网络安全战略与技术发展趋势
(2024年)

紫金山实验室
2024年11月

前　言

网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。2014年2月27日，习近平主持召开中央网络安全和信息化领导小组第一次会议时强调，网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署，统一推进、统一实施。近年来全球网络安全事件频发，对通信、政府机构、能源、交通、科技等多个关键领域造成严重影响，暴露了当前网络安全防护体系的脆弱性，也凸显了网络安全威胁影响范围不断扩大、破坏性显著增强、以及政治化程度日益加深的趋势。随着攻击技术的演进，网络安全事件的破坏力逐渐提升，超越了传统的数据泄露和系统中断，开始对关键基础设施乃至物理设备产生直接破坏，导致不可估量的经济损失与社会动荡。网络空间已成为国家间战略竞争的新前沿，网络攻击愈发成为国家博弈和政治对抗的工具，网络安全问题的复杂性和严重性持续上升。

由于数字产品“代码未写、漏洞已出”的“基因缺陷”，“制造商选择性的忽视(无视)数字产品设计中的网络安全问题”、“补丁摞补丁、反复踩坑的恶性循环”是数字世界的“两大顽疾”。同时，制造端长期缺乏安全责任，产品安全质量难以保障，进一步使高度互联的数字化社会暴露在系统级风险之下，同质化产品一旦发生单点失效，极易引发大规模共模故障，导致上层服务全面崩溃。对于规模庞大、结构复杂的数字基础设施，关键节点或服务的安全缺陷一旦被利用，往往会通过二阶、三阶效应造成多米诺式的系统性安全事件，使脆弱的数字社会面临严峻威胁。近年来，为了应对日益严峻的网络安全风险，欧美各国不约而同地提出网络安全应进行范式转变，“强化数字产品制造侧网络安全责任和监管”“建立可防御且富有弹性的数字生态系统”,并上升为其统筹网络空间“发展与安全”的战略设计，敦促网络安全责任从用户侧向制造侧转移，动员全社会资源以“网络弹性工程”为抓手加强制造侧设计安全，强调数字产品制造商从数字产品全生命周期的初始设计阶段就有意识地确保网络安全是产品开发的关键方面。

当前美欧网络安全的相关政策法规和战略规划，一方面是出于扭转数字社会

日益严峻安全形势之需要，另一方面也是对传统数字生态系统底层驱动范式的变革，美欧大力实施的制造侧设计安全路线仍然建立在各种先验知识库完备性和实时性基础上，强调“打倒可恢复”的网络弹性，仍然跳不出补丁摞补丁恶性循环，虽然能够在某种程度上缓解当前网络空间安全风险，但无法从根本上解决数字化社会的系统级风险。显而易见，只有走不依赖先验知识的网络韧性设计范式，达成“攻而不倒”的网络韧性目标，才可能从根本上实现数字生态系统底层驱动范式转型。

本蓝皮书首先介绍了网络安全威胁事件的现状及趋势，总结了网络安全威胁愈演愈烈的原因。其次，深入分析当前网络安全战略与技术的发展现状和未来趋势，全面评估全球网络安全格局的变化，重点识别我国在这一领域的先发技术优势。最后，客观分析我国网络安全领域面临的挑战和不足，通过深入探讨如何利用我国优势技术推动网络安全责任从用户侧向制造侧转移，如何构建中国特色数字产品安全监管体系，我们期望能够为建立全面的网络安全责任和质量控制体系提供有力支撑，为筑牢数字生态系统基座“根骨”，提出一条领先欧美的数字中国建设新路径。

漏洞/后门问题是所有包含数字元素的软硬件系统底层驱动生态环境中不可能彻底消除的“基因缺陷”，试图通过“封门补漏、打补丁”的方法实现“问题归零”，无法避免“补丁上或补丁后”还可能引入新的安全漏洞的矛盾问题。此外，许多安全事件并非来源于单一的系统组件故障，而是因为非故障组件之间的不安全相互作用所致。漏洞/后门问题是所有包含数字元素的软硬件系统底层驱动生态环境中不可能彻底消除的“基因缺陷”，试图通过“封门补漏、打补丁”的方法实现“问题归零”，无法避免“补丁上或补丁后”还可能引入新的安全漏洞的矛盾问题。此外，许多安全事件并非来源于单一的系统组件故障，而是因为非故障组件之间的不安全相互作用所致。

——中国工程院院士邬江兴

版权声明

本蓝皮书主要贡献者

邬江兴，季新生，贺磊，周鼎，牛玉坤，韩晓鹏，耿进步，谢宇，曹植纲，曹玖新，陈平，刘波，桂杰，纪东辰，周强，赵涵韬

目录

1 引言

1.1 背景

在全球数字化浪潮席卷之际，网络安全已然成为一个不容忽视的关键议题，其重要性与日俱增。随着数字经济的蓬勃发展和新型工业化的加速推进，我们正面临着一个前所未有的复杂安全环境[1-1]。网络安全威胁不再局限于传统的信息域，而是以惊人的速度和规模向物理域和认知域多维渗透，攻击手段也从单纯的信息层面软损害演变为可能导致物理层面硬损毁的复杂形态，更有甚者通过将数字设备武器化威胁国家总体安全。这种多维度、全方位的安全挑战不仅威胁着单个组织的运营安全，更对全球经济体系和社会稳定构成了严峻挑战[1-2]。

权威机构的预测和研究进一步突出了问题的急迫性和严峻性。据Gartner预测，2025年全球将有近半数组织遭受供应链攻击；欧盟委员会联合研究中心的报告揭示，网络犯罪导致的经济损失已经超过子自然灾害和毒品交易的总和[1-3]。如果以经济体量衡量，网络犯罪已是仅次于美国和中国的世界第三大经济体，2023年底，损失达8万亿欧元，到2025年底将达10.5万亿欧元。随着全球互联系统和云服务的快速发展，在推动互联互通、提高效率的同时，也在不断累积网络安全赤字。这种赤字的存在大大增加了系统性网络风险的不确定性，其对全球经济的潜在影响难以估量。

然而，当前数字产品设计制造领域普遍存在的问题是对网络安全的重视程度不够。许多制造商仍然将安全性视为一个事后考虑的问题，而非产品设计和开发过程中的核心要素。这种观念导致了一种以补丁和应急响应为主的被动安全实践，而非从根本上提升产品的固有安全性。这种做法不仅增加了后期维护的成本和复杂性，也为潜在攻击者提供了可乘之机。同时，由于数字产品市场粘性、技术迁移成本巨大以及数字生态系统被垄断企业隐形退化等原因，在处理器、操作系统、数据库、智能手机(硬件)、智能网联车、海底光缆安全等方面，数字产品生态系统同质化严重。制造侧“安全责任长期缺失”、数字产品“安全质量”难以保证、数字产品“同质化”,导致高度互联的数字化社会面临系统级风险。同质化产品单点失效可能引发大规模共模故障，进而导致上层服务全局崩溃。对于大规模、复

杂数字基础设施，关键要地/服务/支撑的单点缺陷被利用后，相关影响的二阶/三阶效应极易造成脆弱的数字化社会出现多米诺骨牌式的系统性安全事件。

国际社会面对这一严峻挑战，已经开始积极行动起来，各国政府和国际组织正通过制定和实施更严格的政策法规计划以加强对数字产品的安全质量监管，强制数字产品制造侧切实担负起设计安全、默认安全的责任，要求将安全视为包含数字元素产品的核心能力，贯穿整个产品设计过程，提出必须从根本上改变数字生态系统的底层驱动范式，建立一个可防御且富有弹性的数字生态系统，构建更安全、透明和可靠的数字产品供应链。这些举措旨在从源头上提高数字产品的安全性，推动建立更加健康和可持续的数字生态系统[1-4]。

在此背景下，本蓝皮书旨在深入分析当前网络安全战略与方法的发展现状和未来趋势，全面评估全球网络安全格局的变化。我们将重点识别我国在这一领域的先发技术优势，如内生安全、可信计算、数据加密等创新成果，同时也将客观分析我国面临的挑战和不足。通过深入探讨如何利用这些优势推动网络安全责任从用户侧向制造侧转移，如何构建中国特色数字产品安全监管体系，我们期望能够为建立全面的网络安全责任和质量控制体系提供有力支撑。这一转变不仅有助于提高数字产品的整体安全性，也将促进整个产业链的协同创新和升级。

1.2 网络安全威胁全球形势

近年来全球网络安全事件频发，对通信、政府机构、能源、交通、科技等多个关键领域造成严重影响。早在1996年，以色列就曾遥控引爆手机，炸死了哈马斯的炸弹制造专家叶海亚 • 阿亚什。2020年12月的SolarWinds 供应链攻击影响了全球超过250家企业，包括美国联邦机构和多家知名科技公司。2021年3月，针对苹果Xcode 的供应链攻击通过GitHub 上的开源项目植入后门，影响相关苹果手机应用程序。2022年3月意大利罗马特米尼火车站及米兰市多处火车站因黑客攻击导致电子信息显示屏故障和售票机无法售票，造成旅客混乱，火车站不得不安排工作人员使用扩音器提供指示和信息。2023年3月，3CX 软件供应商攻击影响了全球约60万家企业用户，涉及金融、工业、能源等多个行业。2023年7月，MOVEit Transfer的漏洞导致2706个组织遭到攻击，影响了政府、金融、IT 服务、能源、大学等多个行业的众多组织，受害者遍布美国、英国、

加拿大、法国、以色列等20多个国家和地区，超过9300万人的个人数据被泄露，Clop勒索软件团伙声称对此次攻击负责，这一事件被认为是2023年杀伤半径最大的供应链攻击。2023年以来，美联邦政府自导自演“伏特台风”事件，不断将网络攻击溯源问题政治化，作为打压中国的工具，我国网络安全机构于今年连续三次发布专题报告，彻底揭穿了美“歇斯底里”和“无底线”的对华政策[1-5]。

进入今年，网络安全事件频发，2024年1月，乌克兰利沃夫市市政能源公司遭受新型恶意软件攻击，导致集中供暖系统中断，市民生活两天无供暖保障。2024年3月，开源软件XZ 压缩库供应链攻击影响了使用Debian、Ubuntu 、Centos等多个 Linux 发行版的系统，同月，美国国家网络安全与基础设施安全局(Cybersecurity and Infrastructure Security Agency,CISA)遭受黑客攻击，黑客利用英万齐软件技术有限公司产品的安全漏洞侵入 CISA 网络系统，迫使CISA紧急关闭两个关键业务系统——基础设施保护网关和化学安全评估工具。2024年4月美国领先通信服务提供商边疆通信公司遭受网络攻击，迫使该公司关闭一些系统以防止威胁行为者横向移动，造成了严重的运营中断。2024年7月19日，美国“众击”公司旗下“隼”网络安全产品更新问题引发全球性信息基础设施中断事件，导致至少全球850万台使用微软视窗系统的设备大规模停止服务，事件规模已经超过了“心脏滴血”、“想哭病毒”等历史上最严重的网络安全事件，已造成数十亿美元的直接或间接经济损失，对全球社会和经济的长期影响难以估量。2024年9月17日和18日，黎巴嫩多地发生传呼机、对讲机等数字产品爆炸事件，造成至少37人死亡和2931人受伤，被视为全球首起基于供应链攻击的大规模数字设备武器化事件。随后，以色列发动“斩首”行动接连击杀包括真主党领导人纳斯鲁拉在内的18名真主党高级成员，展示了以方高超的情报战和科技战能力，以及情报信息与人工智能结合的认知域作战新方式。2024年10月，美国高通公司发布安全警告，称其多达64款芯片组中的数字信号处理器服务中存在一项潜在的严重“零日漏洞”(CVE-2024-43047)， 该漏洞影响范围广泛，涵盖了智能手机、汽车、物联网设备等多个领域。2024年10月12日，伊朗遭遇了严重的网络攻击，几乎所有政府部门的运作都受到了严重干扰，伊朗最高网络安全委员会的前秘书菲鲁扎巴迪表示，网络攻击影响了伊朗政府包括司法、立法和行政在内的几乎所有部门，许多重要信息被盗，伊朗的核设施以及燃料分配、

公共服务、交通和港口等关键网络也遭到攻击。2024年10月16日，中国网络空间安全协会发布《漏洞频发、故障率高应系统排查英特尔产品网络安全风险》一文，指出英特尔产品安全漏洞问题频发，可靠性差等问题，并揭示了英特尔产商假借远程管理之名，行监控用户之实，暗设后门，危害网络和信息安全等行为。

这些事件不仅暴露了当前网络安全防护体系的脆弱性，也凸显了网络安全威胁影响范围不断扩大、破坏性显著增强、以及政治化程度日益加深的趋势。上述事件表明，网络攻击的规模和波及领域迅速扩展，影响已不再局限于特定行业或区域，而是逐渐覆盖多个关键行业和全球范围的企业与政府机构，揭示出信息基础设施的高度相互依赖性。随着攻击技术的演进，网络安全事件的破坏力逐渐提升，超越了传统的数据泄露和系统中断，开始对关键基础设施乃至物理设备产生直接破坏，导致不可估量的经济损失与社会动荡。网络空间已成为国家间战略竞争的新前沿，网络攻击愈发成为国家博弈和政治对抗的工具。这一系列趋势表明，网络安全问题的复杂性和严重性持续上升，未来全球应对网络威胁的能力与策略将面临更大的挑战和压力。

1.3网络安全威胁为什么愈演愈烈

网络安全威胁呈现出愈演愈烈的态势，全球范围内的攻击频率、破坏力和复杂性不断上升，其背后的原因不仅涉及技术层面的挑战，还涵盖了数字生态系统的结构性问题、网络安全责任的缺失等多方面的原因：

1、数字技术安全悖论与底层固有缺陷的叠加效应

数字技术在提供前所未有的能力与效率的同时，不可避免地带来了安全隐患，数字系统的通信能力促进了协作与网络化，但也为潜在入侵者打开了大门，数据和控制的集中虽然提高了运营效率，却大大增加了单一攻击成功所造成的损害[1-6]。此外，数字系统底层技术的固有缺陷——存储程序控制构造的数字系统使得隐匿漏洞和后门难以避免，硬件和软件的复杂性创造了强大的功能，但这种数字技术的复杂性也产生了更多漏洞，降低了对入侵行为的可见性，现有网络安全防御技术限制无法彻底解决路径或状态爆炸问题。

2、多域交织且高度互联的数字化社会存在根深蒂固的脆弱性

物联网设备、关键基础设施以及信息系统的互联互通，使得攻击的范围和复杂性大大增加。认知域网络作战、数字产品武器化逐渐兴起，网络攻击不仅局限于信息系统本身，还通过信息操控、舆论引导等方式影响社会认知，甚至是将数字产品变身“遥控炸弹”发动恐怖袭击，这种跨越“物理、网络与认知域”的复杂联合攻击使得防御难度显著增加。高度互联的数字化社会存在根深蒂固的脆弱性，网络威胁的级联传导极易导致系统性安全事件，安全事件影响难以控制，给网络安全体系带来了前所未有的挑战。

3、数字产品设计制造安全责任缺失导致网络安全威胁失控

当前数字产品设计和制造商缺乏对网络安全的重视，进一步加剧了威胁的严重性，长期以来，数字产业一直秉承“先抢占市场、事后修补”的迭代逻辑，缺乏认真对待网络安全质量的动力往往“选择性忽视”产品设计制造中的网络安全问题，导致网络安全问题往往以附加方式被处理，数字产品已经陷入“补丁越补越多的恶性循环”。网络安全责任与风险的严重失衡，数字产品设计或制造商缺乏明确法定责任，导致安全技术的发展延缓和潜在威胁的滋生、扩展甚至是失控。

2国内外网络安全战略发展现状及趋势

2.1 全球网络安全环境概述

伴随着数字化进程的不断深化，全球网络安全环境呈现出高度复杂的特征。现今，网络安全不仅关乎信息的保护，更关系到国家安全、经济发展与社会稳定。网络威胁已不再局限于单一的技术层面，而是全面渗透到物理与认知领域，构成了多维度的安全挑战。

在此背景下，各国逐渐意识到，追求绝对的网络安全已显得不切实际。越来越多的网络攻击展示出其复杂性和隐蔽性，例如高级持续性威胁 (Advanced Persistent Threat,APT)和零日漏洞的利用，这些威胁不仅对单个组织构成威胁，甚至可能对国家安全产生深远影响。全球的网络安全工作重心正在从简单的防御转向构筑网络弹性，以应对不可避免的网络风险。

为了有效应对这一趋势，美欧等国家开始重构其网络安全战略。网络弹性已被视为核心理念，强调在遭受攻击后，系统能够快速恢复，并保持持续的业务运营。设计安全、零信任架构、供应链安全等新兴概念的提出，标志着网络安全责任从使用环节逐步转向设计环节，这不仅促进了安全乃至更广泛的风险管理理念在产品和服务中的内嵌，也反映出全球对网络安全重要性的重新认识。人工智能等新兴技术的发展，对网络安全既是机遇也是挑战。一方面，人工智能技术可用于增强威胁检测和响应能力，提高安全防护水平；另一方面，攻击者也可能利用人工智能技术发起更为复杂的攻击。同时，人工智能本身的安全性和可信性也成为新的关注点，需要建立相应的伦理和安全规范。

此外，地缘政治因素在全球网络安全环境中的作用愈发显著。各国间的网络竞争日益激烈，网络攻击时常作为国家间博弈的工具。这不仅增强了网络空间的不确定性，也对国际合作带来了挑战。在这样的大背景下，唯有通过建立开放、协作的网络安全治理体系，各国才能共同抵御网络安全威胁，确保全球网络空间的稳定和安全。

因此，在面向未来的全球网络安全战略中，强调合作、弹性与创新将是各国面临的重大课题，如何有效整合各方面的资源和力量，以共同维护网络安全，将是各国政府与组织亟需考虑的重要议题。

2.2美国网络安全战略

进入21 世纪第三个十年，全球战略格局发生深刻变化，大国战略博弈日趋复杂。在此背景下，美国国家安全战略实现了从单一领域威慑向综合威慑[2-1]的重要转型。这一转型的核心动因包括：对我国战略竞争进入新阶段、传统威慑效能相对弱化，以及新型安全领域带来的战略挑战等多重因素。

在新战略框架下，美国重新定位了网络威慑的战略地位。网络威慑通过展示强大的网络进攻能力和防御韧性，旨在塑造对手的战略选择与行为决策。特别是在“新三位一体”国家安全战略中，美国将网络威慑与核威慑、太空威慑并列为关键支柱，构建起涵盖常规、核、网络、太空、信息等多维度的“综合威慑”战略体系。为强化这一战略框架的实效性，美国正积极推进跨域能力建设与一体化运用，通过整合盟友和战略伙伴的外交、军事、情报等资源，打造新型威慑能力矩阵。

在具体的网络安全战略层面，美国正推动以网络弹性为核心的战略转型。这一转型体现了对网络空间攻防规律的深刻认知，即在高度复杂的数字环境中，仅依靠传统防御难以应对日益增长的网络威胁。因此，美国通过设计安全、零信任架构、供应链安全和人工智能等多维度协同，致力于构建一个可防御的、有弹性的数字生态系统。

2.2.1 网络攻击不可避免驱使安全向弹性转型

在数字革命持续推进的背景下，数字技术在提升控制能力和运营效率方面发挥着重要作用，但同时也显著增加了国家关键基础设施的脆弱性。随着技术创新加速和网络威胁日益复杂化，传统的网络安全防御方法已无法完全应对当前的安全挑战。考虑到技术进步的双面性、人为错误的不可避免性以及系统复杂性等因素，网络攻击已成为一种必须面对的客观现实。基于这种认知，美国开始从追求

绝对安全的传统思维转向更具实践意义的弹性战略，着力提升系统在预测、抵御、恢复和适应网络攻击及各类中断事件方面的综合能力。

在这一战略转向过程中，2013年成为美国网络弹性战略发展的关键节点。当年2月，美国发布第21号总统政策指令(PPD-21)《关键基础设施安全与弹性》，首次系统性地定义了弹性概念，将其阐释为“准备好应对并适应变化条件，承受破坏并从中快速恢复的能力”。这一定义为后续政策制定奠定了重要基础。在此指导下，国土安全部(Department of Homeland Security,DHS) 制定了2013版国家基础设施保护计划 (NIPP2013), 创新性地将安全和弹性统一纳入风险管理框架，并建立了完整的风险评估方法、防护措施和恢复机制。

随着实践的深入，美国不断完善其网络弹性政策体系。2019年11月，DHS与国务院联合发布《关键基础设施安全和弹性指南》,进一步细化了关键基础设施保护要求，为各行业部门提供了具体的实施指导。紧随其后，2021 年国家标准与技术研究院(National Institute of Standards and Technology,NIST)发布的网络弹性权威技术文件《开发网络弹性系统： 一种系统安全工程方法》[2-2],从技术层面规范了网络弹性建设要求，提供了具体的实施方法和技术标准。

进入2020年代，美国的网络弹性战略建设进入新的发展阶段。2022年9月，网络安全和基础设施安全局(Cybersecurity &Infrastructure Security Agency,CISA)发布《2023-2025战略规划》,确立了加强网络防御、减少风险和增强弹性、业务协作、统一机构等四大核心目标。2023年3月，美国政府新版《国家网络安全战略》提出了增强网络安全弹性的五大战略支柱，包括保护关键基础设施、塑造市场力量加强网络安全和弹性、通过战略投资和协调合作建立数字生态系统等。该战略特别强调了政府引导与市场机制相结合的方式，旨在构建更具弹性的网络空间。该战略通过两版《国家网络安全战略实施计划》(2023年7月和2024年5月)得到具体落实，涉及31个机构的100多项具体举措。

在推进网络弹性建设的过程中，美国也格外注重创新驱动。2023年12月美国国家科学技术委员会发布的《联邦网络安全研发战略规划》将以人为本的网络安全、可信度和网络弹性列为优先研发领域，体现了美国在该领域的创新导向。2024年2月美国总统科技顾问委员会发布的《网络物理弹性战略》报告进一步

提出了建立性能目标体系、加强研发协调、打破部门壁垒、提升私营部门参与度等四项核心措施。

2024年的政策发展显示了美国在网络弹性领域的持续努力。4月，美国政府发布的《关于关键基础设施安全和弹性的国家安全备忘录 (NSM-22)》 取代了PPD-21，建立了更全面的框架体系，明确了各方责任，并设立了16个关键基础设施部门。同年10月，CISA 发布2025-2026财年国际战略计划，强调通过国际合作提升全球网络安全和基础设施弹性。

值得注意的是，在民用领域大力推进网络弹性建设的同时，美国军方也将网络弹性防御视为维护国家安全的关键支柱。2023 年美国国防部的《网络空间战略》强调了增强联合部队网络弹性的重要性，提出通过零信任架构、现代化加密算法等技术手段提升系统弹性，并注重提高部队在网络受损环境下的作战能力。

在军事领域的具体实践中，2021年启动的安全与网络弹性工程项目(Security and Cyber Resiliency Engineering,SCRE) 发挥了重要作用。该项目采用全生命周期的安全理念，从设计阶段就开始考虑网络安全因素，建立了完整的军事系统网络弹性评估体系，开展了网络弹性技术研究，并将网络弹性要求纳入装备采购评估指标。这些举措不仅反映了美国对未来战争形态的深刻认识，也表明网络弹性已成为美国国家网络安全战略的核心组成部分。通过军事领域的具体实践，美国正在推动网络弹性理念的实质性落地。

通过民用和军事两个领域的协同推进，美国在网络弹性建设方面形成了完整的政策体系和实践经验，为应对日益复杂的网络安全挑战提供了有效解决方案。这种全方位的战略布局，充分体现了美国在网络安全领域从传统防御向综合弹性转型的决心和智慧。

2.2.2制造商责任失衡迫使内生安全设计

网络安全领域的范式正在发生深刻变革。2023年3月，美国《国家网络安全战略》明确指出，现有驱动美国数字生态系统的底层架构存在严重缺陷，必须从根本上改变数字生态系统的底层驱动，向防御优势方转变。该战略提出要彻底纠正市场失灵，重新平衡网络空间安全责任和风险，明确指出过去过分依赖最终用户承担网络安全责任的做法已不能适应当前的网络安全形势。战略强调将网络安

全责任向制造侧“左移”,要求“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，这实质上是对传统网络安全责任分配模式的重大调整。

为推进这一战略转型，美国政府随即采取了一系列具体行动。2023年7月，白宫发布《国家网络安全战略实施计划》,进一步细化了设计安全的具体实施路径，明确提出要推动开发安全设计和默认安全的原则和实践，由专门部门负责实施并设定时间节点，每年进行动态更新。该计划特别强调了产品全生命周期的安全管理，涵盖设计阶段的安全评估、开发过程的安全实践以及部署后的安全维护。2024年5月发布的第2版实施计划进一步完善了相关要求。

在国际合作层面，美国积极推动多边协作。2023年4月，CISA 与美国联邦调查局联合澳大利亚、英国、加拿大、德国等国家的网络安全机构共同发布了《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》,为软件产品的安全设计和配置提供了详细的技术指导。该指南强调，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。2023年10月的更新版本中，捷克、挪威等8个机构的加入进一步扩大了国际合作范围。

事实上，美国在特定领域已开始探索设计安全理念的实践应用。2022年6月，能源部发布的《国家网络知情工程(Cyber-Informed Engineering,CIE)》就鼓励能源部门采用“设计安全”思维方式，强调在系统早期阶段就将网络安全纳入考虑范围，而不是在部署后试图确保这些关键系统的安全。该战略建立在理念宣传、教育培训、技术创新、存量升级和增量转型五大支柱基础上。

在技术层面，美国特别关注内存安全问题。2023年12月，CISA 联合多国网络安全机构发布了《内存安全路线图案例》指南，指出约三分之二的软件漏洞源于内存安全编程的缺失，这促使软件制造商不得不持续发布补丁更新。该指南强烈建议软件制造商优先采用内存安全编程语言，制定内存安全路线图，修改软件开发生命周期，以逐步消除内存不安全代码。这一举措体现了设计安全的三个核心原则：承担安全责任、保持透明度和采用自上而下的方法，最终目标是从根本上消除此类安全威胁，更好地保护软件用户。

2024年的政策发展进一步深化了设计安全理念。2月，美国等十国联合发布6G 发展原则声明，将“设计安全”置于核心地位。声明强调，6G 技术开发必须采用系统性的网络安全方法，包括在技术标准、接口和规范中融入安全要素，确

保基本服务的可用性。同时，新一代通信技术需要充分考虑网络复杂性增加带来的潜在风险，着重解决更大攻击面可能带来的安全威胁，并将个人隐私保护作为设计的基本要求。同月，国家网络总监办公室发布的《回归构建块：迈向安全和可度量软件的途径》报告强调从软件构建的基础要素入手实现设计安全，包括：采用内存安全的编程语言来从源头消除内存安全漏洞，在特殊场景(如航天系统)下通过硬件方案来实现内存安全，以及使用形式化方法通过数学技术来证明软件的正确性。报告强调，与其在漏洞出现后被动修复，不如在设计阶段就主动消除整类漏洞，这样可以显著减少攻击面，提高代码可靠性，减少系统宕机时间，使系统行为更可预测。4月，CISA 加入最低可行安全产品工作组，为组织提供安全评估工具，这可以在很大程度上帮助确保遵循设计安全原则。

美国设计安全相关政策实施已取得了积极进展。2024年5月，美国《网络安全态势报告》显示，通过推进安全设计原则等措施，美国网络安全状况有所改善。同月，CISA 宣布68家全球领先软件制造商加入“设计安全承诺”计划，承诺在七个具体目标上展示可衡量的进展，包括加强多因素认证的使用、减少默认密码、降低漏洞类别、改进安全补丁安装、建立漏洞披露政策、及时发布CVE 漏洞信息以及提升客户收集网络安全入侵证据的能力。截至11月，参与企业数量已增至243家。

持续深化的国际合作也推动了设计安全理念的普及。2024年6月，CISA 与多国机构联合发布《探索关键开源项目中的内存安全》指南，为组织提供开源软件内存安全风险评估指导。9月，CISA 发布联邦民事行政部门运营网络安全调整计划，将防御性架构作为五大优先领域之一，该架构特别强调在设计网络基础设施时，应预料到安全事件的发生，并将弹性视为关键要素。10月，CISA 与 FBI 发布《产品安全不良实践》指南草案，要求软件制造商在2026年前发布内存安全路线图。指南将不良实践分为三大类：产品属性(如使用内存不安全语言开发、SQL 注入漏洞、默认密码等)、安全功能(如缺乏多因素认证、缺乏入侵证据收集能力)以及组织流程政策(如未及时发布CVE 漏洞信息和漏洞披露政策)。同月，CISA 又与澳大利亚等国联合发布《安全软件部署：软件制造商如何确保客户的可靠性》指南。该指南作为CISA 设计安全计划的一部分，详细概述了软

件安全部署的六个关键阶段，包括规划、开发测试、内部推广、部署和金丝雀测试、受控推广以及反馈规划。

种种政策举措反映出美国正在系统性地推进设计安全理念，通过政策引导、国际合作和具体实践，努力实现网络安全责任的有效“左移”,构建更加安全可靠的数字生态系统。

2.2.3身份信任危机引领零信任架构变革

零信任安全理念的兴起标志着网络安全思维模式的重大转变。该概念最早由Forrester研究公司的前分析师约翰 • 金德维格在2010年提出，其核心思想是“从不信任，始终验证”[2-3]。零信任架构以身份为基础，遵循最小权限原则，通过动态授权和访问控制，对企业数据和应用实施细粒度保护。这一理念可以较好地解决传统安全体系中过度信任和持续访问控制等问题，因此迅速成为网络安全领域的研究热点。

2019年成为零信任发展的重要转折点。这一年，零信任安全理念及其防护效能在网络安全行业获得广泛认可，并完成了初步的技术验证和实践探索。美国国家标准与技术研究院随即着手推动零信任的标准化进程，在2019至2020年期间相继发布了两版《零信任架构》[2-4]标准草案。

政府部门对零信任架构的推进呈现出系统化、制度化的特点。2021年2月，美国国家安全局发布《拥抱零信任安全模型》指南，强烈建议国家安全系统采用零信任安全模型。同年5月，拜登政府通过第14028号行政命令明确要求联邦政府机构实施零信任方法。2022年1月，管理和预算办公室发布《联邦政府零信任战略》,进一步细化了实施路径。2023年7月，Fortinet 发布的《2023年零信任状态报告》显示，尽管零信任部署比例稳步提升，但组织在实施过程中仍面临挑战，其中近31%的组织将访问延迟视为急需解决的重大问题。

在军事领域，美军对零信任架构的探索始于2020年之前，当时正在寻找替代联合区域安全堆栈 (Joint Region Security Stack,JRSS) 的安全方案。2019年零信任相关试验获得认可后，美军开始系统性推广零信任安全，将其作为支撑国防部数字化战略的重要手段。2021年5月，美国国防信息系统局 (Defense Information Systems Agency,DISA)和国家安全局零信任工程组发布《国防部零

信任参考架构》,为国防信息系统安全环境建设提供了指导框架。2024年5月，DISA发布的《DISA 2025-2029年战略计划》将零信任工具发展作为八大目标之一，预计到2027财年第四季度，DISA 的国防部信息网部分将符合零信任参考架构。

为确保零信任战略的有效落地，美军采取了一系列具体举措。2022年1月，成立国防部零信任投资组合办公室，负责制定迁移计划并统筹资源保障。同年11月，国防部发布《零信任战略》,提出了到2027财年全面实施零信任安全架构的战略愿景，确立了建立零信任文化、保护信息系统、加速技术部署和实现无缝协作四个总体目标。

在实践层面，美军于2021年7月启动了“雷霆穹顶”零信任安全试点项目。2022年1月，博思艾伦咨询公司获得680万美元合同，负责开发原型系统。该项目通过构建零信任原型，为大规模推广积累经验和树立示范。

近期，零信任架构的发展继续深化。2023年4月，网络安全和基础设施安全局发布《零信任成熟度模型2.0版》,旨在降低实施壁垒。2024年的发展进一步聚焦具体领域，4月国家安全局发布《在数据支柱中推进零信任成熟度》报告，强化数据安全指导。5月，CISA 发布加密DNS 实施指南，为联邦机构提供符合零信任战略的具体指导。10月，联邦首席信息安全官委员会和首席数据官委员会联合发布了一份具有里程碑意义的《零信任数据安全指南》,这是对管理与预算办公室2022年备忘录的重要响应。该指南由超过30个联邦机构和部门共同参与编写，主要面向系统所有者、管理员、数据管理者和网络安全工程师，提供了详细的零信任原则指导。指南强调数据是实施零信任的基础支柱，将安全重点从传统的边界防护转向数据本身的安全性，并提供了具体的数据保护行动建议和最佳实践，包括跨职能协作、持续学习和定期评估等内容，旨在帮助联邦机构在日益复杂的网络环境中更好地保护数据资产。

这一系列持续演进的政策和实践表明，美国正在政府和军事两个层面系统推进零信任安全架构的应用。从最初的概念探索到现在的全面实施，零信任已经发展成为应对复杂网络安全威胁的重要策略选择。通过建立完整的政策框架、开展试点示范、推动技术创新，美国正在构建一个更加安全可靠的网络防护体系。

2.2.4地缘政治博弈加速供应链安全重构

供应链安全已成为美国国家安全战略的重要支柱。2023年美国国家科技委员会在《联邦网络安全研发战略规划》中明确指出，当前网络弹性实施在安全供应链等方面仍存在不足，并将保护软件和硬件供应链列为三大优先应用场景之一。这一认识是建立在多年实践和政策演进基础之上的。

早在2018年12月，美国就已开始系统性布局供应链安全。网络安全和基础设施安全局(Cybersecurity and Infrastructure Security Agency,CISA) 成立信息和通信技术(Information and Communications Technology,ICT)供应链风险管理工作组，致力于增强国家关键基础设施的 ICT 供应链安全性，促进信息共享，提高风险认知。2019年5月，第13873号行政命令的签署进一步强化了这一方向，要求联邦政府防范外国势力利用ICT 供应链漏洞，保护敏感信息安全。

拜登政府上台后，供应链安全政策进入快速发展期。2021年2月发布的第14017号行政命令《美国供应链行政命令》强调建立“弹性、多样化和安全的供应链”,将供应链弹性提升至国家战略高度。同年5月的《关于改善国家网络安全的行政命令》进一步聚焦软件供应链安全，要求建立软件开发基准安全标准，并创建类似“能源之星”的安全标签认证机制。

2023年成为供应链安全政策的重要里程碑。9月，CISA 联合国家安全局发布《保护软件供应链：软件物料清单消费的推荐做法》,通过持久安全框架为软件开发商和供应商提供最佳实践指南，包括管理开源软件和软件物料清单 (Software Bills of Materials,SBOM),以维护和提供对软件安全性的认识。同时，CISA 还发布了新的硬件物料清单 (Hardware Bill of Materials,HBOM) 框架，为供应商和采购商提供标准化的硬件组件风险评估工具。

2024年，美国进一步完善供应链安全治理体系。6月，拜登总统签署行政命令成立白宫供应链弹性委员会，要求每四年对关键行业进行供应链审查，首份报告将于2024年底提交。同月，能源部与爱达荷国家实验室合作发布供应链网络安全原则，分别是：影响驱动的风险管理、基于框架的防御、网络安全基础、安全开发与实施、透明度与信任建设、实施指南、生命周期支持与管理、主动漏洞管理、主动事件响应，以及业务与运营弹性。该原则得到包括 GE Vernova、施耐德电气等在内的多家能源行业供应商支持。

在具体实施层面，2024年8月CISA 发布《政府企业消费者软件采购指南》，聚焦软件生命周期活动中的安全保障。随后，CISA 与 FBI 联合发布《需求安全指南》,强调软件物料清单的标准化和开源组件的安全审查。9月，CISA 发布的联邦民事行政部门运营网络安全调整计划将网络供应链风险管理列为五大优先领域之一，特别强调快速识别和降低第三方风险。

2.2.5 智能技术革新驱动网络安全新布局

在人工智能快速发展的背景下，美国政府对AI 的战略布局经历了系统性演进，从确立领导地位、完善监管框架到推动安全发展，体现了在把握发展机遇的同时，着力防范相关风险的战略考量。

美国政府最早通过2019年2月签署的第13859号行政命令《保持美国在人工智能 (Artificial Intelligence,AI) 领域的领导地位》确立了AI 发展的战略基调。该命令要求预算管理办公室 (Office of Management and Budget,OMB) 制定 AI 应用监管指南，并将 AI 列为研发投资、数据共享和劳动力发展的优先领域。随后在2020年1月，OMB 发布的《备忘录M-21-06》进一步细化了监管指导框架。

2020年成为美国 AI 政策框架的关键转折点。这一年9月美国国会通过的《2020年人工智能政府法案》提出建立AI 卓越中心，推动政府采用AI 技术。到了12月，《2020年国家人工智能倡议法案》更是提供了数十亿美元支持 AI 研发，并授权NIST 开发AI 风险管理框架。在同一个月签署的第13960号行政命令中，政府确立了联邦机构使用AI 的九项核心原则，强调合法性、安全性和问责制，为后续发展奠定了基础。

随着AI 技术的深入发展，美国政府开始更加关注制度建设和安全保障。2022年10月，白宫科技政策办公室发布《人工智能权利法案蓝图》,提出确保系统安全、防止歧视、保护隐私等五项原则，强调在推动创新的同时要保护公民权利。进入2023年，NIST 发布AI 风险管理框架1.0版(AIRMF 1.0)[2-5],为 AI 产品和系统的全生命周期管理提供了具体指导。

2023年美国政府先是在7月和9月与15家领先AI 公司达成自愿性承诺，确立了安全性、保障性和信任三个基本原则，具体包括在产品发布前进行内部和

外部安全测试、投资网络安全保护措施、开发水印等技术机制识别AI生成内容、公开报告AI系统能力和局限性、优先研究社会风险等内容。10月签署的第14110号行政命令则对AI发展与管理做出全面部署，提出八项指导原则，涵盖安全评估、创新竞争、人才吸引等多个方面，其中包括建立AI安全测试机制、促进AI研发创新、简化AI人才签证程序、加强AI应用监管以及推动国际合作等，旨在巩固美国在全球AI发展中的领导地位。11月，美国国家安全局人工智能安全中心联合CISA、FBI以及来自澳大利亚、加拿大、新西兰、英国等23个网络安全机构共同发布《安全人工智能开发指南》,它是对美国确保安全、可靠AI自愿承诺的重要补充。这份指南强调了“设计安全”原则，适用于所有类型的AI系统，不仅限于前沿模型，为数据科学家、开发人员、管理者、决策者和风险所有者提供了关于AI系统安全设计、模型开发、系统开发、部署和运营方面的建议和缓解措施。CISA同时发布了AI路线图，展示了其对AI技术和网络安全的战略愿景，并邀请所有利益相关者、合作伙伴和公众共同探讨这份指南。

进入2024年，美国进一步推进AI安全战略的具体落地。4月，能源部发布AI在关键能源基础设施中的应用评估报告。报告指出，AI技术可以显著改善能源部门的安全性、可靠性和弹性等方面，但同时也识别出了四类主要风险：AI意外故障、对抗性攻击、恶意应用和软件供应链泄露。同月，美国-欧盟就AI治理达成合作共识，并重申了基于风险的人工智能监管方针，标志着国际合作进入新阶段。7月，NIST发布了NIST-AI-600-1《人工智能风险管理框架：生成式人工智能概况》[2-6],它可以帮助组织识别生成式AI带来的独特风险，并提出最符合其目标和优先事项的生成式AI风险管理行动。与此同时，能源部启动“科学、安全和技术人工智能前沿计划”(Frontiers in Artificial Intelligence for Science, Security,and Technology,FASST),该计划将依托DOE的17个国家实验室和先进的超级计算基础设施，建立世界上最强大的综合科学AI系统，服务于科学、能源和国家安全领域。FASST计划将把DOE用户设施产生的大量科学数据转化为AI就绪数据，并建设新一代高能效AI超级计算机，为包括4万名国家实验室科学家在内的研究人员提供可信的基础AI模型开发平台。

最新的重要进展出现在2024年10月，美国政府发布《人工智能国家安全备忘录》,提出了三大核心目标：确立美国在安全、可靠的人工智能发展方面的全

球领导地位；合理运用人工智能实现国家安全目标；以及培育稳定、负责任的国际人工智能治理环境。备忘录要求各政府部门建立完善的AI 安全评估和风险管理框架，设立首席 AI 官员和 AI 治理委员会，加强跨部门协调，并与盟友合作推动建立国际 AI 治理标准。该备忘录强调了 AI 技术在国家安全方面的多种应用，包括网络安全、反间谍、后勤支持和军事行动。

2.3欧盟网络安全战略

欧盟在网络安全战略方面，通过建立系统性的立法框架，构建起全方位的网络安全防护体系。纵观欧盟的网络安全战略演进，其核心特征在于以立法为抓手，通过法律规制推动安全治理的制度化、规范化发展。2020年，欧盟发布《关于关键实体弹性的法案草案》和《未来数字化十年的网络安全战略》等，要求所有联网设备在设计上确保安全，对网络攻击具有弹性，并能迅速发现和修补漏洞。这些文件的出台标志着欧盟将网络安全从事后补救转向事前预防，体现了其在网络安全治理上的前瞻性思维。

在这一战略框架下，欧盟陆续推出了一系列具有里程碑意义的立法举措。欧盟于2020年9月提出《数字运营弹性法案》(Digital Operational Resilience Act, DORA) 提案，并于2022年11月获欧盟理事会通过。该法案主要针对金融服务生态系统，要求金融机构和关键信息通信技术服务提供商实施全面的网络弹性措施。具体而言，DORA 要求建立完整的ICT 风险管理框架，实施定期的网络弹性测试，建立统一的事件报告机制，并对关键ICT 服务提供商实施监管。同时，法案特别强调了第三方风险管理的重要性，要求金融机构对其 ICT 服务提供商进行有效管理和监督。

进一步深化网络安全立法的重要成果是2022年9月发布的全球首个《网络弹性法案》。该法案经过多个阶段的审议和完善，于2023年12月达成一致，2024年3月获得欧洲议会批准，并于2024年10月获得欧盟理事会批准。法案采用分阶段实施策略：在生效后的21个月内，所有数字产品制造商将需承担报告主动利用的漏洞和相关事件的义务；36个月后，进入欧盟市场的数字产品必须满足网络弹性方面的强制要求，其中要求制造商需制定一份以常用格式编制的软件物

料清单 (Software Bills of Materials,SBOM), 至少涵盖产品的顶层依赖关系，SBOM 应包含在技术文档中，并在要求时提供给市场监管机构。

在欧盟成员国层面，各国也积极响应欧盟的战略部署。英国在2022年密集发布了《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》等文件，将网络弹性列为重要支柱。德国着重强化关键基础设施保护，法国推进数字主权建设，北欧国家则积极推进区域性合作，形成了多层次的网络安全防护体系。

这些政策措施的实施产生了广泛的积极影响。首先，显著提升了欧盟数字产品的整体安全水平；其次，推动了网络安全产业的发展，激发了创新动力；第三，促进了国际网络安全标准的统一化进程；最后，增强了数字供应链的透明度和可追溯性。然而，政策实施也面临着一些挑战，包括技术标准的统一与协调问题、中小企业的合规成本压力、跨境执法的协调机制建设，以及与国际贸易规则的协调等。欧盟的实践表明，将网络安全要求纳入法律框架是提升整体安全水平的有效途径。通过建立多层次、多领域的法律体系，欧盟正在构建一个全面的网络安全防护网络。将安全要求前移到设计阶段的做法，体现了对网络安全治理的前瞻性认识，也为全球网络安全治理提供了重要借鉴。

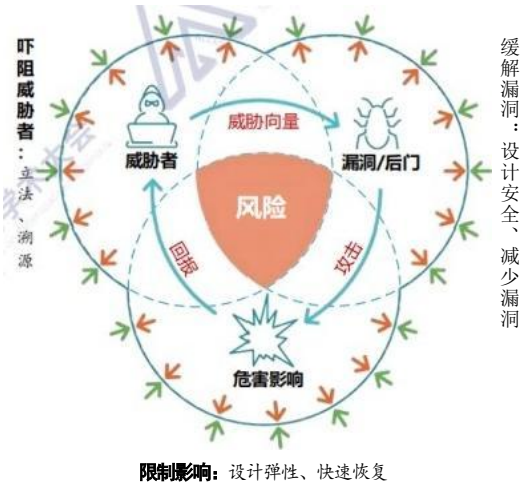

图2-1 欧盟JRC提出的网络安全风险各组成部分之间的逻辑联系概念模型

欧盟的网络弹性和设计安全理论主要基于欧盟委员会联合研究中心 (Joint Research Centre,JRC) 在2020年发布的研究报告《网络安全——我们的数字之锚》[2-7]。该报告汇集了 JRC 不同学科领域的研究成果，在新冠疫情带来新的网络安全挑战的背景下，为塑造欧盟数字社会的未来提供了重要的理论基础和政策建议。

报告提出的网络安全风险演变概念模型将风险定义为两个主要因素的组合：负面网络事件发生的可能性以及此类事件的潜在后果。即使某个事件发生的可能性不大，但如果其影响巨大，由此产生的风险仍然非常显著。基于这一认识，该报告提出网络安全风险演变概念模型(如图2-1所示),将网络安全风险缓解策略概括为威慑威胁行为者、缓解漏洞和通过网络弹性限制影响三个方面。其中，设计安全、默认安全、漏洞管理及弹性设计构成了风险缓解策略的核心原则。这一模型为理解和应对网络安全风险提供了系统性的框架。

在设计安全和默认安全方面，报告强调了“安全性设计”原则的重要性。这要求系统的默认配置必须采用最安全的设置，即使最终用户并不知晓或无需启用这些设置。例如，社交网络平台应该将用户的个人资料默认设置为最注重隐私的选项，从一开始就限制第三方访问用户的个人信息。这一建议直接影响了欧盟后续的数据保护和网络安全政策制定。

在网络弹性方面，报告指出弹性不仅是工程和技术系统设计的问题，更与社会维度密切相关。报告强调，欧洲社会的网络弹性很大程度上取决于个人公民的行为，这一观点推动了欧盟在网络安全教育和能力建设方面的政策发展。特别是在2016年NIS 指令通过后，欧盟显著加强了对网络安全的重视，进一步推动产业和相关参与者减少漏洞并加强弹性建设。

报告的这些核心观点为欧盟制定跨部门、跨社会的网络安全战略提供了重要指导。在欧盟层面，网络安全被定义为“保护网络和信息系统、此类系统的用户以及受网络威胁影响的其他人所必需的活动”。这一定义反映了报告中强调的全面性思维，即网络安全不仅是基础研究(如密码学)的问题，也是技术、社会立场、教育、文化和政策的综合性议题。

这份报告对欧盟网络安全政策产生了深远影响，推动欧盟在网络安全设计和部署方式上进行了范式转变，使其更具前瞻性，更好地与社会需求相联系。特别是在合作机制、知识共享、教育培训等方面的建议，为欧盟构建更具韧性的网络空间提供了重要的理论支撑和实践指导。

在供应链安全方面，2024年5月欧盟议会通过的《企业可持续发展尽职调查指令》(也被称为欧盟“供应链法案”)要求在欧盟运营的公司对其自身、子

公司及价值链中的业务伙伴活动进行全面的尽责管理，预计最早将于2026年下半年开始实施。

随着人工智能技术的快速发，欧盟于2024年7月发布《人工智能法案》，开创性地建立了全球首个综合性AI 监管框架。该法案采用基于风险的分级管理方法，将 AI 系统分为不可接受风险、高风险、有限风险和最小风险四个等级，并针对不同风险级别制定相应的监管要求。该法案重点关注高风险AI 系统的管理，要求其在投放市场前必须满足严格的要求，包括风险评估、数据质量和人工监督等；同时规定了透明度义务，如要求聊天机器人明确告知用户其机器身份，AI生成内容必须明确标识等。该法案于8月1日生效，并将在2年后(2026年8月2日)完全适用，但有一些例外：禁令将在6个月后生效，通用AI 模型规则12个月后适用，并由2024年2月在欧盟委员会内成立的欧洲人工智能办公室负责监督实施。该法案是支持可信赖AI 开发的更广泛一揽子政策措施的一部分，其中还包括AI 创新包和AI 协调计划。这些措施共同保障了人们和企业在AI 方面的安全和基本权利。它们还加强了整个欧盟对AI 的吸收、投资和创新。

2.4 中国网络安全战略

十年来，在习近平总书记关于“网络安全和信息化是一体之两翼、驱动之双轮”等一系列重要思想指引下，我国网络安全事业取得了历史性成就。特别是在“没有网络安全就没有国家安全”的战略定位下，我国初步构建了网络安全“四梁八柱”,走出了一条具有中国特色的网络安全发展道路。这一发展道路既体现了中国智慧，也为全球网络空间治理贡献了中国方案。

在战略规划方面，我国构建了以《国家网络空间安全战略》为统领的顶层设计体系。2016年中共中央办公厅、国务院办公厅印发的《国家网络空间安全战略》,明确了维护国家网络空间主权、安全和发展利益的总体要求，提出了九大战略任务。这一战略规划充分体现了总书记关于网络强国的重要思想，为我国网络安全事业发展指明了方向。特别是在数字经济蓬勃发展的新时期，该战略更加突出了发展和安全的辩证统一，强调了高质量发展与高水平安全的良性互动。

在法律体系建设方面，我国已经形成了以《中华人民共和国网络安全法》为基础，《数据安全法》、《个人信息保护法》等法律法规为支撑的网络安全法律

体系，同时出台了《网络安全审查办法》《云计算服务安全评估办法》《汽车数据安全管理若干规定(试行)》《生成式人工智能服务管理暂行办法》等一系列政策文件作为补充。这一体系不仅明确了网络运营者的安全责任，而且对个人信息和重要数据的保护提出了具体要求，实现了从技术治理向法治化治理的重要转变。特别是在数据安全和个人信息保护方面的立法，充分体现了我国对数字时代公民权益保护的高度重视，也为全球数据治理提供了中国经验。

在关键信息基础设施保护方面，我国建立了完善的制度保障体系。通过实施网络安全等级保护制度[2-8]和关键信息基础设施安全保护制度，构建起了全方位的防护体系。2021 年国务院颁布的《关键信息基础设施安全保护条例》进一步细化了保护要求，明确了各相关部门的职责分工，为提升关键信息基础设施安全防护能力提供了制度保障。这些制度的实施显著提升了我国网络空间的整体安全性和韧性，为数字经济的健康发展提供了坚实保障。

在技术创新方面，我国取得了一系列具有国际影响力的原创性突破。在“十四五”规划的指导下，我国重点布局了安全度量、内生安全、抗量子密码等前沿领域的研究。在拟态防御、数据加密等关键技术领域取得重要突破，部分技术达到国际领先水平。同时，我国积极推进网络安全标准化工作，建立了涵盖基础通用、关键技术、安全管理、产品应用等各个层面的标准体系，为产业发展提供了有力支撑。

在产业发展方面，我国推动网络安全产业实现了跨越式发展。通过实施《“十四五”数字经济发展规划》等政策措施，培育了一批具有国际竞争力的网络安全企业，形成了完整的产业生态链。特别是在新一代信息技术与网络安全深度融合方面，我国推动人工智能、区块链等技术在网络安全领域的创新应用，催生了一批新的安全防护模式和解决方案。

在人才培养方面，我国建立了多层次的人才培养体系。通过设立网络安全学院、推动产学研合作等方式，培养了大批高水平网络安全人才。同时，通过举办网络安全竞赛、建设实训基地等方式，提升了全社会的网络安全意识和技能水平。这些措施为我国网络安全事业的持续发展提供了人才保障。

在国际合作方面，我国积极推动构建网络空间命运共同体。通过提出“四项原则”和“五点主张”的中国方案，为全球网络空间治理提供了中国智慧。我国

积极参与联合国框架下的网络安全国际规则制定，推动建立公平、民主、透明的国际网络治理体系。通过“一带一路”数字丝绸之路建设，深化了与沿线国家在网络安全领域的务实合作，推动形成了互利共赢的合作格局。

在中国发展、安全、文明“三大倡议”指引下，我国的网络安全实践不断深化和完善。通过构建全方位、多层次的网络安全体系，我国在维护网络主权、保障数字经济发展、保护公民权益等方面取得了显著成效。“建设包容、普惠、有韧性的数字世界”的中国方案，已经成为推动全球数字生态系统转型的重要力量，为构建网络空间命运共同体作出了重要贡献。

2.5网络安全战略发展趋势分析

随着数字技术在社会各领域的广泛渗透以及人们对网络安全问题认知的不断深化，网络安全正由一种技术选择项 (technological option) 演变为社会必需项 (societal must)。这一转变推动了网络安全战略的重大调整，主要体现在五个方面：网络安全目标向网络弹性范式转变，安全责任由用户侧向制造侧转移，安全发展聚焦以人为本、可信度和网络弹性等关键领域，加强供应链安全和人工智能技术在网络安全中的应用与发展。这些趋势反映了网络安全战略在应对日益复杂的数字环境挑战时的系统性思考和前瞻性布局。

1. 网络安全目标致力于向网络弹性范式转变

在当前复杂多变的网络环境中，完全避免网络攻击已不现实。网络安全的目标正在经历一个重要的范式转换，从单纯阻止网络事故的发生转向缓解事故带来的危害，从被动抵御攻击转变为主动保障业务连续性、可用性和快速恢复能力。这种转变体现了对网络安全更加全面和动态的理解。

美国网络安全战略明确提出了向网络弹性范式转变的目标，将网络安全、可信度和任务生存能力视为系统设计和使用中的基础要素。该战略强调网络弹性必须内置于系统架构和管理中，与功能和性能同等重要。同时，欧盟正加快制定网络弹性法案，要求数字产品制造商实施网络弹性设计，并对因产品设计缺陷导致的网络安全事故承担责任。这些政策举措反映了主要发达国家对网络弹性重要性的共识。

各国积极推进网络弹性科学研究，致力于确定网络弹性的基本属性和指标要求，描述影响网络弹性的各种因素间的相互作用，并强调将人类及社会的需求纳入考虑范围。这种全方位的研究方法有助于构建更加完善的网络弹性评估体系，为政策制定和实践提供科学依据。

2. 网络安全责任由用户侧到制造侧转移

随着数字化转型的深入推进，以高级持续性威胁(Advanced Persistent Threat, APT) 和零日漏洞(0 day)为代表的网络安全问题日益突出，其规模和危害程度不断升级。更为严重的是，数字制造商的安全责任失衡问题愈发明显，部分企业将经济利益置于产品安全之上，选择性忽视潜在的安全风险。

欧盟委员会联合研究中心的报告指出，“数字行业缺乏有效竞争，且容易出现激励错位。”一方面，数字产品为了迅速占领市场，往往忽视安全性；另一方面，由于用户粘性强，产品更换成本高，这种“胜者通吃”的网络效应进一步加剧了制造商忽视产品安全性的倾向。美国2023年发布的《国家网络安全战略》中明确指出，“现有驱动美国数字生态系统的底层架构存在严重缺陷。”

为应对这些挑战，美欧国家提出了“设计安全”的概念，旨在从源头上解决网络安全问题。这一概念的提出反映了对网络安全责任的深刻反思，强调将安全责任从用户侧转移到制造侧。美国CISA 执行总监在2023年2月的演讲“停止在网络安全问题上推卸责任”中强调，企业必须将安全融入科技产品，体现了美国在这一问题上的坚定立场。

美欧认为，传统的“外挂式”网络安全方法已不能满足当今数字化转型的需求。只有通过制造侧发力，在系统工程的早期阶段就将网络安全问题纳入考虑，才能最大程度地降低网络安全风险。这种思路转变标志着网络安全策略正在向更加主动、系统的方向发展。

3. 网络安全发展聚焦以人为本、可信度、网络弹性等关键领域

随着网络攻击手段的不断演进，越来越多的攻击开始利用最终用户的行为特征、无意识错误和心理倾向。这一趋势凸显了以人为本的网络安全方法的重要性。该方法强调在确定信息技术系统的目的、设计、操作和安全选择时，必须将人的需求、动机、激励、行为和能力放在首位。这种方法不仅有助于提高系统的安全性，还能增强用户体验和系统的整体效能。

在网络空间中，确定实体的可信度以及建立各方和各组成部分之间的信任机制仍是一个亟待解决的问题。当前零信任战略通过“永不信任，始终验证”的理念，将网络安全从传统的边界防护转向基于身份和行为的动态信任评估，但还不足够。未来的网络安全发展需要建立能够在所有计算层中执行所需信任级别的机制，从硬件层开始，涵盖操作系统、软件应用程序、网络等各个层面，以及电子商务、社交媒体等服务。这种全方位的信任机制将为构建更安全、可靠的网络环境奠定基础。

网络弹性已成为任务和业务保障总体战略中的关键因素。未来的网络安全战略必须超越传统的预防、保护和恢复模式，更加关注如何有效地设计、开发和运行系统，使其能够在面对持续攻击甚至系统受损的情况下仍能维持适当水平的任务执行能力。这种转变要求我们重新思考系统设计的原则，将网络弹性作为核心属性嵌入到系统的每个层面。

4.网络安全布局强化供应链安全

随着全球化和数字化的深入发展，供应链的复杂性和互联性日益增加，供应链安全已成为网络安全战略中的关键关注点。近年来，供应链攻击事件频发，攻击者利用供应链环节中的脆弱性，对目标系统实施攻击，造成严重后果。因此，加强供应链安全已成为各国网络安全战略的重要趋势。

美 国CISA 在2024年9月发布的联邦民事行政部门运营网络安全调整计划中，将网络供应链风险管理列为五大优先领域之一，特别强调要快速识别和降低对联邦IT 环境构成的风险，包括来自第三方的风险。同时，美国政府还推出了软件供应链安全相关政策，要求检查制造商是否以标准的、机器可读的格式生成软件物料清单，并审查其所包含的开源软件组件的安全性。

欧盟通过一系列法律法规，构建了全面的网络安全防护网络。特别是在供应链安全方面，欧盟要求所有联网设备在设计上确保安全，对网络攻击具有弹性，并能迅速发现和修补漏洞。这种将安全要求前移到设计阶段的做法，体现了对网络安全治理的前瞻性认识。

为加强供应链安全，各国主要采取以下措施：强化供应链风险评估与管理，建立全面的供应链安全审查机制；推进供应链透明化，增强对软硬件组件来源的

可追溯性；制定和实施供应链安全标准与合规要求；加强国际合作，构建全球供应链安全合作机制。

5. 网络安全战略注重人工智能技术的应用与发展

随着人工智能(Artificial Intelligence,AI)技术的迅猛发展，其在网络安全领域的应用和影响日益凸显。 一方面，AI 技术为网络安全提供了全新的解决方案，例如利用机器学习和深度学习算法进行威胁预测、入侵检测和异常行为分析，大幅提升了网络防御的效率和准确性。另一方面，AI 也被不法分子利用，生成更为复杂和难以检测的网络攻击，如利用生成对抗网络创建高级伪装的攻击代码或采用自动化工具进行大规模攻击。

各国在网络安全战略中高度重视AI 技术的双重作用。美国在2024年的《人工智能国家安全备忘录》中提出要建立完善的AI 安全评估和风险管理框架，并强调了AI 技术在国家安全方面的多种应用，包括网络安全、反间谍、后勤支持和军事行动。欧盟则通过《人工智能法案》规范AI 技术的开发和应用，确保其安全性、可靠性和伦理合规性。我国在《新一代人工智能发展规划》等政策中也提出，人工智能在安全领域有广泛应用潜力，可准确感知、预测、预警基础设施和社会安全运行的重大态势，及时把握群体认知及心理变化，主动决策反应，显著提高社会治理的能力和水平，对有效维护社会稳定具有不可替代的作用。但同时也指出，人工智能作为影响面广的颠覆性技术，可能带来侵犯个人隐私、挑战国际关系准则等问题，对政府管理、经济安全和社会稳定乃至全球治理产生深远影响。因此，在大力发展人工智能应用于网络安全的同时，必须高度重视可能带来的安全风险挑战，加强前瞻预防与约束引导，最大限度降低风险，确保人工智能安全、可靠、可控发展。

加强AI 在网络安全中的应用，主要包括以下措施：加大对 AI 安全技术的研发投入，提升对新型网络威胁的感知和应对能力；建立 AI 技术的安全标准和伦理规范，防范 AI 技术的滥用和潜在风险；培养跨学科的专业人才，促进 AI 与网络安全领域的协同创新；加强国际合作，构建针对AI 相关安全问题的全球治理机制。

总之，网络安全战略的这些发展趋势反映了对网络安全更加全面、系统和前瞻性的认识。通过向网络弹性范式转变、将安全责任转移到制造侧、聚焦以人为

本、可信度和网络弹性等关键领域，加强供应链安全，以及强化人工智能技术在网络安全中的应用和发展，网络安全战略正在适应日益复杂的数字环境，为构建更安全、更可靠的网络空间奠定基础。这些趋势的深入发展将持续推动网络安全领域的创新和进步，为数字时代的安全保障提供新的思路和方法。

3 国内外网络安全技术发展现状及趋势

3.1 国外网络安全技术发展现状

随着当今的社会活动越来越依赖于复杂且相互关联的网络系统和数字基础设施，网络安全威胁种类越来越多，规模越来越大，造成的损失也越来越严重。由于潜在安全威胁的不可预测性，极度不确定性和快速演变的特性，人们逐渐认识到要保证网络空间绝对安全是不现实的。国内外网络安全研究机构正积极探索和实践新型安全架构与技术，以提升整体网络防御能力和应对未来网络安全挑战。本节将重点阐述三种在国际网络安全领域备受关注的前沿技术：网络弹性(Cyber Resilience)[3-1]、设计安全(Security by Design)[3-2]以及零信任(Zero Trust)[3-3]。

3.1.1 网络弹性技术

面对当今日益严峻的网络安全形势，欧美国家逐渐认识到，传统的网络安全范式追求绝对安全或“不破防”的目标是不现实的。在复杂多变的网络攻击环境中，必须从单纯抵御攻击转向保障业务连续性和可用性，构建快速恢复能力，以尽可能维持业务的正常运营。因此，网络弹性已受到各国政府和网络安全产业的高度关注，对网络安全的创新以及信息化的可持续发展产生越来越深远的影响。

网络弹性被定义为系统在面对网络攻击以及自然或意外中断时，预测、抵御、恢复和适应的能力[3-4]。它通常被视为弹性工程、网络安全和任务保障工程的交叉产物，具备以下五个独特特征：(1)聚焦于任务或业务功能；(2)关注复杂攻击（如 APT) 的影响；(3)假设环境不断变化； (4)假设攻击者一定能攻破系统；(5)假设攻击者长期存在。网络弹性特别聚焦于复杂系统和极端不利环境等场景，形成独特的研究领域。

与传统网络安全相比，网络弹性强调从任务视角保障系统能力。它不仅关注防止攻击和保护数据，更重视在防护失效时如何确保关键任务的持续完成。这意味着，即使遭遇网络攻击或系统故障，组织依然能够迅速调整和恢复运作，从而保持业务连续性。因此，网络安全与网络弹性相辅相成，前者提供防御，后者确保在防护失效时的恢复与应对能力。两者之间的关系体现为从传统安全到弹性的

连续体过渡，这一转变强调在传统框架基础上进行微调，例如通过“连续运营计划”来确保备份的安全，而非留下后门。同时，网络弹性通过新颖或增强的方法来实现安全能力，例如利用人工智能提升入侵检测、运用防火墙和微分割技术构建安全的内部飞地。它还借鉴了其他学科的应对策略，如体育和军事中的误导信息与欺骗环境，以及随机改变行为来迷惑攻击者。此外，通过引入随机编译器、多个操作系统和虚拟化技术，网络弹性有效应对非对抗性威胁，增强系统的多样性和生存能力。

网络弹性技术的发展历史如下：2010年，美国MITRE 研究所发表了《构建安全的、弹性的架构以实现网络使命保障》一文，强调保护任务关键功能的连续性，并指出必须考虑在防护失效时采取补偿措施，以确保在遭受攻击的情况下仍能实现关键功能。此外，文章提到应结合弹性架构和弹性运营，以应对所有的“未知的未知”(unknown unknown)。2011年，《网络弹性工程框架》(Cyber Resiliency Engineering Framework)首次提出网络弹性工程和网络弹性工程框架的概念，其中网络弹性工程是弹性工程、网络安全和任务保障工程三个学科交叉融合的结果。2017年，MITRE 在《网络弹性设计原则》(Cyber Resiliency Design Principles)中提出了一系列具有代表性的设计原则，这些原则可在整个系统生命周期中以不同的方式和程度进行应用。网络弹性与弹性工程、任务保障、网络安全防护、业务连续性和备份恢复等领域密切相关，不仅关注应对外部网络攻击，还注重系统的健壮性与可靠性。2018年，MITRE 发布了网络弹性评估指标(Cyber Resiliency Metrics) 系列文件，描述了近500个具有代表性的指标，用于评估系统方案、技术、产品或流程的弹性能力，以提高系统的网络弹性和任务保障能力。

2021年，美国国家标准与技术研究院 (NIST) 正式发布了《开发网络弹性系统——一种系统安全工程方法》 (NIST SP 800-160V2R1)[3-5],标志着网络弹性领域首个权威技术文件的问世。同年，美国国防部启动了安全与网络弹性工程 (Secure Cyber Resilient Engineering,SCRE)项目，截至目前已发布18本蓝皮书，提出了美国武器装备系统的网络弹性战略考量、可信设计原则和损失控制设计原则等。2023年12月，美国国家科学技术委员会 (National Science and Technology Council,NSTC)发布了《网络安全研发战略计划(2024-2027)》，梳理了网络弹性的发展趋势，并制定了推进网络弹性科学、通过设计提高网络弹

性和提升运行期间的网络弹性等研究目标，为未来美国网络弹性的发展指明了方向。

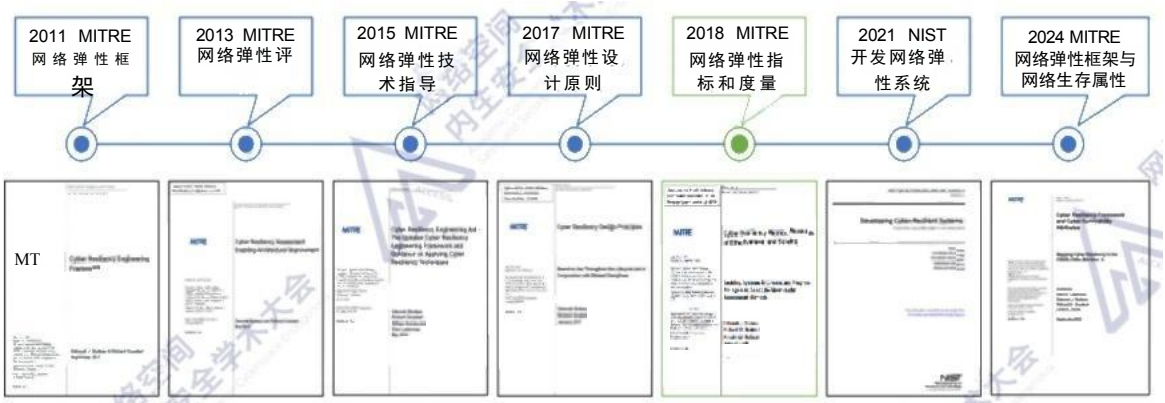

图3-1 网络弹性技术发展历史

为开发网络弹性系统，NIST 提出了一个理解和应用网络弹性的系统工程框架，包括网络弹性工程概念、网络弹性构成要素、工程实践和解决方案等。网络弹性工程框架包括4个网络弹性顶层目的：预测(anticipate)、抵御(withstand)、恢复(recover)和适应(Evolve),8 个网络弹性需求目标(对应分解为若干子目标及需求能力):阻止/避免、准备、持续、扼制、理解、重建、转变、重构，14项网络弹性支撑技术(实现网络弹性顶层目的和需求目标的方法),分别是自适应响应、分析监测、协调保护、欺骗混淆、多样性、动态定位、动态表示、非持久化、权限限制、重新调整、冗余、分段/分割、完整性证明、不可预测性，5项网络弹性策略原则：关注公共关键资产、支持敏捷性和架构适应性、减小攻击面、假设资源会受损、预计对手会进化，和14项网络弹性设计原则，分别是保持态势感知、充分利用运行状况和状态数据、确定持续的可信度、限制对信任的需求、控制使用和可见性、遏制和排除行为、分层防御和分区资源、自适应管理、计划和管理多样性、保持冗余、资源位置多样化、最大化瞬态、改变或破坏攻击面、创造对用户透明的欺骗效果和不可预测性。网络弹性顶层目的和需求目标确定了网络弹性系统需包含哪些属性和特性，网络弹性支撑技术和构建原则描述了实现网络弹性的路径和方式。网络弹性工程实践是用于辨识、提出解决方案的方法、流程、建模和分析技术。这些实践在系统生命周期过程中可提供足够水平的网络弹性，以满足风险相关者的需求，并在存在各种威胁源(包括 APT)时降低组织任务或业务能力风险。

当前，网络弹性技术发展也存在不足之处，影响了关键业务系统的抗击能力和恢复能力。首先，现有网络弹性框架过于依赖已知任务的异常检测，对未知网络攻击的隐性异常关注不足，导致对“未知的未知”威胁的**抗打击能力缺乏**。其次，缺乏统领性的架构设计使得各项技术和策略无法有效整合，限制了**系统在复杂攻击下的恢复能力。**最后，在网络弹性评估中，**量化和核心能力度量不足，**缺乏明确标准和统一框架，制约了评估的有效性和实用性。这些问题亟待解决，以提高网络弹性的整体可靠性。

3.1.2设计安全技术

“设计安全”概念源于制造领域的安全目标与愿景，反映了欧美国家对网络安全责任的深刻反思，旨在应对日益突出的网络安全挑战，如高级持续性威胁(APT)和零日漏洞。随着数字化转型的加速，网络安全威胁不断扩大，许多企业将经济利益置于产品安全之上，忽视潜在风险。该概念的提出标志着网络安全责任向制造侧转移，强调制造商应切实承担网络安全责任，这一模式转变体现了欧美国家的思维变化，要求数字产品制造商主动承担安全责任。

各国主要网络安全机构已提出多项策略、政策和指南，支持和指导“设计安全”的实施，并普遍认为网络安全需要范式转变，敦促责任从用户侧向制造侧转移。制造商必须将“设计安全”作为产品设计和开发的核心，从产品全生命周期的初始设计阶段开始，往动确保网络安全。

传统的“先发布，后修补”模式常常导致安全漏洞被利用的时间窗口过大，造成严重的安全隐患。同时，各国政府和监管机构开始出台更严格的数据保护和网络安全法规，要求制造商在产品设计阶段就考虑安全因素。随着全球化生产的普及，供应链安全成为关键问题，确保产品在设计和生产过程中的安全性变得至关重要。此外，从成本效益角度来看，在设计阶段解决安全问题通常比事后修复更具优势，有助于降低整体的安全支出，提升产品的市场竞争力。整体而言，设计安全的落实不仅能增强产品的安全性，还能提升消费者信任，推动数字经济的可持续发展。

2023年4月和10月，美国多个机构联合五眼联盟以及德国、荷兰、捷克、挪威、以色列、新加坡、韩国、日本和美洲等多国机构，发布制造侧安全指南文

件《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》[3-6]。该指南指出，“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”。该指南将“设计安全”一词解释为包含“设计安全”和“默认安全”两方面。其认为当前阶段，技术制造商比以往任何时候都更需要将“设计安全”和“默认安全”作为产品设计和开发过程的焦点。为了创造一个技术和相关产品对客户更安全的未来，这些机构敦促制造商修改他们的设计和开发计划，只允许向客户运送设计安全和默认安全的产品。其中设计安全的产品是指客户的安全是核心业务目标，而不仅仅是技术功能；而默认安全的产品是指可以安全使用的、几乎不需要或根本不需要更改配置的、并且没有额外成本的“开箱即用”产品。总之，这两个原则将保证安全的大部分负担转移给了制造商，并减少了客户因配置错误、补丁速度不够快或许多其他常见问题而成为安全事件受害者的机会。

针对设计安全概念，美国国家标准与技术研究院发布的《安全软件开发框架》制定了一份简要的设计安全技术策略，其包括：

- **内存安全编程语言：** 尽可能优先使用内存安全语言；
- **安全硬件基础：**包含能够实现细粒度内存保护的体系结构功能；
- **安全软件组件：** 从经过验证的商业、开源和其他第三方开发人员处获取并维护安全性良好的软件组件；
- **Web 模板框架：**使用实现用户输入自动转义的Web 模板框架，以避免跨站点脚本等Web 攻击；
- **参数化查询：**使用参数化查询，而不是在查询中包含用户输入，以避免SQL 注入攻击；
- **静态和动态应用程序安全测试：**使用安全测试工具来分析产品源代码和应用程序行为，以检测容易出错的做法；
- **代码评审：**努力确保提交到产品中的代码通过其他开发人员的同行评审，以确保更高的质量。
- **漏洞披露计划：**建立让安全研究者报告漏洞的漏洞公开方案。
- **常见漏洞与公开威胁完整性：** 确保已发布的常见漏洞与公开威胁包括根本原因或常见弱点列举，以实现软件安全设计缺陷的全行业分析。
- **纵深防御技术：** 设计基础设施，多层次保证系统的安全。

通过在开发初期就考虑安全因素，可以更好地应对复杂多变的网络威胁，降低后期修复和补丁的需求，设计安全可以创造出更加安全、可靠且用户友好的产品以及更安全、可靠的供应链。

当前设计安全面临多重不足。首先，现有设计安全的出发点依然集中于减少和修补漏洞，未能有效应对未知的安全威胁，缺乏主动感知潜在攻击的能力。**现有设计安全方法下的系统无法实时应对未知的未知安全威胁。** 其次，**缺乏一体化的安全系统架构设计导致各项安全措施冗余且复杂，**降低了系统的鲁棒性和管理效率，难以形成合力应对复杂的网络威胁。最后，**安全量化测试与认证方法尚未完善，缺乏全球公认的标准和有效评估工具，**使得数字产品的安全性难以自证与管理，制约了制造商在安全责任上的落实。

3.1.3零信任技术

零信任技术的提出源于传统的基于边界安全模型在当今复杂的网络环境中日益显现出的局限性。传统的边界安全模型基于“城堡和护城河”的概念，即在组织网络边界设置防御措施，如防火墙、入侵探测系统等，以阻挡外部威胁。这种方法假设组织内部网络是可信的， 一旦用户或设备通过了边界验证，就被赋予了较高的信任度和访问权限。然而，随着技术的发展和业务模式的变革，这种基于边界的安全模型逐渐暴露出诸多问题。云计算、移动设备和远程工作的普及使得传统网络边界变得模糊不清。用户无论从哪个位置、使用多种设备都可以访问企业资源，这就造成了网络边界越来越难以界定。其次，内部威胁的增加也挑战了“内部可信”的假设。无论是有意为之，还是无意为之，许多安全事件都是从已经取得访问权限的内部人员中衍生出来的。此外，组织需要与外部合作伙伴共享数据和资源，这就要求安全模型能够更精细地控制访问权限。同时，网络攻击的复杂性和持久性也在不断提高。高级持续性威胁能够突破传统的边界防御，长期潜伏在网络内部，这使得仅依靠边界防御变得不够充分。面对这些挑战，零信任技术应运而生。

零信任发展脉络如图3-2所示，随着零信任理论和实践的不断完善(理念探索、产业实践和国家战略推动),零信任逐渐从原型概念演进为主流网络安全技术架构。2021年5月，美国总统拜登签署的14028号行政令要求将网络安全架

构迁移至零信任架构。随后，美联邦政府和国防部相继发布了《联邦零信任战略》和《国防部零信任战略》[3-7]。联邦战略通过备忘录《推动美国政府迈向零信任网络安全原则》概述了零信任架构的五大支柱：用户、设备、网络、应用和工作负载，以及数据，并提供了推进零信任战略的“任务矩阵”。美国网络安全和基础设施安全局 (CISA) 发布的《零信任成熟度模型》详细介绍了这五大支柱的具体关键能力和目标等级，为政府机构、供应商、企业用户和安全研究人员在设计和实施零信任项目时提供了路线图和资源。为了创建一个具有防御能力、可扩展性、弹性和可审计性的国防信息环境，2022年11月，美国国防部发布了《国防部零信任战略》。该战略涵盖用户、设备、网络和环境、应用和工作负载、数据、自动化与编排、可视化与分析等七大支柱，提出了45项关键能力，构成了完整的国防部零信任能力框架。

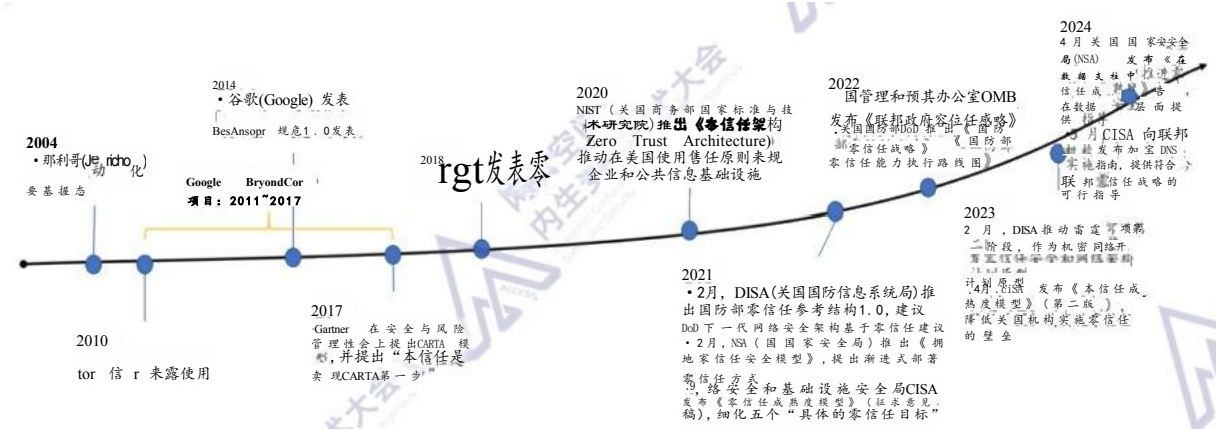

图3-2零信任技术发展历史

零信任摒弃了传统模型“内在可信”的假想，其核心理念是“永不信任，永远验证”。零信任要求对每次访问请求进行严格的身份验证和授权，无论请求来自组织内部还是外部。核心原则包括：**最小特权原则—**用户仅能访问必需资源以降低潜在攻击面、**多层次的安全—**结合多因素身份验证以增强身份确认、**持续监测—**实时监控用户和设备活动以及时识别潜在威胁。实施零信任需要一系列技术工具，主要包括细粒度访问控制(动态管理用户访问权限)、多因素身份验证(结合知识因素、拥有因素和生物识别因素以增强安全性)、网络分割(将网络划分为多个隔离区域以降低横向移动攻击风险)，以及日志和分析(收集和分析日志

数据以检测异常活动)。通过这些技术，组织能够有效提升网络安全性，快速响应安全事件。

零信任架构是实施零信任战略的技术框架，涵盖具体的技术工具、系统设计和实施方案。目前，主流的零信任架构包括美国国防部的架构和NIST （美国国家标准与技术研究院)发布的《零信任架构》 (SP 800-207)。NIST架构定义了零信任的概念、逻辑组件、部署场景及潜在威胁，并提供总体实施路线图。其基本流程包括：用户发起访问请求后，控制单元进行身份认证与评估，策略管理器据此决定授权策略并建立安全连接；策略引擎持续监测用户行为，及时识别异常；如有必要，策略管理器调整授权策略并通知安全代理以确保资源安全。2021年5月，美国国防信息系统局 (DISA) 发布了《国防部零信任参考架构》1.0版本，并于2022年7月推出2.0版本，这些参考架构制定了一系列安全原则和能力基线，以指导国防部信息系统中零信任的实现和安全环境建设，其基本流程与NIST架构类似。

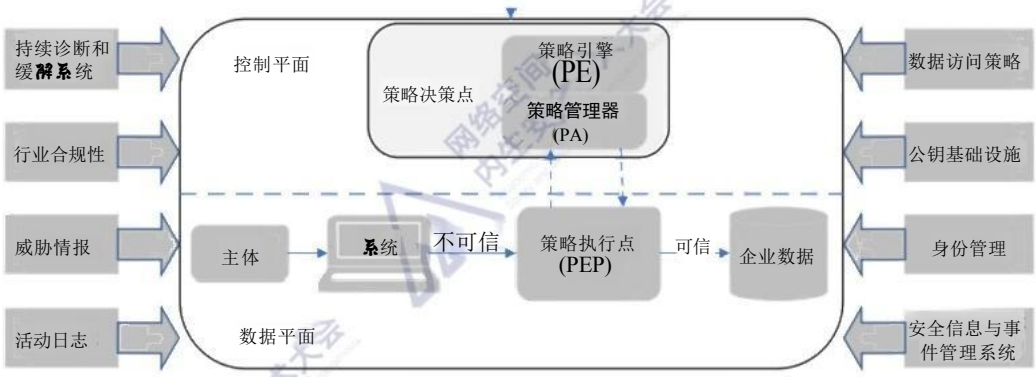

图3-3零信任逻辑架构图(来自NIST SP800-207《零信任架构》)

零信任架构作为前瞻性的安全策略，通过持续验证和精细控制应对复杂的网络威胁，但面临多重挑战。首先，尽管集成了加密、身份认证和微隔离等技术，零信任架构仍未能有效整合这些技术，无法彻底消除实现过程中的漏洞和后门，导致制造侧难以应对分布式认证节点中的网络威胁。其次，实施零信任的设计和实施复杂性高，需深入分析和重构现有网络，这可能导致高昂的初始成本及技术挑战，同时频繁的身份验证和流量检查可能影响用户体验和系统响应速度。最后，深入监控用户行为和数据分析可能引发合规性和隐私问题，需在确保安全与遵守隐私法规之间找到平衡，同时缺乏有效体系来评估目标系统的弹性和主动防御能力。

3.2国内网络安全技术发展现状

随着信息技术的快速发展和数字化改造的深入推进，网络安全问题已经成为国家战略层面的重要问题。我国网络安全产业正处于快速成长期，但仍面临着诸多挑战，如关键核心技术受制于人、安全防护体系不完善等问题。为应对这些挑战，国内学术界和产业界积极探索创新性的网络安全方法论及技术路线。其中，“网络韧性”和“可信计算”作为两种具有中国特色的网络安全理念和方法，近年来得到了广泛关注和实践。这两种方法分别从系统架构设计和计算环境可信性的角度，为构建自主可控、安全可靠的网络空间提供了新的思路和技术支撑。

3.2.1可信计算技术

随着云计算、物联网、5G、大数据等新技术涌现而来，网络安全边界不断弱化，带来的风险和不确定性增加。网站、网络窃密与内部失密，内忧外患之中，若仅凭单一的安全软件产品很难起到应有效果。在此背景下，软硬结合的“可信计算”模式或是解决现阶段信息安全问题的“良方”。传统的网络安全模型主要依赖于事后防御和被动响应，难以应对日益复杂和高级的网络威胁。随着云计算和物联网技术的快速发展，数据和计算资源越来越分散，传统的边界安全已不足以保护复杂的分布式系统。同时，在供应链安全问题日益突出的全球化背景下，软硬件的可信性成为重点考量因素。此外，国家安全和数字主权的需求也推动了可信计算的发展，各国都在寻求建立自主可控的信息技术体系。可信计算旨在从根本上提高系统的安全性和可靠性，构建从硬件、固件到操作系统和应用软件的全栈可信链，可度量、可验证、可控制的计算环境。这种方法不仅能够主动防御潜在威胁，还能为复杂的分布式环境提供端到端的安全保障，同时满足国家层面对技术自主性的要求。因此，可信计算这一广受学术界和产业界关注的领域被认为是一种创新的解决当前网络安全挑战的方法[3-8]。

可信计算的提出主要源于传统安全模型的局限性、新兴技术带来的挑战以及日益严峻的网络安全形势。在可信体系中，信任链以可信根(TPM) 为起点而建立，在此基础上再将信任关系逐级传递到系统的各个模块，从而建立整个系统的信任关系。可信计算一般涉及可信根、信任链和可信加密技术三个部分。

我国在1992年开始进行可信计算方面的研究与实践，至今可信计算经历了三个阶段，第一个阶段主要是通过冗余备份的手段来排除软硬件故障；第二个阶段是将硬件芯片作为信任根，确保硬件可信，当前我国处于可信计算的第三阶段。我国学者从传统计算机架构入手，考虑到传统冯诺依曼架构存在的安全设计缺陷，提出了“可信计算3.0”技术体系，即以密码为基因，在计算运行、实施身份识别、状态度量、保密存储等功能的同时，对自身和非自身成分进行及时识别的可信计算模式，对进入机体内的有害物质进行破坏和排斥，即“主动免疫安全可信计算”技术。

3.2.2 网络韧性技术

2023年12月，美国国家科技委员会发布《联邦网络安全研究与发展战略规划》(2024-2027),指出当前网络弹性工程在理论模型、架构设计和度量评估方面面临“设计难、选择难、度量难”三大核心挑战：一是现有网络弹性多为描述性框架，缺乏科学支撑的理论模型；二是网络弹性需作为系统架构的内在部分，设计并展现高水平弹性；三是改善网络弹性需通过有效的度量和指标评估设计效果。这些观点验证了邬江兴院士团队于2023年7月出版的著作《内生安全赋能网络弹性工程》中关于美欧网络弹性工程“三大硬核问题”的前瞻性结论。该著作以内生安全理论为基础，提出解决方案和技术实践，开辟了内生安全赋能网络弹性的新方向一—网络韧性系统工程。内生安全从科学理论、架构设计到测试度量全面赋能网络韧性，率先实现美国战略规划中的核心目标，开创了“开箱即用、默认安全”的网络韧性新路径，形成中国原创、国际领先的内生安全韧性设计范式，在近几年国际上掀起的基于设计安全的网络韧性发展热潮中处于引领性地位。

内生安全网络韧性设计不仅追求恢复，更致力于在攻击发生时即使受到冲击，系统依然能够维持核心功能，甚至避免损失，实现从“恢复”到“免疫”的跃迁，在“打倒了可恢复”的网络弹性基础上达成了“攻而难倒”的网络韧性目标，突破了欧美在网络弹性上尚未解决的瓶颈问题。因此，网络韧性是信息系统在不可避免的网络攻击或其他不利条件下，超越传统网络弹性以实现“攻而难倒”的综合能力，强调通过内生安全等创新理论与技术手段，提升系统在面对威胁时的动态抗扰性、快速恢复能力及持续适应性，从而保障关键任务功能的稳定运行，构

建高可信、可控、可验证的数字生态安全体系。网络韧性不仅关注攻击后的恢复与适应，更注重从设计阶段强化系统结构安全，达成难以被攻破、持续稳定运行的目标，是网络弹性发展的高级阶段。

网络内生安全机理与构造不仅是一个重大的科学发现而且也是一项颠覆性的技术发明。基于我国原创的内生安全赋能网络弹性理论，能够引领国际网络韧性发展新潮流。内生安全网络韧性设计技术[3-9]的提出是为了应对和解决是解决网络空间普遍存在的内生安全共性问题，转变单纯地依靠漏洞后门和攻击特征精确发现以及缩小攻击表面的技术发展路线，其借鉴系统工程理论、可靠性设计理论、生物仿生和免疫理论等，在国际上首次提出一种不依赖(但不排斥)漏洞后门发现和攻击特征分析等先验知识的内生安全理论与体系，建立一套有效解决网络空间内生安全共性问题的实践规范，以创新的广义鲁棒控制构造破解目前功能安全与网络安全不能量化设计、无法验证度量的工程技术难题，从根本上实现当前网络安全领域思维视角与方法论的转变，破解如何有效防范未知的未知威胁、如何基于相对性构造原理抑制内生安全共性问题影响等亟待解决的重大科学问题。内生安全理论提出了一个新的概念：内生安全问题。其指出当某个事物在其主要功能之外，还具有一些意料之外的负面效果或隐藏功能时，就会出现安全隐患。同样，如果一个系统或模型中存在一些由其自身结构决定的、相互依赖但又相互矛盾的内在因素，也属于内生安全问题的范畴。

内生安全理论指出，**动态性/随机性、多样性/异构性、冗余性**这三大网络安全防御领域的核心技术要素对于增加不确定性和防范未知威胁至关重要[3-10]。内生型安全理论基于上述思想，提供了动态异构冗余的创新架构，如图3-4所示，其能够有效抑制“已知的未知”和“未知的未知”等构造中存在的异常扰动所产生的不良影响，其不依赖于先验知识，自然获得高可靠、高可信、高可用的三位一体的内生安全属性。

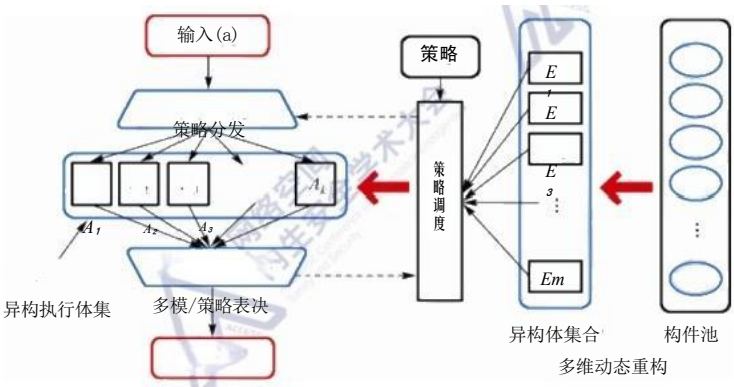

图3-4内生安全动态异构冗余架构图

中国原创的网络韧性研究以内生安全理论为核心，经10余年迭代发展，在原创性理论、颠覆性技术、核心发明专利、技术标准体系、典型领域应用、测试评估度量、知识体系建设等方面取得体系化创新成果，形成中国原创、国际领先的网络空间内生安全学派，在近几年国际上掀起的基于设计安全的网络弹性发展热潮中处于引领性地位。先后初版《内生安全赋能网络弹性工程》等专著,奠定了动态、多样、冗余 (DVR)　防御模型和结构加密等原创理论基础，深刻阐明了我国原创的网络空间内生安全理论与当前国际网络弹性发展热潮的关系；发布 11 项拟态防御技术标准，内生安全拟态防御技术标准体系已初步建立，规范了网络弹性设备的研发和应用；研发全球首个内生安全架构拟态调度器专用芯片，并在“强网”挑战赛中展示卓越网络弹性能力；开辟了内生安全车联网新方向，为智能网联汽车产业发展中的基础性关键问题提供了一种“中国独创独有”的解决方案；创建全球首个内生安全实验场，提出内生安全白盒测试金标准，连续六年面向全球开展众测攻防竞赛，内生安全赋能的数字设备均能保持不坏金身，实践证明内生安全理论和技术具有领先优势!构建内生安全知识体系，培育开发者网络安全培养新模式。团队的成果涵盖车联网、6G、工业互联网等领域，为构建韧性网络提供了系统化解决方案，同时通过“五色石”计划推动人才培养，助力数字生态转型，提升中国在网络空间安全领域的国际话语权。

内生安全为全球正在兴起的数字生态系统底层驱动范式转型提供了“中国智慧与方案”,开辟了基于内生安全构造的数字产品网络安全设计新方向，为构建数字经济新生态提供不可或缺的新质生产力[3-11]。需要指出的是，相较于网络弹性、设计安全、零信任等挑战，中国原创内生安全韧性设计技术具备五大特色，可一体化解决网络空间三重威胁交织问题：

(1)不依赖关于攻击者的先验信息。能在不依赖(但不排斥)攻击者先验信息的条件下，有效避免已知的未知或未知的未知等广义功能安全问题导致的安全事件；

(2)可以一体化构造赋能。基于数学物理加密性质的赋能构造，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，架构内即使存在内生安全问题也难以演变为安全事件；

(3)安全性可量化设计。不论是已知的未知概率问题，或者未知的未知不确定性问题所造成的广义不确定扰动都能变换为广义可靠性(概率)量纲呈现的可量化设计与验证度量指标；

(4)完美拒止试错攻击。能够从机理上颠覆试错攻击所必须的背景不变假设前提，阻断或屏蔽攻击者的单向透明优势，使得攻击者没有比穷举攻击更好的选择；

(5)具备内生安全黄金检验法，即白盒注入。内生安全 DHR 架构完美安全性质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”,测试者可在DHR 架构输入端构造测试例相应的激励序列并观察输出端的响应信息，依此可测量出现安全事件的发生概率。

特别是，与欧美网络弹性方案相比，内生安全还具备两项独有能力。 一是具备感知并抵御基于未知漏洞后门的网络攻击的能力；二是具有同时抵御随机故障失效和人为网络攻击的一体化安全能力。

总之，基于中国原创的内生安全赋能网络弹性创新方案，能够不依赖(可融合)基于先验知识的网络安全理论与方法，实现可量化设计/验证度量的设计安全，有效避免我国在数字化产业生态安全转型过程中被再度“牵鼻子/卡脖子”，引领国际网络弹性/设计安全/零信任技术发展新潮流。

3.3网络安全技术发展趋势分析

随着数字技术的快速发展和网络环境的日益复杂，传统的网络安全技术已经难以应对当前的安全挑战。为了更好地保护数字资产和信息系统，网络安全领域正在经历一系列重要的变革。这些变革反映了网络安全技术的几个关键发展趋势，不仅体现了安全理念的转变，也展示了技术应用的创新。具体而言，可以观察到

以下四个主要趋势：首先是安全策略的综合化，其次是安全机制的内生化，再次是防护范围的整体化，最后是评估方法的量化。

1.针对越来越复杂的数字生态系统，需要将目标加固、损害限制和业务恢复综合考虑

针对日益复杂的数字生态系统，网络安全策略必须全面且系统地考虑多个层面。首先，目标加固是基础，它要求在系统设计之初就纳入安全性，通过实施最小权限原则、强身份验证和定期漏洞扫描等措施，最大限度地减少潜在的攻击面。这种前期预防措施能够有效降低安全事件发生的概率，为后续的防护奠定坚实基础[。

其次，在面对现实的网络攻击时，损害限制成为关键环节。此策略要求组织在发现安全事件时迅速采取响应措施，以控制事态发展并减少损失。这包括实施实时监控和应急响应计划，确保在攻击发生后能够迅速隔离受影响的系统和数据，防止攻击扩散。同时，组织还需进行持续的威胁评估，以便及时更新和优化响应策略，增强对未来攻击的抵御能力。

最后，业务恢复是网络安全管理中不可或缺的一部分。即便在实施了目标加固和损害限制措施后，组织仍需准备好迅速恢复正常业务运营。这涉及到制定和测试灾难恢复计划，确保在遭遇攻击后，关键业务能够尽快恢复，从而减少对客户和合作伙伴的影响。通过构建健全的备份和恢复机制，组织可以在面临安全事件时迅速恢复系统功能，实现业务连续性。

综合考虑目标加固、损害限制和业务恢复是构建现代网络安全体系的关键。这一系统性方法不仅能增强组织的安全防护能力，还能提高其应对复杂网络威胁的灵活性和韧性。在未来的数字生态系统中，组织需要不断完善这一闭环安全策略，以适应快速变化的威胁环境。

2. 随着网络边界融合化，网络安全技术从“叠加式”“外挂式”的安全向“内生”安全转变

随着云计算、人工智能等数字技术的深入应用，智慧城市展现出融合、协同与智能化的特征。这一趋势通过网络更有效地连接智慧城市的服务、居民和企业，使信息实现高度集中与共享。然而，信息资源的集中共享也带来了更为集中的安全风险。

在这个新的发展阶段，智慧城市逐步由稳态系统转向敏态系统，数据从静态转向实时，空间和时间的维度也从单一物理转向多维社会网络。这一变化导致网络安全的边界日益模糊，呈现出复杂性和不确定性，传统的边界防护模式如防火墙和堡垒机逐渐失去效果。此外，传统的“打补丁”、“局部整改”以及“事后补救”的网络安全措施，已经无法满足未来经济社会的安全需求。业界逐渐意识到，仅依靠外部安全措施已无法应对现代网络环境中的挑战，因此，系统性地部署网络安全策略和基础设施将成为未来发展的主流方向。

在此背景下，“内生”安全理念的提出，强调在系统设计的早期阶段就考虑安全因素。通过全局视角开展网络安全的顶层设计，确保安全性与功能性同等重要。安全机制在设计和开发过程中同步实施，使其更紧密地嵌入到系统中。这种集成的安全策略不仅提升了系统的安全性能，也增强了抵御潜在威胁的能力，将安全置于系统的核心，而非附属。

此外，内生安全的理念促进了整个组织内安全意识的建立。开发团队、运维团队与安全团队之间的协作愈发重要，通过信息共享和最佳实践，确保在软件生命周期内持续关注安全问题。这种跨职能的合作有助于迅速识别和应对安全威胁，从而有效降低潜在损失。

网络安全的“内生”转变标志着安全理念的深刻变革，通过将安全设计融入系统架构，组织能够在复杂多变的数字环境中构建更强大、更灵活的防护机制，从而有效应对不断演变的安全威胁。这一转变不仅提升了系统的安全性能，还增强了组织的整体抵御能力，为未来的网络安全实践奠定了坚实的基础。

3. 网络安全技术从安全要素局部层面向系统整体层面转变，满足实战化监管需求

在国家主管部门以“实战化、体系化、常态化”为安全监管新理念，以“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”为新举措，构建国家网络安全综合防控系统的背景下，实战攻防演习成为政企用户网络安全保护的常态化工作，也成为政企用户检验网络安全防御体系有效性、全面提升网络安全综合防护能力的重要手段，有效地推动了政企用户增加对网络安全实战化、体系化及安全运行能力的建设投入。

但是，过去的网络安全措施通常集中在某些局部要素上，例如防火墙、杀毒

软件等单点防御。这种“点式防御”虽然在一定程度上提供了保护，但往往无法有效应对复杂的攻击手段和不断演化的威胁。在当前数字化环境中，攻击者常常利用多种技术和策略进行协调攻击，单一的防护措施显得捉襟见肘。网络安全正在经历从局部防护措施向系统整体安全管理的转变。

现代网络安全方法强调整体防护的重要性，要求从全局视角出发，综合考虑系统内各个组成部分的安全性，覆盖信息系统的整个生命周期。它强调安全要素之间的协同整合，以及安全措施与业务流程的深度融合，以实现全面和有效的安全保护。因此，系统整体安全不仅关注单一的安全工具或技术，而是将安全作为系统设计和实施的核心元素，从而提供持续性的保护。通过在系统的各个阶段融入安全考量，组织能够在设计、开发、部署和维护过程中确保安全性，减少潜在风险。例如，身份认证、访问控制、数据加密、入侵检测和响应等安全措施需要相互配合，共同构建一个多层次的防御体系。这种整合不仅提高了安全防护的效率，也增强了对新型攻击的抵御能力。

在这一整体安全管理框架下，网络安全措施将更加系统化和动态化。与传统的静态防护不同，现代安全管理需要实时监测和评估系统状态，以便及时响应新出现的威胁和漏洞。这种持续的监测和反馈机制使组织能够在面对不断变化的网络环境时，迅速调整和优化其安全策略，从而实现更高的安全韧性。这样的转变不仅提升了整体防护能力，也为组织在面对未来复杂威胁时提供了更为坚实的保障 。

4. 网络安全防御能力评估从防御效能定性分析向定量确保转变

网络安全防御能力评估正经历从定性分析向定量确保的转变。这一变化不仅补充了传统评估方法，更是满足现代系统设计、开发和运维需求的重要一步。随着网络环境的日益复杂，仅依靠定性判断已无法全面反映系统在随机失效和人为攻击下的可用性和生存性。因此，采用量化指标和科学评估方法显得尤为重要。

通过量化设计，网络安全评估的准确性和客观性得以显著提升。这使组织能够更深入地理解自身的安全防护能力，识别具体的弱点和改进空间。量化指标不仅提供了明确的数据支持，还帮助安全团队分析不同防御措施的有效性，明确哪些环节需要加强或调整。这种深入分析促进了针对性改进措施的制定，为优化网络安全策略奠定了坚实的基础，从而使安全防护更加科学和精准。

引入定量评估后，组织能够更加客观地衡量其安全防御能力，使得安全防护效果可以通过具体的数字和指标来表达，为决策者提供了更为可靠的依据。例如，通过计算系统的安全事件响应时间、攻击成功率和恢复时间等指标，组织可以深入分析防御措施的有效性，从而为安全策略的优化提供实证支持。

最后，定量评估为持续改进和对标分析提供了坚实的基础。通过定期监测和评估安全防御能力，组织能够及时识别薄弱环节并制定相应的改进措施。同时，量化指标使得与行业标准或最佳实践的对比分析更加便捷，促进了整个安全体系的不断完善和提升。这一系列变革将使网络安全防御能力评估不仅仅局限于“合格”与“未合格”的简单判断，而是形成一种动态、可持续优化的安全管理机制。

5.AI 提升网络安全技术自动化水平

通过机器学习和数据分析，AI 可以实时监测网络流量，识别异常行为，迅速检测潜在威胁。这种智能化的监控不仅提高了识别攻击的准确性，还能有效减少误报，确保安全团队能够专注于真正的安全事件[3-12]。

自2022年底，以LLM（大语言模型)为核心的生成式人工智能带来了新的技术与产业革命，被认为“改变游戏规则”的战略性科技，促成网络安全产品功能、性能提升。AI 还能够通过自动化响应机制，快速处理已识别的安全事件。例如，在遭遇网络攻击时，AI 可以即时执行封锁、隔离受影响的系统，甚至启动预设的防御措施，从而显著降低攻击造成的损害。同时，AI 的学习能力使其能够不断适应新的攻击模式，提升对未来威胁的预警能力。在数据分析方面，AI 可以处理海量的安全日志和事件数据，帮助安全团队识别潜在的安全隐患和漏洞。通过深度学习算法，AI 能够从历史数据中提取出有价值的见解，为系统安全策略制定提供支持。此外，AI 还可以辅助进行合规性检查，确保遵循相关法律法规。

总之，AI 赋能网络安全不仅提高了防御效率，还增强了安全体系的灵活性和智能化，使企业在面对日益复杂的网络威胁时能够更从容地应对挑战。随着技术的不断进步，AI 将在网络安全领域发挥越来越重要的作用。

4我国网络安全领域的优势、不足及建议

4.1 我国网络安全领域的优势

随着全球网络安全形势的复杂化与挑战加剧，尤其是在美国升级对中国网络科技的打压策略下，网络安全已成为国家安全与数字经济发展的重要战略支柱。十年来，在总书记关于“网络安全和信息化是一体之两翼、驱动之双轮”等一系列重要思想指引下，凭借独特的制度优势和强大的执行力，网络安全发展成效显著,网络安全水平不断提升，已初步构建了网络安全“四梁八柱”、基本完善了政策法规标准体系、取得了原创性理论和颠覆性技术突破。

一、政策法规和管理体系逐步完善

我国持续加强网络安全的顶层设计，围绕国家战略需求进行系统性布局，在数据安全、关键信息基础设施安全、新兴领域安全和产业安全等方面陆续出台多项法律政策，逐步构建了自上而下的政策法规与安全管理体系。

在立法层面，自《中华人民共和国网络安全法》作为我国首部网络安全基础性法律颁布以来，《中华人民共和国密码法》《中华人民共和国数据安全法》相继出台，《电信法》的立法进程也在不断推进，构成了网络空间安全治理的核心法律框架[4-1]。该法律体系为各行业的网络安全与数据安全监管提供了明确的法律依据，有力保障了我国数字经济的安全、有序发展。配套制度建设方面，各领域相关政策法规不断完善，以强化网络安全监管力度。关键信息基础设施专项安全条例即将发布，《网络安全审查办法》也正结合《数据安全法》进行修订，重点加强对科技、金融等重要领域企业境外上市的数据安全审查和风险管控能力，数据安全治理体系初步建立[4-2]。工信部、国家互联网信息办公室和公安部联合发布了《网络产品安全漏洞管理规定》,同时网络安全产业发展行动计划稳步推进，细化了行业领域安全管理和服务政策，促进各项安全措施的落实。安全标准建设方面，已逐步形成了国家、行业、团体标准协同推进的工作机制。当前，网络安全相关标准已达300余项，涵盖了各类安全管理和技术要求，成为指导网络安全工作的基本规范，并为网络安全国际标准合作奠定了基础。

二、强大且发展持续向好的网络安全市场

我国拥有庞大的数字经济市场和丰富的应用场景，为网络安全技术的创新和产品的迭代优化提供了广阔的实践空间。数字经济的迅猛发展使得网络安全需求大幅增加，覆盖了从电子商务、金融科技到智慧城市、工业互联网等多领域。这些多元化和复杂化的应用场景不仅迫使技术不断升级以应对新的安全威胁，也为新技术和新产品提供了丰富的试验田。快速增长的网络安全需求推动了产业规模的扩大，形成了从基础设施建设、技术研发到安全服务的全产业链布局，产业规模呈现持续高速增长态势，网络安全投入显著提升。特别是在政府大力支持下，国内网络安全市场在2023年已突破2000亿元，并在未来几年保持高速增长[4-3]。

完整的信息产业链为网络安全的自主可控发展奠定了坚实基础。在网络安全产业链中，我国拥有从芯片设计、半导体制造到操作系统开发、应用软件等全方位的信息产业链，形成了全面的技术体系，相关安全企业稳步发展，市场活力不断涌现，催生出许多新兴的网络安全企业，如奇安信、深信服等，网络安全企业营收水平和盈利能力逐步增强，融资并购活动持续活跃，深度布局安全市场[4-4]。这些企业不仅为政府、企业用户提供全面的网络安全产品与解决方案，还积极参与国家标准的制定和技术研究，构建了完善的网络安全产业生态。中小型企业在政府的支持下，也开始在细分领域，如数据安全、身份管理等，提供创新型解决方案，进一步充实了网络安全市场的多样性和覆盖面[4-5]。

三、技术创新的加速推进与多维度布局

在新威胁、新需求的牵引下，传统防火墙、抗DDoS、入侵检测等固化单一形态的安全技术向集流量监测、DDoS 防护、威胁处置等全面云化、协同联动的安全即服务方案演变。依托国家重点实验室、研究机构和科技企业的协同创新，中国在自主研发和技术应用上形成了良好的创新生态系统，取得了网络空间内生安全原创理论突破，独创的网络韧性设计范式突破了欧美技术路线中的瓶颈问题，拟态防御、零信任、可信计算等新兴安全技术逐步成熟落地[4-6]。大型科技企业，如华为、腾讯等，在网络安全技术的前沿探索中起到了带头作用，如华为在5G通信安全技术、区块链应用领域取得了突破；腾讯在反欺诈、威胁情报等领域形成了成熟的技术解决方案。同时，我国还注重 AI 应用于安全技术中的发展，推动智能检测和响应技术，大幅提高了应对高级持续性威胁(APT) 攻击的能力[4-7]。

在相关政策、资金扶持下，以工业互联网、车联网、5G、人工智能等为代表的产业布局和深层次拓展持续加速，新技术产业化安全防护体系布局逐步形成[4-8]。已形成了强大的研发能力和系统集成经验，通过网络安全能力成熟度评价、先进技术应用试点示范等促进网络安全能力持续提升，构建了覆盖底层基础设施安全至上层应用场景服务安全等多个维度的网络安全产品体系，着力面向自适应安全、网络弹性、智能对抗等高端能力等重点方向攻关，形成了理论与工程领先优势，在应对复杂攻击和新型网络威胁时具备了更多的主动权。

四、网络安全人才培养机制日臻完善

我国在网络安全人才培养方面进行了系统化部署，投入巨大，通过政产学研的深度融合，使网络安全人才建设取得了显著进展。近年来，国家相继发布了一系列政策，为网络安全人才培养提供了有力的政策引导与支持，涵盖学科专业建设、人才培养机制、教师队伍建设以及校企合作的多方面内容，进一步明确了网络安全学科专业建设方向和人才培养重点，完善了网络安全人才培养体系[4-9]。与此同时，国内网络安全和互联网龙头企业积极参与高等院校网络安全人才培养，通过共建网络空间安全研究院和制定联合培养计划等手段协同育人，以定向培养为目标，为网络安全人才培养、技术创新与产业发展构建了良性生态链。为促进网络安全人才的多样化选拔，我国还鼓励网络安全科研人员积极参与国际联合研究和学术交流，提升人才的学术水平与国际交流能力，同时通过举办全国性网络安全技能竞赛和实战化攻防演练，挖掘优秀的网络安全人才。

五、国际合作的广泛推进与全球影响力的提升

我国在网络安全领域的国际合作不断深化，积极履行国际责任，与国际社会携手提高数据安全和个人信息保护合作水平，共同打击网络犯罪和网络恐怖主义。我国已与81个国家和地区的274个计算机应急响应组织建立“CNCERT 国际合作伙伴”关系，并与其中33个组织签订网络安全合作备忘录[4-10]。在金砖国家、上合组织等区域网络安全进程中发挥积极作用，推动达成《金砖国家网络安全务实合作路线图》和《上合组织成员国保障国际信息安全合作计划》。与东盟联合建立网络安全交流培训中心，连续多年向东盟国家开展网络安全培训交流活动。此外，我国还积极参与联合国等多边机构的网络安全合作，推动全球网络安全治理。

我国提出的“构建网络空间命运共同体”理念得到国际社会的广泛认同，网络空间命运共同体等重要理念深入人心。积极推动全球数据安全治理、加强个人信息保护领域的合作，在保障个人信息和重要数据安全的前提下，与世界各国开展交流合作，发布《全球数据安全倡议》,为制定全球数据安全规则提供了蓝本，并与多个国家签署数据安全合作倡议。通过加强国际网络问题的信息共享及在网络安全技术和管理工作方面的沟通与合作，积极参与全球网络安全技术标准的制定，推动技术和政策方面的合作，积极汲取其他国家的成功经验和技术，主动争取网络空间的主导权和话语权[4-11]。在保证公开、公正的前提下，持续开展交流合作，共促技术发展，并致力于完善全球网络安全治理。

4.2我国网络安全领域存在的不足

虽然网络安全领域的总体“时”与“势”持续向好，但随着全球科技竞争日益激烈，尤其在高新技术领域的国际博弈加剧，我国网络安全领域仍面临一些亟待解决的不足与挑战：

一、网络安全监管的协调性和统一性不足

尽管国家层面高度重视网络安全，制定了一系列法律法规政策，但缺乏配套的标准规范予以细化，可操作性有待加强，各项法规之间存在一定的不协调性和执行上的差异，尤其是地方和行业层面的监管标准不一，导致政策落实效果参差不齐，与美国提倡的统一监管框架不同，中国的监管制度仍较为复杂，未能有效消除跨部门之间的冲突，亟需建立一套连贯、精简的监管体系，以应对多样化的网络安全威胁并促进创新[4-12]。同时，战略规划的长期性和系统性考虑不足，未能充分应对全球网络安全形势变化，治理的全链条管理和协同机制较为薄弱，尤其是在跨部门和跨区域的协调上存在障碍，信息共享和应急响应机制也有待加强，与美国强调的跨政府及公共和私营部门的无缝合作相比，中国在推动多利益相关方之间的协作上力度不足，尤其是缺乏快速、全面应对网络攻击的有效机制。

二、数字产品制造侧网络安全监管尚处在“荒漠区”

当前，我国“重发展、轻安全”的观念仍然根深蒂固，与能够快速见效的信息化投入相比，我国在网络安全方面的投入相对较低，大部分未将网络安全视为刚需，对网络安全产品与服务的需求仅是被“合规”所驱使，甚至部分用户将网络安

全建设视为一种成本负担。根据 IDC 数据显示，我国网络安全的投入占信息化整体投入的比例一直低于2%,远低于全球平均水平3.05%,与美国、日本等发达国家10%以上的投入比例相比存在数倍差距。同时，目前对数字产品网络安全质量监管还处在“荒漠区”,虽然强调“谁运营、谁负责；谁主管、谁负责”,但对数字产品设计或制造商还没有明确法定责任，信息化、数字化和网络安全“两张皮”的管理格局也并未发生根本改变。美欧等提出“在市场机制失灵的地方，必须加强政府干预”,纷纷快速出台加强数字产品制造侧安全质量监管的政策和法规，以实现用户侧和制造侧网络安全风险和责任的平衡，着力构建抵御“系统性网络风险”的弹性和韧性[4-13]。相比之下，我国虽已出台网络安全审查、等级保护2.0等制度性文件，但尚未制定数字产品安全质量监管体系，设计制造侧“安全责任”缺失，亟待尽快出台数字产品网络安全新政、法规及标准规范，强制将网络安全责任向制造侧“左移”,明确制造商网络安全责任，提升设计安全和网络弹性以奠定数字产业安全底座。

三、前沿核心技术创新能力有待提升

与发达国家相比，我国网络安全领域的前沿核心技术创新能力存在明显差距，在自主创新的芯片、操作系统方面，核心产品在功能性和安全性上与国际先进水平存在差距。在高可靠性的安全芯片、操作系统、密码算法等底层技术上，中国的研发进展相对滞后，尽管人工智能、区块链、5G 等领域的安全技术在国际上位居前列，但依然存在“重场景安全，轻底层技术逻辑”的问题，限制了整体网络安全体系的韧性[4-14]。

此外，尽管我国网络安全企业数量众多，但在国际上具备竞争力的企业相对较少，核心技术创新力和市场主导力有限，多数企业的研发资源集中于解决短期应用问题，底层技术创新缺乏，导致行业内产品同质化严重，企业之间低水平重复研发的现象普遍，削弱了行业整体创新动力。与此同时，在应对网络威胁的技术前瞻性和先进性上，企业与科研机构的投入力度还不够，缺乏能够从根本上提升核心竞争力的长远规划。

四、网络安全人才供给不足及结构性缺陷

《2023年网络安全产业人才发展报告》显示，我国对网络安全人才的总需求量达150万以上，且每年新增需求量约为4.5万人，而高校每年培养的网络安

全人才不到3万人，高校产出人才数量远远不能适应社会发展对网络安全人才的需求，人才总量特别是实战型人才匮乏，特别是高层次、复合型人才尤为匮乏[4-15]。《2024年网络安全产业人才发展报告》指出，随着全球网络安全技能缺口的持续扩大，尤其是在云计算安全、人工智能和机器学习等前沿领域，人才短缺的问题更加严峻。

此外，人才培养与实际需求之间的错位问题同样突出，网络安全领域各技术方向的人才分布存在较大比例失衡，运营维护和技术支持等岗位人员较多，而战略规划、架构设计、政策研究等领域的高素质专业人才则相对短缺。同时，高校网络安全课程体系设置比较僵化，普遍存在“重理论，缺实践”的现象，大多数课程更关注基础理论和学术性内容，而实践性较强的应用课程和综合实验课程相对不足，导致毕业学生与工作岗位的实际需求之间存在显著差距。相比之下，欧美国家在高端网络安全人才的培养和激励方面有着更为成熟的体系和多样化的支持政策，我国在该领域的差距显而易见。

4.3我国网络安全领域发展建议

当前，我国在数字生态系统的掌控能力与发达国家相比仍存在差距，网络安全发展模式尚未完全突破传统框架。为实现具有中国特色的数字生态系统转型，亟需采取创新路径，构建基于内生安全的网络安全架构，以应对各种已知和未知的网络攻击，实现安全性的“可量化设计/可验证度量”,超越美欧网络弹性系统工程方法。基于此，本蓝皮书提出以下建议：

一、加快制定中国特色的网络安全政策法规，强化数字产品开发侧网络安全责任

针对我国实际国情，基于“防范系统性安全风险”的长远战略考量，应当加快出台“国家制造侧网络安全”政策法案。该法案应明确规定制造商在产品设计、生产、销售和售后等环节的网络安全责任，制定数字产品的刚性安全标准，建立可量化评估的安全方法。制造商必须在产品的硬件安全、软件安全和数据安全等方面严格遵循这些标准，并随技术发展和威胁形势的变化而动态更新。同时，应设立科学、客观、可操作的安全评估体系，除传统静态分析、动态测试和渗透测试外，还应包括我国内生安全“白盒测试”金标准等，确保产品安全性能可以被准确

量化和评估。为确保政策法案的有效性，还应设立相应的惩戒机制，对违反安全标准或未能履行安全责任的制造商，实施包括经济处罚、市场准入限制等多层次惩戒措施。通过这些措施，形成一个“可管理”的共治共管体系，平衡制造侧与应用侧的安全责任，确保"谁设计谁负责，谁制造谁负责"的原则得到贯彻，为数字产业底层驱动技术的网络安全转型奠定坚实基础，推动整个数字产品产业链向更高的安全标准迈进。

二、建立我国数字设施安全质量标准体系，推动“网络安全/弹性信任标识”计划

借鉴美欧先进经验，我们应推动设立“中国网络安全/网络弹性信任标识”系统。该标识系统将为符合网络弹性工程要求、满足如内生安全“白盒测试”金标准的数字产品授予“信任标签”。为实现这一目标，需成立由政府部门、行业专家和企业代表组成的标准制定委员会，负责制定详细的评估标准和认证流程。建立多层次的评估体系，包括功能安全、网络安全和信息/数据安全等不同级别，以适应不同应用场景的需求。设立专门的认证机构，负责产品评估、认证和日常监管工作，确保认证过程的公正性和权威性。同时，建立动态评估机制，定期对已认证产品进行复审，确保其持续满足安全标准要求。在政府采购和重点行业等领域优先使用“信任标识”产品，为高质量安全产品创造市场优势。通过严格实施市场准入制度和刚性标准，有效阻止缺乏网络弹性质量保证的数字产品进入关键基础设施建设领域，如公众通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等国家重点行业。确保数字产品的网络弹性质量对使用者或营运者“透明可见”,符合“开箱即用默认安全”的新质量规范，从而全面提升我国数字基础设施的安全性和可靠性。

三、发挥我国原创网络安全理论先发优势，启动数字生态系统网络韧性重大专项工程

鉴于我国在网络安全理论研究方面取得的显著成果，尤其是内生安全理论在解决“未知威胁”检测和防御等美欧主流方法难以应对的问题上展现出的引领性优势。应当充分利用这一先发优势，加大对以内生安全为代表的制造侧安全技术实践的支持力度，借鉴欧美等国统筹20多个国家战略科技力量联合攻关的做法，充分发挥政府主导的举国体制优势，设立重大专项有效推进从知识体系、基础理

论、关键技术、核心产品、测试评估和典型示范的全链条网络韧性工程体系化工作，解决全生命周期安全的工程技术问题，解决数字产品“不可信任”的“心腹大患”难题。在信息通信、智能制造、金融和能源等关键基础领域选择若干典型行业，启动规模化示范推广项目。

四 、推动我国自主、多样的数字生态建设，构建自主可控且多样化的弹性供应链

为确保国家数字主权和安全，必须构建自主可控且多样化的弹性供应链。这一目标的实现需要从多个层面同时发力。在供应链安全管理方面，建立关键数字产品和服务的全生命周期追溯系统，实施严格的供应商资质认证制度。在技术研发与创新方面，加大对核心技术的自主研发投入，包括芯片、操作系统和数据库等基础软硬件。通过上述措施，显著增强我国在全球数字生态系统中的自主性，构建具有中国特色、世界领先的网络安全体系，为我国数字经济的持续健康发展提供坚实保障。

5 总 结

在全球数字生态系统底层驱动范式转型的推动下，网络安全已成为一个至关重要的议题，其重要性与日俱增。本蓝皮书深入分析了当前网络安全战略与技术的发展现状和未来趋势，全面评估了全球网络安全格局的变化，其中详细介绍了国外网络安全战略的发展，重点分析了美国和欧盟的相关政策；并探讨了网络弹性、设计安全和零信任等国际主流网络安全方法，以及我国原创的内生安全赋能网络弹性——网络韧性技术。在此基础上从网络安全政策法规、安全质量标准体系、弹性供应链等多个角度提出网络安全发展建议。

本蓝皮书受紫金山实验室重大科研任务“内生安全基础理论与工具链研究”项目资助。

本蓝皮书受国家重点研发计划网络空间安全专项“云边协同的工业智能控制器安全防护技术”项目资助。

参考文献

[1-1]钞小静，王宸威.数字经济影响经济高质量发展研究综述与展望[J]. 电 子科技大学学报社科版，2023,25(3):1-7,58.

[1-2]侯艳玲，谢兴昶，洪之坤，等.数字经济时代网络信息安全基本现状与发展趋势[J].山东工业技术，2023(3):60-64.

[1-3]Nai Fovino I,Baldini G.,Chaudron S.,et al.Cybersecurity,our digital anchor[R].Luxembourg:Publications Office of the European Union,2020.

[1-4]Burri M,Zihlmann Z.The EU Cyber Resilience Act -An Appraisal and Contextualization[J].Zeitschrift für Europarecht (EuZ),2023,2(2023): B1-B45.

[1-5]“伏特台风”III——揭密美国政府机构实施的网络间谍和虚假信息行动[R].国家计算机病毒应急处理中心，2024.

[1-6]Danzig R.Surviving on a diet of poisoned fruit:Reducing the National Security Risks of America's Cyber Dependencies[M].Center for a New American Security,2014.

[2-1]唐新华.美国综合威慑战略中的技术互操作性[J]. 太平洋学报，2022,30(12):15-25

[2-2]Ross R,Pillitteri V,Graubart R,et al.Developing cyber resilient systems:a systems security engineering approach[R].National Institute of Standards and Technology,2019.

[2-3]Wylde A.Zero trust:Never trust,always verify[C].2021 international conference on cyber situational awareness,data analytics and assessment (cybersa).IEEE,2021:1-4.

[2-4]Stafford V.Zero trust architecture[J].NIST special publication,2020,800: 207.

[2-5]AI N.Artificial Intelligence Risk Management Framework (AI RMF 1.0)[J]. 2023.

[2-6]AI N.Artificial Intelligence Risk Management Framework:Generative

Artificial Intelligence Profile[J].2024.

[2-7]Gianmarco B,Josefa B,Stephane C,et al.Cybersecurity,our digital anchor[J]. 2020.

[2-8]何占博，王颖，刘军.我国网络安全等级保护现状与2.0标准体系研究[J]. 信息技术与网络安全，2019,38(3):9-14,19.

[3-1]Petrenko S.Cyber resilience[M].River Publishers,2022.

[3-2]Souppaya M,Scarfone K,Dodson D.Secure software development framework (ssdf)version 1.1[J].NIST Special Publication,2022,800:218.

[3-3]Stafford V.Zero trust architecture[J].NIST special publication,2020,800:207.

[3-4]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25.6(2024):106-115.

[3-5]Ron Ross,Victoria Pillitteri,Richard Graubart,Deborah Bodeau,Rosalie McQuaid.Developing Cyber-Resilient Systems:A Systems Security Engineering Approach.NIST SP 800-160 Vol.2 Rev.1.2021.

[3-6]Cybersecurity and Infrastructure Security Agency (CISA).Shifting the Balance of Cybersecurity Risk:Security-by-Design and Default Principles.2023.

[3-7]Chief Information Officer U.S.DoD.,DoD Zero Trust Strategy,Nov.2021. [EB/OL]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[3-8]胡俊，沈昌祥，公备.可信计算3.0工程初步[M]. 中国图书.,2017.

[3-9]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.

[3-10]邬江兴.网络空间拟态防御研究[J].信息安全学报，2016,1(4)

[3-11]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.

[3-12]彬袁.新时代下人工智能在网络安全运维服务中的相关运用[J].大数据与人工智能5.5(2024):1-3.

[4-1]孙佑海.网络安全法：保障网络安全的根本举措——学习贯彻《中华人民共和国网络安全法》[J].中国信息安全，2016(12):30-33.

[4-2]刘金瑞.切实维护关键信息基础设施供应链安全——评析《网络安全审查办法》的五大重要变化.

[4-3]中国网络安全产业分析报告[R]. 中国网络安全产业联盟，2024.

[4-4]丰诗朵，高婧杰，李慎之，等，ICT 供应链安全制度演进趋势研究[J].信 息通信技术与政策，2023,49(2):49.

[4-5]任江红.企业网络安全的重要性及防护策略[J]. 电子通信与计算机科学，2023,5(7):168-170

[4-6]谢玮，焦贝贝.网络安全发展形势分析与趋势展望[J].通信世界，2022(007):10-19.

[4-7]陈毅，华蕊. 国家安全体系和能力现代化视域下数据安全治理的困境及突围路径[J]. 学习与探索，2023(12):41-47.

[4-8]应芳芳，赵震.我国网络安全产业发展态势研究[J].广东通信技术，2024,44(4):7-10.DOI:10.3969/j.issn.1006-6403.2024.04.002.

[4-9]李春源，王磊，徐子竞.新工科背景下网络安全研究生人才培养模式研究与实践[J].黑龙江教育(高教研究与评估),2024.

[4-10]张立，李丹浓，尤江东，等.网络空间安全领域国际科研合作特征及演化趋势分析[J]. 信息工程大学学报，2023,24(6):741-748.

[4-11]熊光清，王瑞.网络主权：互联网时代对主权观念的重塑[J].中国人民大学学报，2024,38(1):126-138.

[4-12]厉晓彬.欧盟多层次网络安全治理研究[D].吉林大学，2024.

[4-13]Alhidaifi S M,Asghar M R,Ansari I S.A Survey on cyber resilience:Key strategies,research challenges,and future directions[J].ACM Computing Surveys,2024,56(8):1-48.

[4-14]周俊.国产基础软硬件密码技术融合研究与实践[J].通信技术，2022(008):055.

[4-15]2024年网络安全产业人才发展报告[R]. 中国信息通信研究院，2024.

THE 7th
"QIANGWANG"

INTERNATIONAL ELITE
CHALLENGE
ON CVBER MIMIC
DEFENSE