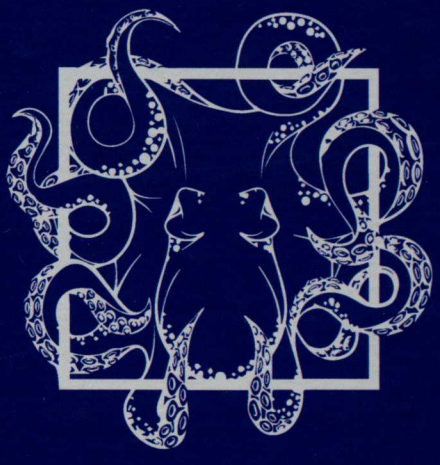
网络空间拟态防御导论

（下册）



Introduction to
Cyberspace
Mimic Defense

鄔江兴　著

科学出版社

NTRODUCTION TO CYBERSPACE MIMIC DEFENSE

网络空间拟态防御导论

下　册

邬江兴　著

科学出版社

北京

内 容 简 介

本书围绕网络空间安全威胁之漏洞后门问题展开，系统地诠释了“网络空间拟态防御”思想与理论的形成过程、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问题等，并通过几个原理验证系统应用实例和权威测试评估报告等相关内容，理论与实践相结合，证明了拟态构造的独创性与有效性。最后，基于广义随机 Petri 网理论和方法，分别为信息系统典型的非冗余、非相似余度及拟态架构建立了相关数学模型，并尝试着给出了对应的抗攻击性和可靠性的定量分析结论。

本书可供计算机、信息安全、工业控制等领域的科研人员、工程技术人员以及普通高校的教师、研究生阅读参考。

图书在版编目 (CIP) 数据

网络空间拟态防御导论. 下册 / 邬江兴著. —北京：科学出版社，2017.12

ISBN 978-7-03-055668-4

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(2017)第 289806 号

责任编辑：任 静 / 责任校对：郭瑞芝

责任印制：张克忠 / 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

北京汇瑞嘉合文化发展有限公司印刷

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 3 月第三次印刷 印张：23 3/4

字数：287 000

定价：115.00 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。1982 年毕业于解放军工程技术学院计算机科学与工程专业。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。作为中国信息通信与网络交换领域著名专家，先后担任“八五”“九五”“十五”“十一五”国家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 90 年代初主持研制成功中国首台大容量数字程控交换机——HJD04，本世纪初先后主持开发成功中国首台高速核心路由器、世界首台大规模汇聚接入路由器——ACR、国际上第一个柔性可重构网络等信息通信基础设施核心装备。2013 年首次在全球推出基于拟态计算原理的高效能计算机原型系统，2013 年基于拟态计算原理又提出网络空间拟态防御理论，并于 2016 年完成原理验证系统测试评估。先后获得国家科技进步一等奖 3 项，国家科技进步二等奖 3 项，国家教学成果一等奖 1 项。还曾获得 1995 年度何梁何利科学与技术进步奖、2015 年度何梁何利科学与技术成就奖。他所领导的研究团队曾获得 4 个国家科技进步一等奖、9 个国家科技进步二等奖，2015 年被授予国家科技进步奖网络与交换技术创新团队。

Forward 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本任务难题的切入点。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，结构也可以决定效能”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(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，再者系统要能自主调度合适的功能模块(算法)执行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不同能效比模块或算法来获得理想的任务处理效能。出于对拟态章鱼神奇表现的赞叹和生物拟态现象之灵感激发，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，

参照当时主流计算系统的能效比，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。需要特别强调的是，这种指向能效的变结构计算可以非常容易地转换为针对性能的变结构计算，因而拟态计算系统能够实现性能与效能目标的高度统一。

作为变结构计算机制的深度利用，拟态计算系统的运行场景具有内在的多样性、动态性和冗余性，其服务功能与视在结构的不确定性关系，恰好能避免传统信息系统或控制装置在应对基于漏洞后门攻击时的静态性、确定性和相似性之构造缺陷问题。一个直观的推论就是，针对网络空间目标对象“单向透明”场景下的“里应外合”式攻击行动，有意识地在信息系统或控制装置中运用功能等价动态变结构技术体制，其内生效应无疑可以扰乱或瓦解基于目标对象漏洞后门等攻击链的稳定性，创造出以视在的不确定目标场景应对网络空间安全威胁的新型防御机制。以变结构计算的“它山之石”来攻目标场景动态可变的“防御之玉”，这就是网络空间拟态防御原理最初的构想。读者将不难发现，拟态计算和拟态防御本质都是基于功能等价条件下的变结构处理技术，只不过是后者的经典应用模式需要有多数表决功能而已。从一定程度上说，将拟态防御视为拟态计算的某种特殊构造效应，也许更能揭示出两者之间的因果关系。

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，半导体工艺和虚拟化等技术的不断进步，拟态理论不仅能对高效能、高可信的 ICT 系统架构技术带来“改变网络空间游戏规则”的变革，而且能对绿色、高鲁棒性的 IT 系统构造技术发展产生划时代意义的影响。

在国家科技部和上海市科学技术委员会近十年时间的不断支持下，在国家数字交换系统工程技术研究中心、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，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：首先是能将针对目标对象执行体个体漏洞后门的、人为的、确定性的攻击行动，转变为系统层面攻击效果不确定的事件；其次是能将系统效果不确定的攻击事件变换为概率可控的可靠性问题；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信息或行为特征情况下感知不确定威胁；五是能将非传统安全威胁变换或归一化为经典的可靠性和鲁棒性问题并处理之。为此，我将这种动态异构冗余架构及其鲁棒控制功能和机制所形成的内生性安全效应，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，“改变游戏规则”的广义鲁棒控制构造及其内生性安全机制正不断彰显出生机与活力，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，运用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。

我们深信，随着拟态防御理论的不断完善和应用技术的持续创新，网络空间“易攻难守”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”的严重对立状况将能在经济全球化环境中得到极大的统一，基于目标对象软硬件代码缺陷的攻击理论及方法将面临前所未有的挑战，信息技术与产业也将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性安全机理的新一代信息系统、工业控制装置、网络基础设施、信息服务平台甚至终端设备等必将重塑网络空间安全新秩序。

邬江兴

2017 年 11 月于郑州

Preface 前 言

今天，人类社会正在以前所未有的速度迈入信息时代，数字革命推动的信息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据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，已经成为网络时代的“阿喀琉斯之踵”。

网络空间安全问题的表现形式尽管多种多样、令人惊诧，但其本质原因却是十分简单明了。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，现有的科技理论和方法尚不能有效地彻查信息系统中的漏洞后门等“暗功能”。四是，网络攻击的技术门槛低，似乎任何具备基础网络知识或对系统软硬件漏洞有所发现的人，都可以轻易地在网络空间成为“神秘黑客”。

如此之低的技术门槛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，不会处心积虑地运用“隐匿漏洞、植入后门”等控制手段，谋求直接产品利润之外掌控用户“数据资源”的不当利益。作为一种潜规则，漏洞后门等“暗功能”事实上已成为网络空间战略性资源，任何国家和政府都不会无视这种涉及

“制网权”与“制信息权”的非对称战力之建设与运用。

现有的主被动防御理论与方法均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”的防御模式。对于“已知的未知”安全风险或者“未知的未知”安全威胁，除了条件许可情况下的加密认证措施外，几乎不设防。确切地说，迄今为止，既未找到任何不依赖于攻击特征或行为信息的防御新思路，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。即使是以美国人提出的“移动目标防御（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已取得不错的功效，但在应对潜藏于系统内部的隐匿攻击方面，仍旧处于束手无策的境地。

生物免疫学知识告诉我们，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，即机体具有“除了不伤及自体外，能够通杀任何抗原”的能力，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，特异性免疫总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”的办法去竭力应对“面防御”任务。理性的预料和严酷的事实

表明，结局一定是“堵不胜堵、防不胜防、漏洞百出”，战略上始终无法摆脱处处掣肘、被动应付的地位。

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如何做到精准的“敌我识别”。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“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能否构建起一种可以不依赖任何先验知识，或“攻击特征与行为信息”的技术架构以及内生性的安全机制，既可以降低基于目标对象漏洞后门或病毒木马等未知攻击的确定性，又能将非协同或“差模”攻击效果转变为概率可控的可靠性事件，进而使目标系统具有抑制包括未知威胁在内的广义不确定扰动能力，即具有稳定鲁棒性和品质鲁棒性。

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“相对正确”公理，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。该公理的一种等价逻辑表达——异构冗余表决构造和多模表决机制，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下的可认知问题场景，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层面的相对性判识上来，进而

将多数人的认知结果作为“相对正确”的置信准则。但是，即便如此，小概率情况下多数人的认知结果也存在“相对错误”的可能。只要是相对性结果就存在量子叠加态的“薛定谔猫”效应，正确与错误同时存在，只是概率不同而已。这一等价构造和机制在可靠性领域的成功应用就是非相似余度构造。基于该构造的目标系统在一定的前提条件下，即使其物理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，都可以在给定语义和语法约束条件下，被多模输出矢量表决机制变换为可用概率表达的可靠性事件，从而使我们可以通过构造技术来显著地增强系统的可靠性。同理，该构造对于网络空间不确定威胁也具有相同或相似的作用。尽管不确定性威胁的攻击效果对于异构冗余的个体而言往往不是概率问题，但是这些基于个体的攻击效果常常取决于攻击者能否在系统层面，实现多模输出矢量时空维度上的一致性表达，是典型的概率问题。由于相对性表决机制会迫使攻击方必须面对“非配合条件下协同一致攻击难度”的挑战，因而没有坚实的科技和经济基础支撑几乎不可能克服这一挑战，于是，成为“黑客”的技术门槛就被极大地提升了。不过，一定时间内，基于 DRS 构造的目标对象虽然能够抑制包括未知攻击在内的不确定扰动，且具有可设计标定、可度量验证的品质鲁棒性。但是，因为无法克服“试错式”协同攻击的影响，非相似余度构造缺乏稳定鲁棒性。

按照网络空间安全领域的传统理论，现今信息系统技术架构和防御机制下，网络空间基于漏洞后门等的攻击，一方面因为目标对象的静态性、确定性和相似性而出现防御环境“被透明”的状况，或者因为隐藏的病毒木马等导致防御环境“被渗透”的局面；另一方面由于防御方缺乏关于攻击者的先验知识、行为特征信息，或者无从知晓内部何处存在未知的“暗功能”，而始终无法摆脱不确定威胁之梦魇。

如果从鲁棒控制的观点分析，不难得出，目前网络空间大多数的安全事件是由针对目标对象内部漏洞后门、病毒木马等不确定扰动引起的。换言之，由于人类目前尚缺乏为其软硬件系统提供抑制包括漏洞后门等“暗功能”在内的广义不确定扰动能力，所以原本属于目标对象或网络元素设计和制造过程中的质量控制问题，就万般无奈地“溢出”成为网络空间最主要的安全挑战，“潘多拉魔盒”就是这样被打开的。生产厂家或企业“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责任”的行为，都可以归结为“世界难题”所致。因此，公众只好被迫接受网络空间这一几乎与“耍赖行为”无异的商业现实。经济技术全球化时代，恢复产品质量神圣承诺和商业信誉，治理被严重毒化污染的网络空间环境，将魔鬼关回到潘多拉盒中，需要优先解决软硬件产品的广义鲁棒控制问题。

破解当前网络空间安全困境的第一要务是构建“双向防御迷雾”。不仅能使基于目标对象漏洞后门的“单向透明”攻击失去确定性效果，而且要能有效瓦解基于目标对象内部病毒木马的“里应外合”式攻击。一般而言，在不考虑目标对象性价比的条件下，增加运行环境的动态性或随机性可以在不同程度上达成前一个愿望，但无法实现后一个目的。因此需要借助“结构决定安全”公理的启迪，通过目标对象控制架构的创新来获得与生物拟态伪装机制相同或相近的构造效应，则有可能体系化地实现这一双重性质的要务。

其次，仅仅使攻击效果不确定或者只能在不同程度上瓦解攻击行动不是防御者的终极诉求。理想目标是，无论对已知风险还是未知威胁导致的确定或不确定性攻击效果，都能被某种构造或机制变换为概率可控的可靠性问题，以便借助成熟的可靠性理论和方法统一解决。

再者，必须开发出一种具有广义鲁棒性功效的控制构造，不仅能有效抑制目标对象内部传统的不确定扰动影响，也能在基于漏洞后门等人为攻击扰动下维持系统服务功能和性能的鲁棒性，从而能

在很大程度上抵消网络元素广义鲁棒控制功能缺位对网络空间安全态势造成的负面影响。

显然，若能在非相似余度的可靠性技术架构中导入拟态伪装和“测不准”机制，并创造出一种能够通过构造效应抑制“差模故障和差模攻击、共模故障和协同攻击”的新型系统架构，则达成“服务提供、可信防御、鲁棒控制”一体化实现的目标是可能的。“网络空间拟态防御”就是沿着这一思路不断深化研究的成果。

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。”

为了便于读者理解拟态防御原理和体现导论题材表述的循序渐进特点，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发起的，通过感悟与思考方式提出了转变防御理念，突破了思维惯性。第 2 章“网络攻击形式化描述”由李光松、曾俊杰、吴承荣负责编撰，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、定制可信空间以及移动目标防御等新型安全防御技术思路，并指出了存在的主要问题。比较详尽地分析了多样性、随机性和动态性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、王伟、杨本朝、李光松等共同参与撰写，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。概略地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“基于异构冗余的动态防御”由刘彩霞、斯雪明、王伟等共同参与撰写，提出了一种称之为“动态异构冗余”的系统架构，其内生的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蓄意行为，必须面对“动态冗余空间，非配合条件下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策略的设想，期望造成攻击者对目标对象防御环境（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，获得“即使攻击成功，也可能只是一次”的不确定效应。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“典型架构抗攻击性与可靠性分析”由贺磊、任权等负责撰写，提出了非冗余、非相似余度、拟态构造

的广义随机 Petri 网模型，并给出了相应的抗攻击性与可靠性的量化分析结论。

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体制机制缺陷；从可靠性领域基于“相对正确”公理等价逻辑表达出发，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之启示；提出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，并指出该构造在机理上具有生物拟态伪装相同或相似的效应和内在的“测不准”机理；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，具有内生的安全特性和防御效应，可独立应对基于目标系统漏洞后门等“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；给出了几个带有原理验证性的应用实例；介绍了原理验证系统的测试评估情况与验证结果；最后，为非冗余、非相似余度和动态异构冗余构造建立了基于 GSPN 的数学模型，并给出了相应的抗攻击性与可靠性的定量分析结论。

诚然，拟态防御理论在传统工程意义上看来，必然会增加设计成本、体积功耗、维护使用等方面的开销，在价格敏感应用领域也许会带来不小的挑战。但是，当今时代微电子技术、软件技术、可重构技术以及虚拟化技术等手段和工具的持续进步，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工程师们的“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(包括网络空间安全防护等在内)的综合投资和使用效益方

面。因而作者相信，随着拟态防御原理和技术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，新一代基于内生防御机理的广义鲁棒控制系统或软硬件装置呼之欲出，拟态防御理论引导下的技术创新之花必将在相关应用领域蓬勃绽放。

目前，拟态防御理论和相关方法仅仅达成了理论自洽与原理验证，难免存在研究不够深入细致、分析不够全面准确、试验验证不够完备、方法不够严密精湛等初创阶段无法回避的问题，书中在理论和实践层面也给出了一些亟待研究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，尤其像拟态防御和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”之功效，达成“众人拾柴火焰高”之目的。衷心欢迎广大读者通过本书提供的微信公众号（拟态防御）和拟态防御网站（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，普适性的广义鲁棒控制架构能够为 IT 产业以及相关领域带来强劲的创新活力与旺盛的产品换代需求。

需要特别声明的是，拟态防御从纯技术角度视之，只是广义鲁棒控制构造和相关机制产生的内生性安全效应，不可能也不奢望能解决网络空间所有的安全问题。反之，拟态构造的发现或发明倒是确实解决了传统鲁棒控制不能抑制包括未知威胁在内的广义不确定扰动难题。

本书适合作为网络空间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技术应用或有志向完善拟态防御理论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编排逻辑，便于专业人士选择性阅读之需要，特附“各章关系视图”以供参考。

各章关系视图