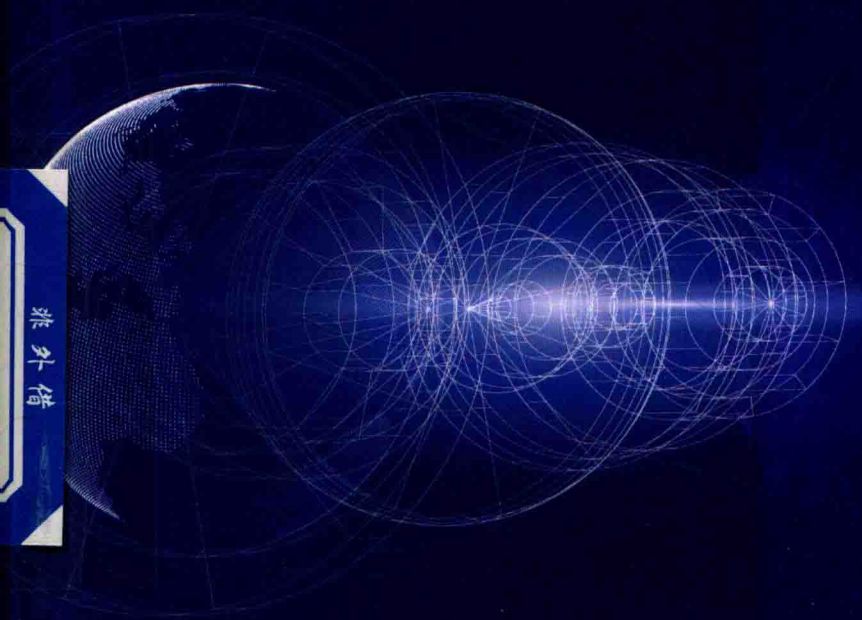
网络空间主动防御技术

陈福才　扈红超　刘文彦　程国振
刘彩霞　霍树民　梁　浩　编著



科学出版社

网络空间主动防御技术

陈福才　扈红超　刘文彦　程国振
刘彩霞　霍树民　梁　浩　编著

科学出版社
北京

内 容 简 介

本书对网络空间主动防御技术进行了系统性的介绍。首先梳理了网络空间安全的基本知识，分析了网络威胁的表现形式与成因、网络防御技术的起源与演进，进而对不同代系的主动防御技术，包括基于隔离的沙箱技术，基于欺骗的蜜罐技术，可屏蔽和遏制入侵的入侵容忍技术，基于可信链的可信计算技术，基于多样化、随机化、动态化机制的移动目标防御技术等进行了详细分析和介绍。在此基础上，针对持续深化的网络空间安全需求，对最新出现的网络防御技术创新发展动向进行了简析。最后还介绍了常用的网络安全分析评估模型及相关的数学基础知识。

本书可供高等院校网络空间安全、信息安全等相关专业的研究生或高年级本科生使用，也可作为从事相关科研工作的学者和工程技术人员的参考资料。

图书在版编目（CIP）数据

网络空间主动防御技术 / 陈福才等编著. — 北京：科学出版社，2018.10

ISBN 978-7-03-059098-5

Ⅰ. ①网… Ⅱ. ①陈… Ⅲ. ①计算机网络－安全技术－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 236578 号

责任编辑：任 静 / 责任校对：郭瑞芝

责任印制：张 伟 / 封面设计：迷底书装

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京虎彩文化传播有限公司印刷

科学出版社发行 各地新华书店经销

*

2018 年 10 月第 一 版 开本：720×1 000 1/16

2018 年 10 月第一次印刷 印张：20 3/4

字数：401 000

定价：125.00 元

（如有印装质量问题，我社负责调换）

作 者 简 介

陈福才 国家数字交换系统工程技术研究中心研究员。长期从事信息通信和网络安全技术研究工作，作为课题组组长或研究骨干，先后承担国家863计划、国家科技支撑计划、国家重点研发计划和国家自然科学基金创新研究群体项目9项，相关成果获国家科技进步奖一等奖1项，二等奖1项，省部级科技进步奖一、二等奖3项，2015年，作为“网络通信与交换技术团队”骨干成员，获得国家科技进步创新团队奖。发表学术论文40余篇，获发明专利7项。目前的主要研究方向为电信网安全和网络防御。

扈红超 国家数字交换系统工程技术研究中心副研究员，硕士生导师。长期从事新型网络技术和新型安全技术的研发工作，主持国家科技支撑计划项目、国家自然科学基金项目2项，参加国家863计划、国家重点研发计划、国家自然科学基金创新研究群体项目5项，相关成果获国家科技进步奖二等奖1项，省部级科技进步奖一、二等奖2项，撰写的博士学位论文被评为河南省优秀博士学位论文，发表学术论文30余篇，申请发明专利10余项。目前的主要研究方向为网络空间主动防御技术、拟态防御技术等。

前　言

网络空间(cyberspace)是人类在信息时代的基础活动空间，自其出现以来，就在不断演进变革的网络信息技术的驱动下，以超乎想象的速度扩张，对世界政治、经济、文化、社会、生态、军事等持续产生巨大影响。随着万物互联时代的来临，以及新一代信息技术、人工智能技术的创新发展，网络空间进一步融合人类社会、信息世界和物理世界，成为与人类息息相关、支撑人类面向未来生存和发展的重要的空间域。

作为由人类创造出来的虚拟空间，由于早期安全观念的不足和现阶段人类认知与科技发展的局限，网络空间在快速扩张的同时，也如同打开了的“潘多拉魔盒”，各类安全问题层出不穷。无论是2017年爆发的波及全球150多个国家和地区的勒索病毒，还是近年来在我国猖獗发生的以通信信息诈骗为代表的新型网络违法犯罪活动，都凸显了网络安全问题的严重性及其对社会经济发展的巨大破坏力。网络空间已经成为信息时代人类发展的“双刃剑”，一方面人们对其依赖程度不断加深，另一方面人们对其信任恐惧持续加剧，网络安全问题已被公认为信息时代最为严峻的挑战之一。

2014年2月，中国国家主席习近平着眼网络空间安全面临的重大威胁，提出了“没有网络安全就没有国家安全”的重要论断，强调指出“网络安全和信息化是一体之两翼、驱动之双轮”。2015年12月，在世界互联网大会开幕式上，习主席进一步指出网络安全是全球性挑战，维护网络安全是国际社会的共同责任，世界各国应携手努力共同构建网络空间命运共同体，标志着网络空间安全已经上升为事关全球发展和国家安全的战略性问题。在此背景下，2015年国务院学位委员会和教育部批准增设“网络空间安全”一级学科，将安全基础、密码学、系统安全、网络安全、应用安全等纳入学科方向，以期建立规范化的学科知识体系，成体系、成规模、多层次地培养网络空间安全专业人才，并促进网络空间安全基础理论和基本技术的研究发展。

网络空间安全的本质是对抗，而对抗的本质又在于攻防两端能力的较量。自网络空间出现以来，网络攻击与防御就一直处于螺旋式发展态势。发展先进的网络防御方法及技术手段，围绕关键信息基础设施、重要网络信息资源等构建形成整体防御能力，始终是保障网络空间安全的基本要求和主要技术途径。

网络安全防御技术的起源可追溯到网络空间诞生之初。最初人们通过网络加密技术来解决网络传输过程中的信息安全问题，其后随着网络空间范畴的持续拓展和网络服务渗透至人类社会、实体世界的方方面面，网络防御的概念内涵也不断丰富，

拓展至信息确保、计算机网络防御、关键信息基础设施防护等领域，由此也产生了诸如入侵检测、防火墙、漏洞扫描、威胁感知、病毒查杀、系统修补与恢复等防御方法或技术。与传统的物理实体间攻防对抗时“易守难攻”的特性不同，虚拟网络空间的基本安全态势是“易攻难守”，特别是随着近年来网络信息技术进入全球化、开放式产业链时代，以及网络与信息系统的功能设计、服务应用越来越复杂，网络安全漏洞几乎“无处不在”，加之诸如 APT(advanced persistent threat)等先进攻击方法和智能化攻击工具的不断发展，基于已知威胁特征或攻击行为等先验知识的被动式防御技术越来越力不从心。发展积极感知安全风险、不依赖于攻击先验知识，特别是具备内生式安全机制的主动防御技术成为网络防御的主要方向。

网络空间主动防御期望实现对网络攻击达成“事前”的防御效果，不依赖于攻击代码和攻击行为特征的感知，也不是建立在实时消除漏洞、堵塞后门、清除病毒木马等传统防护技术的基础上，而是以提供运行环境的动态性、冗余性、异构性等技术手段，改变系统的静态性、确定性和相似性，以最大限度地降低漏洞等的成功利用率，破坏或扰乱后门等的可控性，阻断或干扰攻击的可达性，从而显著增加攻击难度和成本。

本书是作者在长期跟踪研究网络防御技术的基础上，对既有的主动防御技术进行的系统性分析和总结，旨在为从事网络防御技术研究和人才培养的工作者提供一份兼具科普性和一定专业性的参考资料。全书共 10 章。第 1 章由陈福才、梁浩负责编撰，对网络空间安全的基本概念、网络威胁的表现形式与成因、网络空间安全的技术体系等进行介绍。第 2 章由程国振负责编撰，分析网络防御技术的起源、演进和不同代系网络防御的技术机理及能力范畴，对典型的主被动防御技术进行归纳简析，并梳理总结网络空间主动防御的基本概念。第 3 章由程国振、吴奇负责编撰。第 4 章由陈福才、梁浩负责编撰。第 5 章由霍树民、扈红超负责编撰。第 3～5 章对三种早期出现的典型主动防御技术，包括基于隔离的沙箱技术、基于欺骗的蜜罐技术、可屏蔽和遏制入侵的入侵容忍技术，从技术起源、演进路线、主要机制机理、典型技术产品或应用等方面进行详细的分析介绍。第 6 章由扈红超负责编撰，对可信计算的起源、基本理论、发展演进、典型应用进行介绍，重点分析可信计算平台、可信网络连接、定制的可信空间等关键平台及技术的功能结构和实现机制。第 7 章由刘文彦负责编撰，对移动目标防御(moving target defense，MTD)的内涵特征，多样化、随机化、动态化核心机制，有效性评估与分析方法等进行深入分析，并介绍 MTD 的典型应用及项目，对后续研究动向进行了梳理。第 8 章由刘彩霞、刘文彦负责编撰，在总结提炼上述主动防御技术能力范畴的基础上，针对持续深化的网络空间安全需求，分析网络防御技术的发展动向，对最新出现的融合人工智能的网络防御技术、网络空间拟态防御技术(cyberspace mimic defense，CMD)等创新性防御技术进行简述。第 9 章由刘文彦负责编撰，介绍网络空间安全的评估标准及指标，对

攻击树模型、攻击图模型、攻击链模型、攻击表面模型、网络传染病模型等各类主流的网络安全分析评估模型进行深入研究。第 10 章由霍树民负责编撰，对与网络安全研究密切相关的概率论与随机过程、最优化理论、博弈论等数学基础知识进行简要介绍。全书由陈福才、扈红超负责统稿。

本书得到国家自然科学基金创新研究群体项目“网络空间拟态防御基础理论研究”(批准号：61521003)和国家自然科学基金青年基金项目“动态非相似余度拟态防御有效性分析和评估”(批准号：61602509)的支持。写作过程中，项目组成员毛宇星、齐超、艾健健、吴奇、王亚文、李凌书、仝青等博士和赵硕、卢振平、王禛鹏、张淼、吕迎迎、陈扬等硕士查阅了大量的资料，参与了本书的编撰工作，为本书的完成提供了至关重要的帮助。在此，对所有为本书付出辛勤劳动的同事和同学表示衷心的感谢。

由于作者水平有限，加之网络防御技术本身仍处于快速发展时期，书中难免存在纰漏和不足，恳请读者批评指正。

作　者

2018 年 2 月

目　录

第 1 章　网络空间安全概述

网络空间(cyberspace)是人们为刻画所生存的信息环境而创造出来的虚拟空间，将人类社会、信息世界和物理世界紧密地联系在一起，已成为与陆地、海洋、天空、太空同等重要的人类活动新领域，也是人类在信息时代的基础活动空间。网络空间安全与国家经济、政治、社会、文化、军事等领域紧密相关，是事关国家发展和国家安全的重大战略问题，保障网络空间安全已成为人们享受全球信息化发展成果和维护国家安全、维护人类共同利益的基本前提。

1.1　网络空间的起源及其概念演进

“网络空间”一词首次出现于 1981 年美国科幻作家威廉·吉布森(William Gibson)所著的短篇科幻小说《燃烧的铬》(*Burning Chrome*)，意为计算机所创建的虚拟信息空间。1984 年，威廉·吉布森在其长篇小说《神经漫游者》(*Neuromancer*)中再度使用该词，并预示了 20 世纪 90 年代的计算机网络世界，Cyberspace 一词也凭借该小说三次荣获科幻文学大奖而为世人所熟知。但由于当时计算机应用尚未普及，Cyberspace 的概念更多的是对未来情景的一种幻想描述，离现实生活还比较遥远。其后随着计算机网络的发展，特别是互联网的兴起，Cyberspace 所描述的预言幻想渐成事实，人们开始用 Cyberspace 来命名这个人类创造的用于产生、存储和交换信息的虚拟空间，对其概念的表述则随着信息技术、网络技术的发展及其与人类社会的融合深化而不断演变。2001 年 4 月，美国国防部联合出版物《军事及其相关术语词典》中将 Cyberspace 定义为“数字化信息在计算机网络中通信时形成的一种抽象环境”[1]。这一定义赋予 Cyberspace 虚拟性的抽象概念，但局限于计算机网络的狭义范畴。2003 年 2 月，美国政府发布《保障网络空间的国家安全战略》，认为“网络空间是国家的中枢神经系统，它由无数相互关联的计算机、服务器、路由器、交换机和光缆组成，它们支持着关键基础设施的运转，网络空间的良性运转是国家安全和经济安全的基础”[2]，该定义清晰地描述了构成 Cyberspace 的物质载体及其在国家关键基础设施中的地位，但其基本含义限定在互联网范畴。2006 年 12 月，美军参谋长联席会议发布了《网络空间行动的国家军事战略》，首次将 Cyberspace 界定为“域(domain)”，认为其主要特征是“使用电子技术和电磁频谱对信息进行存储、修改和交换，并通过网络化的信息系统和物理基础设施达到此目的”[3]，此时 Cyberspace 的概念已开始超越互联网或计算机网络的范畴。2008 年 1 月，美国总统

布什签署了第54号国家安全政策总统令和第23号国土安全总统令，对Cyberspace给出了最新的定义："它是信息环境中的一个整体域，由连接各种信息技术基础设施的网络以及所承载的信息活动构成人类社会活动空间，包括互联网、电信网、计算机系统以及关键工业系统中的嵌入式处理器和控制器等，同时涉及虚拟信息环境，以及人与人之间的相互影响"[4]。这个定义首次明确指出Cyberspace的范围不限于互联网或计算机网络，还包括传统电信网、工业控制网络、军事网络以及在这些网络与信息系统中产生、传送、交换信息的相关环境。2008年5月，美国国防部常务副部长戈登·英格兰(Gordon England)在关于Cyberspace定义的备忘录中进一步修正了以往的定义，明确"网络空间是全球信息环境中的一个领域，由众多相互依存的信息基础设施网络组成，包括互联网、电信网、计算机网络、嵌入式处理器和控制器等"[5]。这个定义突出强调了Cyberspace"全球性"特征和"信息环境"的本质属性。2009年4月，美国国防大学出版了《网络权力(Cyberpower)和国家安全》一书[6]，对Cyberspace的定义进行了全面解读，认为：①它是一个可运作的空间领域，虽然是人造的，但并非某一个组织或个人所能控制的，这个空间中有人类宝贵的战略资源，不仅可用于作战，还可用于政治、经济、外交等活动；②与陆地、海洋、天空、太空等物理空间域相比，人类依赖电子技术和电磁频谱等手段才能进入网络空间，更好地开发和利用该空间资源，正如人类需要借助船、飞机、飞船才能进入海洋、天空、太空空间一样；③开发网络空间的目的是创建、存储、修改、交换和利用信息，信息是网络空间的本质，没有信息流通的网络空间就好比电网中没有电流，公路上没有汽车；④构建网络空间的物质基础是网络化的、基于信息通信技术(information and communication technology，ICT)的基础设施，包括联网的各种信息系统和信息设备，网络化是网络空间的基本特征和必要前提。2010年，国际电信联盟也对Cyberspace进行了描述，认为它是由计算机、计算机系统、网络及其软件、计算机数据、内容数据、数据流量以及用户等要素创建或组成的物理或非物理的交互领域，该描述涵盖了用户、物理设施和内容逻辑三个层面，赋予了Cyberspace新的概念内涵。同年2月，美国国防部发布了《四年防务评估报告》，认为Cyberspace是一个"由互联网和电磁通信网络等相互依存的信息技术基础设施构成的全球性领域"[7]，并将Cyberspace定位为继陆地、海洋、天空、太空四大物理空间域之后的第五维战略空间。2011年，美军参谋长联席会议发布了《美国国家军事战略报告——重新界定美国军事领导权》，明确阐述了Cyberspace与传统四大空间的关系，该报告将网络空间描述为全球连通的领域，并指出"网络空间作为一种媒介已将传统的空间连在一起，陆地、海洋、天空和太空通过网络空间聚合在一起，迸发出新的活力"[8]。

我国对网络空间至今尚未形成统一、标准的定义。武汉大学张焕国教授等认为"网络空间是信息时代人们赖以生存的信息环境，是所有信息系统的集合"[9]。东

南大学罗军舟教授在综合网络空间相关概念表述的基础上，认为“网络空间虽然定义有所区别，但是研究人员普遍认可网络空间是一种包含互联网、通信网、物联网、工控网等信息基础设施，并由人-机-物相互作用而形成的动态虚拟空间”[10]。2015 年 4 月，上海社会科学院信息研究所等发布《网络空间安全蓝皮书：中国网络空间安全发展报告(2015)》，将网络空间的内涵归纳为“一个由用户、信息、计算机(包括大型计算机、个人台式机、笔记本电脑、平板电脑、智能手机以及其他智能物体)、通信线路和设备、软件等基本要素交互所形成的人造空间，该空间使生物、物体和陆、海、空、天自然空间建立起智能联系，是人类社会活动和财富创造的全新领域”[11]。2015 年 12 月，中国工程院方滨兴院士发表文章，将网络空间定义为“所有由可对外交换信息的电磁设备作为载体，通过与人互动而形成的虚拟空间，包括互联网、通信网、广电网、物联网、社交网络、计算系统、通信系统、控制系统等”[12]，该定义一是强调了网络空间的信息交换途径是以“电磁设备作为载体”，二是明确了信息交换的范围不仅包括全局范围连接，而且包括局域连接，如某些物理隔离的网络、Ad-hoc 网络等，这一点与美国 54 号总统令对网络空间的定义有所不同。2016 年 12 月，国家互联网信息办公室发布了《国家网络空间安全战略》，指出“由互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变着人们的生产和生活方式，深刻影响着人类社会的历史发展进程”[13]。

从当前国内外有关网络空间的概念描述可知，网络空间是人类为促进人与人之间的交流互动、为促进信息的使用和探索而创设的新空间，其以各种形态的网络、设备、信息系统、电子器件和电磁频谱为物质基础，以相关系统和设备所产生、传递、处理、利用的数据及其蕴含的信息为核心资源，以信息技术、人工智能技术等为纽带，融会贯通人类社会、信息世界和物理世界(人-机-物)三元世界，成为与人类息息相关、支撑人类面向未来生存和发展最为重要的空间域。

与天然存在的陆地、海洋、天空、太空等物理空间相比，网络空间的特性可归纳为以下几方面。

(1)人造性。即人是创造、改变和利用网络空间的主体，人类对新的生产和生活方式的向往和追求是网络空间得以产生和持续发展的根本动力，人类的思维创造力对网络空间的演变具有决定性影响。这是网络空间不同于客观存在、难以随人的意志而改变的自然实体空间的最大特点，网络空间的这种人造性也为人类想象力和创造力的充分发挥提供了一个巨大的承载空间。

(2)互连性。互连性是网络空间的基本属性。网络空间的起源和演进始终以突破自然时空限制、拉近人与人之间的互动距离、连通人与物之间的认知鸿沟为根本目标。互连性体现在三个层面：首先是基于网络实体的互连实现人与人的互动；进而实现人与信息的互动，人们可以随时随地借助网络空间获取和利用信息资源；最终

达到人-机-物三元世界深度融合，实现万物泛在互连。前两个层面赋予了网络空间的全球性和无国界属性，第三个层面赋予万物以智慧，解决了人与物的单向信息交流问题，使网络空间虚拟世界与自然实体世界紧密交织，更为多元化和智慧化。

(3)信息性。网络空间的本质是信息活动的载体，没有信息流通的网络空间就好比电网中没有电流，公路上没有汽车，失去了其本身存在的意义。网络空间最大限度地开发和利用信息资源，任意个体均可进行信息发布和信息传播，访问、整合、共享各类网络信息资源，与世界各地联网的个体进行信息交互，从而大大降低信息流动、信息获取的成本，推动信息资源成为全人类共同拥有的宝贵财富。

(4)动态性。即网络空间具有长期演化性，其内涵和外延随着信息技术、网络通信技术和人工智能技术等的不断发展而持续丰富和拓展。这一点从网络空间自身的定义也得到了充分体现，从最初的计算机网络发展至互联网范畴，进而成为全球信息环境的整体域。可以预见，未来的网络空间还将继续朝着链接泛在化、结构动态化、安全属性化、数据知识化、控制智能化等方向快速发展，网络空间也必将融会贯通和包容所有物理空间，成为人类认知世界、改造世界最重要的战略空间。

1.2　网络空间安全的定义

根据国家标准 GB/T 28001 的定义，“安全”是指免除了不可接受的损害风险的状态。具体到什么叫网络空间安全，由于人们对网络空间概念本身尚无统一定论，所以对网络空间安全的定义也有所差异。欧洲网络与信息安全局发布的《国家网络空间安全战略：制定和实施的实践指南》[14]认为“网络空间安全尚无统一的定义，与信息安全的概念存在重叠，后者主要关注保护特定系统或组织内的信息安全，而网络空间安全则侧重于保护基础设施及关键信息基础设施所构成的网络”。美国国家标准技术研究院(National Institute of Standards and Technology，NIST)于 2014 年发布的《增强关键基础设施网络空间安全框架》[15]中对网络空间安全的定义是“通过预防、检测和对攻击作出响应来保护信息的过程”。美国国家安全电信和信息系统安全委员会对网络安全的定义是“在应对网络攻击中保护或防御信息和信息系统，确保其可用性、完整性、可认证性、机密性、不可抵赖性等特性，这包括在信息系统中融入保护、监测、反应，并提供信息系统的恢复能力”[16]。法国 2011 年发布的《信息系统防御和安全战略》认为网络空间安全意味着一种最终状态，在该状态下网络系统可以抵御各种可能对所存储、传输、处理的数据和与系统相关或者连接的相关服务的机密性、完整性和可用性造成的损害。百度百科将网络安全定义为“网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断”。我国 2016 年出台的《网络安全法》将网络安全定义为“通过采取必要措施，防范对