国防科技著作精品译丛
网电空间安全系列

Cybersecurity
Public Sector Threats and Responses

网电空间安全
——公共部门的威胁与响应

【美】 Kim Andreasson 著
李欣欣 方 芳 彭玉婷 马 亭 赵凰吕 缪 蔚 等译

CRC Press
Taylor & Francis Group
国防工业出版社
National Defense Industry Press

网电空间安全

——公共部门的威胁与响应

Cybersecurity: Public Sector Threats and Responses

[美] Kim Andreasson 著

李欣欣 方 芳 彭玉婷 等译
马 亭 赵凰吕 缪 蔚

国防工业出版社
National Defense Industry Press

著作权合同登记　图字：军-2012-068号

图书在版编目（CIP）数据

网电空间安全：公共部门的威胁与响应 /（美）安德雷森（Andreasson, K.）著；李欣欣等译. — 北京：国防工业出版社，2013.8
（国防科技著作精品译丛. 网电空间安全系列）
书名原文：Cybersecurity：Public sector threats and responses
ISBN 978-7-118-08596-9
Ⅰ. ①网… Ⅱ. ①安… ②李… Ⅲ. ①互联网络-安全技术-研究 Ⅳ. ①TP393.408

中国版本图书馆 CIP 数据核字（2013）第141606号

网电空间安全——公共部门的威胁与响应
[美] Kim Andreasson 著
李欣欣　方　芳　彭玉婷　马　亭　赵凰吕　缪　蔚　等译

出版发行　国防工业出版社
地址邮编　北京市海淀区紫竹院南路 23 号　100048
经　　售　新华书店
印　　刷　北京嘉恒彩色印刷有限公司印刷
开　　本　700 × 1000　1/16
印　　张　17¾
字　　数　228 千字
版 印 次　2013 年 8 月第 1 版第 1 次印刷
印　　数　1—2500 册
定　　价　78.00 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

译审组名单

翻　译：李欣欣　方　芳　彭玉婷　马　亭　赵凰吕
缪　蔚　王玉宝　张　鹏　刘　磊　缘珊珊
刘　阳　陈奇伟　江红玲　仝俊义

审　校：拜丽萍　张　龙　唐　斌　李东阳

译者序

《网电空间安全》一书的副标题是“公共部门的威胁与响应”，这就道出了本书区别于其他探讨网电空间安全问题书籍的独特之处，即关注公共部门如何应对网电空间安全挑战。本书主要描述当今社会公共部门在网电空间所面临的机遇、挑战与风险，重点介绍了美国、日本和欧洲国家政府机构以及国际电信联盟等国际性组织在网电空间安全领域开展的工作，并针对公共部门应对网电空间安全威胁的问题，提出了实用的建议与参考。

本书的编者主要来自世界各国政府部门、军事机构、知名高校与咨询公司从事信息与通信技术、公共政策与管理等领域工作的学者、政策制定者和咨询专家，对网电空间安全和公共部门政策具有深刻认识、独到见解和丰富的实践经验。原著的出版也得到了前美国总统行政办公室电子政府与信息技术领域资深管理者、“美国网电空间挑战”项目总监 Karen S. Evans 女士的大力支持，并亲自为本书作序。

本书的论述严谨系统，案例翔实生动，语言深入浅出，是一本能启发思考、引导发展的论著。为了更加直接地传递原文所表达的内容，并尽可能还原其本来的写作风格，本书主要运用直译的方法，在保证语义准确的前提下，最大限度地使用原著的句序、用词等。

本书的翻译出版过程前后经历了一年多时间，各个环节的参与人员都力求准确传达作者本意并注重每个细节的雕琢，在此向各位译者以及提供

帮助的众多专家与同仁表示由衷的感谢。在本书出版过程中，国防工业出版社崔晓莉编辑进行了大量的协调工作，并提出了很多有益的建议，在此也一并表示感谢。

由于水平有限，本书尚有不足之处，敬请广大读者批评指正。

译　者

2013 年 5 月

序一

Cyberspace 由 Cyber 和 Space 复合而成, Cyber 一词源于希腊语, 本意为管理和控制。1948 年, 控制论奠基者美国数学家诺伯特·维纳发表了《控制论》一书, 首次引入了以 Cyber 为词根的 "Cybernetics" (控制论) 一词, 赋予控制相关的含义。1954 年, 我国科学家钱学森在美国出版的英文版《工程控制论》中也使用了 Cybernetics 一词。进入 21 世纪, Cyber 被赋予了更多新的含义, 代表了以综合集成、计算机网络和人工智能为基础的现代的管理和控制。

Cyberspace, 国内目前大多译成赛博空间或网络电磁空间 (即网电空间)。Wikipedia 对网电空间的解释是可以通过电子技术和电磁能量调变来开发与访问利用的电磁域空间, 并借助此空间以实现更广泛的通信与控制能力。网电空间集成了大量的实体, 包括传感器、信号连接与传输、处理器、控制器, 与实际的地理位置无关, 以通信与控制为目的, 形成一个虚拟集成的世界。

在现实中, 网电空间构建了相互依赖的信息技术基础设施网络与电信传输网络, 如因特网、计算机系统、综合传感器、系统控制网络、嵌入式处理器、通用控制器等。从社会的角度讲, 可以通过网电空间实现信息的交换与分享, 服务的提供, 活动的组织等。美国已经将网电空间作为其核心的关键的基础设施。

对网电空间的认识尚处在不断深化的阶段。对于网电空间安全问题，美国兰德公司在 1995 年进行了一次想定：美军向沙特派兵直接威胁到伊朗，而伊朗打破常规，避实就虚，不在沙漠与美军做常规的正面较量，转而动用大量网电专家，将攻击目标悄然锁定美国的经济命脉。最终推演的结果是：各种计算机病毒使华盛顿信息系统运行失灵，股市狂泻；逻辑炸弹使交通混乱，民航系统瘫痪；军事指挥系统和数据库遭到严重摧毁，作战系统发生紊乱，直至美军不战而退。这个推演结论令美国政府和军方大为震惊。时隔 12 年，爱沙尼亚成为历史上第一个政府和关键基础设施经历大规模网络攻击的国家，当分布式拒止服务攻击横扫重要行业和政府部门网站（包括爱沙尼亚议会、银行以及媒体集团）时，该国各方面的运行瘫痪了数周。2010 年 9 月，“震网”计算机蠕虫入侵了伊朗布什尔核电站的计算机系统，导致有毒的放射性物质泄漏，其危害不亚于 1986 年发生的切尔诺贝利核电站事故。

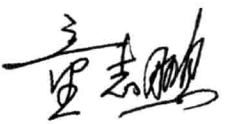
如今，随着科学技术特别是信息技术的空前发展，使得“信息疆域”成为国家利益的重要战略空间。这一空间不仅包括了人们通常所理解的狭义互联网，更包括了高效运行的诸如金融、电力、电信、运输、能源、军事等事关国家安全、社会保障体系及其核心命脉的网络系统。所以，我们在看到信息时代在为国家和人们生活提供了全新的机遇和发展空间的同时，也必须高度重视网电空间带来的新的安全威胁。

当前，许多国家信息与网络安全防护体系建设尚处在不断完善的关键阶段，网电空间安全事件屡屡发生。除网络战争外，网电空间领域的非传统安全危机正严重威胁到各国的安全与利益，这种威胁不同于传统的网络攻击或数据窃取，而是以一种更加隐蔽的形态存在于各国网络生活中，对于设防薄弱的网电系统而言，一旦被侵袭控制和利用，轻则导致经济损失和社会生活混乱，重则可成为兵不血刃的利器，导致整个战略目标运行体系陷入崩溃。因此，应对网电空间时代的非传统安全威胁将成为各国重要任务。

国内外学术界对网电空间的探讨如火如荼。目前该领域的论著主要集中在两个主题，一是网电空间本身的定义、内涵、范围、作用及其影响；二是网电空间战，包括其涉及领域、作战范围、作战形式、作战力量、进攻与防御、影响与危害等。本书是第一本从战略规划与战略决策的角度出发，

聚焦公共部门网电空间安全威胁及其响应方法的论著，书中描述的网电空间攻击案例为全世界敲响了警钟，国际组织和各国政府网电空间安全政策措施可为我们提供决策参考。本书的翻译出版具有相当的现实意义。

中国工程院　院士



2013 年 6 月 18 日

序二

“网电空间” (Cyberspace, 又称 “赛博空间”) 一词最早出现在 1984 年威廉·吉布森 (William Gibson) 的科幻小说《神经漫游者》(Neuromancer) 一书中。吉布森用险象环生的故事将人们带入了一个梦魇般的世界, 一个“屏幕之中的真实空间, 这一空间人们看不到, 但知道它就在那儿。它是一种真实的活动领域, 几乎像一幅风景画!” 这个幻想空间里不仅有人类的思想, 还有人类制造的各种虚拟智能系统。近三十年后的今天, 吉布森所描述的空间却真真切切地出现在我们的现实世界里, 并上演着更加变幻莫测、扣人心弦的故事。

随着人类社会实践和技术的发展, 经过三十多年的演进, “网电空间”一词已拥有更深刻、更广泛的内涵。人们对它的认识经历了从传统的网络空间概念到一种涵盖物理逻辑和社会领域全新理念的过程。它是一个真实存在的客观领域, 被列为与陆、海、空、天并存的第五维空间, 其间发生的行为并非只能创造虚拟效果, 而是虚实融为一体, 将人类带入了一个更加广阔、绚丽多彩的世界, 并对现实世界产生全面实在的影响。

随着信息化时代的到来, 网电空间的触角迅速延伸至政治、经济、军事、文化、外交等各个领域, 世界各国公共部门都在积极利用该空间带来的优势, 不断提升服务便利度、提高业务透明度、增强管理职能、降低运行成本。它为我们带来的好处不胜枚举: 不出家门即可办理要办的业务, 不费周折就能获取想要的信息, 能更好地对公共权力进行监督, 能更多地参与

公共事务……。然而，网络系统越发达的国家，在面对威胁时也越脆弱。因为，网电空间覆盖的范围有多广，可能遭到攻击的范围就会有多大。

网电空间里的对抗从未停歇，并且愈演愈烈。此间的对抗并非都是像以色列“舒特”系统突破叙利亚防空系统这样的军事行动，更多是以公共部门信息化设施为目标：2008 年，“蜂群”式服务拒止攻击重创格鲁吉亚政府网络，使其在“俄格冲突”中劣势凸显；2009 年，大规模网络攻击突袭美国和韩国政府网站，引发民众恐慌；2010 年，“震网”病毒神秘出现，成功破坏伊朗核设施，开创网电手段攻击国家关键基础设施的先河；还有“维基解密”披露大量机密文件，引发美国政府外交危机……。这些事件无一不在提醒我们，网电空间正日益成为国家之间利益争夺的焦点，而公共部门则正处在这焦点的最前沿，所面临的威胁也与日俱增。

关注网电空间带来的机遇与挑战，抢占网电空间战略制高点，公共部门首当其冲，责无旁贷。在这场战略博弈中，美国政府率先打出了一套“组合拳”—— 确立核、太空、网电空间“三位一体”的新国家安全布局，组建战略层面的网电司令部，制定网电空间行动战略，建设“国家网电靶场”，策划“网电风暴”系列演习 —— 以期在网电空间中确立其“领头羊”的地位。其他国家也不甘落后，纷纷针对网电空间出台战略“蓝图”，制定发展“路线图”，描绘技术“创新图”。英国、俄罗斯、德国、法国、日本、印度等国家相继设立了专门的网电空间部门，成立相应的军事机构，出台新的网电空间政策，以网电空间为背景的军事演习也陆续拉开帷幕。

围绕网电空间主导权、控制权、话语权的争夺愈演愈烈，本书正是在这种剧烈变化的大背景下，从全球趋势、国家与地方政策、实际措施三个方面展开论述。首先探讨了世界范围的电子政府趋势及其带来的影响，分析了日益普遍的网电空间威胁事件，然后介绍了各国政府与国际组织当前的网电空间安全政策，并通过具体案例，分析了各级公共部门在网电空间安全领域扮演的角色，最后为公共部门应对网电空间挑战提供了一些实用性的建议与参考。

参与原著编写的作者是一个世界级的专家群体，他们有的担任联合国电子政府顾问，有的是国际电信联盟的信息技术专家，有的曾为世界各地相关部门提供信息社会与知识经济方面的咨询服务，有的是网电空间公共政策方面的知名学者。这些作者横跨计算机、电子、法律、公共关系、战略咨询、风险管理等多个专业领域，从技术、政策、法律等多维角度对网电空间问题进行了深入剖析。因此，本书的观点和论述具有相当的权威性。作者们的合作，在本书中产生了奇妙的化学反应，带给人耳目一新的感受，

同时启发思考、指引方向。

面对这波涛汹涌的发展现实和严峻的威胁与挑战，我们决不能掉以轻心和等闲视之。为了我国家利益和长治久安，我们必须以战略眼光和全球视角，发展网电空间威慑力量，建设网电空间制衡手段，以捍卫我国在“第五维空间”的主权与安全。本书正是第一本从公共部门角度出发，聚焦网电空间安全威胁与响应机制，以及相关战略、政策与措施的论著，对我们有很强的借鉴与指导意义。同时，它以严谨系统的论述和生动翔实的案例，向人们证实了网电空间安全并不只是 IT 专家的事，更是政府、社会乃至我们每个人必须考虑的问题。因此，深入研究本书中描述的全球趋势、机遇挑战与应对策略，师夷长技以自强，是非常必要和及时的。

军事专家

2013 年 3 月　北京

序

Karen S. Evans

“当我们最初开始这项进程的时候 …… 人们并不知道他们不知道什么。”

Karen S. Evans

美国联邦管理与预算办公室, 电子政府与信息技术负责人。
摘自 2008 年 2 月 28 日于美国议院国土安全委员会所作的发言。

在网电安全这个发展迅速且瞬息万变的领域里, 没人能错失任何一次学习机会。因此, 不管这个机会在何时何地出现, 你和你的团队最好随时准备着, 因为你对待它的方式可能决定了你能否成功驾驭风险和时刻保护你的组织。

就是这样一个学习机会在 1996 年来到我面前, 深刻影响了我个人的观点以及我团队的信息技术资源与服务工作。那一年, 所有联邦政府部门和机构都被要求建立官方网站, 为公众提供在线服务。那时候, 电子邮件正在逐渐普及, 互联网也越来越盛行。我们团队要为司法部的互联网服务打 “地基”, 为之搭建运营环境。

然而, 就在环境建成前的那个周末, 司法部网站被黑客攻击了。我们一边竭尽全力进行恢复, 一边还得向领导报告、向执法机构提供信息, 找出漏洞所在, 制定解决方案。这件事重塑了我对风险管理、政策、认证鉴

定以及机构 “响应” (而非 “反应”) 能力的看法。就在那个周末, 我认识到了备份、沟通、响应计划、配置管理还有政策的重要性。

“政策” 真应该成为专有名词而非泛泛所指, 因为我认识到, 操作层面上有效政策的重要性不容小视。司法部也有其政策, 而且我们根据其政策认真撰写了必要的文件。但我们所写的实际上都还很初级, 不是最终需要的东西, 因为我们在重视技术的同时往往忽略了风险评估的其他关键因素。我认识到, 要形成能持续有效评估风险的政策, 必须采用一种更具整体性的、考虑更全面的方式, 能同时照顾到生产、技术以及服务风险等各方面因素。

所有这些都引出了如下问题: “风险是什么?” 提供服务的过程中高层领导希望施加多少安全控制? 有没有互补性控制手段? 事件发生时如何响应? 对于我 —— 联邦管理与预算办公室的电子政府与信息技术负责人、管理者和首席信息官 —— 来说, 这些问题在评估可能提供的服务、项目、投资、政策和法规时非常关键。向高层领导说明技术风险很重要, 不管他们是联邦政府的部门领导, 还是公司的首席执行官。他们需要确认风险已经被明确, 还要知道管理这些风险的方法和应对服务故障的计划。

联邦政府出台了一系列法规来规范信息资源管理的发展, 如 1987 年的 “计算机安全法案”、“政府信息资源安全法案” (后来成为 “联邦信息安全管理法 (FISMA)”) 和 2002 年的 “电子政府法案”。这些法案催生了很多政策, 如管理与预算办公室的各种通知、备忘录和指南, 包括国家标准与技术研究所 (NIST) 发布的指南和刊物。政策已经足够繁杂了, 但最基本的问题还是:

(1) 风险是什么?

(2) 风险可以控制吗?

(3) 你是否能承担尚存的风险?

(4) 服务受阻时你的响应计划是什么?

根据所处环境不同, 这些问题的答案可能异常复杂, 但是不管是什么组织、处于什么环境, 服务提供者都应建立响应机制和制定相关战略。在鉴定认证 (C&A) 领域, 必须经过指定的授权官员授权后, 才能开始运营。很多人批评 C&A 流程只是纸上文章, 我承认自己也并非真心认可这些流程, 直到我亲身经历了前面所述的 “学习机会” 并看到我的项目登上了报纸头版头条。我遵守规则, 但没有真正理解这是为了将风险降至可控水平。希望不是每个人都要经历我们所经历的 “危机周末” 后才能将自己掌握的知识落到实处。我认为, 不管在公共部门还是私营部门, 风险管理都是成

功的关键因素。

在风险管理中还有其他要考虑的因素，例如建立系统所需的资金、时间等。我不直接讨论资金的问题，虽然资金会影响计划，而且对降低服务风险的能力有明显影响，然而，就算全部资金都到位，设计的解决方案也可能太过复杂，耗费大量时间，导致漏洞出现。

公共部门提供的服务必须是成本最小化和纳税人利益最大化的。20世纪人们在信息安全方面自顾自的模式已经不再适用。现在，从联邦政府、各州到各地的所有部门、机构、项目都不可能在封闭环境中运行，不能画地为牢，更不可能干脆停止所有业务。当今世界，我们不能总是指望临时应急措施，而是要主动创造一个吸引计算机高手并且能保障信息和数据完好的环境。

在我们走向电子政府的过程中，关键问题不是关于技术，而是关于信任与责任，关于最大化利用职权。我们曾说，“在保障隐私和安全的同时，你将花同样甚至更少的价钱，得到同样水平甚至更好的服务”。这个基本目标并未改变。

最后我要回到最根本的问题 —— 风险。我们是否知道谁在从我们的网络获取服务？他们是否有权获取这些服务和数据？了解系统和对系统分类对于组织规划至关重要。利用组织构架及相关支撑行动等工具能帮助我们了解风险管理的局势和制定必要的过渡规划，从而将有效的系统落实到位。把这项工作与财务计划结合起来，能帮助我们制定能最好地支撑风险管理系统的投资战略，而风险管理系统对企业当前与未来安全非常重要。

Karen S. Evans

前言

全球互联网正在迅速发展。据联合国专门机构国际电信同盟 (ITU) 预测, 到 2015 年将有 50 亿网民。同样据 ITU 估计, 目前有 143 个国家提供 3G 服务, 可能通过智能手机向预计 53 亿移动用户提供互联网通道, 其中有 38 亿来自发展中国家。

然而不幸的是, 随着网络化程度越来越高, 我们面对网电威胁也越来越脆弱。本书对全世界的网电安全趋势与战略进行分析, 以引起人们重视, 并初步探讨了公共部门的网电安全问题。大体来讲, 公共部门网电安全问题就是计算机系统 (包括互联网网站) 在抵御未授权访问或攻击方面的脆弱性问题, 以及相关的防护政策措施。

要理解公共部门的网电安全问题, 必须认识到有三种力量正在融合, 即全球化、互联化和公共部门职能网络化 (俗称电子政府)。

互联网为所有人提供了一个参与全球化的共同平台。你可以在任何地方同样方便地登录某个网站, 全世界人们都在兴冲冲地这么做。根据 "互联网世界数据" 网站 2011 年初发布的数据, 互联网用户的数量在过去十年内增长了 445%, 全球渗透率达到 29%。信息与通信技术 (Information and Communication Technology) 能带来众多益处, 因此世界各国也在努力使其剩余的国民也享受到网络服务。咨询研究机构 "麦肯锡全球研究所 (Mckinsey Global Institute)" 于 2011 年 5 月发布的一份报告称, 八国集团、韩国、瑞典、巴西、中国和印度等国 GDP 中互联网所占份额为 3.4%; 在成熟经济体中, 过去五年的 GDP 增幅有 21% 来自互联网。

欧洲统计机构 “欧盟统计局 (Eurostat)” 的数据表明, 欧盟 15 国的家庭中拥有互联网连接的比例在 2002 年是 39%, 到 2010 年达到 68%。2000 年, 韩国家庭中 30% 拥有宽带网络连接, 到 2009 年这个数字达到 96%。同一时间内, 美国家庭拥有宽带网络连接的比例从 4% 上升到了 64%。这些数据都来自经济合作与发展组织 (OECD), 该组织的报告还称, 宽带包月平均价格在 2010 年下降到了约 40 美元。

人们花在网络上的时间也越来越多。根据 comScore 咨询公司的数据, 2010 年美国人 “平均” 每月花 32 小时在互联网上, 尽管事实上有 1/5 的美国人是完全不上网的。

我们对互联网的依赖可能有增无减。例如, 射频识别 (RFID) 技术的发展和互联网协议 6 (IPv6) 的引入提供了一个创建 “物联网” 的平台。“物联网” 通俗地说就是将所有事物联网, 包括汽车这样的日常事物。为什么不能在紧急情况下远程解开车锁呢? 或者在车里加装无线设备以获取更好的通信服务?

互联网带来了众多便利, 因此也被公共部门积极利用。互联网帮助提高效率的一个典型例子是网上纳税。2011 年瑞典税务部门预计有 65% 的人在网上纳税, 既为政府节省时间、金钱和劳动, 也为自己带来方便。联合国 2003 年 “世界公共部门报告” 中清楚写道,“政府越来越意识到利用电子政府来改进公共服务的重要性” (第 128 页)。但是网络环境带来的不仅仅是便利服务, 还为各级政府提供了改进可靠性、发展、效率和透明度的机会。

多项国际电子政府基准调查表明过去十年取得了很大进展, 以下观点部分证明了这一点: 世界大多数国家已经 “电子就绪”。因此, 对联合国来说, 评估标准已经从 “是否就绪” 变为 “是否取得实际进展”。经济学家情报机构 (Economist Intelligence Unit) 咨询公司甚至将其报告沿用十年的名称 —— “电子就绪度排名” 在 2010 年改为 “数字经济排名”, 以此来反映这种趋势。根据欧洲第九份电子政府基准报告, 欧盟 27 国 20 项重要在线公共服务的平均可用率从 2009 年的 69% 上升到了 2010 年的 82%, 这足以说明发展之快。

尽管对电子政府的需求 (利用) 滞后于其可用性 (供应), 但各地政府都在鼓励居民使用在线服务、利用在线信息。在欧盟 27 国, 16 岁至 74 岁的人群中 42%正在利用互联网与公共部门进行交流。“数字日程 (Digital Agenda)” 是欧盟为利用数字工具来发展经济制定的战略, 其中一个关键目标是让上述数字在 2015 年达到 50%。网络融合, 或者电子融合, 也是 “数