装备科技译著出版基金

国防科技著作精品译丛

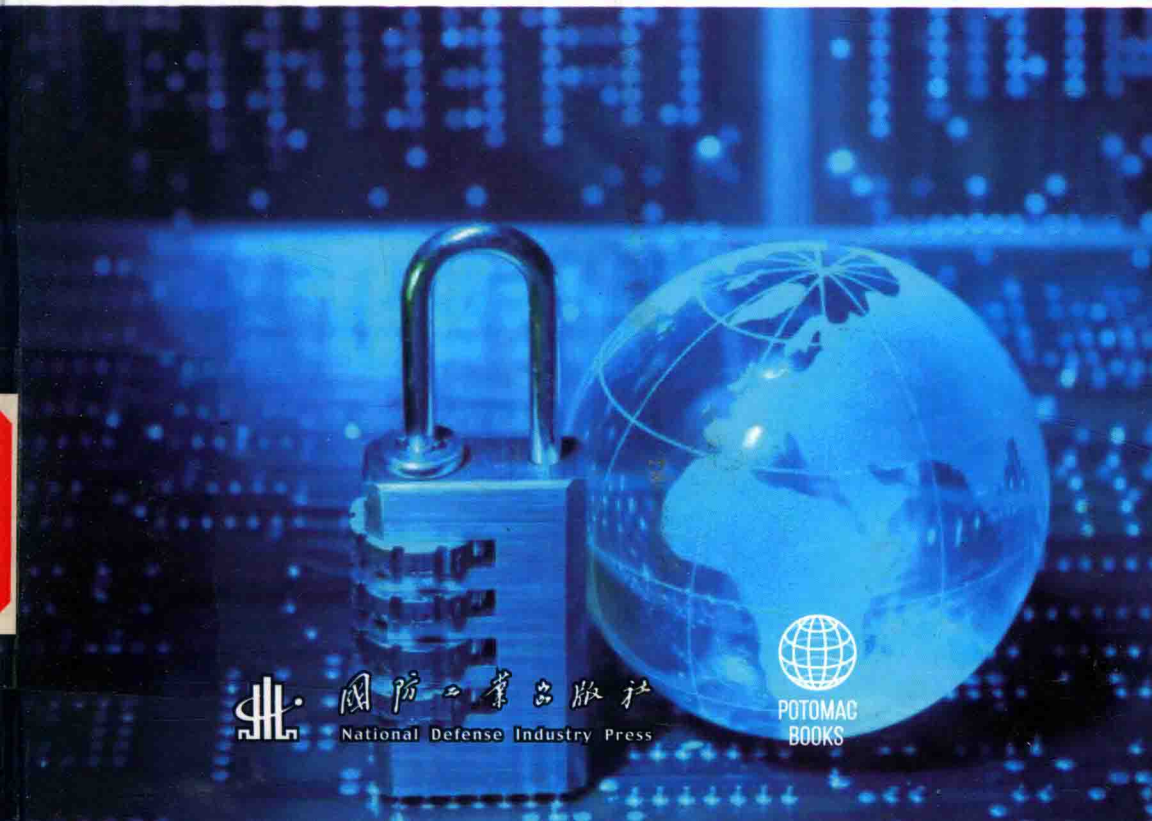
网电空间安全系列

Cyberpower and National Security

赛博力量与国家安全

【美】Franklin D. Kramer Stuart H. Starr Larry K. Wentz 编著

赵刚 况晓辉 方兰 王东霞 许飞 唐剑 译



国防工业出版社
National Defense Industry Press

POTOMAC BOOKS

装备科技译著出版基金

赛博力量与国家安全

Cyberpower and National Security

[美] Franklin D. Kramer
Stuart H. Starr
Larry K. Wentz

赵 刚 况晓辉 方 兰
王东霞 许 飞 唐 剑 译

国防工业出版社
National Defense Industry Press

著作权合同登记　图字：军 - 2011 - 089 号

图书在版编目（CIP）数据

赛博力量与国家安全/(美) 弗兰金·D. 克拉默 (Franklin D. Kramer),
(美) 斯图尔特·H. 斯塔尔 (Stuart H. starr), (美) 拉里·K. 温茨 (Larry K. Wentz) 编著;
赵刚等译. — 北京: 国防工业出版社, 2017. 1
(国防科技著作精品译丛. 网电空间安全系列)
书名原文: Cyberpower and National Security
ISBN 978-7-118-10889-7

Ⅰ. ①赛… Ⅱ. ①弗… ②斯… ③拉… ④赵… Ⅲ. ①计算机网络-安全技术
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2016）第 295275 号

赛博力量与国家安全
Franklin D. Kramer　Stuart H. Starr　Larry K. Wentz　编著
赵　刚　况晓辉　方　兰　王东霞　许　飞　唐　剑　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责任公司
开　　本　710 × 1000　1/16
印　　张　38 ¾
字　　数　650 千字
版 印 次　2017 年 1 月第 1 版第 1 次印刷
印　　数　1—2000 册
定　　价　178.00 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

译者序

随着人类大踏步进入信息社会，赛博空间已经渗透到国家的政治、军事、经济、文化、外交以及社会生活的方方面面。赛博空间相关问题，事关国家战略安全和发展，引起了世界各国的高度重视。这是一个摆在各国面前的全新的综合性领域，相关研究已成为国际热点。尤其是美国，在技术、战略和行动上都走在了世界前列，了解其认识、做法、经验和教训无疑有着重要的价值。但是，系统梳理、研究相关问题的书籍还不多见。本书原版由美国国防大学技术与国家安全策略中心编撰出版，从国家安全和战略角度，较系统地总结介绍了与赛博空间及国家安全相关的各类战略性问题，作者都是该领域世界级的专家学者，有相当的权威性。我们把这本书翻译介绍到国内，相信对这一领域的研究很有意义。

翻译这本书的难度超出我们原先的预料。一个原因是本书涉及领域太宽，包括了政治、军事、外交、法律、技术、舆论等方面，每个领域都有其自己的术语和知识体系，准确把握这些是很困难的。另一个原因是内容新，很多词汇的翻译在国内还没有定论。例如，“Cyberspace”这个词，如何翻译有很大争议，我们了解到的就有网络空间、网电空间、信息空间、赛博空间、控域、网空、网域等等。经过反复斟酌，我们采用了音译的方法，主要基于以下考虑：一是没有合适的中文词汇，由本书的内容可知，该词内涵丰富，中文确还没有合适的、同等含义的词与之对应；二是避免混乱，虽然在很多中文权威文献中，把该词译为“网络空间”，但在本书中，有不少同一段落同时出现“Cyber”和“Network”的情况，把“Cyber”也译为“网络”或“网”会带来极大的混

乱；三是翻译上有此先例，中文也还顺畅。因此，我们把 “Cyberspace” 译为 “赛博空间”，由此，“Cyber” 也自然译为 “赛博” 了。再一个词就是 “Cyberpower”，这个词也是本书的核心词，直接出现在书名中，困扰我们的是与另外两个词的类比 —— “Seapower” 和 “Airpower”，在很多战略和军事类书中，把它们分别译为了 “海权/制海权” “制空权”，最著名的是马汉的《海权论》。如果仅就书名来说，我们开始很想把该词译为 “制网权”，这样书名就是 “制网权与国家安全”，还是很吸引眼球的。在决定把 “Cyber” 译为 “赛博” 后，就成了 “制赛博权”，虽然中文气势上不如 “制网权”，也还可以接受。但在本书具体章节的翻译中，我们渐渐感到，翻译为 “制 × 权” 有很大不妥：一是军事味道过浓，把这个词也涉及国家其他方面的内涵淹没掉了；二是 Cyberpower 是国家众多力量或手段之一，需要发展、建设和运用，而 “权” 这个词不便表达这样的含义，尤其是很多上下文讨论的都是力量或手段建设，很难与 “权” 挂钩。因此我们索性将该词直译为 “赛博力量”，但对 “Seapower” 和 “Airpower”，在一些已经约定俗成的地方，我们采用了 “海权/制海权” “制空权” 的译法，而在讨论其力量或手段建设时，一般还是翻译为 “海上力量” 和 “空中力量”。如此等等，还有很多。限于译者水平有限，翻译中定有很多错误和不当之处，请读者批评指正。

参加本书翻译和校对的有赵刚、况晓辉、方兰、王东霞、许飞、唐剑。由于工作繁忙和水平有限，翻译此书前后用了两年多的时间，在此我们深表感谢和歉意。

译者

2016 年 10 月 25 日

编者

Franklin D. Kramer 是一位独立顾问, 担任过国防大学技术与国家安全政策中心特聘研究人员。Kramer 先生是两任政府的高级政策顾问, 在威廉 · 克林顿总统、国防部部长佩里和国防部部长科恩任职时期担任负责国际安全事务的助理国防部部长, 此前担任总统吉米 · 卡特和国防部部长哈罗德 · 布朗的首席副助理国防部部长。

Stuart H. Starr 是国防大学技术与国家安全政策中心特聘研究员。他还同时担任巴克罗夫特研究所 (Barcroft Research Institute) 主任, 负责指挥和控制 (C^2) 问题的咨询研究, 担任国防工业的高级咨询委员会委员, 在全球进行 C^2 问题的讲座, 并是一些一流委员会的成员。此前, Starr 博士曾在 MITRE 公司、国防分析研究所和国防部部长办公室工作。

Larry K. Wentz 是国防大学技术与国家安全政策中心高级研究员, 负责指挥与控制问题的研究, 曾任 MITRE 公司的联合和防务领域指挥、控制和通信部门的技术总监。他是一位经验丰富的经理、战略策划人员, 以及指挥、控制、通信、计算机、情报、监视、侦察 (C^4ISR) 系统工程师, 在核 C^2、政府 C^2 衔接、多国部队的 C^2, 指挥、控制、通信、情报系统的互操作性, 保障维和的民事军事行动和信息作战行动, 以及其他许多军事 C^4ISR 系统的活动等方面, 具有十分丰富的经验。

撰稿人

Charles L. Barry 是国防大学技术与国家安全政策中心高级研究员。他也是巴里咨询公司 (Barry Consulting) 的主要负责人, 该公司是一个关注战略规划、国家安全和信息管理的机构。**Barry** 博士在美军中曾担任过作战指挥人员, 在欧洲和华盛顿担任了 9 年高级战略规划人员。他的研究领域涵盖了指挥和控制网络、多国部队和民事军事组织机构设置。

Marjory S. Blumenthal 自 2003 年 8 月起担任乔治城大学学院副院长。1987 年 7 月至 2003 年 8 月担任美国国家科学院计算机科学与通信委员会执行主任, 其间规划、指导、管理计算和通信领域有关技术和政策问题的协作研究项目、论坛和专题讨论会。Blumenthal 讲授并指导学生互联网政策方面的内容, 她在该领域已持续耕耘多年。

Chris Burrow 在本书撰写期间是 Zeichner 风险分析公司的研究助理。

Gerard J. Christman 是 Femme 股份有限公司 (FCI) 的项目经理, 主要负责配合网络和信息集成的助理国防部部长工作。在 2003 年加入 FCI 前, 他曾担任美国陆军通信兵军官长达 23 年。

David D. Clark 自 20 世纪 70 年代以来一直引领着互联网的发展。1981 年到 1989 年, 他是互联网发展的主要协议架构师, 并主持互联网活动委员会。他是国家研究委员会计算机科学与电信委员会前主席, 并且是麻省理工学院的高级研究员。

Maeve Dion 是乔治 · 梅森大学法学院关键基础设施保护计划的

项目经理。

Leon Fuerth 是乔治·华盛顿大学 Elliot 国际事务学院国际事务研究教授。他是副总统戈尔的国家安全顾问, 并在国家安全委员会下部长级委员会任职。

Daniel T. Kuehl 在国防大学信息资源管理学院教授军事战略和国家安全政策课程。他是信息战略集中项目 (Information Strategies Concentration Program) 的负责人。该项目为国家战争学院、武装部队工业学院的相关学生提供国家力量中信息相关部分的专业课程。

Richard L. Kugler 曾任国防大学技术与国家安全政策中心特聘研究教授。他的专长是美国的国防战略、全球和北大西洋公约组织 (北约) 的安全事务。Kugler 博士为国防部部长办公室、参联会和跨部门组织的高层人员提供建议。他是关于美国国防战略和计划、北约和全球安全事务的多本书籍、文章、官方研究报告的作者。

Harold Kwalwasser 是华盛顿特区的一名独立电信业顾问。他是美国国际电信联盟协会的主席, 该组织由对国际电信联盟的运作有兴趣的电信业相关公司和顾问组成。此前,Kwalwasser 先生从事法律工作 16 年。

Irving Lachow 是国防大学信息资源管理学院的高级研究教授, 教授信息保障、关键基础设施保护、信息作战的国际视野、全球企业网络和电信等课程。Lachow 博士曾为 Booz Allen Hamilton 公司、兰德公司、国防部副部长助理办公室 (负责先进系统与概念) 工作。

Martin C. Libicki 自 1998 年以来担任兰德公司的高级政策分析员, 研究信息技术和国家安全之间的关系。此前, 他曾在国防大学国家战略研究所担任高级研究员 12 年。Libicki 博士曾撰写大量信息技术标准以及军事革命和信息战领域的文章。

John A. McCarthy 在本书撰写期间是乔治·梅森大学法学院关键基础设施保护项目 (现在的基础设施保护中心) 主任。该中心整合了法律、政策和技术以进行全面的基础设施保护相关的国内和国际安全研究, 并为关键基础设施利益相关者提供对美国关键基础设施的赛博、物力、人力和经济框架方面有价值的分析。

William D. O'Neil 是一名私人顾问和作家。他曾担任海军军官和国防部文职官员, 以及私营企业的工程师和总经理。

Olivia Pacheco 是乔治·梅森大学法学院基础设施保护中心 CIP 报告的编辑。

Gregory J. Rattray 是三角洲风险咨询公司 (Delta Risk Consulting)

的合伙人, 为政府和私营部门的客户提供风险管理策略和赛博安全能力建设方法。在作为美国空军军官的 23 年期间, 他担任白宫国家安全委员会负责赛博安全的主任, 领导国家的政策发展和国家安全委员会对赛博安全的监督, 他指导了对伊拉克电信重建的监督。他是外交关系委员会的正式成员。

Edward Skoudis 是 Intelguardians Network Intelligence 有限责任公司的创始人和高级安全顾问, 该公司是总部位于华盛顿特区的网络安全咨询公司。他也是 SANS Internet Storm Center 的教练。他的专长包括黑客攻击和防御、信息安全产业以及计算机隐私问题。他做过众多安全评估, 为财富 500 强企业筹划过信息安全管理和运营团队, 为在金融、高科技、医疗保健和其他行业的客户做过计算机攻击响应。

Timothy L. Thomas 是堪萨斯州莱文沃斯堡外国军事研究办公室的高级分析师。1993 年以美国陆军中校身份退休前, 是专注于苏联/俄罗斯等国外地区研究的官员。Thomas 先生在维和、信息战、心理战、低强度冲突和政治军事等领域做了广泛的研究, 并出版了专著。

Clay Wilson 退休前是美国国会研究服务部 (CRS) 外交事务、国防和贸易分部的技术和国家安全研究专家。此前, 他在马里兰大学和国家圣路易斯大学教授计算机的安全性和风险分析。Wilson 博士在关键基础设施协调小组担任政府代表, 以促进产业界和政府遵守美国总统第 63 号决策指令展开合作。

Thomas C. Wingfield 是弗吉尼亚州贝尔沃堡美国陆军指挥和参谋学院的副教授。他也是美国天主教大学哥伦布法学院的讲师, 波托马克政策研究所兼职研究员, 乔治敦公共政策研究所兼职教授。Wingfield 先生专门研究武力使用问题, 特别是信息作战中武装冲突法的应用问题。

Elihu Zimet 曾任国防大学技术与国家安全政策中心的特聘研究员。此前, Zimet 博士曾领导海军研究办公室的远征作战科学与技术部门, 指导导弹、定向能、飞机和隐身以及海军陆战队科学和技术支持等领域的科学和技术项目。

前言

赛博领域正在经历翻天覆地的变化, 给其使用者带来异乎寻常的机遇。这种变革不但表现在赛博空间参与者数量的不断增长, 而且表现在参与者在技术及社会层面的质量。例如, 到 2010 年, 估计有 20 亿用户连接互联网。如果 Myspace 网站的用户组成一个国家, 那么它的人口总数可排在世界第 11 位。然而, 赛博空间在发展变化的同时也带来了诸多挑战。这些挑战主要源于赛博空间中的恶意用户 (如恐怖分子和罪犯), 以及一直困扰着这个空间的众多安全脆弱性 (如拒绝服务攻击、敏感数据的非法获取或破坏等)。

为了充分利用赛博空间所带来的机遇, 克服面临的挑战, 需要着手对赛博领域的相关知识体系进行系统梳理。本书由美国国防大学技术与国家安全政策中心编撰出版, 作者都是该领域世界级的专家学者。本书的特色是从整体的视角阐述了赛博领域内的复杂问题, 给出了赛博域相关知识体系的基础。

本书的主要贡献之一, 是系统梳理了各种场景下赛博所面临的关键问题, 并有针对性地向决策者提出了全面的措施建议。同时, 本书也指出了高层决策者在不久的将来必须关注的赛博领域关键问题, 包括建立解决赛博问题的人力资源储备、在公民自由和国家安全间取得平衡、为应对赛博挑战开展国际合作等。我们强烈推荐那些已经认识到赛博领域的机会, 并决心克服所面临挑战的人阅读此书。

目录

第二部分 赛博空间