国防科技图书出版基金

网络与信息安全前沿技术丛书

信息安全主动防护技术

郝尧 赵越 吴开均 陈剑锋 编著

Information Security Active Protection Technologies

国防工业出版社
National Defense Industry Press

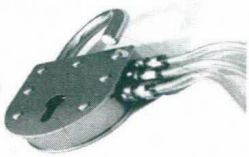
国防科技图书出版基金

网络与信息安全前沿技术丛书

郝尧　赵越　吴开均　陈剑锋　编著

信息安全
主动防护技术

Information Security Active Protection Technologies



主动防御是网络空间安全的重要手段和技术发展方向。本书较为全面地论述了安全预警、应急响应、安全评估、数据泄漏防护在主动防御方面的新发展，以及移动目标防御、网络攻击追踪溯源等新型信息安全主动防护技术的概念与内涵，是该领域科研和技术人员了解并运用信息安全主动防护技术的有益参考。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

信息安全主动防护技术 / 郝尧等编著. — 北京：国防工业出版社，2018.12
（网络与信息安全前沿技术丛书）
ISBN 978-7-118-11704-2

Ⅰ. ①信… Ⅱ. ①郝… Ⅲ. ①信息安全-安全技术 Ⅳ. ①G203

中国版本图书馆 CIP 数据核字(2018)第 250553 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号　邮政编码 100048）
天津嘉恒印务有限公司印刷
新华书店经售
*
开本 710×1000　1/16　**印张** 21　**字数** 393 千字
2018 年 12 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 126.00 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

致　读　者

本书由中央军委装备发展部**国防科技图书出版基金**资助出版。

为了促进国防科技和武器装备发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。这是一项具有深远意义的创举。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在中央军委装备发展部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由中央军委装备发展部国防工业出版社出版发行。

国防科技和武器装备发展已经取得了举世瞩目的成就，国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。开展好评审工作，使有限的基金发挥出巨大的效能，需要不断摸索、认真总结和及时改进，更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第七届评审委员会组成人员

主任委员	潘银喜			
副主任委员	吴有生	傅兴男	赵伯桥	
秘书长	赵伯桥			
副秘书长	邢海鹰	谢晓阳		
委员 （按姓氏笔画排序）	才鸿年	马伟明	王小谟	王群书
	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	芮筱亭	李言荣
	李德仁	李德毅	杨　伟	肖志力
	吴宏鑫	张文栋	张信威	陆　军
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺，魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全，反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的《网络与信息安全前沿技术丛书》即将分期出版。丛书有如下特点。一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本丛书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

信息安全的概念是随着信息技术的发展而不断发展的，当前信息技术已从基本通信阶段、计算机与网络阶段发展到网络空间阶段，信息安全也从通信保密、计算机安全、网络安全、信息安全保障发展到网络空间安全阶段。

网络空间是人类利用信息设施构造，实现信息交互，进而影响人类思想和行为的虚实结合的空间，其实体是信息技术基础设施构成的相互依赖的网络，包含计算机、通信网络系统、信息系统、嵌入式处理器、控制器以及其中所保有的数据。网络空间与传统的陆、海、空、天物理空间相互交织，形成虚拟与现实交织的国家利益的新疆域。

网络空间深刻地影响着人类社会的政治、经济、军事、文化等领域，但同时对网络空间依赖度的增加不仅带来机遇也带来威胁。网络空间的全球性、匿名性、开放性、脆弱性等特点使得过于依赖于网络空间将面临巨大的威胁。世界各国纷纷开始关注网络空间的安全问题。美国作为互联网的发起国，先后出台了多个网络空间安全战略，寻求建立以美国为主导的网络空间国际秩序。而其他一些国家如法国、德国、印度、日本、荷兰、捷克等国，也都加强了对网络安全的重视，纷纷调整其网络空间的战略部署。当前，网络空间已成为陆、海、空、天之外的第五大国家主权空间，保卫网络安全就是保卫国家主权。习近平总书记在2014年2月27日主持召开中央网络安全和信息化领导小组第一次会议中指出："没有网络安全就没有国家安全。"

当前网络空间对抗日趋激烈，加强信息安全防护能力是适应时代发展的必然要求，是确保国家安全、社会稳定的基本前提，也是提高信息化建设效益的重要保障。在日新月异的信息威胁面前，传统的静态、局部、被动的防御手段无法有效应对，以动态、全局、自动化为特征的主动防御技术应运而生。主动防御将已有信息安全技术与新型防护手段有效结合，实现了安全资源间的协同感知、入侵响应、联动防御和响应处置等，能够极大地提升安全防护的效能。在主动防御中所采用的具备主动特征的信息安全技术

手段即为信息安全主动防护技术。

目前尚无较为全面介绍信息安全主动防护技术的书籍，本书通过梳理主动防护相关的信息安全技术，介绍其原理、方法、工具，有助于读者了解信息安全主动防护技术及其发展趋势。

本书选取了一些具有主动防护特性的信息安全技术，这些技术有些基于传统信息安全技术，如安全预警、应急响应、数据保护、安全评估，已经过多年的发展，然而在近期其主动防护特性得到较大发展，对于网络空间的主动防御有着重要的价值。因此，在本书中作为一章单独描述。另外一些技术属于信息安全防护领域的新技术，主要涉及两个方面：一是摆脱被动式防御，主动反制、反击攻击者的网络攻击追踪溯源技术；二是动态变化信息系统，破坏攻击者对系统和安全手段的认知，从而降低安全威胁的移动目标防御技术。追踪溯源与移动目标防御技术目前还处于发展的早期阶段，虽然有一些相关的产品，但领先技术多处于试验阶段。然而，这些技术代表信息安全技术的未来发展趋势，阅读相关的章节有助于读者领会相关技术的基础知识和发展形势，帮助读者在实际工作中使用相关技术的早期产品，对于提升信息安全防护实践水平仍有重要的意义。

网络空间主动防御及支撑主动防御的信息安全主动防护技术仍在不断地发展之中，虽然本书试图给出网络空间主动防御相关技术的比较全面的景象，但限于本书的篇幅和主动防护技术的多样性，无法全面涵盖网络空间主动防御这一领域，只能根据作者对该领域的理解，选取监测预警、应急响应、数据泄漏主动防护、移动目标防御、网络攻击追踪溯源等具有代表性的信息安全主动防护技术予以介绍。本书着重阐述上述技术的原理、方法，并兼顾其在网络空间安全领域的应用。希望通过阅读本书，能使读者对信息安全主动防护技术有一个相对全面的了解，并对读者的学习或工作有所助益。如果读者希望了解某项技术更深入的信息，可以根据参考文献扩展阅读。

本书的第1、7章由郝尧编写，第2、3、4章由赵越、陈剑锋编写，第5、6章由吴开均编写，陈周国、蒲石等对第7章内容也有贡献。全书由郝尧、赵越、吴开均统稿并校稿。

本书的编写得到了祝世雄研究员、田波研究员和张文政研究员的具体指导与支持，出版社王晓光老师对本书的编写也非常重视，对相关材料多次审阅并提出修改意见，在此一并表示感谢。

限于作者水平，本书难免有错误和不足，还望读者和同行专家不吝批评和指正。

编著者

2018年10月

目　录

Contents