样重要。

（5）安全是一种风险降低过程，而不是风险消除。因此，可能也应当采取具体步骤来降低而不是消除网络攻击给国家信息基础设施带来的风险。

（6）从任何现实衡量标准来看，都必须将国家信息基础设施遭受网络攻击的灾难性风险视为最高。基本或根本不采取行动来降低此种风险是一项愚蠢的国家决策。

基于以上理念，本书的各章分别阐述了 10 条基本原则，以期从根本上降低网络攻击给国家信息基础设施带来的风险。这些原则的提出得益于我对世界上最大、最复杂信息基础设施之一进行安全管理所获得的经验，和在不同商业和政府组织机构里的多年学习，以及与安全领域的学生和学者之间的多年互动。同时，还得益于我在很大范围内应对成功和不成功网络攻击时所获得的个人经验，其中包括处理那些针对重大价值信息基础设施的攻击行为。不过，10 条基本原则的贯彻实施需要国家下定决心，对国家信息基

础设施环境下计算和网络要素的设计、构建和运行方式加以改变。我希望本书提出的建议能够让决策过程变得更加容易。

学习版

为了帮助老师在课堂上更加方便地讲授上述基本原则，学习版增加了由《计算机和信息安全手册》的主编 John R. Vacca 先生提供的新内容，主要目的是增加学生的学习体验，使其成为网络安全、信息安全、数字安全、国家安全、情报研究、技术与基础设施保护和其他类似课程的主要学习教材。

学习版增加了“案例分析”，主要用来展示本书讨论的实际实现场景。同时还增加了一系列帮助学习的新的教学要素，包括章节总结、学习要点、课后习题等。

若要获取相关的习题库、演示文稿、课堂计划和解决方案手册等帮助内容请登录 http://textbooks.elsevier.com/web/Manuals.aspx?isbn=9780123918550。

（1）习题库——使用 Windows 风格的免费编制工具中的在线评分功能，来挑选、定制和输出试题，使授课老师能够方便地采用专为本书创建的多选题和判断题来编制试卷。同时，提供的编制工具还能将定制好的试题直接输出到 Blackboard、WebCT、eCollege、Angel 和其他主要的学习系统中。而且，所有的习题库文件都能方便地以 Word 格式提供。

（2）PowerPoint 演示文稿——采用有重点的 PowerPoint 演示文稿来加强关键主题的展示，提供完美的可视化大纲来帮助学习。本书的每一章都有专门的幻灯片。

（3）课堂计划——围绕可定制的课堂计划来设计自己的教学课程。每一个课堂计划都是一份独立的教学大纲，其中包括内容重点、关键术语、补充材料网站链接和专为激励课堂讨论而设计的开放式重点问题。另外，这些课堂计划还描述了章节目标与具体教学资源的相互关系，以便授课老师能够按照自己的方式对资源进行分类。

目　录

1 引言

约翰·冯·诺伊曼在他的论著中给出了一个论断，他认为，对于简单机制，描述如何做往往比说明做什么更加容易，而对于那些复杂机制，情况往往是相反的。

——荷兰计算机科学家，图灵奖获得者，艾兹格·迪科斯彻[①]

国家信息基础设施是指那些复杂的底层信息传输和支持系统，它们承载着一个国家视为命脉的所有大规模服务，包括应急响应、执法数据库、监控与数据采集（Supervisory Control and Data Acquisition，SCADA）系统、电力控制网络、军事支持服务、消费娱乐系统、金融应用和移动通信。有些国家性服务由政府直接提供，而大多数则由互联网服务提供商、航空公司和银行之类的商业团体提供。有意思的是，被一国视为至关重要的某些服务可能会依靠他国组织机构控制的基础设施来提供支持。这种全球相互依赖趋势被托马斯·弗雷德曼统一称为“扁平世界”[②]。

在美国，国家信息基础设施一直容易遭受恶意的物理攻击，如设备被篡改、电缆被割断、设施被爆损和资产被盗窃。例如，2001 年的“911事件”就是近十几年来最有名的一次针对国家信息基础设施的大规模物理攻击。然而现在，情况发生了一些变化。在过去几十年里，大量的国家信息基础设施开始依赖软件、计算机和网络，这种依赖性一般还包括允许远程登录，经常是通过国际互联网，来访问那些控制国家服务的系统。因此，敌人可以使用蠕虫、病毒、信息泄露等手段，发起针对信息基础设施的网络攻击，进而通过相关的自动化控制系统，间接地指向国家信息基础设施（图1.1）。

在应对这种国家网络威胁时，一种看似显而易见的方法是使用那些享有盛誉的计算机安全技术。毕竟，计算机安全技术在过去几十年内已逐渐成熟，它们在如何保护软件、计算机和网络方面已积累了相当多的专业知识。在当前的国家安全体系中，常规作法包括：一是将防火墙、入侵检测系统、杀毒软件、口令保护、扫描器、审计和加密之类的安全保护措施直接嵌入信息基础设施当中，就像目前在小规模环境中所做的那样；二是

① 艾兹格·迪科斯彻，《计算技术选读——个人视角》，Springer-Verlag，纽约，1982 年，第 212 ～ 213 页。

② 托马斯·弗雷德曼，《世界是扁平的——21 世纪简史》，Farrar, Straus,and Giroux，纽约，2007 年（对于本章中提到的全球性网络攻击趋势，弗雷德曼提供了有用的经济背景知识）。

将这些国家安全系统连接至集中式威胁管理系统，同时遵循人们所熟悉的企业流程模式进行事件响应；三是为确保符合安全策略，向那些构建和运行国家信息基础设施的人员提供终端用户认知、安全培训和第三方审计等常规程序计划。目前，所提出的几乎每一项国家信息基础设施保护计划都遵循了这种看起来非常直接的工作路线[①]。

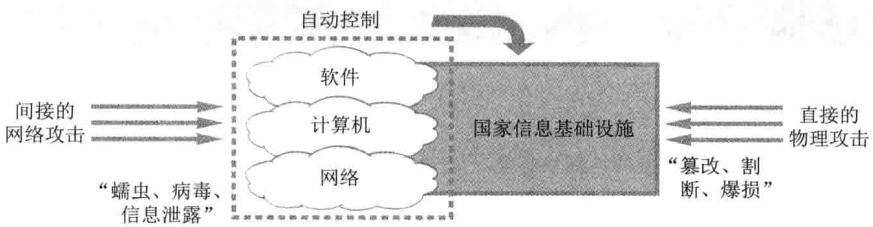

图 1.1 国家信息基础设施网络攻击和物理攻击

尽管这些知名的计算机安全技术肯定会对国家信息基础设施有用，但迄今为止的大多数实践经验表明，仅有上述传统方法并不够。一个主要原因在于复杂的国家信息基础设施本身的容量、规模和范围。例如，一家企业也许只包含规模可控的资产，而国家信息基础设施却需要异常强大的计算能力，来处理容量巨大的数据。对于典型的企业安全工具，如商业威胁管理系统来说，这种大数据量将轻而易举地超出其存储容量和处理能力。不幸的是，这种不兼容性与政府和业界的当前计划存在冲突，因为后者一直试图通过货架式通用商业产品的使用来实现降低基础设施成本。

此外，在发生安全灾难时，企业系统可以依赖本地专家的人工介入，而大规模国家信息基础设施一般需要安全专家团队按照预定流程来精心组织、协调应对。这些专家通常分布在不同的群体和组织，甚至不同的国家。最糟糕的情形是，只有受到政府强迫他们才会合作，并且通常只分享最少量的信息以规避法律后果。还有一个问题是，国家信息基础设施的复杂性会导致奇怪情况的发生，而响应团队却常对其中底层系统的工作方式一知半解或存在错误认识。出于这些原因，尝试将现有的小规模安全流程应用于响应大规模基础设施攻击，虽然看起来方便，但实际效果值得商榷（图1.2）。

因此，需要一种全新的国家信息基础设施保护方法，将现有计算机和网络安全技术中的精华部分与大规模复杂国家服务带来的特殊而艰巨的挑战结合在一起。本书提供的正是这样一种国家信息基础设施保护方法，它所依据的是 25 年来我们为政府、商业和消费者信息基础设施提供网络安全系统设计、建造和运行时所获得的实践经验，这些均物化为可应用到新的或现有系统中的一系列保护原则。由于国家信息基础设施的特殊需求，特别是其庞大的容量、规模和范围，上述保护方法中的某

① 总统行政办公室，《网络空间策略评估——确保可信且灵活的信息和通信基础设施》，美国白宫，华盛顿特区，2009 年（http://handle.dtic.mil/100.2/ADA501541）。