网络空间内生安全

——拟态防御与广义鲁棒控制

（上册）

邬江兴　著

科学出版社

网络空间内生安全

——拟态防御与广义鲁棒控制

（上册）

邬江兴　著

科学出版社

北京

内 容 简 介

本书从“结构决定功能”的内源性安全机理诠释了改变游戏规则的“网络空间拟态防御”思想与技术形成过程、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。通过包括原理验证在内的应用实例和权威测试评估报告等相关材料，从理论与实践的结合上，证明了由创新的动态异构冗余构造形成的内生安全机制。作为一种不可或缺的使能技术，可赋予IT、ICT、CPS等相关领域新一代软硬件产品高可信、高可靠、高可用三位一体的内生安全机制与融合式防御功能。

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

图书在版编目（CIP）数据

网络空间内生安全：拟态防御与广义鲁棒控制. 上册 / 邬江兴著. —北京：科学出版社，2020.6

ISBN 978-7-03-065218-8

Ⅰ. ①网… Ⅱ. ①邬… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2020)第088433号

责任编辑：任 静 / 责任校对：王萌萌

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

*

2020年6月第 一 版 开本：720×1 000 1/16

2020年6月第一次印刷 印张：22 1/4

字数：446 000

定价：168.00元

（如有印装质量问题，我社负责调换）

此为试读，需要完整PDF请访问：www.ertongbook.com

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。本世纪初先后发明了“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机制的 IPTV”等网络通信技术，主持开发世界首套基于全 IP 的复合移动通信系统 CMT、中国首台高速核心路由器、世界首个支持 IPTV 业务的大规模汇聚接入路由器——ACR 等信息通信网络核心装备。2008 年提出面向领域高效计算的“基于主动认知的多维可重构软硬件协同计算架构——拟态计算”，2013 年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”。2013 年，提出了网络空间内生安全思想，创立了基于广义鲁棒控制和内生安全机制的网络空间拟态防御理论，2017 年起，先后出版了《网络空间拟态防御导论》《网络空间拟态防御原理》中文专著和《网络空间拟态防御——广义鲁棒控制与内生安全》英文版专著。先后获得过国家科技进步一等奖 3 项，国家科技进步二等奖 4 项。曾获得 1995 年度和 2015 年度何梁何利科学与技术进步奖、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。

出 版 说 明

近些年来，基于内生安全(Endogenous Safety and Security，ESS)和广义鲁棒控制(Generalized Robust Control，GRC)理论的拟态防御技术，借助国家工业和信息化部(以下简称工信部)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COTS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”检验了拟态构造技术对抗注入式后门或恶意代码的防御能力。2019年5月22日，在南京举办的第二届拟态防御国际精英挑战赛，参加的团队包括2018年全球排名前15名的10支战队和国内19支顶尖团队，比赛采用了创新的“黑盒/白盒/登顶”BWM赛制，历时20多个小时，实施了296万次有效攻击和5700多次高危漏洞攻击，无一人一队得手。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“自主编制的测试例”也有着“金刚不坏之躯”的抗攻击能力。2019年6月26日，紫金山实验室(PML)开通了世界上首个面向全球、全时域、采用常年赏金制度的网络内生安全试验床(NEST)，既能为全球黑客提供彰显 “无坚不克”众测功夫的专业场合，又能为全球信息产品生产厂家展现其 “固若金汤”的舞台。两年多来的试点应用，积累了大量“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的内生安全机制，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之独特功效。有力佐证了建立在系统工程理论基础之上的拟态构造，能够使信息系统在全寿命周期内达成高可靠、高可用、高可信“三位一体”的经济技术目标。2019年4月，国家工信部在郑州组织了试

点任务技术测试验收，对线上拟态构造设备进行了服务功能、性能及黑盒、白盒安全性测试，结果表明“被测设备的服务性能与安全性能完全达到了理论预期”。同年 9 月，国家工信部组织了试点任务的评估验收会，会议认为“拟态构造在技术成熟度、普适性和经济性方面都达到了可推广应用程度”“试点任务执行情况完全达到了拟态防御预期目标”。其“改变网络空间游戏规则”的革命性意义，预示着“可量化设计、可验证度量”的内生安全机制必将成为信息领域及其相关领域新一代软硬件产品标志性的使能技术之一。

从科学研究或技术发展意义上说，基于内生安全体制机制的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、可验证度量的技术发展阶段。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瓶颈问题。2018 年 5 月，在南京正式宣布成立的全国性的“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”之重任，以开放、开源、协同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环境。

本书提出的相对正确公理及其再发现以及创新的编码信道纠错理论，是内生安全体制机制感知或管控确定或不确定威胁的基本理论依据，发明的具有内源性测不准机制和广义鲁棒控制特性的动态异构冗余构造，能为目标对象提供高可靠、高可信、高可用三位一体内源性安全的服务功能，可有效瓦解或规避基于内生安全问题的蓄意攻击和扰动。此次修订出版，为了强调内生安全体制机制对拟态防御应用的根本性支撑作用，以及内生安全体制机制对广义鲁棒控制的普适性意义，故对《网络空间拟态防御导论(第二版)》的部分内容做了重要修订和补充完善，调整和增加了一些章节内容，专门撰写了“编码信道数学模型与分析”一章，并将主书名定为“网络空间内生安全”，副书名定为“拟态防御与广义鲁棒控制”，以强调内生安全与拟态防御和广义鲁棒控制间的因果关系。

邬江兴

2020 年 3 月于珠海

序　言

信息世界网络空间与现实世界物理空间一样有着相同的哲学本质，如同德国哲学大师黑格尔所说的那样“一切事物都是自在(内生)的矛盾，矛盾是一切运动和生命力的根源。”矛盾的同一性指出，同一性是事物存在和发展的前提，且互为发展条件。矛盾的斗争性则会促进矛盾双方此消彼长，造成双方力量的发展不平衡，为对立面的转化和事物质变创造条件。“有利必有弊”的矛盾有着与形式逻辑中完全不同的意义。以信息技术为例，大数据技术能够根据算法和数据样本发现未知的规律或特征，而蓄意污染数据样本、恶意触发算法缺陷也可能使人们误入歧途，结果的不可解释性是其内生安全问题；初级人工智能靠大数据、大算力、深度学习等算法获得前行动力，而结果的不可解释性与不可推论性则是其内生安全问题；区块链技术开辟了无中心记账方式的新纪元，大于等于51%的共识机制却不能避免市场占有率大于51%的COTS级软硬件产品中的漏洞后门问题，后者就是区块链1.0时代的内生安全问题；采用共享资源机制的信息通信网络技术，业务传送拥塞就是网络的内生安全问题；当代计算技术的发展使人类步入了辉煌的信息时代，但是既有计算技术本身的缺陷也使得网络空间充满风险和不确定威胁。譬如，分支预测(branch prediction)是一种解决CPU处理分支指令(if-then-else)导致流水线失败的数据处理优化方法。然而，幽灵漏洞(spectre)正是这种降低内存延迟、加快执行速度的“预测执行”的副作用或暗功能，一旦被恶意程序利用，就可能使受害进程保存的敏感数据被识别，即发生基于时间敏感侧信道的信息泄露事件等自在矛盾所特有的表现，不再一一列举。推广到一般：从网络空间的现象观察，一个确定功能总是存在着显式副作用或隐式暗功能；从网络空间的工程实践经验可知，无法获得一个没有伴生或衍生功能的纯粹功能；从一般哲学意义上讲，自然界或人工系统中不存在逻辑意义上的“当且仅当的功能”，即不存在没有矛盾的事物。如果一个软硬件实体的暗功能和副作用能被某种因素触发而影响到实体服务功能的可信性，则称这些副作用和暗功能为“内生安全”(Endogenous Safety and Security，ESS)问题。作者以为，内生安全问题应当具有若干技术特征：① 内生安全问题属于元功能或本征功能的已知或未知效应；②内生安全问题涉及的功能与元功

能是同一构造上的负面形态表达，所有工程技术上的努力只可能降低其负面功能的影响而不可能消除内生安全问题本身；③内生安全问题是内因，通常需要外因扰动才可能导致内生安全风险或安全威胁；④内生安全问题与内生安全功能同为自身构造或算法的内源性表达，后者的作用就是借助构造本身的作用或效应尽量降低前者受到外部因素扰动时的不良影响。由于人类技术发展和认知水平的阶段性特征导致软硬件设计脆弱性或漏洞问题不可能彻底避免；全球化时代，开放式产业生态环境，开源协同技术模式和“你中有我、我中有你”的产业链使得软硬件后门问题不可能完全杜绝；就一般意义而言，穷尽或彻查目标系统软硬件代码漏洞或后门问题在可以预见的将来，仍然存在难以克服的理论与技术挑战；因而对于一个拥有成千上万行软硬件代码及相关实体构件的信息系统或控制装置，只要存在一个高危漏洞或被植入一个后门(陷门)，就可能导致整个系统的服务不可信或部分乃至所有功能的失效。换言之，迄今为止，对基于内生安全问题的不确定性威胁防御几乎无计可施，信息系统或控制装置安全性不可量化设计、无法验证度量似乎已成为网络空间的“永恒之痛”。

作者将内生安全问题抽象为两类问题。一类是狭义内生安全(Narrow Endogenous Safety and Security，NESS)问题，特指一个软硬件系统除预期的设计功能之外，总存在包括副作用、脆弱性、自然失效等因素在内的显式或隐式表达的非期望功能；另一类是广义内生安全(General Endogenous Safety and Security，GESS)问题，除了狭义内生安全问题之外，还包括刻意设计让最终用户不可见功能，或不向使用者明确声明或披露的软硬件隐匿功能等人为因素，例如蓄意设计的前门、后门、陷门等“暗功能”问题。与此相对应的有，直接或间接利用基于软硬件广义内生安全问题引发的非期望事件，称为广义不确定扰动(General Uncertainty Disturbance，GUD)。显然，广义不确定扰动包含自然因素和人为因素引发的安全扰动。可能引发两类安全威胁：一是显著影响目标对象本体功能或服务功能的可靠性、可信性和可用性；二是非法获得或侵犯他人隐私信息与数据资源。作者统一将其称为不确定安全威胁(Uncertainty Security Threaten，UST)。

大量的网络安全事件表明，网络空间绝大部分安全威胁都是由人为攻击这个外因，通过目标对象自身存在的“内生安全问题”的内因相互作用而形成的。一个直观的推论就是，欲彻底解除网络空间安全威胁就必须彻底排除其内生的安全问题，因为外因毕竟只能通过内因起作用。然而，从哲学原理上说，内生安全问题是不可能“彻底消除”的，只能在时空约束前提下实施“条件规避或危害控制”。换句话说，无论理论和实践层面，任何试图无条件地彻底消除或根

除内生安全问题的努力都是徒劳的。遗憾的是，迄今为止，传统的网络安全思维模式和技术路线很少能跳出“尽力而为、问题归零”的惯性思维，挖漏洞、打补丁、查毒杀马乃至设蜜罐、布沙箱，层层叠叠的附加式防护措施，包括内置层次化的检测与外置后台处理的组织方式(借鉴生物学的内共生思想)，在引入安全功能的同时不可避免地会引入新的内生安全隐患。即使作为网络空间“底线防御”的加密认证措施，算法的数学意义也许极其强壮，但是实现算法的宿主软硬件却不能保证没有内生安全问题的存在，“面多了加水，水多了加面”的游戏总是在反复上演，始终挣脱不出逻辑悖论之魔咒。至此，网络空间安全为什么会陷入万劫不复的境地也就不难理解了。但是，怎样才能“条件规避或化解”基于内生安全问题的不确定威胁影响，这是个既需要重大理论创新又需要重大技术发明才能解决的科学技术难题。

2008 年，作者曾根据“结构决定功能、结构决定性能、结构决定效能”的公理，提出了面向领域的软硬件协同计算架构——拟态计算架构，该架构不同于经典的冯·诺依曼结构，采用的是“结构服从应用”的技术路线，基于主动认知的多维环境动态重构思想，实时感知计算任务关于时间的负载分布和能耗状况，调度合适的软硬件功能模块(算粒)，协同完成当前的计算任务以拟合期望的能效曲线。使得同一任务在不同时段、不同负载、不同资源、不同运行场景下，系统能够通过主动认知的方式选择合适能效比的模块或算粒来获得理想的全任务处理效能。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软硬件协同计算命名为拟态计算(Mimic Structure Calculation，MSC)。十年后，ISCA2018 年会上，图灵奖得主 Petterson、Hennessy 共同预言，这类领域专用软硬件协同计算架构(Domain Specific Architecture，DSA)将成为未来十年计算机体系结构发展的重要方向之一。

需要特别指出的是，这种基于能效的软硬件变结构协同计算很容易转换为基于性能的变结构协同处理，因而拟态计算架构在效能和性能目标间具有自由转换、联合优化与动态管理的功能。而传统的面向性能的计算处理架构往往是刚性的，其处理环境通常是静态的、确定的和相似的，加之缺乏安全性分析及相关设计指标体系，导致系统构建时就存在一些错误的安全性假设，既无法证明自身的安全性也无法回避众多的内生安全问题。而拟态计算环境则具有内源性的基于主动认知的多样性、动态性和随机性的协同处理特点，其任务功能与算法结构间的非确定性关系如同一团“防御迷雾”，恰好能弥补传统信息处理系统在应对基于内生安全问题攻击时的静态性、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环境内生安全问题实施的“里应外合”式的蓄意行动，有意识地运用基于威胁感知的功能等价动态变结构协同处理环境的非确定性，应当可以扰乱或瓦解以内生安全问题为基础的攻击链的稳定性与有效性，创造出以内源性的“测不准”效应规避内生安全问题的新型防御体制机制。既然内生安全问题出自结构本身，那么功能等价条件下，变化结构本身无疑能成为内生安全问题新的解决之道。拟态计算的变结构协同计算的“它山之石”就可以打磨目标环境不确定变化的“防御之玉”，这就是基于构造效应的内生安全(以下简称内生安全)机制最初的构想。读者不难发现，拟态计算和内生安全的本质都是功能等价条件下的软硬件变结构协同处理体制机制。因此，将内生安全机制视为基于主动认知的变构造计算在应用维度上的一种变换，在理论和实践意义上都是十分贴切的。

2013 年，作者正式提出并创建了基于内源性安全机制的网络空间拟态防御概念和内生安全思想，并大胆提出了一个基于“结构决定安全”的猜想：“是否存在这样一种结构或算法能将针对目标对象内生安全问题的网络威胁，归一化为可靠性和鲁棒控制理论与方法能够处理的确定或不确定扰动问题”。2016 年，由国家数字交换系统工程技术研究中心(NDSC)牵头研制的、基于内生安全机理的拟态防御原理验证系统通过了国家组织的权威性测试评估。其独特的基于内生安全机制的广义鲁棒控制架构突出表现在五个方面：一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；二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产生的“测不准”防御迷雾，可以瓦解试错或盲攻击的前提条件；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；五是能将非传统安全威胁归一化为广义鲁棒控制问题并可实现一体化的处理。为此，作者将基于动态异构冗余架构测不准效应形成的“防御迷雾”，用于化解或规避目标对象内部“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)。与此同时，相应的内生安全理论框架也初见端倪。

令人振奋的是，随着具有内生安全机制的拟态构造信息系统或控制装置不断得到广泛应用，“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机制正不断彰显出其勃勃生机与旺盛活力，有望在软硬构件即便存在不能彻底消除的内生安全问题时，也能依靠创新的内生安全机制规避或瓦解来自网络空间的不确定威胁。

此为试读，需要完整PDF请访问：www.ertongbook.com

序　言

作者深信，人类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”“自主可控与安全可信”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不可避免地会受到颠覆性的挑战，信息领域与相关行业既有的技术与产业格局也将重新洗牌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、网络通信设备等基础设施必将重塑网络空间安全新秩序。

邬江兴

2020 年 3 月于珠海

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、虚拟世界甚至心灵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，网络空间内生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，已经成为当今网络世界、现实世界乃至智能世界发展的“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，对人类生活与生产活动造成的威胁之广泛和深远更是前所未有，但对信息系统或控制装置等的不确定安全威胁的本质原因则可以归结为以下五个方面：一是，哲学原理注定无法彻底避免信息系统软硬件设计缺陷可能导致的安全漏洞问题；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内生安全问题随着数字经济或社会信息化的加速，而成为网络世界陷入万劫不复境地的主要根源之一；五是，相对补救性质的防御代价而言，网络攻击成本之低，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和践踏网络空间诚信准则的“黑客”。因此，内源性的安全问题无所不在，由此相关的网络安全威胁也无所不在。

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”等全局性制网手段，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新形态的恐怖力量，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，无论是否公开宣称军事化，网络空间早已成为常态化、白热化、无硝烟的真实战场，各利益攸关方的博弈无所不用其极。但是，目前总的态势仍然是“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零信任安全架构(Zero-Trust Architecture，ZTA)的全面身份认证措施，由于都无法彻底排除或杜绝内生安全问题，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，全球既未提出任何不依赖于攻击特征或行为信息的威胁感知新理论，也未发现技术上有效，经济上可承受，且能普适化运用的新型防御体制。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，或者以内置探针联合后台大数据智能分析为代表的“内共生”(Endosymbiosis)防御技术，或者以本质(Intrinsic)安全为代表的网络安全协议技术，在干扰或阻断基于目标对象漏洞之攻击链可靠性方面，以及靠大数据协同分析发现已知的未知威胁方面，或者用安全协议方式对抗中间人劫持、DDOS 攻击方面，确能取得不错的功效。但在应对目标系统内部固有的暗功能影响或潜藏的基于软硬件后门的不确定威胁方面，即使施以认证加密类的底限防御手段，也无法彻底避免蓄意利用宿主对象内生安全问题“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、定性描述的技术体系和“摸着石头过河”的工程实践，无论是在支持“云-网-端”新型使用或应用模式，还是在零信任安全架构 ZTA 部署等方面都已经遭遇难以逾越的技术壁垒。

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基于精确特征的“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高频度的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泛在化、内源性的“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，在二次应答中起作用，且生物个体间的特异性免疫存在质和量上的差别。至此，我们知道脊椎动物因为具有“点面”结合的双重性质的融合免疫机制，才获得了抵御已知或未知抗原入侵的非凡能力。遗憾的是，人类在网络空间从未创造出这种“具有面防御性质的非特异性免疫和点防御性质的特异性免疫融合机制”，总是以点防御的特异性力量竭力去应对千变万化的面防御任务。理性的预期和严酷的现实表明，“堵不胜堵、防不胜防、漏洞百出”是必然之结局，战略上就不可能根本摆脱被动应付的态势。

造成这种尴尬局面的核心问题是，一方面因为生物科技界至今未搞清楚非特异性免疫是如何做到既有广泛性又不关注具体特征的 “敌我识别”机制，只是猜测，可能的识别机制是吞噬细胞与被吞噬颗粒(抗原)之间的表面亲水性差异。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(截至目前没有证据表明后天免疫抗体具有遗传性状)，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，无法用“他山之石攻玉”。另一方面网络空间虽然可以基于已发现的漏洞后门或病毒木马等行为特征形成各种漏洞或关于攻击的信息库，但当前的库信息中肯定不包含未知的漏洞后门或病毒木马等特征信息，更无法囊括明天或未来什么形式的攻击特征信息，只能等待亡羊补牢。我们这样提出问题的目的不是“指责”生物科技界至今未能弄清楚“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可能存在类似的敌我识别和融合式防御机制，可以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之内源性的功能，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体制机制。运用这样的体制机制、构造功能和协同效应，可以将基于内生安全问题的攻击事件归一化为经典的可靠性扰动问题，借助鲁棒控制与可靠性理论和方法，以及编码信道纠错理论，使得信息系统或控制装置能获得管控广义不确定扰动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融合处理可靠性与可信性问题新的解决途径。

作者在多年的技术实践中深深感到，传统网络安全技术前行动力即将耗尽，

亟待创新理论提供新动能。首先是，无论从哲学原理还是软件工程上来说，不可能设计出无缺陷或无漏洞的软硬件代码(有人曾给出 10%缺陷代码量的激进估计)，因为任何事物有利必有弊，给定一个功能总会存在显式的副作用或隐式的暗功能，矛盾的双方存在对立统一关系。其次是，在目标对象上无论打多少补丁或堵多少漏洞，堵漏过程中难免会引入新的副作用或暗功能，这种“叠罗汉”式的不可持续机制，理论上就不存在使内生安全问题归零的可能性。再者，从哲学意义上说，任何附加式防御或基于层次化组织效应的“内共生”措施，或者“本质安全”类的安全协议技术都不可能从根本上消除目标对象的内生安全问题，至多起到隔离或影响攻击链可靠性或有效性的作用，但对从内部发起的主动攻击几乎完全无效，更糟糕的是，附加安全措施自身的内生安全问题还可能给目标对象带来新的不确定威胁。显而易见，规避或弱化目标对象特定场景下的内生安全问题影响，最有效的方式就是发明一种能自动识别和规避特定场景中内生安全问题的新机制，该机制不奢望“问题归零”，只期望能达到“兵来将挡、水来土掩”的目的。换言之，就是需要创造和发明一种新的理论与构造来颠覆既有的基于软硬件代码设计缺陷的攻击理论和方法。

首先要克服的理论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，这个问题乍看起来似乎有悖于认识论的基本教义。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，能够在功能等价及相关约束条件下，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差模或共模问题，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，基于同一构造和机制的原因，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，因此理论上就不可能支持“绝对正确”的说法。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(Dissimilarity

Redundancy Structure，DRS)。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故障，或者存在未知设计缺陷导致的统计意义上的不确定失效，都可以被多模表决机制变换为能用概率表达的差模或共模事件，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用性。对于利用目标对象内生安全问题的不确定威胁而言，非相似余度构造从某种意义上说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功能等价的异构冗余个体而言往往不是概率问题，但是这种攻击事件在群体层面的反映通常会以差模形态呈现(除非攻击者能协调一致的实现异构冗余部件时空维度上的共模表达)，而这恰恰又属于典型的概率问题。换言之，在给定的约束条件下，不确定的个体表现可以被相对正确公理变换为群体层面的概率问题。不过，在小尺度空间上，基于 DRS 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、相似性和确定性等安全缺陷，决定了其内生安全问题仍然具有相当程度的可利用性，“试错攻击”等手段常常会破坏 DRS 构造目标对象的稳定鲁棒性。

其次，绝大多数安全事件如果从鲁棒控制的观点视之，也可以认为是由针对目标对象内生安全问题引起的广义不确定扰动之模型摄动。换言之，哲学原理告诉我们，人类不可能具备彻底管控或抑制软硬件产品副作用或暗功能的能力，所以产品设计、制造或运维服务过程中，因为存在“无法彻底消除的内生安全问题”，要么在强约束条件下对特定应用环境的安全性作“尽力而为”的努力，要么只能“万般无奈地放任”其成为网络空间最主要的安全污染源。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“哲学原理或世界性难题”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，从源头治理被恶性污染的网络空间生态环境，除了要具备可感知基于内生安全问题的不确定扰动功能外，还需要创造出一个能够有效规避“试错攻击”的鲁棒控制构造，这个构造应当具备四个基本特性：①使试错攻击前提条件难以成立；②使攻击者很难感知试错攻击的效果；③应能尽快消除系统差模或有感共模记忆状态；④能为目标对象规避不确定安全威胁提供稳定鲁棒性和品质鲁棒性。显然，这样的构造相对攻击者而言，具有“测不准”的性质。

再者，不可能指望广义鲁棒控制构造及其内生安全机制产生的内源性安全效应能够规避来自网络空间的所有安全威胁，甚至不敢奢望能彻底规避针对目

标对象内生安全问题引发的所有安全威胁。但是，我们仍然期望创新的广义鲁棒构造和内生安全体制机制能够从原理上自然地融合(吸纳)现有或未来的网络安全技术，以增强构造内的多样性、动态性和随机性。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安全性获得指数量级的增长。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、关键技术攻关、原理系统验证到应用试点、行业示范全过程的工程实践。

基于内生安全体制机制的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。

2013 年 11 月，作者提出基于拟态计算的变结构协同计算模式的内生安全特性来构建拟态防御的设想，并得到国家科技部和上海市科学技术委员会的立项支持。翌年 5 月，“拟态防御原理验证系统”研究项目启动，同时，内生安全思想正式诞生。

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。” 彰显了内生安全机理的“神奇”作用和富有前途的实用化意义。

2017 年 12 月，《网络空间拟态防御导论》面世，内生安全理论初见端倪；2018 年 10 月，《网络空间拟态防御原理——广义鲁棒控制与内生安全》出版，内生安全理论框架基本形成；2019 年 12 月，《网络空间拟态防御——广义鲁棒控制与内生安全》英文版由德国 Springer 公司向全球发行，内生安全理论得到进一步充实完善。

2018 年 1 月，世界首台拟态构造的域名服务器在中国联合网络通信有限公司河南分公司上网运行；2018 年 4 月，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，首次在河南景安网络公司体系化部署并投入线上服务；2018 年 5 月和 2019 年 5 月，基于拟态构造的信息通信网络成套设备，作为中国南京“强网”拟态防御国际精英挑战赛“人机大战”的目标设施；2019 年 6 月，南京紫金山实验室(PML)，面向全球，全天时的开放基于内生安全功能的 COTS 级信息产品的众测服务环境——网络内生安全试验床(NEST，网址https://nest.ichunqiu.com)。

2019 年 4 月和 9 月，国家工信部在郑州分别组织了试点设备线上测试及应

此为试读，需要完整PDF请访问：www.ertongbook.com