DOI 10.15302/J-SSCAE-2023.06.018

内生安全赋能网络弹性的构想、方法与策略

邬江兴[1,2]，邹宏[1*]，薛向阳[1]，张帆[2]，尚玉婷[1]

（1. 复旦大学大数据研究院，上海 200433；2. 国家数字交换系统工程技术研究中心，郑州 450002）

摘要：网络弹性工程是美国、欧洲等发达国家和地区针对数字化转型、新发展形势下的网络安全挑战所采取的技术性措施，旨在以网络弹性标准为依托，构建数字技术准入“壁垒”，同时从应用服务侧和设备供应侧同时发力，提高自身数字设施和数字产品的安全能力。本文着眼网络弹性工程实施对我国发展新一代网络信息技术带来的影响和挑战，递次阐述了弹性、网络弹性、网络弹性工程的概念，从网络弹性工程的政策驱动、战略考量、发展困境等方面剖析了国外网络弹性工程的应用进展；基于内生安全理论提出了一种新的动态异构冗余架构，描述了内生安全赋能网络弹性的内在机理，阐释了内生安全赋能网络弹性的基本构想与应用方法。研究建议，加快技术创新，抵消发达国家网络弹性工程的组合效应；推动建立中国特色网络弹性政策法规体系；建立相应监管体系，明确网络安全责任边界；建立可量化、可验证、具有公信力的测试评价体系；采取市场化金融手段，多路径助力网络弹性实施，以期系统性增强我国网络弹性，推动网络强国建设。

关键词：网络空间；内生安全；网络弹性；结构加密；动态异构冗余架构

中图分类号：TP393　　**文献标识码：**A

Cyber Resilience Enabled by Endogenous Security and Safety: Vision, Techniques, and Strategies

Wu Jiangxing[1,2], Zou Hong[1*], Xue Xiangyang[1], Zhang Fan[2], Shang Yuting[1]

(1. Institute of Big Data, Fudan University, Shanghai 200433, China; 2. National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: Cyber resilience engineering is a technical approach embraced by countries and regions such as the United States and Europe to implement digital transformation and address network security challenges under new circumstances. It aims to keep the barriers to entry high for digital technologies based on the cyber resilience standard and to improve the digital infrastructure security capability of China from both the application service and device supply sides. This study focuses on the impact and challenges brought by the initiatives of cyber resilience engineering in the United States and Europe on the development of new-generation network information technology in China. It starts from a concept introduction of resilience, cyber resilience, and cyber resilience engineering. Subsequently, it elaborates on the application progress of cyber resilience engineering in the United States and Europe in terms of policy drivers, strategic considerations, and development dilemmas. Moreover, the study goes further to propose a dynamic heterogeneous redundancy architecture based on an endogenous security and safety (ESS) theory. It describes and illustrates the intrinsic mechanism, basic concepts, and application methods of cyber resilience empowered by ESS. Furthermore, we propose that China should accelerate innovation to offset the combined effects of cyber resilience engineering in developed countries, introduce a cyber resilience policy and law system with Chinese characteristics, establish corresponding regulatory systems to clarify the network security responsibilities, establish a quantifiable, verifiable, and credible testing and evaluation system, and boost the holistic implementation of cyber resilience with a multi-

收稿日期：2023-11-17；**修回日期：**2023-12-06

通讯作者：*邹宏，复旦大学大数据研究院副院长，研究方向为网络空间安全；E-mail: hongzou@fudan.edu.cn

资助项目：国家重点研发计划项目(2022YFB3102901)；中国工程院咨询项目“新发展理念引领的网络强国战略研究”(2022-HYZD-02)

本刊网址：www.engineering.org.cn/ch/journal/sscae

pronged approach including financial marketization, hoping to systematically enhance the cyber resilience and strength of China.
Keywords: cyberspace; endogenous security and safety; cyber resilience; structure encryption; dynamic heterogeneous redundancy architecture

一、前言

随着全球数字化、智能化转型加速，人类社会的运转更多借助于数字基础设施，平衡数字生态系统发展和网络安全风险成为各国关注的热点问题。在突破网络空间安全问题的过程中，确保网络绝对安全、“问题归零”是不现实的，研究并建设具有弹性的网络空间成为当务之急。构建弹性的网络空间，一方面可以减少安全失陷，另一方面可以缓解因安全失陷造成的危害并从中快速恢复[1]，提高网络空间的安全韧性。

近年来，以美国、欧盟、英国为代表的发达国家和地区提出并推动了网络弹性工程建设，力求构建“可信赖”的数字系统，形成应对高级持续性威胁（APT）的可靠能力。然而，这一网络弹性工程缺乏基础理论创新，多沿用在系统构建之后通过渗透测试等手段对系统进行反复修改进而实现目标能力的技术路线；缺乏一体化保障信息物理系统网络安全和功能安全的能力，在感知并抵御“未知的未知”网络攻击、保证关键业务的持续可信运行、对网络安全性能进行可量化设计与可验证度量等方面存在短板，致使在实际应用中难以充分发挥预期作用。

本文针对数字生态系统底层驱动范式转型的新态势，分析国际现有网络弹性工程的应用进展，提出以“结构决定安全”的内生安全理论赋能网络弹性的总体构想，分析其工作机理，给出相应的技术路线、技术体系和技术运用方法，以期弥补现有网络弹性工程的缺陷，为赋能具备网络弹性的新一代关键基础设施提供支持。

二、网络弹性、网络弹性工程的概念

（一）弹性

弹性（Resilience/Resiliency，也可译为“韧性”）是力学、生态学中的一个专业术语。弹性的定义为系统在持续遭受内外部扰动影响时仍能以接近平衡的状态进行运转的能力[2]。生态弹性描述的是生态系统在受到外部干扰时表现出的持久性和复原力[3]，关乎系统如何吸纳变动和干预以维持群体 / 状态变量间的稳定关系。因此，生态弹性指生态系统能够保持其活跃的稳定状态，而非指保持其种群的静态稳定[4,5]。弹性概念引导人们转向系统性思维，着重理解问题的本质和根源，是一种促进可持续发展的重要工具[6]。近年来，随着网络威胁愈演愈烈，在系统工程、信息技术和计算机网络领域也逐渐引入了弹性概念[7,8]。

（二）网络弹性与网络弹性工程

2010 年，美国 MITRE 研究所发表了网络弹性领域的相关研究[1]，认为在网络安全领域实现 100% 保护的想法不仅不现实，而且会导致一种错误的安全感；应更注意保护任务关键功能的连续性，考虑在防护失效的情况下，通过采取补偿措施以确保在遭受攻击的情况下仍能够达成任务。针对于此，网络弹性架构设想包括保护 / 威慑、检测 / 监测、遏制 / 隔离、维护 / 恢复、自适应进化 5 个目标，实现网络弹性目标的关键技术涵盖多样性、冗余、完整性、隔离 / 分段 / 遏制、检测 / 监测、最小特权、非持久化、分布式与移动目标防御、自适应管理与响应、随机化与不可预测性、欺骗等方面。自此，网络弹性作为一种新的安全理念开始受到政府和业界的高度重视[9]。

2011 年 9 月，美国 MITRE 研究所发布了网络弹性工程框架，从系统工程视角将弹性工程、网络安全和任务保证工程的交叉点界定为网络弹性工程（见图 1）[10]。2011 年 10 月，美国卡内基梅隆大学计算机应急响应小组（CERT）发布了一套信息安全领域的弹性管理模型（CERT-RMM）[11]。2021 年，美国国家标准与技术研究院（NIST）正式发布《开发网络弹性系统——一种系统安全工程方法》（NIST SP 800-160V2R1），成为网络弹性领域首个重要技术文件[12]。NIST 将网络弹性定义为：拥有网络资源的实体所具备的对各种不利条件、压力、攻击或损害的预防、抵御、恢复和适应能力。网络弹性具有 5 个主要特征：聚焦任务或业务功能、聚焦

APT攻击的影响、假设环境不断变化、假设对手必将攻破系统、假设对手长期存在于系统或组织中。网络弹性可以同时针对来自网络和非网络的对抗与非对抗威胁。网络弹性与网络安全的关系如图2所示。网络弹性是网络安全向纵深发展的重要一步，可以化被动为主动，侧重事前设计和强固网络系统的承受力、吸收力和恢复力，有助于更好地应对“未知的未知”威胁[13]。

三、国际网络弹性工程的应用进展

（一）网络弹性工程的政策驱动

1. 美国

美国在《国土安全战略》（2007年）中将网络弹性作为支撑国土安全综合方案的三大关键概念之一，在2010年发布的《国家安全战略》和2011年公布的第8号总统政策指令中呼吁提高美国的网络弹性，在2018年发布的《国家网络战略》中提出了提升国家信息和信息系统的安全与弹性的目标。自此，网络弹性在美国由单一领域内的网络安全能力构建上升至国家网络安全战略层面。2019年，美国国土安全部和国务院联合发布《关键基础设施安全和弹性指南》，总结了提高关键基础设施安全和弹性的方法。2022年，美国制定《国家安全战略》《国防安全战略》，强调为关键基础设施制定标准以快速提高网络弹性，并建立快速应对攻击的集体能力。沿续弹性设计的技术思路，2023年美国提出了“设计安全”“默认安全”的概念，强调将安全措施“内置”为体系结构和设计的基本部分；相应地，网络安全责任从应用服务侧向制造侧转移。此战略风向还见于美国发布的《2023国家网络安全战略》，围绕建立可防御、有弹性的数字生态系统提出了具体的策略与措施以推进“制造侧安全”。

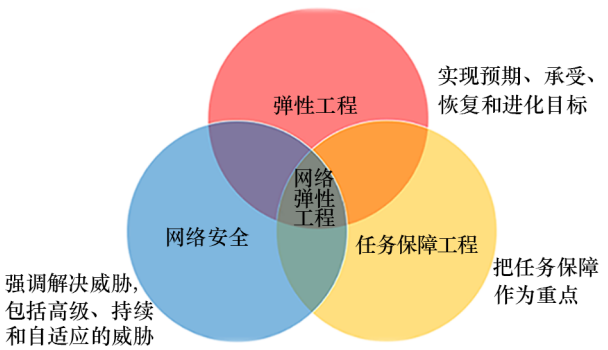

图1　网络弹性工程框架

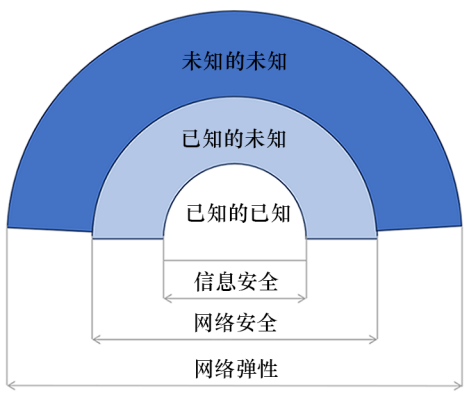

图2　网络弹性与网络安全的关系

2. 欧盟

欧盟自2008年起，发布了多份增强网络弹性的政策文件，着力推动网络弹性由概念走向落地应用，如《改善公共电子通信网络的弹性》（2008年）、《通信网络弹性规范化存在的差距》（2009年）、《启用和管理网络端对端弹性》（2011年）、《网络与服务弹性的测量标准和架构》（2011年）、《向着网络安全迈进》（2012年）等。此外，欧盟还注重网络弹性立法工作，提出了《数字运营弹性法案》《网络弹性法案》（CRA），要求欧盟境内销售的可联网数字化设备和软件在全生命周期内都必须满足强制性安全标准和透明度要求，对网络攻击具有弹性。欧盟已于2023年11月30日就CRA技术层面议题达成一致，将提交欧洲议会和欧盟理事会审议。

3. 英国

英国将网络弹性列为国家网络战略的重要支柱之一，于2022年发布了《国家网络战略2022》《国防网络弹性战略》和《2022—2030政府网络安全战略——建立一个具有网络弹性的公共部门》等政策文件。其中，《国防网络弹性战略》明确提出了建立国防弹性网络体系的愿景和具体任务及目标，同时呼吁尽快推进网络弹性立法。

（二）网络弹性工程的战略考量

一是强化制造供应侧安全。2023年，美国、澳大利亚、加拿大、英国、德国、荷兰等国家联合发布了《向平衡网络安全风险转变：基于设计与默认安全的方法和原则》，强调将安全作为包含数字元素产品的核心能力，贯穿产品设计过程，而非仅仅

作为产品的一项技术特性，要求实现产品开箱即可抵御普遍存在的攻击[14]。同年，美国发布《2023 国家网络安全战略》，提出通过立法，将安全责任转移到产品提供者，倒逼软硬件制造商承担网络安全责任。这表明美国、欧洲等发达国家和地区已认识到即使最先进的网络安全技术也不能做到防止所有漏洞，需要在软硬件实体上采取合理的预防措施来保护其应用和服务安全，促使软硬件供应商履行对消费者、企业、关键基础设施的安全责任和义务，从而推动市场提供更安全的产品和服务。

二是采取“小院高墙”的方式保护本土产业。近年来，世界主要经济体在在科技和数字领域的战略竞争持续深入。美国作为全球数字经济的领导者，为保持强国地位，持续升级在高新技术领域、特别是数字产业的竞争策略，加强自身技术保护，通过持续的改革和投入以保持竞争优势。欧盟在数字经济和互联网领域的发展虽然较为一般，但在以德国、法国为代表的传统技术强国的努力下，积极通过立法保护“数字安全”，并征收“数字税”，在保护本土企业的同时推动境内企业在技术、管理、运维等方面进行整合，形成新的技术优势，实现产业升级。

三是提高网络和数字安全准入门槛以保证自身安全。近年来，美国、欧洲等发达国家和地区的关键基础设施供应商遭受网络攻击的频次增加。欧盟虽出台多部涉及数字化产品的法律，但遭受网络攻击的现象仍愈演愈烈，约有 60% 以上的设备处于监管盲区，只有 50% 的相关公司对网络攻击采取了保护措施。为确保整体安全、防范“黑天鹅事件”，采用更有效力的网络风险评估和管理策略尤为重要，而其核心即是网络弹性。为此，欧盟重视从立法层面进行干预，提供可操作、可评估的标准加以指导。

四是增强在网络空间、数字空间的话语权。在全球数字化转型的趋势下，一个国家和地区如果能率先提出数据要素流通或数字安全保障方面的有效方案，就有可能影响其他国家，引领全球风向。美国、欧盟等发达国家和地区希望依靠先行优势，在筑牢数字经济安全基石方面占据主导优势，抢占话语权。欧盟在 2018 年发布《一般数据保护条例》，提高了在全球数据治理中的影响力，获得了远超数字经济体量的话语权。自此，欧盟通过网络弹性立法等工作，希望抢占未来国际规则制定先机，将“欧盟模式”推向世界。

（三）网络弹性工程的发展困境

一是难以应对网络空间“未知的未知”安全威胁。现有网络弹性工程框架主要基于先验知识对关键任务及其业务流程的顺利执行进行保障，其思路是通过对业务功能和性能异常的感知，触发保护及恢复机制[15]。但是，对于未知网络攻击，因缺少先验知识可能无法感知相关异常，致使难以保障关键业务系统承载平台的安全性和关键业务系统的可信性，更无法达成“使命确保”的核心目标[16]。虽然现有的网络弹性工程框架设定了“假设资源会失陷”的原则，给出了面对未知威胁应采取的策略，指出了存在无法检测未知威胁的可能性[17]，但目前给出的解决思路仅限于被动的失陷影响分析，未能给出主动的应对方法。

二是网络弹性工程框架缺乏顶层设计。自网络弹性概念及其工程框架提出以来，实现网络弹性始终是研究重点。网络弹性工程框架应能抵御攻击，受到攻击时继续提供基本服务，被攻击后能快速恢复功能。迄今为止，满足上述要求的网络弹性工程框架尚未形成。网络弹性工程的框架设计是需要解决的五大硬核问题之一[18]，但研究进展有限[19]。网络弹性度越强，网络可生存能力就越强[20,21]，但是由于没有统领性的网络弹性工程框架，目前无法实施有效统一的抵抗网络安全威胁策略。

三是网络弹性评估缺乏科学度量方法[22]。美国、欧洲等国家和地区虽高度重视网络弹性评估，但始终未能解决“数字化产品”安全性能验证度量这一世界性难题，无法给出安全性能量化验证的技术指标[23]。美国国防部提出了网络弹性存在三大挑战：系统具备良好网络弹性的判定标准，不同系统之间网络弹性的比较，系统网络弹性核心能力的评估。这些挑战性问题悬而未决致使网络弹性工程及网络弹性法案难以落地。究其原因主要是：存在评估复杂性与重大核心能力指标选取关系问题[24]；评估度量结果的可比性存在较大挑战，度量值对度量评估环境很敏感；难以评估系统的可塑性和涌现性，由于网络安全 / 信息安全、功能安全和弹性是系统的涌现特性，难以从该系统的各构成模块的行为特性中推导出来。

四、内生安全赋能网络弹性的机理分析

针对网络弹性工程发展面临的挑战，本文基于内生安全理论提出了一种新的动态异构冗余架构（DHR），可以有效抑制“未知的未知”网络威胁，同时给出了体系化的工程框架，可为解决安全性可量化设计与可验证度量难题提供技术路径。内生安全理论的内涵是以“结构决定安全”的系统工程论为指导，以“构造加密双盲理论”为基础，以安全性可量化设计、可验证度量为实践规范，允许在“有毒带菌”的环境下确保数字技术装备或系统的网络弹性。

（一）内生安全问题是网络空间安全的本源

从网络空间的现象观察可知，一个确定功能的网络系统总是存在着显式“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。从一般哲学意义上看，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[25]。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其预设功能，则称其为该系统的内生安全问题[26]。

内生安全问题具有4个基本特征。① 内生安全问题属于元功能或本征功能的已知 / 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负面功能的影响而不可能将其完全消除；③ 内生安全问题是内因，通常需要外因触发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，后者是借助构造本身的作用或效应以尽量降低前者受到外部因素扰动时的不良影响。

（二）内生安全问题不能消除只能转化

内生安全问题只可能演进、转化或和解，而不可能彻底消除[26]。人类技术发展和认知水平的阶段性特点决定了软硬件设计必然存在脆弱性或漏洞问题；全球化时代、开放式产业生态系统、开源协同技术模式和交织的的产业链分工，决定了软硬件后门问题不可能杜绝。因此，任何有违矛盾同一性和斗争性的安全技术发展路线以及试图穷尽漏洞后门等问题的工程技术方法或措施，在哲学层面势必会陷入逻辑悖论[27]。

传统的网络安全技术范式建立在“尽力而为、问题归零”的惯性思维之上，布设多层附加式的防护措施，如内置层次化的检测与外置后台处理的体系构造，但在构建安全功能的同时不可避免地会引入新的内生安全隐患[28]。即使网络空间的加密认证措施、加密算法很完备，也不能保证实现算法的软硬件中没有内生安全问题。因此，为有条件规避或控制基于内生安全问题的不确定威胁影响，亟需重大理论创新、重大技术发明予以解决。

（三）内生安全开辟网络空间防御新范式

大量网络安全事件表明，网络空间安全威胁多是因人为攻击目标对象自身存在的内生安全问题形成的。网络空间因为广泛存在内生的且共性的安全问题，攻击者只要能找到合适的攻击面及可利用的软硬件资源，就可以建立起有效的攻击链，进而构成安全威胁或破坏。当网络攻击不可达或漏洞后门无法注入攻击代码时，内生安全共性问题通常不会自动成为网络安全事件[27]。显然，若要彻底解除网络空间安全威胁或破坏，必须设法阻断内部和外部之间的连接关系。

DHR架构是一种具有内生安全属性的系统架构，在非相似余度构造[28,29]上导入基于策略裁决的动态反馈控制和运行环境结构加密等新机制[30,31]，具有拟态伪装迷雾、熵不减与不确定效应[27]、广义功能安全问题降维求解、涌现性安全增益和结构编码 / 环境加密等特点。基于内生安全共性问题的广义不确定摄动或扰动能被DHR构造的内生安全机制变换为构造内的差模或共模扰动问题，理论上所有差模扰动都能被动态屏蔽（或纠错），这使得攻击者无法识别目标、攻击效果难以评估、攻击经验无法继承、攻击场景难以复现[26]。2018年以来，连续举办了5届“拟态防御国际精英挑战赛”，邀请全球12个国家数百支顶尖白帽黑客战队，对具有内生安全功能的成套网络设备和工业控制系统进行了千万次量级的“白盒注入”式众测攻击。实践证明，内生安全理论与方法能够一体化地提升数字产品的功能安全和网络安全水平，可以从根本上扭转当前网络空间“易攻难守”的战略颓势，可为未来网络空间提供可信可靠的新一代关键基础设施“安全底座”。

（四）内生安全“双盲效应”能够解决网络弹性应对未知攻击的难题

DHR 架构提供了一种用密码学基本原理诠释内生安全机理的新视角。在解决网络安全问题时，可以借鉴完美保密理念[32]，探索一种内生的“完美安全”系统，即使在系统缺陷对于攻击者单向透明，而防御者在没有任何有关攻击者能力、攻击方式、缺陷样式和攻击效果等先验或后验知识的前提下，使攻击者在攻击时面临的认知困境最大化（即随机性最大化）、获得的缺陷样式信息最小化，从而最大程度地确保本征功能的实现。DHR 架构可以实现以下四方面目标：① 将形式多样、种类繁多、不断发展的功能安全、网络安全以及信息安全三重交织的问题影响映射成动态异构冗余空间内以差模或共模方式表达的安全事件；② 将工程实现复杂度高的全局静态异构冗余转变为具有技术经济性优势的局部动态异构冗余；③ 将无法区别差模与有感共模的大数表决机制替换为基于策略性、多参量的迭代裁决；④ 将“问题归零”“打补丁”的处理机制转变为屏蔽或纠错输出状态，采用问题场景时空迁移和安全矛盾性质变换等问题规避策略。作为一种对本征功能无需“解密”处理、对非期望功能进行结构编码（或加密）的“双盲”处理模式（防御者在不依赖先验知识的条件下，通过对构造内的广义功能安全问题进行“构造加密”，实现对攻击的“盲屏蔽”；攻击者虽然已知系统内部缺陷集合和载体等条件，却无法从攻击输入、输出中获得有用信息，难以找出“盲试错”、穷举攻击之外更好的攻击方式[33]）。DHR 架构有望达成网络弹性工程所期望的目标和愿景。

五、内生安全赋能网络弹性的构想与方法

（一）内生安全赋能网络弹性的构想

内生安全赋能的网络弹性除了可实现 NIST 提出的网络弹性工程目标外，还能实现预防、抵御、恢复和适应等目标，有效抑制事前、事中、事后阶段中的“已知的未知”“未知的未知”的网络威胁或攻击；通过功能安全确保向网络安全、功能安全（乃至信息安全）一体化防护领域迁移，从关注自然因素影响的传统弹性工程向包括人为攻击在内的网络弹性工程拓展，在全生命周期内对抗 APT。

1. 既定目标：赋能网络弹性

内生安全可以增强网络弹性在预防、抵御、恢复、适应 4 个既定目标维度上的能力。在预防方面，可实现对于未知威胁的感知发现；在抵御方面，可提供对网络攻击及随机故障的一体化抵御能力，特别是在抵御人为攻击方面，可有效应对基于 0-day/n-day 漏洞、预置后门（陷门）的网络攻击，发现并拒止 APT 类的持续不断试错攻击；在恢复方面，可利用异构资源池提供的组件资源，快速进行故障组件的替换和系统重构，迅速恢复服务能力；在适应方面，通过智能的策略裁决与执行体调度，实现类似生物体对环境变化的自适应能力，进一步学习后可以形成新的策略。

2. 基本特性

（1）具有 1+1＞2 的网络攻击感知灵敏度

传统网络安全的多样性、冗余性仅能提供资源备份、替补修复的能力[34,35]，而内生安全能够通过功能等价异构冗余配置的策略裁决提供对“未知的未知”网络攻击的感知能力。同时，内生安全技术中的策略裁决也兼具对任务 / 业务功能性能指标的感知能力，将传统网络弹性的任务 / 业务运行状态感知和基于内生安全机理的未知攻击感知无缝衔接，以达成对“见所未见”的感知能力。

（2）具备网络攻击面的微缩效应

内生安全技术打破了传统多样性、冗余性技术会增加网络攻击面的“常规认知”，通过固有的结构加密特征和“双盲效应”显著缩小了攻击面，加之固有的迷惑性、欺骗性等对抗性网络弹性机制，可以将自然因素的威胁管控和人为攻击的网络弹性等技术融合在一起，接纳和发挥传统“无法自证清白”的“网络安全保镖”技术带来的异构性网络弹性增益，实现系统广义功能安全性的可量化设计和可验证度量。

（3）实现“系统大于部分之和”的网络安全效应和网络弹性

内生安全技术架构基于开放的体系接口，具有模块化、松耦合和高效内聚的系统结构，支持全球商用现成品或技术（COTS）供应链级部件和产品使用，不苛求软硬构件本身存在的内生安全共性问题，具备“系统大于部件之和”的网络安全与弹性，使先进性与可信性、开放性与安全性的矛盾能在 DHR 架构基础上得到良好平衡。

（二）内生安全赋能网络弹性的方法

目前，国际上公认的网络弹性工程方法存在回避未知威胁问题、没有形成聚合多种技术的技术框架、缺乏安全性度量能力等技术瓶颈[36]，而内生安全可以解决这三大难题。内生安全赋能网络弹性的方法具体如下。

1. 围绕重要目标构建受信任执行环境

美国《国家网络空间战略》（2023年）提出，致力于创建一个基于信任的“网络中的网络”，推动网络防御者采取集体同步行动，保护关键基础设施。构建“网络中的网络”可视作要地防御的重要方法，其内涵是针对信息系统内发挥重要功能、攻击成本较低、容易受攻击的代码/模块/组件等关键部位，投入较为完善的防护设计、较多的防护成本进行重点保护，而针对信息系统内其他部分投入相对较少，以此达到整体安全且成本可控效果的防御方式。通过要地防御，可有效降低网络弹性工程构建的成本，以最小代价实现网络弹性的增益最大化。内生安全机理在具体的系统应用实现时需遵循“隘口设防、要地防御”的原则，即在系统设计时明确需要优先保护的资源/功能，并将其视为防御要地，有目标地创建受信任执行环境（TEE），对任何潜在的破坏都要关注对抗性。TEE所包含的资源和功能模块需要尽可能纳入到拟态防御界内。也就是说，不可信的或供应链安全性无法保证而功能等价的异构部件（也可能是“黑盒”部件），只要按照DHR架构组装，也可以构成自主可控、安全可信的TEE平台。

2. 建构多样化的软硬件体系架构

理论上，如果两个执行体之间的差异性足够大，则可以保证任意一种独立的攻击方法对于两个异构执行体是极难同时生效的。因此，系统架构中的执行体多样性越强、差异性越大，整体异构性和冗余性越强，调节自身组成方式应对外界扰动或破坏的能力就越强，调节自身组成方式保持正常工作效能的能力就越强[37]，对于已知/未知安全威胁的防御就越全面、越高效，对网络弹性的赋能效果就越突出。DHR架构可应用于系统的各个层次，覆盖基础硬件到顶层应用，采用系统控制方法和体系化构造原则指导拟态防御实现机制，可获得高性价比的可靠性和抗攻击性。① 在基础硬件层面，可采用不同中央处理器指令集的COTS级处理器产品，包括但不限于X86、进阶精简指令集机器（ARM）系列处理器和国产自主处理器等。② 在操作系统层面，可采用不同体系结构的操作系统产品，包括但不限于国际主流的Windows系列、各个Linux的发行版本、国产自主的操作系统产品及其相关支撑环境的软/硬件产品等。③ 在虚拟化层面，针对各类网络设备和应用系统运行所依赖的虚拟化环境，可采用不同的虚拟化技术实现，包括但不限于键盘、视频或鼠标直连（KVM），应用容器引擎（Docker），开放源代码虚拟机监视器（Xen），威睿虚拟化软件（VMware）等。

3. 协同运用多种安全技术

综合运用多种安全策略和技术应对未来的网络攻击，是提高网络弹性的重要方法[38]。DHR架构赋能数字产品创造了“供给侧”新需求，同质异构产品市场不再是排他性的“零和博弈”，多样化的附加式安全产品能够为DHR架构系统带来指数量级的安全增益；DHR架构的赋能作用反馈市场并带来更为强劲的开放性（阻止泛化网络安全壁垒的趋势）、互补性和多元化动力，为同类非同源产品提供了广阔的市场生存空间[28]。不同层次的安全技术均可以在DHR框架下进行协同处理，通过安全技术的多样性、动态性和冗余性实现DHR架构系统在广义不确定性扰动下的弹性赋能，从而获得稳定的网络弹性。以蜜罐技术为例，即使同属蜜罐系列的产品，由于采用的技术方案不同也会导致攻击链实现上的差异。如果在DHR运行环境内差异化地部署多个非同源的蜜罐产品，即使攻击者具备成功识别并绕过某种蜜罐产品的能力，但因为无法获得非配合条件下的协同攻击能力，DHR架构依然能通过差模感知机制有效抑制攻击。

4. 增强网络弹性的可量化特性

通过评估差距推动实体网络整体安全态势增强，是网络弹性的重要目标[39]。但是，信息系统或数字产品除了可靠性，其网络安全性尚无法给出可量化的设计指标与可验证度量的测评方法。换言之，正因为数字产品“网络安全性无法量化”仍然是世界性难题，所以软硬件产品制造侧通常选择性地忽视网络安全质量[33]。内生安全理论和方法可以将“未知的未知”安全问题转变为“已知的未知”安全问题，将无法量化控制的问题转换为基于可控概率的问题，将内生安全共性问题转变为经典可靠性理论

与自动控制技术可以管控的事务，为网络空间防御提供了改变游戏规则的革命性技术[26]。DHR 架构独有的内生安全特性和结构加密效应决定了“已知的未知”/“未知的未知”攻击、随机性摄动 / 不确定扰动、非人为影响 / 蓄意行为所致的安全问题，只要在其架构内表现为可感知的差模性质扰动，就可以得到有效抑制，并通过广义功能安全性开展可量化设计、可验证度量。基于仿真实验，用稳态可用概率、可靠度、首次故障前平均时间和降级概率刻画目标架构的可靠性，展示了DHR架构的稳定鲁棒性和品质鲁棒性（见表1）。DHR构造理论能够破解数字系统或控制装置的内生安全共性问题，使从制造侧管控基于数字技术的相关领域产品安全缺陷成为可能；漏洞后门将失去战略性作用，隐匿漏洞、设置后门不再具有潜在攻击意义[33]，从而使任何通过漏洞 / 后门技术获得战略优势的努力成为徒劳之举。

六、推进中国特色网络弹性工程的若干建议

内生安全理论和方法开辟了网络空间安全新的技术范式，创立了广义功能安全问题防御新视角，提出了基于动态异构冗余架构的赋能方法，建构出可量化设计、可验证度量的内生安全工程实践规范，为发展具有构造性增益的网络弹性工程、筑牢国家网络空间安全屏障开拓了新的技术路线。

（一）加快技术创新，抵消发达国家网络弹性工程的组合效应

发达国家在推进网络弹性工程方面使用了“组合拳”方式，在制定500多项弹性具体标准的同时，全面加强对漏洞等战略资源的管控。美国于2022年5月发布了针对网络安全领域新的出口管制规定《信息安全控制：网络安全物项》，强化了对漏洞披露的管制和漏洞检测分析技术的限制。欧盟也推出了《协同漏洞披露策略》，倾向借鉴美国的做法。这些政策文件的出台，其根本目的是切断与我国在漏洞资源方面的分享渠道，使我国高技术企业无法获得与国际同步的漏洞检测能力、将我国数字产品排除在网络弹性工程之外，试图把我国变成全球网络的“洼地”。技术问题的解决需要用创新技术来应对，要坚持“以技术对技术”的基本方略。为此，应积极推动网络空间内生安全技术的应用，用内生安全赋能网络弹性，使我国数字产品、信息产业的网络安全能力不再强依赖于漏洞 / 后门、先验知识，以开辟一条自主创新、自立自强的新路径，突破发达国家构建的网络安全领域技术壁垒。

（二）推动建立中国特色网络弹性政策法规体系

近年来，为维护网络设施和网络服务安全，我国出台了多项网络安全相关法规，如《中华人民共和国网络安全法》规范了网络的使用和运维，《中华人民共和国数据安全法》规范了公民的数据处理活动，《中华人民共和国个人信息保护法》对个人使用网络的隐私保护提出了明确要求。但是，我国仍然缺少对数字产品的全流程规范性法律约束，尤其是缺乏对数字产品软 / 硬件制造商、供应商的网络安全责任约束。建议借鉴美国、欧洲等国家和地区在推动网络弹性方面的立法经验，建立具有中国特色的网络弹性法规体系，坚持应用服务侧和制造供应侧网络安全同等重要，明确数字技术产品功能安全和网络安全的法律底线。

（三）建立相应监管体系，明确网络安全责任边界

弹性设计要求在非数字、数字系统的全生命周期中都融入网络安全风险假设和风险规避策略。建议设立专门的机构或指定现有部门机构对数字产品开发全生命周期的网络弹性予以要求；进行高效监督管理，明确各方网络安全责任；将设计安全、开箱即用的默认安全作为新一代数字产品的质量规范和准入条件，杜绝网络安全质量没有保证的软硬件产品流入市场，坚决清除国家数字化建设中的“暗

表1　非冗余、非相似余度和DHR架构系统的可靠性度量

概率	非冗余系统	非相似余度系统	DHR架构系统
稳定可用概率	0	0	$9.999\,999\times10^{-1}$
首次故障前平均时间/小时	1×10^{2}	$1.000\,083\times10^{7}$	∞
降级概率	1×10^{-3}	3×10^{-6}	3×10^{-6}

功能”。数字产品网络安全质量监管部门的职责应包括对新开发数字产品进行备案、网络弹性评估、审批、准入等，把控数字产品的准入门槛，对数字产品的网络安全质量进行可量化的评估；同时，把握好监督管理的灵活度，在维护网络安全、规范数据安全的同时，鼓励制造商进行产品创新，实现管理与激励的创造性平衡。

（四）建立可量化、可验证、具有公信力的测试评价体系

我国已在南京、杭州、上海、郑州建立了网络空间内生安全的测试平台，可以针对网络核心设备、智能网联设备、数字化产品开展网络安全与功能安全的一体化测试评估，精准标定产品网络弹性的质量。建议国家主管部门制定衡量网络弹性性能的通用指标，建立统分结合的国家级测评机构体系，通过构建“内生安全系数”定量描述网络弹性，为网络弹性的评估提供可执行、可量化的标准，为我国数字化产业“走出去”提供有国际公信力的质量保证。

（五）采取市场化金融手段，多路径助力网络弹性实施

网络弹性对数字产品提出了新的安全要求，也增加了企业（尤其是中小企业）的合规成本和开发难度。建议利用市场化手段激发各相关主体的活力，包括网络安全公司、保险公司，共同参与网络弹性工程建设，形成良好的行业生态。金融保险机构在网络安全功能可定制、安全指标可度量的基础上，为符合网络弹性标准的产品提供保险服务，提供包含工具、方案与损失赔偿在内的保险产品；在赔偿责任方面，为数字产品可能发生的网络安全问题提供经济兜底和风险分散，为具有内生安全属性的数字产品提供信用担保，助力相关技术的快速应用。

致谢

张为华、赵星、汤海波对稿件撰写提供了宝贵意见，朱莹、林陈威、陈佳浠为稿件成文提供了直接帮助，谨致谢意。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: November 17, 2023; Revised date: December 6, 2023

Corresponding author: Zou Hong is the deputy dean from the Institute of Big Data, Fudan University. His major research field is cyberspace security. E-mail: hongzou@fudan.edu.cn.

Funding project: National Key R&D Program of China (2022YFB3102901); Chinese Academy of Engineering project “Strategic Studies on Becoming A Strong Cyber Power Guided by the New Development Philosophy” (2022-HYZD-02)

参考文献

[1] Goldman H. Building secure, resilient architectures for cyber mission assurance [R]. McLean: MITRE Corporation, 2010.

[2] Kalutarage H, Shaikh S A, Lee B, et al. Early warning systems for cyber defence [C]. Zurich: International Workshop on Open Problems in Network Security, 2015.

[3] Holling C S. Resilience and stability of ecological systems [J]. Annual Review of Ecology and Systematics, 1973, 4: 1–23.

[4] Pimm S L. The complexity and stability of ecosystems [J]. Nature, 1984, 307(5949): 321–326.

[5] Gunderson L H. Ecological resilience—In theory and application [J]. Annual Review of Ecology and Systematics, 2000, 31: 425–439.

[6] Pisano U. Resilience and Sustainable Development: Theory of resilience, systems thinking and adaptive governance [R]. Vienna: Vienna University of Economics and Business, 2012.

[7] Jhawar R, Piuri V. Fault tolerance and resilience in cloud computing environments [M]. Amsterdam: Elsevier, 2014: 1–28.

[8] Stine K M. Framework for improving critical infrastructure cybersecurity: Version 1.0 [R]. Gaithersburg: National Institute of Standards and Technology, 2014.

[9] Colman-Meixner C, Develder C, Tornatore M, et al. A survey on resiliency techniques in cloud computing infrastructures and applications [J]. IEEE Communications Surveys & Tutorials, 2016, 18 (3): 2244–2281.

[10] Deborah J B, Richard G. Cyber resiliency engineering framework [R]. Bedford: The MITRE Corporation, 2011.

[11] Richard A C, Julia H A, David W W, et al. CERT® resilience management model, Version 1.2 [EB/OL]. (2016-02-20)[2023-02-18]. https://insights.sei.cmu.edu/documents/1629/2016_002_001_514462.pdf.

[12] Ronald S R, Victoria P, Richard G, et al. Developing cyber-resilient systems: A systems security engineering approach [R]. Gaithersburg: National Institute of Standards and Technology, 2021.

[13] Petrenko S. Cyber resilience [M]. Aalborg: River Publishers, 2019.

[14] Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software [EB/OL]. [2023-10-20]. https://www. cisa. gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf.

[15] Saeed S, Suayyid S A, Al-Ghamdi M S, et al. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience [J]. Sensors, 2023, 23(16): 7273.

[16] Llansó T, Hedgecock D A, Pendergrass J. The state of cyber resilience: Now and in the future [J]. Johns Hopkins APL Technical Digest, 2021, 35(4): 328–334.

[17] Malatji M, Marnewick A L, Von Solms S. Cybersecurity capabilities for critical infrastructure resilience [J]. Information & Computer Security, 2022, 30(2): 255–279.

[18] Yusif S, Hafeez-Baig A. A conceptual model for cybersecurity governance [J]. Journal of Applied Security Research, 2021, 16 (4): 490–513.

[19] Eckhardt P, Kotovskaia A. The EU's cybersecurity framework: The interplay between the cyber resilience act and the NIS2 directive [J]. International Cybersecurity Law Review, 2023, 4(2): 147–164.

[20] Cyber resilient organization study 2021 [EB/OL]. [2023-03-24]. https://www. ibm. com/resources/guides/cyber-resilient-organization-study.

[21] Pettit T J. Supply chain resilience: Development of conceptual framework, an assessment tool and an implementation process [D]. Olumbus: The Ohio State University (Doctoral dissertation), 2008.

[22] Kulugh V E, Mbanaso U M, Chukwudebe G. Cybersecurity resilience maturity assessment model for critical national information infrastructure [J]. SN Computer Science, 2022, 3(3): 217.

[23] Wu J X. Cyberspace mimic defense: Generalized robust control and endogenous security [M]. Cham: Springer International Publishing, 2020.

[24] Kelly B, Jacky F, Ryan M L, et al. How aligning security and the business creates cyber resilience [C]. Ireland: State of Cybersecurity Resilience 2021, 2021.

[25] 肖前, 李秀林, 汪永祥. 辩证唯物主义原理 [M]. 北京: 人民出版社, 1981.
Xiao Q, Li X L, Wang Y X. Basic tenets of dialectical materialism [M]. Beijing: People's Publishing House, 1981.

[26] 邬江兴. 网络空间内生安全发展范式 [J]. 中国科学: 信息科学, 2022, 52(2): 189–204.
Wu J X. Development paradigms of cyberspace endogenous safety and security [J]. Scientia Sinica Informationis, 2022, 52(2): 189–204.

[27] 邬江兴. 网络空间内生安全——拟态防御与广义鲁棒控制(上册) [M]. 北京: 科学出版社, 2020.
Wu J X. Cyberspace endogenous safety and security: Mimic defense and generalized robust control (Volume I) [M]. Beijing: Science Press, 2020.

[28] Ijaz S, Hamayun M T, Yan L, et al. Adaptive fault tolerant control of dissimilar redundant actuation system of civil aircraft based on integral sliding mode control strategy [J]. Transactions of the Institute of Measurement and Control, 2019, 41 (13): 3756–3768.

[29] Ijaz S, Yan L, Hamayun M T, et al. Active fault tolerant control scheme for aircraft with dissimilar redundant actuation system subject to hydraulic failure [J]. Journal of the Franklin Institute, 2019, 356(3): 1302–1332.

[30] 邬江兴, 季新生, 贺磊, 等. 内生安全赋能网络弹性研究 [J]. 信息通信技术, 2023, 17(4): 4–11.
Wu J X, Ji X S, He L, et al. Research on network elasticity of endogenous security empowerment [J]. Information and Communications Technologies, 2023, 17(4): 4–11.

[31] Ren Q, Guo Z H, Wu J X, et al. SDN-ESRC: A secure and resilient control plane for software-defined networks [J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2366–2381.

[32] Shannon C E. Communication theory of secrecy systems [J]. The Bell System Technical Journal, 1949, 28(4): 656–715.

[33] 邬江兴. 内生安全赋能网络弹性工程 [M]. 北京: 科学出版社, 2023.
Wu J X. Endogenous safety and security (ESS) theory enabled cyber resiliency engineering [M]. Beijing: Science Press, 2023.

[34] Wang C H, Wei S Y. Highly resilient key distribution strategy for multi-level heterogeneous sensor networks by using deployment knowledge [J]. Journal of Shanghai Jiaotong University (Science), 2011, 16(5): 593–599.

[35] Joseph D, Franks J K, Freeman C N. Reliable and resilient end to end connectivity for heterogeneous [R]. New York: International Business Machines Corporation, 2011.

[36] 季新生, 伊鹏, 马海龙, 等. 基于系统架构评估的网络弹性度量技术白皮书 [R]. 南京: 紫金山实验室, 2023.
Ji X S, Yi P, Ma H L, et al. Measurement of cyber resiliency based on system architecture assessment [R]. Nanjing: Purple Mountain Laboratories, 2023.

[37] Alberts D, Tillman M. NEC2 effectiveness and agility: Analysis methodology, metrics, and experimental results [R]. Alexandria: Institute for Defense Analysis, 2012.

[38] Hosseini S, Barker K, Ramirez-Marquez J E. A review of definitions and measures of system resilience [J]. Reliability Engineering & System Safety, 2016, 145: 47–61.

[39] Hausken K. Cyber resilience in firms, organizations and societies [J]. Internet of Things, 2020, 11: 100204.