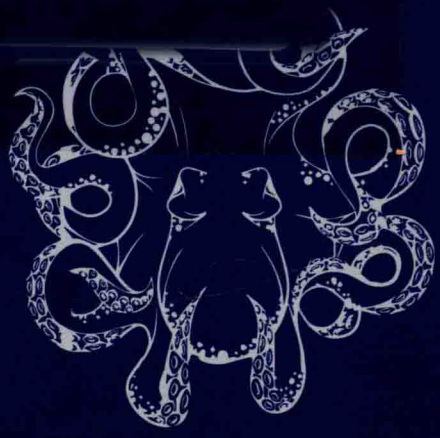
网络空间拟态防御原理

——广义鲁棒控制与内生安全（第二版）

（上册）



邬江兴 著

科学出版社

网络空间拟态防御原理

——广义鲁棒控制与内生安全（第二版）

上册

鄔江兴 著

科学出版社

北京

内 容 简 介

针对网络空间基于目标对象软硬件漏洞后门等暗功能的安全威胁问题，本书从“结构决定安全”的哲学层面诠释了改变游戏规则的“网络空间拟态防御”思想与理论形成过程、原意与愿景、原理与方法、实现基础与工程代价以及尚需完善的理论和方法等。在理论与实践结合的基础上，证明了在创新的“动态异构冗余”构造上运用生物拟态伪装机制可获得内生性的“测不准防御”效应。在不依赖关于攻击者的先验知识和行为特征信息的情况下，按照可量化设计的指标管控拟态界内未知的未知攻击或者已知的未知失效引起的广义不确定扰动影响，并能以一体化的方式处理信息系统传统与非传统安全问题。建立了拟态构造模型，并就抗攻击性和可靠性等问题给出了初步的定量分析结论以及第三方完成的“白盒实验”结果。

本书可供信息技术、网络安全、工业控制等领域科研人员、工程技术人员以及普通高校教师、研究生阅读参考。

图书在版编目（CIP）数据

网络空间拟态防御原理：广义鲁棒控制与内生安全. 上 / 邬江兴著. —2 版. —北京：科学出版社，2018.11

ISBN 978-7-03-059097-8

Ⅰ. ①网… Ⅱ. ①邬… 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 236579 号

责任编辑：任 静 / 责任校对：郭瑞芝

责任印制：师艳茹 / 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

三河市春园印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2017 年 12 月第 一 版 开本：720×1 000 1/16

2018 年 11 月第 二 版 印张：20 1/4

2018 年 11 月第一次印刷 字数：407 000

定价：126.00 元

（如有印装质量问题，我社负责调换

作者简介

邬江兴，1953 年生于浙江省嘉兴市。现任国家数字交换系统工程技术研究中心(NDSC)主任、教授，2003 年当选中国工程院院士。先后担任国家“八五”“九五”“十五”“十一五”高技术研究发展计划(863 计划)通信技术主题专家、副组长、信息领域专家组副组长，国家重大专项任务“高速信息示范网”“中国高性能宽带信息网——3Tnet”“中国下一代广播电视网——NGB”“新概念高效能计算机体系结构研究与系统开发”总体组组长，“新一代高可信网络”“可重构柔性网络”专项任务编制组负责人，移动通信国家重大专项论证委员会主任，国家“三网融合”专家组第一副组长等职务。20 世纪 80 年代中期发明了软件定义功能、复制 T 型数字交换网络、逐级分布式控制构造等程控交换核心技术，90 年代初主持研制成功具有自主知识产权的中国首台大容量数字程控交换机——HJD04，带动了我国通信高技术产业在全球的崛起。21 世纪初先后发明了全 IP 移动通信、不定长分组异步交换网络、可重构柔性网络架构、基于路由器选择发送广播机制的 IPTV 等网络通信技术，主持开发成功世界首套基于全 IP 的复合移动通信系统 CMT、中国首台高速核心路由器、世界首个大规模汇聚接入路由器——ACR 等信息通信网络核心装备。2010 年提出了面向高效能计算的“基于主动认知的多维可重构软硬件协同计算构造——拟态计算构造”。2013 年在全球首次推出基于拟态构造的高效能计算机原型系统并通过了国家验收，被中国科学院和中国工程院两院院士评为 2013 年度“中国十大科技进展”。同年，创立了网络空间拟态防御理论，2016 年完成原理验证系统国家测试评估，2017 年 12 月出版《网络空间拟态防御导论(上、下)》专著。先后获得国家科技进步奖一等奖 3 项，国家科技进步奖二等奖 4 项。曾获得 1995 年度和 2015 年度何梁何利基金科学与技术进步奖、科学与技术成就奖。其领衔的网络与交换研究团队还获得 2015 年度国家科技进步奖创新团队奖。

更名出版说明

本书主要内容源自2017年12月由科学出版社出版发行的《网络空间拟态防御导论(上、下)》。一年多来，拟态防御基本理论与方法借助国家工业和信息化部专项试点计划的推动，快速步入实用化阶段。继2018年1月13日，世界首台拟态构造的域名服务器在中国联合通信公司河南分公司上网运行，4月14日又有多种基于拟态构造的 Web 服务器、路由/交换系统、云服务平台、防火墙等网络装置在河南景安网络科技公司体系化地投入线上运营服务。5月11日，基于拟态构造的COST级信息通信网络设备，作为中国南京拟态防御首届国际精英挑战赛——“人机大战”的目标设施，与包括全国第二届“强网杯”前20名网络战队和特邀的 6 支国外顶级团队在内的豪华阵容开展了激烈的人机博弈，并首次增加了“线下白盒”注入式攻击比赛内容，用“改变了的游戏规则”检验了拟态防御技术对抗植入式后门或恶意代码的能力。比赛结果证明，拟态构造的网络服务设备不仅能自然阻断基于软硬件代码漏洞的攻击，而且对白盒条件下由各战队现场植入的“自主编制测试例”也有着超乎寻常的抑制能力。截至7月底，网上试点应用积累了大量现有安全防御手段未能感知的“已知的未知”或“未知的未知”攻击场景快照(也包括目标设备软硬件自身的偶发性故障)，采集到了可供进一步分析的高价值问题场景数据，甚至发现了一些利用尚未公布或披露的漏洞后门、病毒木马实施网络攻击的可复现场景，以线上服务的统计数据诠释了拟态防御构造内生安全机制，在抑制拟态界内包括未知安全威胁在内的广义不确定扰动的独特功效，有力佐证了建立在系统工程理论基础之上的拟态构造，能够使信息系统全生命周期内达成高可靠、高可用、高可信“三位一体”的技术经济目标。其“改变游戏规则”的变革意义，预示着“可设计、可验证”的内生安全必将成为新一代信息系统的标志性功能之一。

从科学研究程序意义或技术发展实践意义上说，拟态防御只是初步完成了“发现、认知、度量、控制”四个阶段的基础性研究工作。换言之，也只是将基于目标对象漏洞后门等的防御问题从定性、描述性研究阶段提升到可定量设计、实验验证的研究阶段。但是，高性价比、低使用门槛的工程实现技术，特别是领域专用软硬模块和设计工具的开发，仍是降低拟态构造应用复杂度需要努力克服的技术瓶颈。2018年5月在南京正式成立的全国“拟态技术与产业创新联盟”，

将担负起“众人拾柴成就燎原大火”的重任，以开放、开源模式致力于打造全球化的产业技术命运共同体，并联合保险业等社会金融资本营造起合作多赢的商业生态环境。

本书是作者在《网络空间拟态防御导论(上、下)》一书的基础上完成的，对相当一部分内容做了重要的更正和修订完善，调整和补充了一些章节内容，并力争做到文字表述的严谨性。为突出拟态防御原理的工程应用意义，作者结合近年来在产品技术研发方面的具体案例，专门增加了“拟态防御应用示范与现网测试”章节。以“网络空间拟态防御原理——广义鲁棒控制与内生安全”为标题，更名出版。

邬江兴

2018 年 9 月于郑州

Preface 序 言

中国有句古话：它山之石可以攻玉。

记得10年前，我在主持国家高技术研究发展计划(863计划)重大专项任务——“新概念高效能计算机体系结构研究与系统开发”时，最具挑战性的问题是，在排除物理、工艺和资源管理机制等改良或改进因素外，如何以系统结构技术的创新，显著提升计算或处理效能。

“结构决定功能，结构决定性能”是众所周知的公理。据此，探讨结构、功能与效能之间的关系应当是破解当前研究难题的切入点。幸运的是，“给定功能条件下往往存在不同的实现结构”且“不同实现结构往往具有不同的性能与效能”也是路人皆晓的常识。于是，“功能等价条件下，结构可以决定性能，结构同样可以决定效能”就是一个自然而然的推论。基于这个推论构造的计算或处理系统应具备3个基本特征：首先是系统需要预先配置多种不同能效比的功能等价处理模块(或算法)，其次是系统要能够实时感知计算任务关于时间的负载分布和能耗状况，再者系统要能联合调度合适的软硬件功能模块(算法)，协同完成当前的计算任务以拟合期望的能效曲线。于是，同一任务在不同时段、不同负载、不同资源、不同运行场景等情况下，系统能够通过主动认知的方式选择合适能效比模块或算法来获得理想的任务处理效能。出于对条纹章鱼(俗称拟态章鱼)神奇功能的赞叹和受到生物拟态现象的灵感激发，我将这种功能等价条件下，基于主动认知的动态变结构协同计算命名为拟态计算(Mimic Structure Calculation，MSC)。

2013年7月，国家科技部在上海组织了世界上首台拟态计算原理验证系统的测试评估。结果表明，基于计算密集、存储密集和输入输出密集三类十余项经典测试用例，在排除其他节能降耗因素后，参照当时主流服务器的能效比，拟态计算系统具有数十到数百倍以上的比较优势，开创了运用功能等价动态变结构协同计算技术解决信息处理系统能效问题的新方法和新途径。需要强调的是，这种指向能效的变结构协同计算可以容易地转换为针对性能的变结构协同处理，因而拟态计算架构具有效能和性能目标间自由转换以及联合优化与管理的功能。

众所周知，传统计算处理系统采用面向性能的主体设计思想，缺乏安全性分析和相关设计指标体系，例如缓冲行为、分支预测器、存储管理、debug 模式、BIOS 自举机制以及功耗和内部传感器等对安全性的影响。加之体系结构设计对软件开发者的“黑盒”效应，导致系统构建时存在一些错误的安全性假设，既无法实现效能与性能联合优化及可信性管理，也无法证明自身的安全性。而拟态计算系统具有基于主动认知的多样性、动态性和随机性的协同处理场景，其任务功能与算法结构间的非确定性关系，恰好能弥补传统信息处理系统在应对基于漏洞后门等攻击时的静态性、确定性和相似性安全缺陷。一个直观的推论就是，针对攻击者利用目标对象未知漏洞后门实施的“里应外合”式蓄意行动，有意识地运用功能等价动态变结构处理场景的非确定性关系，应当可以扰乱或瓦解基于漏洞后门等攻击链的稳定性与有效性，创造出以内生的“测不准”机制应对网络空间安全威胁的新型构造技术。以变结构协同计算的“它山之石”来打磨目标场景不确定改变的“防御之玉”，这就是网络空间拟态防御最初的构想。读者将不难发现，拟态计算和拟态防御本质都是功能等价条件下的变结构协同处理技术，只不过后者的经典应用模式需要有包括共识机制在内的多模裁决算法而已。因此，将拟态防御视为主动认知的拟态计算场景在时空维度上的变换，也许更能凸显两者之间“大道至简”的哲学意义。

需要特别指出的是，随着“万物互联”、云计算、大数据时代的来临，微电子和虚拟化等技术的不断进步，拟态防御理论不仅能给高可靠、高可用、高可信的信息系统或控制装置架构技术带来“改变网络空间游戏规则”的变革，而且能使新一代信息技术产品获得不可或缺的广义鲁棒控制功能，对于从源头治理软硬件产品安全漏洞污染网络环境问题具有里程碑意义。

在国家科技部和上海市科学技术委员会为时十年的长期支持下，在国家数字交换系统工程技术研究中心（NDSC）、复旦大学、上海交通大学、浙江大学、中兴通讯、烽火科技、成都迈普、中国电子科技集团第 32 所等研究机构和企业科研人员的不懈努力下，网络空间拟态防御理论体系得以创立，2016 年原理验证系统通过了国家组织的权威性测试评估。其独特的基于广义鲁棒控制架构技术的内生防御机制突出表现在五个方面：首先是能将针对拟态括号内执行体个体未知漏洞后门的隐匿性攻击，转变为拟态界内攻击效果不确定的事件；其次是能将效果不确定的攻击事件归一化为具有概率属性的广义不确定扰动问题；三是基于拟态裁决的策略调度和多维动态重构负反馈机制能呈现出攻击者视角下的“测不准”效应；四是借助“相对正确”公理的逻辑表达机制，可以在不依赖攻击者先验知识或行为特征信息情况下提供高置信度的敌我识别功能；五

序 言

是能将非传统安全威胁归一化为广义鲁棒控制问题并实现一体化的处理。为此，我将生物拟态伪装机制赋予动态异构冗余架构所获得的测不准效应，用于化解或防范基于目标系统漏洞后门等“已知的未知风险”或“未知的未知威胁”的原理与方法，称之为网络空间拟态防御(Cyberspace Mimic Defense，CMD)。

令人振奋的是，随着基于拟态防御原理的信息系统或控制装置不断进入各个应用领域，“改变网络空间游戏规则”的广义鲁棒控制构造及其内生安全效应正不断彰显出其勃勃生机与旺盛活力，有望在信息系统软硬构件供应链可信性不能确保的全球化生态环境下，以创新的系统构造技术开辟出一条破解软硬构件“自主可控、安全可信”难题的新途径。

作者深信，随着拟态防御理论的不断完善和应用技术的持续创新，我们将迎来以目标对象内生安全功能为核心的网络空间防御技术新时代。网络攻防代价严重失衡的战略格局有望从根本上得到逆转，“安全性与开放性”“先进性与可信性”严重对立状况将能在经济技术全球化环境中得到极大统一，基于目标对象软硬件代码缺陷的攻击理论及方法将受到颠覆性的挑战，信息技术与产业也将由此迸发出裂变式的创新活力并迎来强劲的市场升级换代需求。具有广义鲁棒控制构造和内生安全功能的新一代信息系统、工业控制装置、网络基础设施等必将重塑网络空间安全新秩序。

邬江兴

2018 年 9 月于郑州

Foreward 前 言

今天，人类社会正以前所未有的速度迈入数字经济时代，数字革命推动的信息网络技术全面渗透到人类社会的每一个角落，活生生地创造出一个万物互联、爆炸式扩张的网络空间，一个关联真实世界与虚拟世界的数字空间正深刻改变着人类认识自然与改造自然的能力。然而不幸的是，网络空间的安全问题正日益成为信息时代或数字经济时代最为严峻的挑战之一。正是人类本性之贪婪和科技发展的阶段性特点，使得人类所创造的虚拟世界不可能成为超越现实社会的圣洁之地。不择手段地窥探个人隐私与窃取他人敏感信息，肆意践踏人类社会的共同行为准则和网络空间安全秩序，谋取不正当利益或非法控制权，已经成为当今网络空间发展的“阿喀琉斯之踵”。

网络空间安全问题尽管多种多样，攻击者的手段和目标也日新月异，对人类生产与生活造成的威胁之广泛和深远更是前所未有，但其基本技术原因则可以简单地归结为以下五个方面：一是，人类现有的科技能力尚无法彻底避免信息系统软硬件设计缺陷可能导致的漏洞问题；二是，经济全球化生态环境衍生出的信息系统软硬件后门问题不可能从根本上杜绝；三是，现阶段的科学理论和技术方法尚不能有效地彻查软硬件系统中的漏洞后门等“暗功能”；四是，上述原因致使软硬件产品设计、生产管理和使用维护等环节缺乏有效的安全质量控制手段，造成信息技术产品的漏洞后门问题随着数字经济或社会信息化的加速而严重污染整个网络世界并使之陷入万劫不复的境地；五是，相对补救性质的防御代价而言，网络攻击的技术门槛之低，似乎任何具备网络知识或对目标系统软硬件漏洞具有发现和利用能力的个人或组织，都可以成为随意跨越网络空间诚信准则的“黑客”。

如此悬殊的攻防不对称代价和如此之大的利益诱惑，很难相信网络空间技术先行者们或市场垄断企业，不会处心积虑地利用全球化形成的国家间分工、产业内部分工乃至产品构件分工机会，施以“隐匿漏洞、预留后门、植入病毒木马”等全局性控制手段，谋求在市场直接产品利润之外，通过掌控用户“数据资源”和敏感信息获取不当或不法利益。作为一种可以影响个人、企业、地区、国家甚至全球社会的超级威胁或恐怖力量，网络空间漏洞后门等暗功能事

实上已成为战略性资源，不仅会被众多不法个体或有组织的犯罪团伙或恐怖势力觊觎和利用，而且毫无疑问会成为各国政府谋求“网络威慑能力”“网络反制能力”或“制网络权、制信息权”的战力建设与运用目标。事实上，网络空间早已成为常态化、白热化、无硝烟的战场，各利益攸关方的博弈无所不用其极。但是，目前的态势仍然是“易攻难守”。

现行的主被动防御理论与方法大多以威胁的精确感知为基本前提，遵循“威胁感知，认知决策，问题移除”的边界防御理论和技术模式。实际上，当前情况下无论是网元设备还是附加型防护设施，不论是基于 Intranet 的区域防护还是基于“Zero Trust Architecture”的全面身份认证措施，由于都无法彻底排除或杜绝软硬件设备漏洞后门之类的影响，因而对于“已知的未知”安全风险或者“未知的未知”安全威胁，不仅边界防御在理论层面已经难以自洽，就是实践意义上也无合适的技术手段进行效果可量化的设计布防。更为严峻的是，迄今为止，既未找到任何不依赖于攻击特征或行为信息的威胁感知新思路，也未找到技术上有效与经济上可承受且能普适化运用的防御新方法。以美国人提出的“移动目标防御（Moving Target Defense, MTD）”为代表的各种动态防御技术，在干扰或阻断基于目标对象漏洞之攻击链可靠性方面确能取得不错的功效。但在应对潜藏于目标系统内部的暗功能或基于软硬件后门等的未知攻击方面，即使运用加密认证类的底线防御手段，也无法彻底避免被宿主对象内部漏洞后门功能“旁路、短路或反向加密”的风险，2017 年发现的基于 Windows 漏洞的勒索病毒 WannaCry 就是反向加密的典型案例。事实上，基于边界防御的理论和定性描述的技术体系，无论是支持“云-网-端”新型使用模式还是在零信任安全框架部署方面都已经遭遇难以克服的挑战。

生物免疫学知识告诉我们，脊椎生物的特异性抗体只有受到抗原的多次刺激后才能形成，当同种抗原再度入侵机体时方能实施特异性清除。这与网络空间现有防御模式极其相似，我们不妨将其类比为“点防御”。同时，我们也注意到，脊椎动物所处环境中，时时刻刻存在形态、功能、作用各异，数量繁多的其他生物，也包括科学上已知的有害生物抗原。但健康生物体内并未发生显性的特异性免疫活动，绝大部分的入侵抗原应当是被与生俱来的非特异性选择机制清除或杀灭的，生物学家将这种通过先天遗传机制获得的神奇能力，命名为非特异性免疫。我们不妨将其类比为“面防御”。生物学的发现还揭示，特异性免疫是以非特异性免疫为基础的，后者触发或激活前者，而前者的抗体只有通过后天获得，且生物个体间存在质和量上的差异，迄今未发现关于特异性免疫的任何遗传学证据。至此，我们知道脊椎动物因为具有点面结合的双重免疫机

制，才获得了抵御已知或未知抗原入侵的能力。令人沮丧的是，人类在网络空间并未创造出这种“具有通杀性质的非特异性免疫机制”，总是以点防御的办法竭力去应对面防御任务。理性预料和严酷现实表明，“堵不胜堵、防不胜防、漏洞百出”是必然之结局，战略上不可能摆脱被动应付的局面。

造成这种尴尬局面的核心问题是，科技界至今未搞清楚非特异性免疫是如何做到精准“敌我识别”的。按常理推论，连机体特异性免疫形成的有效信息都不能携带的生物遗传基因，不可能拥有未来所有可能入侵的细菌、病毒、衣原体等抗原特征信息。就如同网络空间基于已发现的漏洞后门或病毒木马等行为特征形成的各种漏洞或攻击信息库那样，今天的库信息中不可能包括明天可能发现的漏洞后门或病毒木马等特征信息，更无法囊括未来什么形式的攻击特征信息。我们这样提出问题的目的不是企图弄明白“造物主如何使脊椎生物具有对入侵抗原实施与生俱来的非特异性选择清除能力”，而是想知道在网络空间是否也存在类似的敌我识别机制，以及能有效抑制包括已知的未知风险或未知的未知威胁在内的广义不确定扰动的控制构造，并能获得不依赖(但不排斥)任何附加式防御技术有效性的内生安全效应。运用这样的机制、构造和效应可以将基于漏洞后门或病毒木马等攻击事件归一化为传统的可靠性问题，借助成熟的鲁棒控制与可靠性理论和方法，使得信息系统或控制装置能同时获得管控软硬件故障和人为攻击影响的稳定鲁棒性与品质鲁棒性，即需要从理论和方法层面找到统一处理可靠性与可信性问题的解决途径。

首先要克服的挑战是如何感知未知的未知威胁，也就是说在不依赖攻击者先验知识或攻击行为特征信息的情况下，怎样才能实现最低虚警、漏警、误警率的敌我识别。其实，哲学意义上本来就没有绝对的已知或毫无悬念的确定性，“未知”或“不确定性”总是相对的或有界的，与认知空间和感知手段强相关。诸如，“人人都有这样或那样的缺点，但独立完成同样任务时，在同一个地点、同时犯完全一样的错误属于小概率事件”的公知(作者将其称为“相对正确”公理，业界也有共识机制的提法)，就对未知或不确定的相对性认知关系给出了具有启迪意义的诠释。相对正确公理的一种等价逻辑表达——异构冗余构造和多模共识机制，能够在功能等价条件下，将单一空间下的未知问题场景转换为功能等价多维异构冗余空间共识机制下的可感知场景，将不确定性问题变换为可用概率表达的可靠性问题，将基于个体的不确定行为认知转移到关于群体(或元素集合)行为层面的相对性判识上来，进而将多数人的认知或共识结果作为相对正确的置信准则(这也是人类社会民主制度的基石)。需要强调的是，凡是相对性判识就一定存在如同量子叠加态的“薛定谔猫”效应，正确与错误总是同时

存在，只是概率不同而已。相对正确公理在可靠性工程领域的成功应用，就是20世纪70年代首先在飞行控制器领域提出的非相似余度构造。基于该构造的目标系统在一定的前提条件下，即使其软硬构件存在分布形式各异的随机性失效，或者存在未知设计缺陷导致的统计意义上的不确定失效，也可以被多模表决机制变换为能用概率表达的可靠性事件，从而使我们不仅能通过提高或改善构件质量的方式提高系统可靠性，也能通过构造技术的创新来显著地增强系统的可靠性与可信性。对于利用软硬件系统漏洞后门的不确定（或缺乏先验知识的人为攻击）威胁而言，非相似余度构造也具有与敌我识别作用相同或相似的功效。尽管不确定威胁的攻击效果对于异构冗余个体而言往往不是概率问题，但是这些攻击事件在群体层面的反映，常常取决于攻击者能否协调一致的实现多模输出矢量时空维度上的共识表达，而这恰恰属于典型的概率问题。不过，在小尺度空间上，一定时间内，基于非相似余度构造的目标对象，虽然能够抑制包括未知的人为攻击在内的广义不确定扰动，且具有可设计标定、验证度量的品质鲁棒性。但是，其构造的静态性、相似性和确定性等基因缺陷，决定了自身漏洞后门等仍然具有相当程度的可利用性，“试错式”或“排除法”等攻击手段，常常会破坏目标对象的稳定鲁棒性。

其次，如果从鲁棒控制的观点视之，网络空间绝大多数安全事件也可以认为是由针对目标对象软硬件漏洞后门等攻击引起的广义不确定扰动。换言之，由于人类目前尚不具备管控或抑制软硬件产品暗功能的能力，所以原本属于设计或制造过程中的安全质量问题，因为存在“无法突破的技术瓶颈”，就“万般无奈地溢出”成为网络空间最主要的安全污染。由此，生产厂家不承诺软硬件产品安全质量，或者不对产品安全质量引起的后果承担任何法律责任的行为，似乎都可以心安理得地归结为“世界性难题”所致。经济技术全球化时代，恢复产品质量神圣承诺和商品经济基本秩序，从源头治理被污染的网络空间生态环境，需要创造出一套能够有效管控“试错式攻击”的新型鲁棒控制构造，以及由生物拟态伪装策略驱动的反馈控制机制产生的测不准效应，为软硬件系统提供稳定鲁棒性和品质鲁棒性。

再者，即使我们不能指望广义鲁棒控制构造和拟态伪装机制产生的内生安全效应能够解决网络空间所有的安全问题，甚至都不敢奢望能彻底解决目标对象软硬件漏洞后门等引发的全部安全问题。但是，我们仍然期望创新的广义鲁棒构造能够从机理上自然融合（吸纳）现有或未来的网络安全技术。无论是导入静态防御、动态防御或是主动防御还是被动防御的技术元素，都应当能使目标对象的防御能力获得指数量级增长。实现信息系统或控制装置“服务提供、

可信防御、鲁棒控制”一体化的经济技术目标，实践“大道至简”的技术憧憬。

最后，还需要从理论和应用的结合上完成体系架构设计、共性技术开发、原理验证到应用试点、行业示范全过程的工程实践。

“网络空间拟态防御”就是上述思想不断迭代发展与实践层面不懈探索的结果。

2016 年 1 月，国家科技部委托上海市科学技术委员会组织了全国 10 余家权威测评机构和研究单位的上百名专家，对“拟态防御原理验证系统”进行了历时 4 个多月的众测验证与技术评估，结果表明：“被测系统完全达到理论预期，原理具有普适性。”

2017 年 12 月，《网络空间拟态防御导论(上，下)》，由科学出版社出版发行。

为了便于读者理解拟态防御原理和体现循序渐进的表述特点，本书分为上、下册，共 14 章。第 1 章“基于漏洞后门的安全威胁”由魏强负责编撰，从漏洞后门的不可避免性分析入手，着重介绍了漏洞后门的防御难题，指出网络空间绝大部分的信息安全事件都是攻击者借助软硬件漏洞后门发起的，通过感悟与思考方式提出了转变防御理念的初衷。第 2 章“网络攻击形式化描述”由李光松、吴承荣、曾俊杰负责编撰，概览或试图总结目前存在的典型网络攻击形式化描述方法，并针对动态异构冗余的复杂网络环境提出了一种网络攻击形式化分析方法。第 3 章“传统防御技术简析”由刘胜利、光焱负责编撰，从不同角度分析了目前网络空间三类防御方法，并指出传统网络安全框架模型存在的四个方面问题，尤其是，目标对象和防御系统对自身可能存在的漏洞后门等安全威胁没有任何的防范措施。第 4 章“新型防御技术及思路”、第 5 章“多样性、随机性和动态性分析”由程国振、吴奇负责编撰，概略性地介绍了可信计算、定制可信空间、移动目标防御以及区块链等新型安全防御技术思路，并指出了存在的主要问题。初步分析了多样性、随机性和动态性等方法对于破坏攻击链稳定性的作用与意义，同时指出了面临的主要技术挑战。第 6 章“异构冗余架构的启示”由斯雪明、贺磊、杨本朝、王伟、李光松、任权等共同参与撰写，概述了基于异构冗余技术抑制不确定性故障对目标系统可靠性影响的作用机理，指出异构冗余架构与相对正确公理逻辑表达等价，具有将不确定问题变换为可控概率事件的内在属性。用定性和定量的方法，分析了非相似余度架构的容侵属性以及至少 5 个方面的挑战，并提出在此架构中导入动态性或随机性能够改善其容侵特性的设想。第 7 章“广义鲁棒控制与动态异构冗余架构”由刘彩霞、斯雪明、贺磊、王伟、任权等共同参与撰写，提出了一种称之为“动态异构冗余”的信息系统广义鲁棒控制架构，并用定量分析证明了内生性防御机制能够在不依赖攻击者任何特征信息的情况下，迫使基于目标对象漏洞后门的

攻击行为，必须面对“非配合条件下，动态多元目标协同一致攻击”难度的挑战。第 8 章“拟态防御原意与愿景”由赵博等共同参与撰写，提出了在动态异构冗余架构基础上引入生物拟态伪装机制形成测不准效应的设想，期望造成攻击者对拟态括号内防御环境（包括其中的漏洞后门等暗功能）的认知困境，以便显著地提升跨域多元动态目标协同一致攻击难度。第 9 章“网络空间拟态防御原理”、第 10 章“拟态防御工程实现”、第 11 章“拟态防御基础与代价”由贺磊、胡宇翔、李军飞、任权等共同参与撰写，系统地介绍了拟态防御基本原理、方法、构造和运行机制，对拟态防御的工程实现做了初步的探索研究，就拟态防御的技术基础和应用代价问题进行了讨论，并指出一些亟待解决的科学与技术问题。第 12 章“拟态原理应用举例”由马海龙、郭玉东、张铮撰写，分别介绍了拟态防御原理在路由交换系统、Web 服务器和网络存储系统中的验证性应用实例。第 13 章“拟态原理验证系统测试评估”由伊鹏、张建辉、张铮、庞建民等撰写，分别介绍了路由器场景和 Web 服务器场景的拟态原理验证测试情况。第 14 章“拟态防御应用示范与现网测试”专门介绍了路由/交换机、Web 服务器、域名服务器等拟态构造产品现网使用和测试情况。

读者不难看出全书的逻辑安排是：指出漏洞后门是网络空间安全威胁的核心问题；分析现有防御理论方法在应对不确定性威胁方面的基因缺陷；从基于相对正确公理的非相似余度构造出发，获得无先验知识条件下将随机性失效转换为概率可控的可靠性事件的启示；提出了基于多模裁决的策略调度和多维动态重构负反馈机制的动态异构冗余构造，并指出在该构造基础上导入拟态伪装机制能够形成攻击者视角下的测不准效应；发现这种类似脊椎动物非特异性和特异性双重免疫机制的广义鲁棒控制架构，具有内生的安全功能和防御效果，可独立应对基于拟态括号内漏洞后门等已知的未知安全风险或未知的未知安全威胁，以及传统的不确定扰动因素影响；系统地阐述了网络空间拟态防御原理、方法、基础与工程实现代价；给出了带有原理验证性的应用实例；介绍了原理验证系统的测评情况与验证结果；最后，给出了拟态构造网络产品现网试点使用情况。

毫无疑问，基于动态异构冗余构造的拟态防御，在带来独特技术优势的同时必然会增加设计成本、体积功耗、使用维护方面的开销。与所有安全防御技术的“效率与成本”规律相同，-“防护效率、防御成本与贴近目标对象的程度呈正比”，拟态防御也不例外。事实上，任何防御技术都是有代价的且不可能泛在化使用，所以“隘口部署、要点防御”才得以成为军事教科书上的金科玉律。通信网络领域的初步应用实践表明，拟态防御技术增加的成本相对于目标系统全生命周期获得的综合收益而言，远不足以削弱其广泛应用的价值。此外，当

前　言

今时代微电子、软件可定义、硬件可重构以及虚拟化等技术手段和开发工具的持续进步，开源社区模式的广泛应用，以及不可逆转的全球化趋势，使得目标产品市场价格只与应用规模强相关而与复杂度相对解耦，“牛刀杀鸡”和模块化集成已成为抢占市场先机的首选模式。更由于“绿色高效、安全可信”使用观念的不断升华，在追求信息系统或控制装置更高性能、更灵活功能的同时，更注重应用的经济性和服务的可信性，促使人们传统的成本价值观念与投资理念转向更加关注系统全生命周期(包括安全防护等在内)的综合投资和使用效益方面。因而作者相信，随着拟态防御理论和方法的不断完善与持续进步，网络空间游戏规则即将发生深刻变革，新一代具有内生安全功能的软硬件产品呼之欲出，拟态技术创新之花必将蓬勃绽放。

目前，拟态防御只是完成了理论自洽、原理工程验证和共性技术突破，正在结合相关行业特点展开有针对性的应用研究开发，一些试点和示范应用项目已取得重要进展并获得了宝贵的工程实践经验。毫无疑问，书中所涉及的内容肯定会存在理论和技术初创阶段无法回避的完备性与成熟性问题，一些技术原理尚未完全脱离“思想实验”阶段，稚嫩和粗糙的表述在所难免。此外，书中也给出了一些理论和实践层面亟待解决的科学与技术问题。不过，作者深信，任何理论或技术的成熟都不可能在书房或实验室里完成，尤其像拟态防御或广义鲁棒控制这类与应用场景、工程实现、等级保护、产业政策等强相关，跨领域、改变游戏规则的挑战性理论与技术，必须经历严格的实践检验和广泛的应用创新才能修成正果。本书的出版发行就是秉承这一理念，以期获得抛砖引玉的功效，达成“众人拾柴火焰高”的目的。衷心欢迎广大读者通过本书提供的拟态防御网站(http://mimictech.cn)，开展多种形式的理论辨析与技术探讨，由衷期望拟态防御理论和基本方法能为当今网络空间“易攻难守”的战略格局带来革命性变化，“结构决定安全”、可量化设计、可实验验证的广义鲁棒控制架构能够为新一代 IT、ICT 或 CPS 以及相关产业带来强劲的创新活力与旺盛的市场换代需求。

本书适合作为网络安全学科研究生教材或相关学科参考书，对有兴趣实践拟态防御应用创新或有志向完善拟态防御理论与方法的科研人员具有入门指南意义。为使读者全面了解本书各章节衔接关系，便于专业人士选择性阅读，特附“各章关系视图”。

作　者

2018 年 9 月于郑州

各章关系视图