附件 1：拟态防御技术简介

自信息革命开始以来，网络正深刻地改变着人们的生产生活方式，成为继陆海空天之后的“第五维空间”，对国家主权、安全、发展利益提出了诸多新的挑战。现阶段，网络空间安全本质就是围绕目标对象漏洞后门等“暗功能”的抑制与利用，展开的基于技术及市场甚至社会工程学方面的博弈，其本源问题可以概括为四个方面：一是软硬件设计缺陷或脆弱性导致的安全漏洞无法彻底避免；二是产品提供者有意设计或产业生态环境中无意引入的具有“暗功能”性质的软硬件代码无法彻底杜绝；三是在可以预见的将来，尚缺乏有效的科学技术手段，难以穷尽或彻查目标系统问题代码及逻辑缺陷；四是网络空间也无法给出严格的操作规范以及行为准则，包括精准、可靠的监管手段。

传统的网络防护理念及技术，既无法预知、更无法应对网络空间中未知的、不确定的安全威胁，“潘多拉魔盒”就是这样被打开了。人们面对从芯片到软件，从器件到部件，从路由器/交换机到数据中心或云服务平台，从桌面、移动终端到工业控制设备乃至工业互联网等云云总总的 IT/ICT/CPS 产品，其服务功能均难以提供安全可信保证。目前，网络空间的攻防不对称局面是，一个复杂系统或控制装置只要存在一个设计缺陷或混入一段恶意代码，就可能导致整个目标系统“遭殃”。对于攻击者来说，因为目标对象构造和运行机制的静态性、相似性及确定性，只要发现一个漏洞或预设一个后门，就可以采取“里应外合、隐匿配合”的攻击方式，形成“单向透明”的行动优势，让防御者处于“无法设防”的窘境。

拟态防御正是在这样的大背景下提出的。“拟态”概念原本出自生物学，2008 年美国国家地理频道（NGC）报道了有关条纹章鱼生物拟态现象和伪装机制的研究情况，由此触发了邬江兴院士的灵感，他把蕴含其中的生物智慧同著名科学家钱学森先生的系统工程论思想结合起来，提出了“结构决定安全”、变结构产生内生安全效应的设想，并为之展开了十年的研究探索，形成了今天的网络空间拟态防御理论体系基础及核心技术方法。

拟态防御包含基于动态异构冗余架构的内生安全机制理论、方法和技术，其通过动态异构冗余构造、基于多模策略（类似区块链技术中的共识）判决的多维动态重构负反馈等机制，策略性的改变网络信息系统的功能结构和运行环境，有效抑制和管控软硬件随机性失效产生的自然扰动，以及基于漏洞后门等的人为攻

击扰动，使目标系统具备广义鲁棒控制能力。

拟态防御具有“结构决定安全”的内在属性和归一化的处理功效，其先进性、革命性可以归纳为五个方面：首先是能将针对目标对象执行体个体未知漏洞后门的、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，使得网络空间“易攻难守”的战略格局有望发生根本性的逆转；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，实现了安全态势可量化感知的突破；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，使得攻击手法和经验难以复现或继承，无法产生可规划、可预期的攻击效果，基于软硬件内部漏洞后门的传统网络攻击方法被彻底颠覆，诸如“挖漏洞”、“设后门”、“植病毒”和“藏木马”等经典攻击套路在机理上不再有效；四是借助“相对正确”公理的逻辑表达（共识）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感知不确定威胁；五是能将传统的随机性扰动和非传统的不确定安全威胁，诸如软硬件内部的随机性“差模”失效和未知“差模”攻击，基于软硬件暗功能的外部攻击和内部渗透攻击等，变换或归一化为经典的可靠性和鲁棒性问题并案处理之。

拟态防御可为网络空间建立先进性与可信性、安全性与开放性、高可靠与高效能融为一体的广义鲁棒控制能力，很可能对当今的 IT 或 ICT 等技术和产业引发“重新洗牌”效应。网络信息系统的安全可信不再以软硬构件的“无毒无菌”为前提，因而能充分适应经济技术全球化的产业生态环境，有望为网络安全和信息化的融合式发展释放出“改变游戏规则”的基础动能，为“一体之两翼，双轮之驱动”发展战略提供“可落地实施”的抓手级技术，为新一代信息技术和产业“换道超车”提供创新活力和市场驱动力，具有引领全球 IT 技术和产业发展新潮流的潜力。2017 年 12 月，《网络空间拟态防御导论》由中国科学出版社正式出版发行，标志着拟态防御完成了从初创构想到理论与方法自洽的过渡，为相关技术研究、系统开发和测试验证建立了基本遵循。