



国防科技著作精品译丛

Deterring Cyber Warfare:
Bolstering Strategic Stability in Cyberspace

威慑赛博战—— 加强赛博空间的战略稳定性

【美】布瑞恩·M·马赞内克 (Brian M.Mazanec) 著

【冰】布拉德利·A·塞耶 (Bradley A.Thayer)

况晓辉 李响 曹华阳 林哲超 张超 译



国防工业出版社
National Defense Industry Press

威慑赛博战——加强赛博空间的战略稳定性

Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace

[美] 布瑞恩·M·马赞内克 (Brian M. Mazanec)

[冰] 布拉德利·A·塞耶 (Bradley A. Thayer) 著

况晓辉 李响 曹华阳 林哲超 张超 译



国防工业

National Defense Industry Press

著作权合同登记 图字：军 -2018 -002 号

图书在版编目 (CIP) 数据

威慑赛博战: 加强赛博空间的战略稳定性 / (美) 布瑞恩·M·马赞内克 (Brian M. Mazanec), (冰) 布拉德利·A·塞耶 (Bradley A. Thayer) 著; 况晓辉等译. — 北京: 国防工业出版社, 2019. 4

(国防科技著作精品译丛)

书名原文: *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*
ISBN 978-7-118-11783-7

I. ①威… II. ①布… ②布… ③况… III. ①信息战—研究 IV. ①E869

中国版本图书馆 CIP 数据核字 (2018) 第 292549 号

First published in English by Palgrave Macmillan, a division of Macmillan Publishers Limited under the title *Deterring Cyber Warfare* by Brian M. Mazanec and Bradley A. Thayer. This edition has been translated and published under licence from Palgrave Macmillan. The author has asserted his right to be identified as the author of the Work.

B. M. Mazanec et al., *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* © Brian M. Mazanec and Bradley A. Thayer 2015

本书简体中文版由 Palgrave Macmillan 授权国防工业出版社独家出版发行, 版权所有, 侵权必究。

威慑赛博战——加强赛博空间的战略稳定性

[美] 布瑞恩·M·马赞内克 (Brian M. Mazanec)

[冰] 布拉德利·A·塞耶 (Bradley A. Thayer) 著

况晓辉 李响 曹华阳 林哲超 张超 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 天津嘉恒印务有限公司

开 本 710 × 1000 1/16

印 张 7

字 数 98 千字

版 次 2019 年 4 月第 1 版第 1 次印刷

印 数 1—1500 册

定 价 48.00 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

随着信息技术的快速发展和广泛应用，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各个方面。同时，赛博空间安全问题日益突出，已经成为各国面临的严峻威胁和重要挑战。为有效应对赛博攻击带来的安全威胁，赛博威慑等相关研究逐渐成为国际热点。美国不但在赛博空间战略、政策、力量和技术等方面均走在世界前列，而且作为威慑概念的提出者，也在积极研究探索赛博威慑的理论和实践，了解其对赛博威慑的认识与思考，具有重要价值。但是，系统阐述赛博威慑的书籍还不多见。本书作者 Brian M. Mazanec 是美国政府问责局的高级防御分析师，长期从事美国相关战略政策评估工作，Bradley A. Thayer 是国际关系领域的知名专家学者。

本书详细介绍了关于赛博空间和赛博战的核心概念，描述了涉及到赛博武器的各种独特或显著特征，阐述了威慑理论的核心思想，从威慑赛博战的角度讨论了面临的挑战，并有针对性地提出了建立有利于战略稳定的规范、加强赛博取证和防护，以及制定宣誓性政策并发展进攻性赛博战武器等三方面的措施建议，相信对这一领域具有借鉴意义。

参加本书翻译的有况晓辉、李响、曹华阳、林哲超和张超。此外，国防工业出版社的编辑为本书的出版付出了辛勤的劳动，特此表示感谢。

赛博空间是一个不断发展的新领域，威慑的内涵又十分丰富和复杂。本书内容涉及赛博空间威慑相关战略、政策、外交、技术等多个领域，翻译本书的难度超出我们的预期。鉴于译者的水平有限，翻译中定有许多不准确甚至不当之处，请读者批评指正。

译者

2018年10月21日

致谢

如果没有大家的支持，本书不可能顺利出版。我们要感谢 Palgrave Macmillan 的编辑 Eleanor Davey Corrigan 对本项目一直以来的支持；感谢同样来自 Palgrave Macmillan 的 Hannah Kašpar 在许多问题上提供的重要帮助。

我们还要感谢直接或间接对本项研究工作做出贡献的人员，包括 Linton Brooks 的代表 Trevow Thrall 博士、Joe Kirschbaum 博士和 Penney Harwell Caramia。我们要感谢两名匿名审稿人 Igor Bernik 博士和 Madeline Carr 博士，他们都同意在本书完成后出现在致谢中。他们提出了许多有价值的批评和建议，非常感谢他们的帮助。

Brian Mazanec 想在此对他深爱且给予他无私支持的妻子 Abby 表示感谢，她审阅了初稿，并提出了许多实质性的建议，使得书稿质量得到显著改善。也想感谢 Abby 和四个孩子（Charlotte、Reagan、Peter 和 2015 年 7 月出生的“B4”）牺牲大量时间并提供重要的激励，使得本项工作能够顺利完成。

Bradley Thayer 想在此感谢 Bath 大学的 Charles Lees 教授和 David Galbreath 教授以及冰岛大学的 Baldurpóhsson 教授对本项目的支持。此外，他还要感谢 Silja Bára Ómarsdóttir 和 2014

年 Þjóðarspegilinn 会议的所有参与者，以及 Elva Ellertsdóttir 在他转移到 Háskóli Íslands 新岗位时帮助解决了许多问题，十分感谢盛情款待。同时，要感谢美国陆军战争学院准许他扩展他和 Thomas M. Skypek 共同撰写的论文“Reaffirming the Utility of Nuclear Weapons” *Parameters*, Vol. 42 (4) /43 (1), Winter/Spring 2013。

目录

第一部分 赛博空间、赛博战和威慑

第 1 章 绪论	3
1.1 引言	3
1.2 威慑赛博战的重要性	5
注释	9
第 2 章 赛博空间和赛博战	13
2.1 引言	13
2.2 赛博空间	15
2.3 赛博战	16
2.4 赛博战实例	19
2.4.1 美国针对苏联的跨西伯利亚管道攻击	19
2.4.2 俄罗斯针对爱沙尼亚的攻击	20
2.4.3 以色列的“果园行动”攻击	21
2.4.4 俄罗斯对格鲁吉亚的攻击	22
2.4.5 “震网”病毒攻击	22
2.4.6 伊朗对沙特阿美公司的攻击	24

2.4.7 伊朗攻击美国的“燕子行动” (Operation Ababil)	25
2.4.8 对乌克兰的“蛇”(Snake)攻击.....	25
注释.....	26
第 3 章 威慑理论及其应用于赛博战所面临的挑战.....	34
3.1 引言.....	34
3.2 赛博攻击感知和溯源	38
3.3 关于赛博武器效能的不确定性.....	42
3.4 关注赛博空间的不确定性以提高威慑力	44
注释.....	44
 第二部分 提高赛博攻击的威慑能力	
第 4 章 建立有利于战略稳定的规范.....	51
4.1 介绍	51
4.2 增强赛博威慑的规范	52
4.3 规范演进理论和赛博规范	53
4.4 赛博攻击威慑规范的发展在当前面临的挑战	58
注释.....	59
第 5 章 持续努力以加强赛博取证和防护.....	63
5.1 从生物和核武器的核查方法中学习	64
5.2 增强对赛博武器的核查	65
5.3 拒止型威慑：增强赛博空间防护	66
注释.....	68
第 6 章 制定宣誓性政策并发展进攻性赛博战武器.....	71
6.1 针对赛博战的宣誓性政策.....	72

6.2 用以划明“红线”和慑止战略性赛博攻击的 赛博宣誓性政策	72
6.3 用以明确国家责任的赛博空间宣誓性政策	73
6.4 用以打击对非国家赛博攻击者的赞助的赛博空间 宣誓性政策	75
6.5 以攻制攻的威慑：发展进攻性赛博能力	75
6.6 通过第三方组织进行威慑：颁发赛博空间的 特许权证	77
注释	77
第 7 章 结论	80
7.1 增强赛博战威慑并加强赛博空间战略稳定	81
注释	83
参考文献	84

第一部分 赛博空间、赛博 战和威慑

摘要：本章阐述了本书的核心问题、中心论点、局限性和意义。解决的主要问题是：鉴于威慑理论应用于赛博战所面临的挑战，美国及其盟国如何成功地阻止重大的赛博攻击？由于赛博技术的独特属性，导致威慑理论应用于赛博战时会面临严峻挑战，有三个方面的工作有助于减轻这些挑战，这也是我们正在从事的研究工作。首先，建立有益的规范来维护战略稳定性；其次，持续努力提升赛博取证和防御能力，包括在赛博攻击溯源和处理庇护“独立”攻击者方面降低取证标准；最后，制定和传达准确清晰的宣示性政策和可信的以攻制攻威慑选项，从而使对手相信冲突升级不可避免且代价高昂。

关键词：计算机网络攻击；赛博安全；赛博战；威慑

Mazanec, Brian M., and Bradley A. Thayer. Detering Cyber Warfare: Bolstering Strategic Stability in Cyberspace.

Basingstoke: Palgrave Macmillan, 2015.

DOI: 10.1057/9781137476180.0004.

1.1 引言

攻击威慑在人类事务中有着悠久的历史，可以追溯到史前时期，与之相对应，新技术的兴起与随之产生的对抵消战略

或威慑武器的需求之间的相互作用，也具有悠久历史¹。新武器的研发、应用及相应的防御措施，与通过调整威慑理论来解决和管理威胁之间陷入了无休止的竞赛，而随着赛博战的兴起，这种竞争进入了一个新的篇章²。赛博战为国际关系带来了新的富有挑战性的威胁，随着赛博能力和攻击事件的激增，情况变得更加恶劣。美国政府最高层也对此表示承认。国防部长查克·哈格尔在其听证会上表示，他有信心，“在此刻，美国已经成功慑止了重大赛博攻击”，但接着解释道，他预计慑止这类重大赛博攻击将会是美国持续面临的主要挑战³。

正如国防部长哈格尔所说，在（赛博空间）这一领域，威慑是具有挑战性的。主要源于威慑理论是为了威慑（应对）动能攻击而建立的，包括：慑止军队力量的使用，如敌方的海、空军等；在核时代，慑止对手战略力量的使用等。然而，在威慑方面，赛博战与之前出现的其他手段在很多方面存在差异，主要源于它不是固有基于动能的。因此，威慑理论学家和实践人员必须调整现有的概念并寻求制定合适的战略以达到赛博战威慑的目的，进而能够促进赛博空间的战略稳定性。事实上，在学术界存在这样一种合理的假设，如学者 Martin Libicki 等，强调赛博威慑可能无法起到与核威慑同样的作用，如果是这样，说明需要进一步关注这项紧迫的挑战⁴。

我们在研究中关注的主要问题是：鉴于威慑理论应用于赛博战面临的种种挑战，美国及其盟友如何成功地慑止重大的赛博攻击？我们的核心观点是虽然由于赛博技术的独特属性，使得威慑理论应用于赛博战面临着较大的挑战，但是在以下三个领域的投入和努力能够帮助减轻这一挑战，具体包括：建立有利于战略稳定性的规范；持续努力加强赛博取证和防护，包括在赛博攻击溯源和处理庇护“独立”攻击者方面降低取证标准；制定和传达明晰的宣示性政策和可信的以攻制攻威慑选项，从而使对手相信冲突升级不可避免和代价高昂。将威慑理论应用于赛博战面临的挑战与以下不确定性有关，首

先是攻击的感知与溯源；其次是攻击效果的不确定性。

由于（赛博攻击）溯源和效能控制方面的困难，使赛博战威慑面临独特的困难。赛博武器的攻击效果缺乏控制，在某些情况下，赛博武器的使用可能会损害攻击人员自身的利益，其所在社会及经济发展，甚至危及其盟友，因此，赛博武器的运用对于攻击者而言既充满诱惑又面临危险。事实上，如果防御人员能够确定攻击者，那么还面临着冲突升级等问题。布鲁金斯研究所的 Peter Singer 和其他研究人员已经将缺乏溯源能力确定为导致威慑理论不能直接和立即应用于赛博领域的关键因素⁵。如果攻击是可溯源的，那么则可以应用传统的威慑（手段），包括可能的动能打击。如果攻击是不可溯源的，或者攻击者坚信溯源会出现错误，那么赛博攻击将成为一种令人难以抗拒的诱人的武器。

这是一个老生常谈的问题——如果你可以做一件坏事并逃避惩罚，你会做么？在历史上，这个问题已经被哲学家和政治领袖们以各种形式思考过。在《理想国》中，柏拉图举了一个关于裘格斯戒指的例子，这个戒指可以让佩戴它的人隐身⁶。那么，当一个人佩戴了裘格斯戒指后还会那么正直吗？他认为答案是否定的。由于无法溯源而逃避惩罚的诱惑实在太大了，即使一个品行端正的人也可能会被这种权利所腐化。赛博武器就是国家手中的裘格斯戒指，我们目睹了越来越多的后果。这种不确定性表明，需要开发一种可裁剪的方法提高应用威慑应对赛博战的能力。我们在本书中指出的三方面工作有助于应对这些挑战。

1.2 威慑赛博战的重要性

以下三个原因可以说明我们研究的论点是重要的。第一，美国需要慑止赛博战，就公开可获得的证据表明，美国在这方面做得并不够好。本研究可引发对这种危险的重视，并且能够

在辅助美国决策人员更好地理解 and 运用赛博攻击威慑的逻辑和困难方面做出贡献。本书通过介绍赛博战，并解释将威慑理论运用于这种新兴的战争形式面临的挑战，为这种讨论奠定了基础。

第二，本项研究的一个独特贡献是，明确了一系列可以启动或加强的具体工作，以提高对赛博攻击的威慑能力。这些解决方案来自诸如生物学等领域的经验教训，以及以前处理恐怖主义和核武器等威胁的经验。例如，微生物法医学提供了重要且有用的例子回答“谁干的”这个关键问题。我们认为，政策制定者可以学习其他领域的经验，如生物武器和法医学，并在此过程中制定一揽子有效的应对措施以增强赛博战威慑力。

第三，赛博战是攻击美国的一种主要途径，并且已经对美国的国家安全利益、盟友利益及其国际政治中的其他国家造成重大损害。我们的研究能够帮助美国通过提高其赛博战威慑能力，以应对这一日益严重的重大威胁。赛博战已成定局，它给国家和其他国际行为体带来了越来越大的挑战，并且日益成为引发冲突的因素。事实上，赛博战应该像国家的其他斗争手段一样被视为国家冲突中的一个组成部分。由于溯源困难且实际上也被广泛使用（由于赛博战规范尚未牢固建立），赛博战的吸引力日益增强。例如，2014年，在乌克兰发生政治危机期间，出现了一种被称为“蛇”（Snake）或“噬身之蛇”（Ouroboros）的复杂赛博武器⁷。Snake 被怀疑来自于俄罗斯，它可使攻击者完全通过远程方式访问控制受攻击的乌克兰（信息）系统。正是由于类似这样的威胁导致美国情报总监 James Clapper 将赛博武器确定为针对美国的主要攻击途径之一⁸。

不幸的事实是，现代生活中每天都有大量针对主要军事、情报和民用目标的间谍式赛博攻击。“诺顿赛博犯罪报告”指出，赛博犯罪造成的直接损失为每年 1130 亿美元，美国的损失达到 380 亿美元。此外，波耐蒙研究所估计，美国 60 个关键公司中的赛博攻击平均年化总损失（直接和间接）为 1160 万

美元。而 2012 年，这些公司的损失估计为 890 万美元，表明威胁与去年相比增加了 26%⁹。MacAfee 公司还曾经给出过一个更加严峻的估计，指出在全球互联网经济产生的 2~3 万亿美元中，赛博犯罪就从中获取了 15%~20%¹⁰。即使考虑到这些数字可能存在的夸大或者误差，赛博攻击的代价也是巨大的。

除了纯粹的经济影响外，赛博攻击对美国的国家安全造成了巨大的损害，包括对美 F-35 战斗机与其他先进武器，以及盟国武器关键信息的窃取。

虽然这种赛博威胁非常大，但是与情报窃取的赛博攻击相比，赛博战更加巨大的破坏性威胁才是最大的风险。而随着赛博能力的不断扩散，出现这种风险的可能性变得越来越大。

赛博空间作战是赛博能力的运用，其首要目的是在赛博空间和通过赛博空间来实现目标¹¹。敌对行动可以以计算机网络利用 (Computer Network Exploitation, CNE) 的形式出现，如前面提到的间谍式的赛博攻击，以及真正的计算机网络攻击 (Computer Network Attack, CNA)¹²。计算机网络攻击是利用计算机网络来破坏、拒绝、降级和摧毁驻留在敌方计算机和计算机网络中的信息，或者计算机和赛博本身。根据上述对赛博战的理解，聚焦于国家行为体之间（直接或通过可否认的非国家行为体）的 CNA 是本书所关注的重点，而那种更加频繁地通过计算机网络搜集对手情报的 CNE 攻击，则不是本书关注的重点¹³。然而，正如可以预料的那样，CNA 和 CNE 之间的界线非常模糊，因为仅仅通过敲击键盘就可以将 CNE 升级为真正的攻击。与其他战争形式一样，CNA 式赛博战可以将社会财富作为打击目标，如美国银行业这类民用目标，也可以将军事力量作为打击目标，锁定军事人员、部队或设施，如美国太平洋司令部。在第 2 章，我们将进一步讨论这个问题。

由于 CNA 式攻击构成了最严重的威胁，我们专注于慑止此类攻击，这对国家安全而言至关重要。2010 年，《经济学人》杂志设想了最极端的 CNA 式赛博攻击，并将它描述为“保持现代