国防科技著作精品译丛

ELSEVIER
爱思唯尔

The Basics of Cyber Warfare

Understanding the Fundamentals of Cyber Warfare in Theory and Practice

赛博战基础

——从理论和实践理解赛博战的基本原理

（美）Steve Winterfeld Jason Andress 著　　周秦 李嘉言 许邦彦 等译

国防工业出版社
National Defense Industry Press

赛博战基础

——从理论和实践理解赛博战的基本原理

The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice

[美] Steve Winterfeld　Jason Andress　著
周　秦　李嘉言　许邦彦　等译

国防工业出版社
National Defense Industry Press

著作权合同登记　图字：军 -2013 -168 号

图书在版编目（CIP）数据

赛博战基础：从理论和实践理解赛博战的基本原理/（美）温特菲尔德（Winterfeld, S.），（美）安德莱斯（Andress, J.）著；周秦等译. -- 北京：国防工业出版社，2016.2
（国防科技著作精品译丛）
书名原文：The Basics of Cyber Warfare:
Understanding the Fundamentals of Cyber Warfare in Theory and Practice
ISBN 978-7-118-10302-1

Ⅰ.①赛… Ⅱ.①温… ②安… ③周… Ⅲ.①信息战 Ⅳ.①E869

中国版本图书馆 CIP 数据核字（2015）第 270615 号

赛博战基础——从理论和实践理解赛博战的基本原理
[美] Steve Winterfeld　Jason Andress　著
周　秦　李嘉言　许邦彦　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责任公司
开　　本　700 × 1000　1/16
印　　张　9¾
字　　数　170 千字
版 印 次　2016 年 2 月第 1 版第 1 次印刷
印　　数　1—2500 册
定　　价　52.00 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

翻译组名单

周　秦　李嘉言　许邦彦　刘吉吉

付少鹏　王　冰　杜紫薇　郭冰逸

胡思农　谢　天　董柏宏　郭雨轩

梁羽博　白　驹

译者序

随着网络深入渗透到社会生活的方方面面，赛博空间成为一个新的作战域，美国政府和军队把赛博空间纳入视野，成立了赛博司令部，赛博空间取代电磁空间成为第五大作战空间。传统的战争形态及战争观急剧变化，赛博空间控制权与制空权、制海权和制陆权一样成为赢得战争的重要保障，争夺日趋激烈。在美国的影响下，俄罗斯、德国、英国和日本等国也加强了赛博空间技战术的研究和开发，并将赛博空间对抗能力提升到新高度，赛博战似乎开始变得真实。

本书旨在回应人们对赛博战概念、赛博战相关技术的关注与疑问，全书在战略、行动、战术等不同层面阐述赛博空间的内涵，从理论和实践两方面为读者提供关于赛博战的基本知识。在内容编排上，首先在第 1 章简述赛博空间威胁，为读者建立赛博攻击方法、技术、工具、攻击者和对这些威胁的防御现状的直观认识；然后在第 2 章尝试进行赛博战概念辨析并建立赛博战与陆、海、空、天等传统作战域之间的联系，进而在第 3 章探讨了当前在国家和军队层面的赛博战条令情况；第 4、5 两章专注于从技术视角介绍实施赛博作战的多种类型工具和抵御攻击的方法，以及实施计算机网络利用/攻击的过程、工具；鉴于作者认为社会工程对组织存在巨大现实威胁，第 6 章专门对社会工程进行了讨论，并指出了抵御社会工程威胁的途径；第 7 章讨论了计算机网络防御的保护要素、防御原则、安全意识、人员培训以及可用的防御策略；第 8、9 章提出了赛博安全面临的挑战和赛博战发展趋势。书中提到了近年来发生的一些事件，意在对相关主题或观点作直观说明。本书的两位作者均长期从事赛博空间和赛博安全的

相关研究，分别具有商业应用背景和军方背景，书中内容能在一定程度上反映其所在领域对赛博战和赛博安全的认识现状。

本书意在为包括政策制定者、行业规则制定者、安全专家、企业机构信息安全主管、渗透测试人员、网络和系统管理员、大学老师等在内的关注赛博战活动的人提供有价值的参考，译介此书是希望为国内安全业者、研究人员、院校师生等相关人员提供一个窗口，便于了解国外研究人员在这一领域的思想观点。

为了尽可能准确地传达作者的观点和看法，我们在翻译时秉持忠实于原作的原则，但需要指出的是，我们对书中所有内容不持任何观点或立场，既不做考证和补充，也并不表示同意或反对其中的说法。

全书由周秦、李嘉言、许邦彦、刘吉吉、付少鹏、王冰、杜紫薇、郭冰逸、胡思农、谢天、董柏宏、郭雨轩、梁羽博、白驹等人共同翻译，周秦负责全书的统稿和审校工作。翻译过程中，得到了国防工业出版社编辑部老师的悉心指导和热心帮助，在此表示衷心感谢。

由于译者的知识、认识水平和时间均有限，本书难免存在疏漏、失当之处，读者如能指正，我们将非常感谢。

译者

2014 年 6 月

致谢

感谢家人和朋友在我们完成本书的过程中给予的指引、支持和勉励。谨将本书献给安全行业中像黑客仁者那样通过努力让世界更美好的人们(对于黑客仁者，您可能见过他们写有 “i hack charities.” 字样的 T 恤，通过网站 http://hackersforcharity.org/ 可以了解更多关于他们的信息)，也献给更多投身这一领域的人。

作者简介

史蒂夫 · 温特菲尔德 (Steve Winterfeld), TASC (The Analytic Sciences Corporation) 公司防务/民用事业集团 CTO、TASC 公司赛博技术主管和高级赛博战士讲师。职业生涯中参与了大量重要的赛博项目, 其中最值得一提的是为负责实时安全监控和入侵行为法庭调查的美国陆军南方军区建立计算机应急响应中心 (Computer Emergency Response Center, CERT), 以及为 "全球鹰" 无人机系统开发首个 CA 认证。计算机信息系统科学硕士, 持有 CISSP、PMP、SANS、GSEC、六西格玛等认证。

杰森 · 安德莱斯 (Jason Andress), (ISSAP, CISSP, GPEN, CISM) 一位经验丰富的安全专业人士, 在学术和商业领域均有深厚造诣。截至目前已为全球多家各种类型公司提供信息安全专业鉴定。自 2005 年起讲授本科和研究生安全课程, 并在数据保护领域开展研究。已撰写多部著作和出版物, 主题涵盖数据安全、网络安全、渗透测试和数字取证。

目录

绪论

本章要点:

- 本书概述和关键内容
- 本书面向的读者
- 本书的组织结构

本书概述和关键内容

本书主要是对当今赛博空间的战略、行动、战术层面的介绍。本书很大程度上是在 2011 年出版的《面向安全人员的赛博战技术、战法和工具》一书基础上更深入的思考, 同时也包括了自第一版发行以来发生的相关事件。

本书分享了两位作者关于赛博战的两种不同观点, 一种观点来自于商业应用背景, 另一种来自于军方观点。本书的每位读者均可以通过本书了解现今社会正在发生什么? 未来我们将要面临哪些问题?

本书在一定程度上可以用来为某些组织制定赛博安全战略提供参考, 同时有助于促进在国家层面上讨论赛博的发展方向问题。

本书面向的读者

本书将为那些关注赛博战活动的人, 包括政策制定者、CEO、CISO、

规则制定者、渗透测试人员、安全专家、网络和系统管理员、大学老师等提供有价值的资源。这些关于赛博战术和攻击的信息有助于设计和开发更加有效的产品和技术防御手段。

对于管理者来说这些信息同样重要，有助于其基于全局立场为组织开发更全面的风险管理策略。本书的某些观点将有助于决定如何进行资源分配，并可用来驱动安全工程和政策，用以缓和某些较大的争议问题。

本书的组织结构

本书通过介绍一系列有内在逻辑关系的事件使读者对当今赛博战空间有一个基本了解，同时本书各章又可以作为独立的信息块，因此在阅读本书时没有必要按从头到尾或某一特定顺序进行。本书所有的引用信息都给出了其参考文献。下面是对本书各章的概述。

第 1 章: 赛博威胁管窥

本章通过一幅图描述了赛博威胁的冰山一角，该图首先描绘了各种攻击方法和攻击资源，并描绘了攻击者和黑客利用这些攻击方法和攻击资源来突破防线 (图中以防守山脉表示) 获取有价值的数据。该图意在表现赛博域的内在交互性和复杂性。黑客使用的方法、工具以及攻击流程通常与安全专家所使用的一样，只不过安全专家拥有实施攻击和行动的授权。

第 2 章: 赛博空间作战行动

第 2 章主要讨论战争内涵是如何改变的，以及我们是否已经处于赛博战之中。我们讨论常规战争与赛博战争之间的不同点，以及如若用常规战对作为等价物的赛博战进行衡量，其将是一个很不恰当的参照。无论是单纯的赛博战还是传统战争结合，赛博战都将会导致全球性灾难，改变我们的经济以及带来更大规模的赛博犯罪和间谍活动。本章还介绍了陆、海、空、天四个传统作战域，因为它们都与赛博空间行动相关。由于赛博已变得更加成熟并被看作第五维作战域，那么我们从中能学到点什么？ 同时，还回顾了各种不同威胁、它们所带来的影响以及这些威胁的可能动机。

第 3 章: 赛博条令

第 3 章主要探究了国家和军队层面的赛博战学说现状，并讨论所有

拥有 IT 基础设施的国家是如何发展其本国战略和能力来保护和行使国家权利的，以及对军队需要适应赛博空间环境的一些传统手段和装备进行测试。本章还包含了一些联邦机构和政府用来在赛博空间环境中进行行为指导的官方指令。最后关注各组织是如何发展赛博新学说并执行其现有计划的。

第 4 章: 赛博工具和技术

第 4 章主要讨论在执行计算机网络行动 (Computer Network Operations, CNO) 中可能使用到的各种工具，以及用来防御入侵的各种方法。主要工具包括侦察工具、访问和权限提升工具、数据窃取工具 (Exfiltration)、对已入侵系统接入入口保留工具 (Sustaining Our Connection to A Compromised System)、系统攻击工具 (Assault Tools)、痕迹销毁工具 (Obfuscation Tools)，这些工具基本都是免费的，或有免费版本且对普通大众来说都是可用的。本章还讨论了物理域和逻辑域的结合点，以及如何改变这两者中某一个域从而对另一个域产生影响，有些时候该影响是灾难性的。另外，本章讨论了供应链问题以及当供应链遭到破坏或中断后带来的潜在后果。

第 5 章: 攻击手段和步骤

第 5 章主要讨论了计算机网络利用 (Computer Network Exploitation, CNE) 和计算机网络攻击 (Computer Network Attack, CNA) 的基本原理。在这里 "利用" 指的是侦察或间谍行为，书中还就其如何实施进行了讨论。接着论述了目标确定，其既包括从功击目标中获取信息，也包括从监视对象中识别目标。我们讨论了赛博战的几个不同要素: 物理域和逻辑域以及电子特性。我们还讨论了攻击过程的不同阶段: 侦察 (Reconnaissance)、扫描 (Scanning)、访问系统 (Accessing Systems)、权限提升 (Escalating Privileges)、窃取数据 (Exfiltrating Data)、攻击目标系统 (Assaulting The System)、保留接入入口 (Sustaining Our Access)、销毁所有入侵痕迹 (Obfuscating Any Traces)。并比较了黑客是如何实施同类和不同类攻击的。

第 6 章: 心理战武器

第 6 章主要讨论了社会工程及其是如何对所有组织和个人构成严重威胁的。我们以军事思维来看这个问题，并讲述他们是如何控制有争议区域以及实施反间谍行动的。本章还讨论了必须如何加强安全政策、文化和

训练才能确保劳动力 (Work Force) 保持警觉, 以及人为因素会对某项杰出的安全技术基础设施造成何种破坏。

第 7 章: 防御手段和步骤

第 7 章主要讨论计算机网络防御 (Computer Network Defense, CND)。这里将讨论我们试图保护的究竟是什么, 如何保证正常用户有权访问的数据和信息的安全性, 并讨论了安全意识、训练效果用来加强我们防御中的薄弱环节。同时, 我们给出了一些在遭受攻击时进行自我防御的策略。

第 8 章: 面临的挑战

第 8 章定义了 30 (译者注: 原著此处有误, 应为 29 种) 种影响赛博安全的关键问题及其分类。接下来我们将这些问题分成了不同困难等级以及解决这些问题所需要的资源等级。同时, 我们还讨论它们之间的联系。最后, 我们关注谁该来解决这些问题以及如何解决这些问题, 包括解决这些问题的一个大概的时间表。

第 9 章: 赛博技术发展及其对赛博战的影响

展望未来, 根据当前的赛博安全技术及其趋势来判断其逻辑发展。对基于技术以及政策的发展的回顾可以基本预见将来可能会发生什么, 技术的发展趋势将会对赛博战产生重大影响, 而政策的发展将对赛博战产生最重要的影响。本章还提供了一些关于当今有争议的虚拟环境防御的最佳方法。

结论

写作本书像是一次真正的旅行。围绕如何建立最好的基础来解决问题, 写作相关人员间发生了多次争论和辩诘, 最终大家在广阔的前景和具体实用技术之间取得了平衡。希望本书能对围绕赛博空间将如何发展和我们每个人能够做些什么的全国性讨论有所贡献。