

全球数字生态系统底层驱动范式转型特征及研究启示

邹宏¹, 张帆², 尚玉婷¹, 鄂江兴^{1,2*}

(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: 当前, 全球正在开启数字生态系统底层驱动范式转型的进程; 深入研究主要发达国家通过数字生态系统底层驱动范式转型防范系统性网络风险、重塑数字产业竞争新格局, 对我国高质量建设网络强国、数字中国、智慧社会具有重要借鉴意义。本文以主要发达国家为研究对象, 运用文献调研、情报分析、比较研究等方法, 剖析了全球数字生态系统底层驱动范式转型的内涵、动因、主要目标以及发展愿景。按照范式研究的一般规律, 从思维视角、方法论、实践规范、推进策略、安全承诺、生态孵化模式等方面分析了转型的基本特征、发展趋势、采用的技术框架、配套的治理规则等, 提出了主要发达国家面临的转型挑战, 总结了我国原创的内生安全理论所具有的赋能增益优势。研究建议, 发挥内生安全理论先发优势, 跳出“牵鼻子”困境; 针对数字化转型关键领域痛点问题精准发力; 发挥国内大市场优势, 用更有效的产业政策助力新范式发展; 更新人才培养理念, 努力培养具有设计安全能力的负责任开发者; 坚持开放可控、包容多样, 增强我国数字产品“走出去”的公信力保证。

关键词: 网络空间安全; 数字生态系统; 内生安全; 网络弹性 / 韧性

中图分类号: TP393 **文献标识码:** A

Underlying-Dynamics Paradigm Shift of Global Digital Ecosystems: Characteristics and Enlightenment

Zou Hong¹, Zhang Fan², Shang Yuting¹, Wu Jiangxing^{1,2*}

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

Abstract: Nowadays, the world is embarking on a process of transformation in the underlying dynamics of the digital ecosystem. With the aim of mitigating systematic cyber risks and reshaping the global competition landscape of digital industries, the developed countries are pushing the paradigm shift in the underlying dynamics of the digital ecosystems. Thorough research on this subject holds immense significance for boosting China's strength in cyber, digital, and intelligent development. Focusing on major developed countries, this study integrates literature reviews, intelligence analysis, and comparison study to investigate the essence, driving factors, primary objectives, and outlook of this shift. Drawing upon the fundamental principles of a paradigm shift, the study explores the core features of this underlying-dynamics shift, spanning aspects like mindset, methodology, practical norms, advancement strategies, security commitments, and ecological incubation models. Additionally, it delineates emerging trends, technological frameworks, and associated governance principles related to this paradigm shift. Challenges faced by developed countries' transformation strategies are discussed, along with the enabling advantages of China's endogenous security and safety (ESS) theory. The research puts forward five recommendations: (1) leveraging the first-mover advantage of the ESS theory to overcome limitations; (2) addressing pain points in

收稿日期: 2024-03-11; 修回日期: 2024-09-23

通讯作者: *鄂江兴, 复旦大学大数据研究院教授, 中国工程院院士, 研究方向为信息通信网络与网络安全; E-mail: jxwu@fudan.edu.cn

资助项目: 中国工程院咨询项目“人工智能关键应用系统及安全战略研究”(2023-XZ-11); 中国工程院咨询项目(2023-XZ-93)

本刊网址: sscae.engineering.org.cn

critical areas of digital transformation; (3) maximizing the advantages of the large-scale domestic market by introducing more effective industrial policies to bolster novel paradigm shifts; (4) renewing the concept of personal training by cultivating responsible developers with “security-by-design” capabilities; and (5) enhancing the trustworthiness of Chinese digital products through technological innovation, thus facilitating China’s Going Global initiative.

Keywords: cyberspace security; digital ecosystem; endogenous security and safety; cyber resilience

一、前言

当前，全球正在开启数字生态系统底层驱动范式转型的进程。主要发达国家作为此次转型的推动力量，相继推出了网络知情工程（CIE）^[1]、网络弹性法案（CRA）^[2]、网络空间再平衡战略等。作为数字经济、数字化、智能化的重要支撑，数字生态系统当前面临的挑战是，在设计和构建过程中均“选择性无视”数字产品的网络/信息安全问题，亟需建立以设计安全为支撑、制造侧安全为重点、政府力量为主导的数字技术和产业发展范式，构建更加富有弹性、可防御的数字生态系统，继续保持在数字空间、网络空间中的战略主动和优势。

我国是全球数字化程度最高的国家之一。截至2023年12月，我国网络消费零售额达15.42万亿元，网民规模达10.92亿人，即时通信用户规模达10.6亿人，网络支付用户规模达9.54亿人，远程办公用户规模达5.37亿人^[3]。在数字化转型的驱动下，我国在全世界首次提出将数据作为生产要素。作为一个新兴的生产要素，不可避免地要走“基础设施建设—制度设计—价值释放”的发展路径，通过一定的软硬件载体来承接数据要素，进而释放巨大价值。数字化转型、数据要素化是大势所趋，若不推动、不加快步伐就可能丧失在这一领域已经获得的宝贵机遇。但是，如不能有效解决数字生态系统的基础问题，将对我国发展数字产业、释放“数据要素乘数效应”埋下“隐患”，甚至会危及国家安全。

目前，我国正在推动数字化转型、“数据要素×”“人工智能+”等重大计划，并在网络信息、数据基础设施等领域开展未来技术发展路线研究。在此背景下，深入研究全球数字生态系统底层驱动范式转型，有利于认清形势、厘清方向，有利于发展我国独创、独有以及具有包容力的网络信息技术，在技术范式转型的基础上更好地支撑高水平安全 and 高质量发展。对于这一领域，已有相关研究集

中在围绕发达国家数字生态系统转型政策文件的解读^[4-6]，但对驱动范式转型的内涵、特征、路径以及存在的问题关注较少。为此，研究探讨数字生态系统底层驱动范式转型，既可以弥补我国在相关领域的研究空白，也是因应国家重大发展需求。

本文在文献调研、专家研讨与项目研究的基础上，总结归纳发达国家数字生态系统底层驱动范式转型的概念设计、核心要素、技术方案、发展趋势；分析其转型过程中面临的重要挑战，以及在设计安全基础理论层面存在的缺陷和问题；通过对不同技术路线的分析比较，提出内生安全范式赋能设计安全所形成的增益优势；结合对全球转型情况和面临挑战的统筹思考，提出推动我国数字生态系统转型、发展新质生产力的研究启示。

二、全球数字生态系统底层驱动范式转型的概念及目标

生态系统一般是指在一定的空间内，生物与环境构成的统一整体。简言之，数字生态系统是在数字空间/网络空间内，数字技术与应用环境构成的统一整体，主要由数字基础设施、数字治理体系、数字经济体系、数字文明体系等构成。数字生态系统的发展与人类社会网络化、数字化发展相伴而生^[7]，核心是通过数字技术连接各领域，通过“数字之手”形成一种“创造性构建”的新力量^[8]。但是，数字生态系统作为“人造系统”，不可避免地存在内源性安全问题或先天性基因缺陷，在其塑造新质生产力、推动社会变革的同时，也会产生新的问题和风险，甚至是不可逆的系统性风险。为应对新型数字化进程中面临的新域、新质安全挑战，有必要对数字生态系统底层驱动范式转型的内涵、动因、目标等开展深入研讨。

（一）数字生态系统的基本内涵

从社会范畴看，数字生态系统是针对自然生态系统而言的“人造系统”，是人类通过数字技术创

造的，与自然系统空间并行、时间同步的新的生活空间^[9]。未来，新的数字生态系统将深化现实与虚拟世界的交互映射，打破时空局限、拓展虚拟空间，带来物理世界和数字世界边界的不断消融^[10]。数字生态系统的概念演进过程如图1所示。①从经济范畴看，数据已然成为新的生产要素，赋能传统行业，发挥乘数效益，为经济转型升级、创新发展注入新动力^[11]。数字生态系统是数字经济发展的支撑环境，数据要素、数字经济对数字生态系统的依赖程度将越来越高^[12]。②从技术范畴看，数字生态系统底层驱动力量是科学技术的创新引擎，发展引领性创新技术已成为在全球数字领域“割据战”中赢得主动权的关键。未来，发达国家不但希望继续保持其在数字技术领域的先发优势，更希望通过制定新的技术规则，抵消新兴数字强国正在形成的后发优势，以维持对技术创新路径的绝对控制权^[13]。③从国家战略范畴来看，数字化的深入推进与高依赖性带来了潜在的系统性安全风险，保证数字生态系统底层安全已经上升为世界主要国家的战略考量。例如，2023年，美国发布的新版“国家网络安全战略”^[14]中82次出现“数字化”（digital），39次出现“数字生态系统”（digital ecosystem），进一步凸显出对数字生态系统底层驱动范式转型的关注。

（二）数字生态系统底层驱动范式转型的动因

发达国家推动数字生态系统转型的原因是多样的。2023年，美国发布的新版“国家网络安全战略”中19次提及系统性风险/挑战/灾难，指出应对系统性安全风险和挑战是数字生态系统底层驱动范式转型的核心动因。①从客观原因来看，发达国家对推动数字化进程一直保持审慎态度，认为数字

技术的渗透力是“硬币的两面”，在带来便捷与繁荣的同时会导致系统性风险与日俱增。“人机物网”多元融合趋势正不断增强，信息技术、运营技术在加速融合^[15]，世界正在进入对数字化愈发依赖的阶段，“物理-信息-认知”三域相互交织带来巨大的负外部性，“网络弹性赤字”的积累将成倍增加不安全系统所造成的系统性风险。②从直接推动原因来看，发达国家需要应对日趋严峻的网络安全威胁。根据网络安全风险投资公司 Cybersecurity Ventures 的报告，2023年网络犯罪给全世界造成了8万亿美元的损失，预计2025年将增长至10.5万亿美元^[16]。③从重塑产业格局来看，发展中国家在数字产品制造领域具有一定的成本优势，发达国家试图用“改变游戏规则”的措施，通过生态系统驱动范式转型重塑数字技术设计、产品制造和市场准入标准，提升产业门槛，抵消发展中国家传统生产力进入数字产业供应链的优势，保护本国数字产业以及数字产品的流通秩序，重新掌控全球制造业和市场竞争的优势。

（三）数字生态系统底层驱动范式转型的目标愿景

从建设目标来看，数字生态系统底层驱动范式转型正在从增强网络空间的威慑与对抗，逐渐演变为建立可先天抵御、有集体弹性的数字生态系统，以抵消全球数字化转型的负面效应，防范系统性风险。2023年，在美国发布的新版“国家网络安全战略”中，以先天防御力、集体复原力、价值同化力3个能力建设为发力点，确立了保护关键基础设施、打击和防范威胁行为体、塑造市场力量推动安全和弹性/韧性、投资打造弹性/韧性未来、建立联盟伙伴关系等措施（见表1）。先天防御力旨在优先考虑可防御和弹性架构的研发，并抑制底层技术的漏

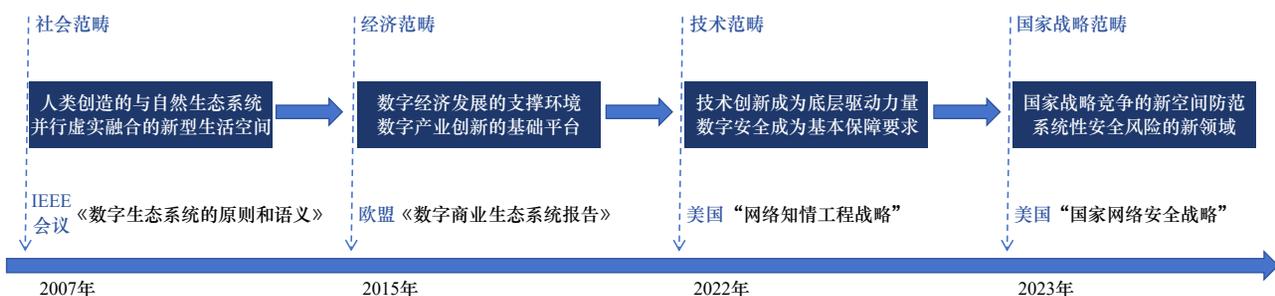


图1 数字生态系统概念的演进过程

注：IEEE为电气电子工程师学会。

洞，确保未来的技术比今天的技术更安全；集体复原力期望建立持久有效的协同防御模式，在部门风险管理机构之间公平分配风险和责任，达到“求助一人就是求助所有人”的效果；价值同化力注重提升合作伙伴的能力，以“举盟之力”推行关于负责任国家行为的全球规范。主要发达国家开展数字生态系统底层驱动范式转型的愿景目标是：发展安全、可靠、可信且符合发达国家伦理设计与价值观的数字产品，能够天然抵御攻击且在防御失效后也不会造成级联式系统性风险，负责任地发展数字技术以实现技术向善，从而迈入更加繁荣、更为稳定且发达国家能始终占据全球战略优势地位的数字化未来^[14]。

三、全球数字生态系统底层驱动范式转型的主要特征

范式概念与理论是美国著名哲学家托马斯·库恩在1962年的一篇长论文中首次提出的，随后又在《科学革命的结构》一书中作了系统阐述^[17]。范式从本质上讲是一种理论体系、理论框架、行为规则，主要包括思维视角、方法论和实践规范等内容。主要发达国家主导的数字生态系统底层驱动范式转型，以构建可信赖、可防御的数字未来为目标，主要呈现出以下特征（见表2）。

（一）新的思维视角

以生产者/企业为主导向以消费者为中心转变。在当前的数字生态系统建设中，企业占据了绝对的主导权，掌握了数字技术的选择权、规则的制定权、产业发展的控制权。这一格局的形成具有深刻的历史成因，根本原因是科技型企业通过“原创技术+商业模式”，推动了基于“互联网+”数字技术的快速普及，并将其渗透到人类生产活动的各个方面，推动了全球的信息化、数字化进程。科技巨头在创造互联网奇迹的同时，往往选择性忽视了数字产品的安全质量，在打开数字化宝库的同时，也毫无忌惮地翻开了“潘多拉魔盒”。随着数字化转型在社会服务、重要基础设施、大众日常生活等国民经济和社会治理领域全面展开，已不能仅从生产者/企业的思维视角来驱动数字生态系统建设，而是需要切换到保护使用者、消费者核心利益和国家重大关切的新视角，按照可持续发展的理念构建能够抵御系统性风险的数字生态系统。

（二）新的方法论

从提升后天防御力向提升先天防御力转变。基于传统的思维视角，数字产业一直秉承“先抢占市场、事后修补”的迭代逻辑，制造商通常将商业利益置于社会责任和道德之上。事实上，全世界数字产品漏洞数量一直持续增长。道德黑客仅在2022年

表1 美国新版“国家网络安全战略”中的数字生态系统转型概要

| 目标 | 任务 | 特征 | 措施 |
|------------------|-----------------|-------|-------------------|
| 实现数字生态系统底层驱动范式转型 | 平衡网络空间安全风险的捍卫责任 | 先天防御力 | 保护关键基础设施 |
| | | 系统 | 打击和防范威胁行为体 |
| | | 复原力 | 塑造市场力量以推动安全和弹性/韧性 |
| | | 价值同化力 | 投资打造富有弹性/韧性的未来 |
| | 调整激励措施以促进长远韧性投资 | | 建立联盟伙伴关系以实现共同目标 |

表2 数字生态系统底层驱动范式转型的主要特征

| 类型 | 数字生态系统 1.0 | 数字生态系统 2.0 |
|------|---------------|----------------|
| 思维视角 | 以生产者/企业为主导 | 以消费者为中心 |
| 方法论 | 提升后天防御力 | 提升先天防御力 |
| 实践规范 | 数字安全与数字化“两张皮” | 设计安全、一体化安全 |
| 推进策略 | 市场驱动 | 政府主导 |
| 安全承诺 | 应用侧安全 | 制造侧安全 |
| 孵化模式 | 追求经济可承受 | 政府投资设计安全和弹性 |
| 建设目标 | 增强网络空间的对抗与威慑 | 可防御、有弹性的数字生态系统 |

就发现了超过 65 000 个漏洞，比 2021 年增加了 21%^[18]。数字产业存在习以为常的“偏差正常化”状况，软硬件产品在设计或制造之初就带有必须通过补丁修复的缺陷，且大部分都是被恶意行为者利用后方可修补。数字产品已陷入补丁越补越多的恶性循环，即使是专门履行“看家护院”职责的各类网络安全产品，也概莫能外。为此，主要发达国家明确提出，我们需要更安全的数字产品，而不是更多的网络安全产品。

（三）新的实践规范

从网络安全 / 数字安全与信息化 / 数字化“两张皮”向设计安全、一体化安全转变（见图2）。在原有数字生态系统中，安全被视为一种需额外付出的“附加选项”，安全与网络化、数字化、智能化是分立状态。而在新的数字生态系统中，需在开发、配置和交付其产品之前就将网络安全功能构建到其设计过程中，实现数字产品先天的“设计安全”。具体目标是将网络安全融入到技术和产品的设计与制造中，不是让两个工程组设计两个系统，用一个保护另外一个；而是按要求设计一个单一系统，在其中融入安全的能力。在新的数字生态系统中，信息化 / 数字化与网络安全 / 数字安全是“一体之两翼、驱动之双轮”的关系，需要一体设计、一体建设、一体推进，安全需要成为发展的内在禀赋和促进因素。

（四）新的推进策略

从市场驱动向政府主导转变。以往数字生态系统的发展依赖于市场机制，造成了制造商和开发者“不负责任”地使用数字技术。欧盟委员会科学联合研究中心指出，数字行业缺乏有效竞争，且很容易出现激励错位^[19]。网络安全是市场机制失灵的地方，需实施一定的政府干预。2023 年，美国网络安全与基础设施安全局（CISA）发布了《2024—2026

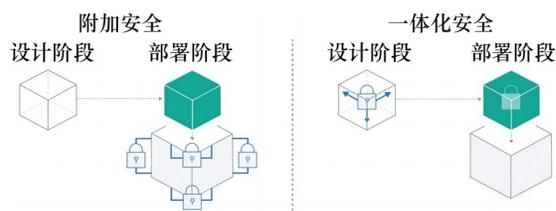


图2 附加安全和一体化安全示意图

财年网络安全战略计划》^[20]并提出，解决眼前的威胁以实现“前哨安全”，“加固地形”以实现关键基础设施的保护，推动制造侧开发默认安全的技术产品以大规模推动安全（见图3）。CISA将网络安全作为一个基本安全问题，优先考虑推动产品设计和技术进步，并通过政府主导的方式来促进、衡量、支持数字系统采用强有力的安全和韧性实践方案，显著降低破坏性入侵的可能性，实现可防御、有韧性的建设目标。

（五）新的安全承诺

从应用侧安全向制造侧安全转变。在现有数字生态系统中，数字产品制造商对产品网络安全质量不必也不会做出任何承诺，认为网络安全不属于产品质量的范畴，将安全责任和风险转嫁至用户或消费者层面。近年来，主要发达国家纷纷快速出台多项战略、法案和法规，不断强化对数字产品设计、制造侧网络安全的责任和监管。2023年3月，美国发布的新版“国家网络安全战略”提出，彻底扭转市场失灵格局，重新平衡网络空间安全的责任和风险，将网络安全责任从用户侧向制造侧“左移”，让规模最大、能力最强、地位最有优势的实体承担更多安全责任。2023年12月，欧盟就《网络弹性法案》在技术和政治层面达成一致，将共同加强联网产品的网络安全，解决硬件和软件中的漏洞问题，让欧洲大陆更安全、更有弹性。该法案已于2024年12月生效，含有数字元素的产品在进入欧盟市场时，需满足欧盟网络安全标准并签署承诺书，并满足网络弹性方面的强制性要求^[21]。

（六）新的生态孵化模式

由追求经济可承受性向政府投资设计安全转

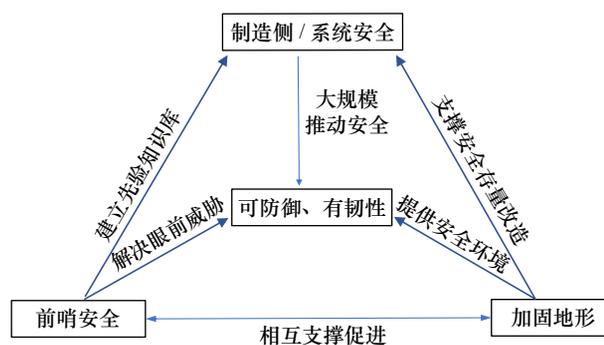


图3 美国CISA2024—2026财年的数字生态系统安全架构

变。在以企业为中心的思维视角下，数字生态系统的建设遵循投入产出比的基本法则，在安全上投入往往很难产生显性的经济效益，以至于企业认为过高的开发和制造成本在经济上难以承受。为此，在推动新型数字生态系统建设中，主要发达国家更加注重从政府侧来投资设计安全和网络弹性，以促进设计安全、制造侧安全相关技术和产业的快速发展与生态的形成。美国在新版“国家网络安全战略”中明确指出，调整激励措施以促进长期投资，将塑造市场活力以促进安全和网络弹性作为最为重要的支柱性策略，提出保持数据管理可靠、发展安全的物联网设备、转移危险软件产品及服务的责任、利用联邦政府拨款及其他激励手段建构安全、利用联邦政府采购改进问责、探索联邦政府网络保险强化安全等6项具体措施。

（七）新的建设目标

从增强网络空间的威慑对抗向建设可防御、有弹性的数字生态系统转变。美国新版“国家网络安全战略”中呈现出了一个清晰的特征，即“韧性”取代“威慑”成为数字生态系统转型的核心理念。基于重大网络安全事件的经验总结，主要发达国家对网络安全的认知逐渐从威慑思维转向韧性理念^[22]。传统威慑理念认为，网络攻击和破坏行为是可以被拒止的；韧性理念则坚持网络安全问题无法彻底避免，确保关键数据和服务在攻击中稳定运行、在“有毒带菌”的环境下保证数字生态系统安全才是关键。研究人员指出，网络空间的威慑政策已经失败，需要通过更有效的防御打破原有战略格局^[23]。

基于对全球数字生态系统底层驱动范式转型的特征分析，此次转型将呈现出5个方面的趋势：①网络安全责任从应用侧向制造侧并重转型将成为世界浪潮，构建弹性/韧性为核心的防御新理念正在成为国际趋势。美国在推动强化制造侧网络安全。欧盟积极行动，已生效的《关于在欧盟全境实现高度统一网络安全措施的指令》（NIS2指令）要求各成员国必须采取网络安全风险管理措施^[24]。澳大利亚政府发布“2023年关键基础设施韧性战略”，提供了一个指导澳大利亚加强关键基础设施韧性建设的全国性框架^[25]。2024年2月，东盟国家通过“构建一个包容可信的数字生态系统”合作宣言，提出

在数字化转型中提高网络韧性、可靠性能力建设。②设计安全已经成为数字生态系统底层驱动范式转型的根本要求。2023年4月，美国、德国、加拿大、日本等18个国家的网络安全机构联合发布《改变网络安全风险平衡：设计安全与默认安全的原则与方法》，明确阐明了对数字生态系统底层转型的要求，即在开发、配置和交付其产品之前就将网络安全功能构建到其设计过程中，实现基础设施的设计安全、出厂安全；只有结合安全的设计实践，才能打破不断创建和应用修复程序的恶性循环。③默认安全将成为一种“开箱即用”的数字产品内生安全质量标准规范。2020年，新加坡提出了“网络安全标签计划”^[26]，通过对物联网（IoT）产品进行网络安全配置的智能评级，帮助消费者识别安全的数字产品，提高内生安全质量标准规范。美国联邦通信委员会启动IoT“网络安全标识计划”，推出了网络信任标识；美国国家标准与技术研究院（NIST）发布了消费类IoT产品网络安全标签的标准建议^[27]。④国家将通过监管、政府补贴等为数字生态系统转型提供支持。2023年7月，美国发布《网络安全战略实施计划》^[28]，进一步明确要求美国政府管理和预算办公室、国家网络总监办公室协同为推进“网络弹性”的预算事项提供高优先级，以落实重点领域的财政支持，并将联邦政府拨款激励列入2025财年网络安全预算备忘录^[29]。⑤教育体系从培养“看家护院的保镖”向“负责任的设计者”转变。2023年，美国发布“国家网络安全劳动力和教育战略”^[30]，将在未来4年向全国7所网络安全强校拨款2400万美元，用于网络安全专项奖学金，目的是提高全民网络素质并培养负责任的数字产品设计师和开发者，从而改变设计或制造侧、用户或使用侧网络安全风险严重失衡的现状。

四、全球数字生态系统底层驱动范式转型的技术路径

（一）推进设计安全的主要技术框架

目前，全球主要有3种推动设计安全的技术框架。①零信任网络安全架构^[31]，秉持永不信任、持续认证的理念，基于最小特权、多层次安全、持续监测等原则，采用多层次安全验证用户、设备和应用程序的访问权限，包括多因素身份验证、网络分

割、日志和分析等措施，能够从框架层面提高网络安全。② 纵深防御安全架构^[32]，使用多种安全产品和实践来保护网络边界、资产、资源等，以建立坚固的安全基础，从而最大程度地保护组织的信息和资产，降低各种威胁带来的风险影响。纵深防御的措施包括物理安全控制、网络安全控制、应用程序安全控制、终端安全控制等，当某一道防线受损之后，其他安全措施可以帮助限制和减轻攻击行为对整个网络和系统的损害^[33]。③ NIST 安全框架。该框架的落脚点是规范全生命周期的安全，针对网络安全事件，进行识别、保护、侦测、应对并恢复网络安全，进而降低风险、保护关键资产和提高网络弹性。近期，美国发布 NIST 2.0 版安全框架^[34]，在识别、保护、检测、响应、恢复等功能基础上增加了“治理”功能，以提高数字生态系统的安全透明度和可问责能力。

（二）完善设计安全的规则和规范

主要发达国家在提出技术框架的同时，高度重视数字生态系统底层驱动范式转型中的规则和规范设计。① 注重全生命周期安全，给出了数字产品开发全生命周期各个阶段的设计安全策略^[35]，包括安全内存语言、安全硬件基础、安全软件组件、静态和动态应用程序安全测试等，帮助开发者、制造商在设计 and 开发阶段就提升产品安全性。② 注重开源软件的质量管理安全。通过建立联邦级开源软件数据库，跟踪和监测开源软件的使用情况；通过推动适应性软件“安全港”开发框架^[14]以明确自动豁免和自动责任条款，建立“安全要地”和“责任飞地”；通过确立 CISA 在支持开源软件安全方面的主导地位，加大开源软件安全中的政府投资。③ 注重国家级漏洞管理和披露限制。主要发达国家普遍认为，及时发现漏洞、有效管理漏洞、防止漏洞被恶意利用是管控风险的重要手段，为此加大了对国家级漏洞库的管控力度；同时，更新了漏洞披露的相关规定，进一步缩小了漏洞披露的范围，对漏洞发现和管理的链条进行了重塑，以保持其拥有先验知识的优势。④ 注重供应链和上下游管理。主要发达国家通过网络安全供应链风险管理实践对企业层、业务层、操作层的供应链进行风险评估、识别和控制/管理，通过发布安全软件物料清单和硬件材料清单来提升

上下游供应链的透明度^[36]。

（三）设计安全的实例分析

2023 年，美国能源部发布《网络空间知情工程（CIE）实施指南》，通过融合零信任安全架构、纵深防御安全加工以及 NIST 安全框架，指导能源部门推动数字生态系统底层驱动范式转型，增强能源系统网络弹性能力。通过 CIE 来实现设计安全，从本质上看，其目标主要体现在，一是实现对网络安全风险的描述，二是通过工程技术手段来实现网络安全风险危害的最小化。CIE 提出了 6 个方面的设计安全原则，具体包括：聚焦后果的设计、减少附加信息安全技术的依赖、确保数据仅以所需方式流动、减少数字系统潜在的暗功能、建立多样化以及冗余性的防御层次、利用实时主动能力延迟威胁活动等。同时，CIE 提出了相应的实施规则，包括：多个学科交叉进行相互依赖性评估、建立数字资产意识、实施网络安全供应链控制、保护敏感的工程信息记录、持续开展设计安全培训等。基于设计安全原则和规则，美国爱达荷州国家实验室在美国国防部和国土安全部的支持下，一方面，着眼建立防范系统性网络风险和潜在灾难性影响的网络弹性，开发了将 CIE 应用于现有数字基础设施的方法；另一方面，在新建设的关键能源设施中集成 CIE 的技术框架，将网络弹性愿景整合到最终系统设计方案之中，防范未知风险以及风险累积效应可能对关键资产的破坏。

（四）设计安全面临的挑战

尽管主要发达国家在数字生态系统底层范式转型中强化了“框架+规则”的推动路径，但依然难以达成其所期望的设计安全的目标任务。究其原因主要在于，当前主要发达国家主导的数字生态系统底层驱动范式转型，依然是以传统的网络空间安全范式作为设计安全的基本遵循，还没有从根本上跳出基于先验知识的“杀毒灭马”“封门补漏”的技术范畴，仍然无法达成能有效应对任何潜在安全威胁与破坏的愿景目标。显然，没有网络空间安全范式的变革，就不可能实现数字生态系统底层驱动范式的根本性变革，就无法解决所面临的 3 个方面的“硬核问题”：① 难以应对“未知的未知安全风险”。现有网络弹性系统工程技术框架严重依赖于对风险的先验性认知^[37]，对未知攻击或破坏缺乏理论层面的

指导和技术层面的创新，以至于不得不放弃对隐形的、非破坏性的、以窃取敏感数据或信息为目标的未知攻击的防范，仅希望通过网络弹性来尽可能恢复显式破坏的影响。② 缺乏一体化的系统安全架构。尽管当前网络弹性系统工程制定了百余种安全 / 弹性工具^[38]，但仍旧无法获得“钢筋混凝土般质地”的一体化安全质量；导致当前的设计安全就如同“开设了一间药材丰富的中药铺”，尽管琳琅满目但没有治病良方；③ 安全质量难以做到可量化设计与可验证评估。目前，仍然采用基于指标体系静态评估以及与已知漏洞库比对的安全测试方式^[39]，存在设计难、选择难、度量难等问题，缺少病理取样式的黄金检测方法，难以突破“未见异常”、事实性而非经验式评估的桎梏。

五、我国在数字生态系统底层驱动范式技术领域的应用探索

面对数字空间的新质安全风险，设计安全应当在安全“左移”的基础上更进一步，将“亡羊补牢”式被动防御变换为不依赖先验知识的主动防御，从“尽力而为”的“打地鼠”范式跃升为安全可量化、可测试、可验证的内生安全范式，使数字生态系统获得原生的或者内源性的安全。2013年，我国提出了网络空间内生安全理论与拟态防御体系，运用“结构决定安全”的系统工程思想，通过“构造编码”形成“环境加密效应”^[40]，有效管控未知的内生安全问题与人为或非人为外部扰动的关联影响。即使在缺乏先验知识的最不利情况下，也能在机理上有效抑制“未知的未知”安全威胁与破

坏，在可信性不能保证或存在安全缺陷的数字生态环境内，仍然可以构建安全性有设计质量保证的数字设施或信息物理系统。内生安全理论改变了传统的网络安全技术范式，有望从根本上解决数字生态系统底层驱动范式转型面临的问题，主要具有以下6个方面的增益优势。

（一）防范未知安全威胁

内生安全的动态异构冗余架构具备不依赖先验知识、能应对“未知的未知”网络攻击或破坏的先天安全防御能力。换言之，只要在设计或制造侧应用内生安全架构，就能有效避免已知的未知或“未知的未知”等广义功能安全威胁导致的局部安全事件，在网络攻击形成破坏效果之前就加以遏制与消除。图4中的红色部分显示了网络攻击进程的阶段演变，内生安全赋能可将未感知到的红色攻击线转变为图5中可感知到的绿色攻击线。可以看出，以绿线表示的对手多次尝试的高级持续性威胁（APT）攻击被扼制在攻击的早期（已经威慑了对手发起后续攻击的意愿），以蓝色线表示的系统功能性能曲线始终维持平稳^[41]。

（二）合理权衡设计安全策略

内生安全架构具有灵活性、可定制性的特征，可以根据数字产品安全性指标、网络弹性能力、应用场景特色进行隘口设防、要地防御、纵深部署^[42]。在设计、制造侧，推广基于内生安全架构的数字生态系统底层驱动范式转型，可以促使数字产品从源头上将安全融入设计和制造过程，掌控数字生态同

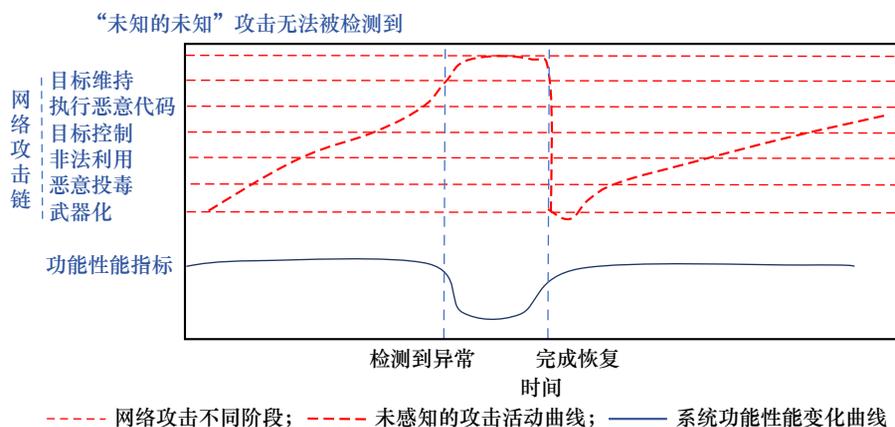


图4 现有网络弹性缺乏对APT攻击本身的早期感知能力

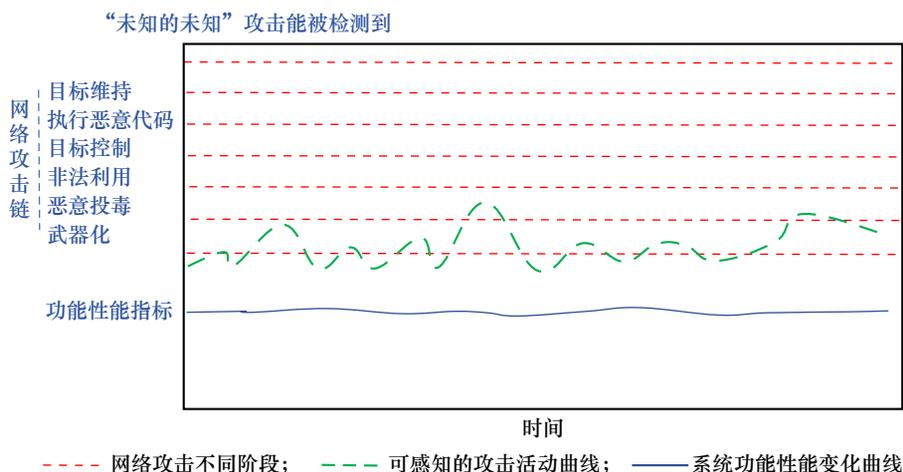


图5 内生安全在感知“未知的未知”攻击方面的网络弹性演变图

质化的“单点”失效风险；通过合理权衡产品全生命周期性价比，使任务或服务系统获得广义功能安全质量保障，全面提升产品与服务的多样性，提高数字产品供应链的韧性。

（三）引入安全功能黄金检测与评估方法

内生安全架构能提供一种创新的注入式或开放性测试（“白盒测试”）评估方法，通过人工置入“测试钩子”或“加载测试例”的方式，允许第三方在目标构造内植入任何数量、差模性质且不为设备制造者和使用者所知悉的测试用例，将被测对象未知的、非破坏性的漏洞后门/病毒木马等测试例代码进行“合法插桩”，观察系统输出端是否出现测试例期望的攻击响应，因而可验证度量数字产品“默认安全”质量，完美解决当前网络弹性系统工程缺乏一体化设计安全评估方法的难题^[43]。“白盒测试”能够测量数字产品面对潜在威胁出现安全事件的发生概率，能够为建立数字产品“安全信任标签”计划提供支撑。

（四）控制局部风险演变为系统性安全事件的发生概率

面对系统内部潜在的错误、故障、人为攻击等广义功能安全威胁，内生安全架构在机理上可以将不确定安全扰动变换为差模性质的“已知的未知”安全事件，且能用成熟的可靠性技术加以处理。因而，架构内即便存在未知的漏洞后门、病毒木马等，也很难成为可有效利用的攻击资源。同时，内

生安全架构可有效应对网络攻击的二阶/三阶效应造成的信息物理系统或数字基础设施系统性安全风险，有效防范多米诺骨牌式的系统安全事件。

（五）基于内生安全机机构造受信任执行环境

内生安全的基本目标是在不可信的数字生态系统中，提供有安全性承诺的应用和服务。达成这一目标，是基于内生安全架构的数学物理加密性质，使其能够阻断广义功能安全问题之内因和人为或非人为扰动之外因间的相互作用，在架构内即使存在内生安全问题也难以演变为安全事件。内生安全架构理论上可以使用存在不确定安全缺陷的软硬组件或部件，构建足够高（可控概率内）安全等级的受信任执行环境，因而可以破解加密认证、区块链、零信任、敏感服务等可信算法或软件长期以来缺乏“值得信赖安全底座”的共性安全难题。

（六）极大拓展了传统网络安全产业的市场空间

内生安全架构在设计之初就具有“钢筋混凝土建筑骨架作用”，能够自然地接纳各种传统网络安全技术和设计安全策略，按照“混凝土砣料”配比方式，在产品的设计、制造、使用、维护全生命周期内实现差异化的部署，可获得“钢筋混凝土般”的指数量级安全增益，能一体化地解决功能安全、网络安全甚至信息或数据安全等多重交织性质的网络弹性系统工程化问题^[40]。这一特性将为拓展网络安全产业空间提供新动力，使得传统网络安全产业获得与数字产业“相同口径”的发展空间，为更安

全的数字产品提供更丰富的“安全组件或零件”，有望将网络安全产业从不足千亿元的规模跃升至万亿元量级。

六、有关我国数字生态系统底层驱动范式转型的思考

面对全球数字生态系统底层驱动范式转型的趋势，我国需要冷静观察、主动应对。从转型的技术特征看，主要发达国家提出的构建有弹性/韧性、可防御的数字生态系统，以及推动负责任创新、构建设计安全技术框架、强化可管理的治理方式、抵御系统性网络风险等重要理念值得学习借鉴，未来的数字安全技术将不再片面强调“附加式安全”，而是更加强调“内生式安全”。但是，从主要发达国家推动数字生态系统转型的实际举措来看，其中带有浓厚的“数字霸权”“小院高墙”“抵消战略”的色彩，其转型的本质既包括保护自身安全、更包括遏制新兴力量的发展。在这种态势下，我国不推动转型将出现“网络安全/数字安全洼地”的窘境；但如果按照主要发达国家的方式和策略推动转型，又可能跌入其预设好的“地雷阵”或陷阱之中。为此，我国需要结合自身情况和发展实际，发挥内生安全理论与技术的先发优势，以内生安全范式赋能数字生态系统底层驱动范式转型，走出一条中国式数字化的新路径，为激活数字要素、繁荣数字经济、发展新质生产力提供重要支撑。

（一）坚定不移走自己的路，在深化转型中跳出“牵鼻子”困境

虽然主要发达国家都在推动数字生态系统底层驱动范式转型，但是其在具体实施策略上还有诸多不同之处。欧洲在这一进程中更加注重自身的独立性，强调要避免成为美国的“数字殖民地”。对我国而言，推动数字生态系统底层驱动范式转型，只能走自己的路，如果盲目跟风、亦步亦趋，生搬硬套西方国家的弹性/韧性概念^[44]，将陷入新的“路径依赖”。我国提出的内生安全理论，不但吸收和借鉴了西方网络弹性/韧性的内容，更加强调防范“未知的未知”安全风险、安全性能可量化设计/可验证度量等，这些都能有效降低对西方网络弹性标准框架、核心技术以及“先验知识控制权”的依

赖性。维护数字生态系统基础安全的技术都是“国之要者”，必须坚持独有独创、自立自强，摒弃跟随式、“换汤不换药”的惯性，在新的转型浪潮中获得竞争优势。

（二）注重从关键领域入手，针对数字化转型痛点问题精准发力

主要发达国家在数字生态系统底层驱动范式转型中，均将信息物理系统安全放在率先推动的重要领域，然而将新的功能和技术叠加到已经相当脆弱的系统上，会使重要系统面临更加复杂和危险的局面。从这一趋势看，我国在推动转型中也需要关注信息物理系统，重点解决功能安全与网络安全/信息安全/数据安全相互交织的现实问题，建立具有一体化安全能力的新型安全体系。例如，在电力能源系统中，随着可再生能源并网比例的提高，信息域、物理域的交互更加频繁，增加了各种节点故障的相关性，使新型电力系统安全风险跨域传播的可能性和路径显著增长^[45]。为此，可针对其未知威胁抵御、安全风险阻断两个核心安全需求，实施电力基础设施内生安全示范工程，为构建高可信、高可靠、高可用三重安全的电力系统提供解题思路，形成从底层硬件到顶层应用的垂直安全生态系统。

（三）发挥国内大市场优势，用更有效的产业政策助力新范式发展

在推动数字生态系统底层驱动范式转型的激励措施上，主要发达国家注重发挥政府的力量，如欧盟指出加大连通性基础设施战略能力投入，美国强调平衡公私责任以政策激励促进长期投资。我国具有超大规模国内大市场的巨大优势，应借鉴发达国家的诸多产业政策，促进具有设计安全能力、默认可安全标准、内生安全品质、引领性的新技术快速应用。① 强化数字产业制造侧网络安全责任，从“谁建设谁负责、谁运营谁负责”向“谁设计谁负责、谁制造谁负责、谁销售谁负责”转变，对数字产品设计者、制造商继续“选择性忽视”网络安全质量、不负责任地将产品安全问题毫无顾忌地转嫁到使用侧的行为采取“零容忍”态度。② 加快建立中国特色数字产业网络弹性政策法规，明确制造商网络安全责任、数字产品刚性安全标准、可量化的验证评估方法，形成“有管理到可管理”的治理体

系。③ 出台中国版的“数字产品信任标签”计划，优先考虑在智能网联汽车等领域开展网络安全标签计划试点，对车联网核心设备、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，精准标定包含数字元素产品的网络弹性质量。

（四）更新人才培养理念，培养大批具有设计安全能力的负责任开发者

数字未来的竞争，归根结底是人才的竞争。面对新形势，传统的“开发者、防御者、渗透者”相对独立的人才培养范式已无法满足转型需求，需要参与数字系统软硬件开发过程的所有人员都应具备安全素养和能力。我国网络安全人才供需矛盾仍然突出。据估算，到2027年，我国网络人才缺口将达到327万人，传统的“保镖”式安全人才年供给量仅约4万人，无法满足数字生态系统转型的需要。目前，内生安全理论已经形成了具有鲜明特色的自主知识体系，科学回答了一体化解决功能安全和网络安全交织问题的基础理论问题，形成了以系统论、整体论为内核的方法论体系，融合和汇聚了信息论、控制论、密码学、计算机科学等多领域的基础知识。我国应发挥作为网络内生安全理论与技术原创地的独特优势，致力于培养具备内生安全知识、掌握设计安全技能、具有默认安全素养的负责任开发者，探索一体化安全人才培养的新范式，从根本上扭转人才培养供需失衡的矛盾。

（五）坚持开放可控、包容多样，让数字产品“走出去”更具公信力

主要发达国家在推进负责任技术创新的治理策略中，提出了诸多衡量数字系统的透明度以及安全质量的指标^[46]。但是，发达国家现有网络弹性/韧性的评价方法主要从技术方法出发评价系统的弹性能力^[47]，对系统架构核心能力缺乏关注，评价方法同样缺乏可操作性和可信性。相比而言，内生安全理论所提出的“白盒测试”，不仅人为引入了功能故障或失效，也可人为引入安全失陷，这为网络弹性/韧性评估提供了一种可验证的安全测试方法。“白盒插桩”等黄金测试有效解决了网络安全无法量化设计、不能量化评估的难题，可以对网络安全性能实现“心中有数”，让数字产品的安全质量能够“看得清”“可度量”。具有广

义功能安全特性的“白盒测试”，可以对数字生态系统及其部件的鲁棒性、安全性进行可复现、可验证的测试评估；既能满足不同国家个性化、分众化的安全需求，也能支持全球性的互联互通、共享共治，可为具有“安全标签”的我国数字技术走向全球提供有力支撑。

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: March 11, 2024; **Revised date:** September 23, 2024

Corresponding author: Wu Jiangxing is a professor from Institute of Big Data, Fudan University, and a member of Chinese Academy of Engineering. His major research fields include communication and information systems and cybersecurity. E-mail: jxwu@fudan.edu.cn

Funding project: Chinese Academy of Engineering project “Strategic Research on the Key AI Application Systems and Security” (2023-XZ-11); Chinese Academy of Engineering project (2023-XZ-93)

参考文献

- [1] Office of Cybersecurity, Energy Security, and Emergency Response. National cyber-informed engineering strategy [R]. Washington DC: The US Department of Energy, 2022.
- [2] European Commission. The European cyber resilience act (CRA) [R]. Brussels: European Commission, 2023.
- [3] 中国互联网络信息中心. 第53次中国互联网络发展状况统计报告 [R]. 北京: 中国互联网络信息中心, 2024.
China Internet Network Information Center. The 53rd statistical report on China's Internet development [R]. Beijing: China Internet Network Information Center, 2024.
- [4] 洪延青, 朱玲凤, 张朝, 等. 欧盟提出“技术主权”概念 引领欧盟数字化转型战略 [J]. 中国信息安全, 2020 (3): 70-74.
Hong Y Q, Zhu L F, Zhang Z, et al. The EU puts forward the concept of “technical sovereignty” to lead the EU's digital transformation strategy [J]. China Information Security, 2020 (3): 70-74.
- [5] 王守都. 拜登政府的网络空间战略体系构建: 发展现状、具体特征及未来趋势 [J]. 情报杂志, 2024, 43(2): 25-32.
Wang S D. The construction of the Biden administration's cyberspace strategy system: Status quo, features and trends [J]. Journal of Intelligence, 2024, 43(2): 25-32.
- [6] 宫云牧. 网络空间与霸权护持——美国网络安全战略的迭代演进与驱动机制 [J]. 国际展望, 2024, 16(1): 54-74, 159.
Gong Y M. Cyberspace and hegemony maintenance: The evolution and driving mechanisms of U.S. national cybersecurity strategies [J]. Global Review, 2024, 16(1): 54-74, 159.
- [7] Krivý M. Digital ecosystem: The journey of a metaphor [J]. Digital Geography and Society, 2023, 5: 100057.
- [8] Acs Z J, Song A K, Szerb L, et al. The evolution of the global digital platform economy: 1971—2021 [J]. Small Business Economics, 2021, 57(4): 1629-1659.
- [9] Boley H, Chang E. Digital ecosystems: Principles and semantics [R]. Cairns: 2007 Inaugural IEEE-IES Digital EcoSystems and Tech-

- nologies Conference, 2007.
- [10] Zeb S, Mahmood A, Ali Hassan S, et al. Industrial digital twins at the nexus of NextG wireless networks and computational intelligence: A survey [J]. *Journal of Network and Computer Applications*, 2022, 200: 103309.
- [11] Senyo P K, Liu K C, Effah J. Digital business ecosystem: Literature review and a framework for future research [J]. *International Journal of Information Management*, 2019, 47: 52–64.
- [12] 吴江, 陶成熙. 激活数据要素 赋能千行万业——《“数据要素”三年行动计划(2024—2026年)》政策解读 [J]. *情报理论与实践*, 2024, 47(3): 16–19.
- Wu J, Tao C X. Activating data elements empowers thousands of businesses: *Policy interpretation of “the data elements” Three-Year Action Plan (2024—2026)* [J]. *Information Studies (Theory & Application)*, 2024, 47(3): 16–19.
- [13] 余建川. 欧盟网络安全建设的新近发展及对我国的启示——基于《欧盟数字十年网络安全战略》的分析 [J]. *情报杂志*, 2022, 41(3): 87–94.
- Yu J C. The recent development and enlightenment of EU cyber security construction—Based on *the EU’s cybersecurity strategy for the digital decade* [J]. *Journal of Intelligence*, 2022, 41(3): 87–94.
- [14] The White House. National cybersecurity strategy [R]. Washington DC: The White House, 2023.
- [15] Rahman M A, Hossain M S. A deep learning assisted software defined security architecture for 6G wireless networks: IIoT perspective [J]. *IEEE Wireless Communications*, 2022, 29(2): 52–59.
- [16] Steve Morgan. Boardroom cybersecurity report on cybercrime [R]. California: Cybersecurity Ventures, 2023.
- [17] Kuhn T S. *The structure of scientific revolutions* [M]. Chicago: University of Chicago Press, 1962.
- [18] HackerOne. 2022 Hacker-powered security report [R]. San Francisco: HackerOne, 2022.
- [19] Gianmarco B, Josefa B, et al. Cybersecurity, our digital anchor: A European perspective [M]. Luxembourg: Publications Office of the European Union, 2020.
- [20] Cybersecurity & Infrastructure Security Agency. Cybersecurity strategic plan FY2024—2026 [R]. Washington DC: Cybersecurity & Infrastructure Security Agency, 2023.
- [21] 俞能海, 张丽, 邹宏. 风险管理视角下的数据安全与隐私保护 [J]. *中国网信*, 2024 (1): 41–44.
- Yu N H, Zhang L, Zou H. Data security and privacy protection from the perspective of risk management [J]. *China Internet Information*, 2024 (1): 41–44.
- [22] 桂畅旒, 刘星. 2023 年国际网络空间形势回顾及发展动向 [J]. *中国信息安全*, 2023 (12): 19–23.
- Gui C N, Liu X. Review and development trend of international cyberspace in 2023 [J]. *China Information Security*, 2023 (12): 19–23.
- [23] Fischerkeller M P, Goldman E O, Harknett R J. Cyber persistence theory: Redefining national security in cyberspace [M]. Oxford: Oxford University Press, 2022.
- [24] European Commission. NIS 2 directive [R]. Brussels: European Commission, 2022.
- [25] Cyber and Infrastructure Security Centre. Critical infrastructure resilience strategy [R]. Canberra: Department of Home Affairs, Australian Government, 2023.
- [26] The Cyber Security Agency of Singapore. Media fact sheet of cybersecurity labeling scheme [R]. Singapore: Cyber Security Agency of Singapore, 2020.
- [27] National Institute of Standards and Technology. Recommended criteria for cybersecurity labeling for consumer Internet of things (IoT) products [R]. Gaithersburg: National Institute of Standards and Technology, 2022.
- [28] The White House. National cybersecurity strategy implementation plan [R]. Washington DC: The White House, 2023.
- [29] Young S D, Walden K E. Administration cybersecurity priorities for the FY 2025 budget [R]. Washington DC: U. S. Executive Office of the President, 2023.
- [30] Office of The National Cyber Director, Executive Office of The President. National cyber workforce and education strategy: Unleashing America’s cyber talent [R]. Washington DC: The White House, 2023.
- [31] Kerman A, Borchert O, Rose S, et al. Zero trust architecture [R]. Gaithersburg: National Institute of Standards and Technology, 2020.
- [32] Vacca J R. *Computer and information security handbook* [M]. Amsterdam: Elsevier, 2013.
- [33] Alsaqour R, Majrashi A, Alreedi M, et al. Defense in depth: Multilayer of security [J]. *International Journal of Communication Networks and Information Security (IJCNIS)*, 2021, 13(2): 242–248.
- [34] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 [R]. Gaithersburg: National Institute of Standards and Technology, 2024.
- [35] Souppaya M, Scarfone K, Dodson D. Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities [R]. Gaithersburg: National Institute of Standards and Technology, 2022.
- [36] Boyens J M, Smith A, Bartol N, et al. Cybersecurity supply chain risk management practices for systems and organizations [R]. Gaithersburg: National Institute of Standards and Technology, 2024.
- [37] Möller D P F. *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* [M]. Cham: Springer, 2023.
- [38] Bodeau D J, Graubart R D, McQuaid R M, et al. Cyber resiliency metrics, measures of effectiveness, and scoring [R]. Bedford: MITRE, 2018.
- [39] Li Z S, Wu G Y, Cassandro R, et al. A review of resilience metrics and modeling methods for cyber-physical power systems (CPPS) [J]. *IEEE Transactions on Reliability*, 2024, 73(1): 59–66.
- [40] 郭江兴. 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.
- [41] 郭江兴, 季新生, 贺磊, 等. 内生安全赋能网络弹性研究 [J]. *信息技术*, 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 Commu-*

- nications Technologies, 2023, 17(4): 4–11.
- [42] 邬江兴, 邹宏, 薛向阳, 等. 内生安全赋能网络弹性的构想、方法与策略 [J]. 中国工程科学, 2023, 25(6): 106–115.
Wu J X, Zou H, Xue X Y, et al. Cyber resilience enabled by endogenous security and safety: Vision, techniques, and strategies [J]. Strategic Study of CAE, 2023, 25(6): 106–115.
- [43] 邬江兴, 季新生, 贺磊, 等. 从设计安全到内生安全技术白皮书 [R]. 南京: 紫金山实验室, 2023.
Wu J X, Ji X S, He L, et al. Technical white paper: From security by design to endogenous security [R]. Nanjing: Purple Mountain Laboratory, 2023.
- [44] Petrenko S. Cyber resilience [M]. Aalborg: River Publishers, 2019.
- [45] Gunduz M Z, Das R. Cyber-security on smart grid: Threats and potential solutions [J]. Computer Networks, 2020, 169: 107094.
- [46] Spagnuolo D, Bartolini C, Lenzini G. Metrics for transparency [R]. Heraklion: 11th International Workshop, DPM2016 and 5th International Workshop, QASA2016, 2016.
- [47] Ross R, Pillitteri V, Graubart R, et al. Developing cyber-resilient systems: A systems security engineering approach [R]. Gaithersburg: National Institute of Standards and Technology, 2021.