6G核心网智能韧性体系构想蓝皮书

（2024年）

紫金山实验室
国家数字交换系统工程技术研究中心
西安电子科技大学

2024年11月

版权声明

本蓝皮书主要贡献者

季新生、游伟、王子龙、廖星星、李聪、杨杰、汤红波、蒋忠元、张向荣、赵宇、陶剑、李俊潇、陈谦、冯润涵、王凯、黄瑞阳、邱航、许明艳、陈云杰、柏溢、王领伟、秦小刚、许畅、王敏、曹淄玉、姜坤、贲星、周颖、周琦、王春晓、张停、王煜杰、赵颖、李尚乐、王森、薛步青、李魏、黄新宇、吴文昊、吴宜昆、闵施茹、吕俊宣、赵启薇、郑李婧、冯欣、郭笑成、房梦欣、周德强、汪清、胡雅妮等。

目 录

图目录

缩略语说明

英文缩写	英文全称	中文解释
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
DHR	Dynamic Heterogeneous Redundancy	动态异构冗余架构
RINGS	Resilient and Intelligent NextG Systems	弹性和智能下一代系统
AI	Artificial Intelligence	人工智能
ITU	International Telecommunication Union	国际电信联盟
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
NGMN	Next Generation Mobile Networks	下一代移动网络
6G SNS	6th Generation Smart Networks and Services	第六代智能网络和服务
SLA	Service Level Agreement	服务水平协议
API	Application Programming Interface	应用程序编程接口
QOS	Quality of Service	服务质量
APT	Advanced Persistent Threat	高级持续性威胁
DDOS	Distributed Denial of Service	分布式拒绝服务攻击
RPKI	Resource Public Key Infrastructure	资源公钥基础设施
BGP	Border Gateway Protocol	边界网关协议
PDU	Protocol Data Unit	协议数据单元
DAN	Distributed Autonomous Network	分布式自治网络
SCU	Small Cloud Unit	微云单元
IPS	Intrusion Prevention System	入侵防御系统
MTD	Mobile Target Defense	移动目标防御
RTO	Recovery Time Objective	恢复时间目标
RPO	Recovery Point Objective	恢复点目标
SIEM	Security Information and Event Management	安全信息和事件管理
VNF	Virtual Network Function	虚拟网络功能
SDN	Software Defined Networking	软件定义网络

NFV	Network Function Virtualization	网络功能虚拟化
MANO	Management and Orchestration	管理和编排
OSS	Operational Support Systems	运营支持系统
ZSM	Zero-Touch Network and Service Management	零接触网络和服务管理
ZT	Zero Trust	零信任
DFP	Dynamic Function Placement	动态功能放置
MLOPs	Machine Learning Operations	机器学习运维
DevOPs	Development and Operations	开发运维
TEE	Trusted Execution Environment	可信执行环境
ARM	Advanced RISC Machine	高级精简指令集计算机
AMD	Advanced Micro Devices, Inc	超威半导体公司
SRv6	Segment Routing over IPv6	基于 IPv6 的段路由

引言

5G 网络的发展推动了网络功能服务化和基础设施虚拟化，这使得网络能够快速整合各种组件的功能，以构建新的用例和场景。然而，随着虚拟化和云化趋势的不断深入，5G 网络中频发的“黑天鹅”事件对电信级可靠性提出了重大挑战。作为支撑人类社会的关键信息基础设施，6G 网络将融合人、机、物三元世界，其风险的叠加和级联将使得挑战更加艰巨。

为此，欧美等在规划 6G 安全愿景时，普遍将网络弹性作为重要考量，期望 6G 在面临自然灾害、故障失效和网络攻击等威胁时，能够保持稳定的服务能力，即使无法避免服务受损，也能够做到有序降级并能够快速恢复服务。在此背景下，美国自然基金委联合多个部门和头部企业，启动了弹性智能的下一代网络项目 RINGS，强调要在下一代网络的各项赋能技术中都考虑设计安全、自主恢复和高度灵活适应性。德国 Open6GHub 项目强调要在 6G 的无线、边缘、核心网和云设施等所有层面都加强“自我意识”、自我重配置和自我保护等网络弹性设计。

我国相关研究团队，依据“结构构造安全”的内生安全长期研究积累，提出 6G 应在“打倒了可恢复”的网络弹性基础上达成“攻而难倒”的网络韧性目标。

在内生安全指导下的网络韧性设计范式不仅追求恢复，更致力于在即使遭遇“未知的未知”等网络攻击时仍能有效避免损失，仍能维持核心功能提供有效服务，从而实现从“恢复”到“免疫”的跃迁。在此背景下的 6G 核心网应综合考虑高动态、高可靠、高可用、高质量等性能要求，在网络原生 AI 赋能下，超越传统移动网络的硬化防护思维，探索电信级可靠性的活化超稳态新范式：网络能够持续稳定地提供可信赖的高质量服务，并能够对各类人为和非人为因素造成的网络扰动和破坏做出实时的自动化响应，在受到扰动和破坏后，网络能够迅速自主演进到新的稳态，确保服务的连续性和可靠性。

1. 网络韧性是 6G 系统的美好愿景

随着移动通信技术的飞速发展，我们正迈向一个全新的网络时代——6G。与以往代际移动通信不同，6G 将服务人机物三元融合的世界，成为未来社会的关键信息基础设施。因此，6G 将更加重视网络安全，除了关注通信安全和隐私保护等传统安全，更加强调保证关键业务的连续性。在 6G 网络中，网络韧性是内生的质量属性，是 6G 赋能人机物三元融合世界坚如磐石的保障。

1.1 国际 6G 网络弹性发展趋势

弹性（Resilience）原本是物理学概念，指事物受干扰后恢复或弹回到原来状态的能力，还可以理解为应变体在由压缩应力引起形变之后恢复其大小和形状的能力。随着网络安全威胁愈演愈烈，欧美在系统工程、信息技术和计算机网络领域也逐渐引入了 Resilience 概念。国内学者将 Resilience 翻译成弹性或韧性，表达的意思既包含准备好应对并适应变化条件，也包括经受故意攻击、意外事件或自然灾害的破坏后，从中迅速恢复的能力。

网络弹性（Network Resilience）概念由斯特本兹等在《通信网络中的弹性和生存能力：策略、原则和学科调查》中提出，表示的是通信网络在面对各种故障和危害正常运行的挑战时能提供和维持可接受服务水平的能力。该概念通常应用于复杂网络的鲁棒性研究。

网络弹性（Cyber Resilience）概念最初是在美国国家安全战略和军事战略调整的大背景下提出的，强调系统在面对由偶然条件或故意行为引起的逆境时恢复和继续运营的能力。2013 年，美国第 21 号总统政策指令《网络基础设施安全与弹性》指出：弹性意味着“准备好应对适应变化条件，承受破坏并从中恢复的能力”。2021 年 12 月，美国 NIST 正式发布了《开发网络弹性系统——种系统安全工程方法》，将网络弹性定义为：包含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。欧盟的《网络弹性法案》已于 2024 年 10 月通过欧盟理事会批准，预计于 2025 年生效，要求所有进入欧盟市场的数字技术产品必须符合网络弹性标准。

美国下一代网络联盟（NEXTGA）在其 6G 路线图《Roadmap to 6G》报告中，把可信、安全和弹性（Trust，Security and Resilience）列为其 6G 六大目标

之首。在《Trust, Security, and Resilience for 6G Systems》报告中，指出 6G 系统要想受到大众、企业和政府的信任，必须具有弹性（resilient）、网络安全（secure）、隐私保护（privacy-preserving）、功能安全（safe）、可信赖（reliable）、可靠（dependable）等特性，并且在任何情况下都可用。美国国家科学基金会发布了弹性智能的下一代网络 RINGS 项目，目的是联合国防部研究与工程部副部长办公室（OUSD R&E）、美国国家标准技术研究院（NIST）和多个行业合作伙伴实现弹性和智能的下一代系统设计。

欧盟智能网络和服务联合体（SNS JU）资助了一系列 6G 项目，其中与可靠服务和智能安全相关的项目有 iTrust6G、NATWORK、ROBUST-6G、SAFE-6G、ELASTIC 等，这些项目优先考虑用户数据保护和隐私、可靠性、信任和弹性，目的是为了确保安全过渡到 6G。

下一代移动网络联盟 NGMN 于 2023 年 10 月发布 6G 安全愿景白皮书《6G Trustworthiness Considerations》，聚焦 6G 的安全可信赖性。白皮书首先分析了 6G 安全可信赖性的四个驱动力——社会需求、网络演进需求、业务驱动需求，以及安全技术驱动需求。基于上述驱动力，白皮书从安全、隐私、弹性、可靠性、人身和公共安全等方面阐述了 6G 相关的需求，进一步探讨实现 6G 安全可信赖的技术考虑，主要包括分布式信任基础设施、动态信任模型、智能安全协同、解耦安全服务、信任风险评估等。

日本通信部发布的 B5G 发展战略提出 2030 社会愿景是可靠的（dependable）、包容的和可持续的，B5G 需具备超安全性和弹性。此外，日本 Beyond 5G 推进联盟发布白皮书《Message to the 2030s》，指出为了应对 B5G 用户的多样化需求，不仅需要在功能和性能的技术创新方面取得进展，还需要提供一个所有利益相关方都可以安全使用的可信赖网络基础设施。该白皮书认为，B5G 网络安全大致可分为网络弹性、隐私和信任三个方面。

国际电信联盟无线电通信部门 5D 工作组（ITU-R WP5D）第 44 次会议于 2023 年 6 月在瑞士日内瓦召开，如期完成了《IMT 面向 2030 及未来发展的框架和总体目标建议书》。该建议书作为 6G 纲领性的文件，汇聚了全球 6G 愿景共识，描绘了 6G 目标与趋势，提出了 6G 的典型场景及能力指标体系，标志着 6G 研究重点正式从愿景需求转向技术方案的新阶段。建议书明确了 6G 的 15 个关键

能力指标，是对 5G 关键能力的增强与维度扩展，安全/隐私/弹性性能指标就是其中的一个。

在学术和产业界方面，爱立信公司在其《6G 网络连接虚拟和现实世界的桥梁白皮书》中指出，随着对“网络成为社会不可或缺的一部分”的期望越来越大，对更高可用性和弹性的要求也随之而来，未来的应用需要利用高性能连接，满足所需的带宽、动态行为、弹性和更多需求，需要从不同的角度来解决网络弹性问题。诺基亚公司在其《6G 时代的安全与信任白皮书》中将安全、隐私和信任提升为 6G 研究的首要领域，并认为积极应对安全挑战将是创建弹性 6G 网络的关键，需要新的思维和新的方法，如果不能对 6G 网络、应用程序和服务提供坚如磐石的安全保证，世界将永远不会接受它们。

1.2 6G 网络韧性新视角

现有网络弹性侧重于网络的稳定性和可靠性，而对网络的灵活性、适应性、尤其是网络抵抗未知的未知攻击能力关注不足，网络缺乏自我进化的能力，无法适应快速变化的网络环境和日益复杂的威胁。此外，现有的网络弹性研究缺乏跨学科的视角，例如，缺乏结合社会学、心理学和生物学等领域的知识来更全面地理解和应对网络威胁。

通过集成先进的人工智能和机器学习技术，6G 网络能够实现更高层次的自主性和智能，使其在面对不断演变的网络威胁时，能够更加灵活和强大。这种新视角下的 6G 网络韧性，不仅关注于技术层面的创新，还涉及到网络设计和运营的整体策略以及跨学科交叉协作，旨在构建一个更加智能、韧性的网络环境。

6G 网络韧性将欧美网络弹性各个子概念（如：Cyber Resilience、Network Resilience、Elasticity）综合集成，共同构筑起一套既能防范当前已知威胁又能适应未来未知风险的动态、灵活和坚韧的安全体系。6G 网络韧性涵盖多个相互交织的实现策略，这些策略共同构成面临不断变化的网络威胁和挑战时能够自我监督、自我保护、自动适应并迅速恢复的全方位防御体系。6G 网络韧性确保在面临复杂多变的网络攻击时，关键系统和服务仍能保持其必要的功能和稳定性。相较于传统的鲁棒性、脆弱性、持续性等概念，6G 网络韧性并没有止步于抗压能力，而是同时兼顾了抗压能力和恢复能力。相较于经典可靠性理论较多地针对一般性大概率风险，6G 网络韧性则更注重或聚焦于小概率极端性风险。

6G 网络韧性超越单项考核，将传统的网络安全方法与更广泛的预防和从恶意攻击中恢复结合起来，重在功能、性能、质量多种属性如何围绕用户融合，对质量属性要求越来越高。其与任务保证、网络安全防护、业务连续性、备份恢复等相关，不仅仅关注应对外部的网络攻击，也关注网络自身的健壮性与可靠性以及业务 QoS 的高稳态性；它并不局限于防御或消除网络攻击，也考虑到与网络攻击共存，在遭受网络攻击时保持网络的可用性以及网络恢复的能力。

6G 网络韧性新视角应构建在冗余、异构、自监督、自适应和自生成等核心要求之上。冗余确保了在部分网络组件失效时，其他组件能够接管其功能，维持网络的连续性；异构则意味着网络能够整合不同类型的技术和资源，提高对攻击的抵抗力；自监督是网络能够自我检测和评估其状态，及时发现并阻止异常行为，在 Cyber 环境下，网络面临的威胁日益复杂和多变，一个强大的自监督机制对于早期识别和应对未知的未知网络攻击至关重要；自适应允许网络根据环境变化和攻击模式动态调整其防御策略；自生成则是指网络能够自我修复和重建，快速从攻击中恢复并适应环境。

2. 6G 核心网智能韧性体系构想

6G 网络韧性的构建必须回答一系列核心问题。首先，必须清晰地界定 6G 网络所面临的安全挑战，这些挑战可能源于引入的新技术，也可能由网络部署方式变化（分布式、云边端）引起。其次，需要深入探讨应从哪些关键维度着手获得网络韧性，以及网络韧性应具备哪些关键能力，不同维度上能够解决什么问题。此外，还需考虑如何在网络设计的初期阶段就将网络韧性思维全面融入各个网络平面，确保网络设计之初便具备应对未来不确定性的内在能力。最后，还需研究如何测试和评估网络韧性的能力，以确保网络在面对可能出现的各种挑战时能够保持服务连续性。

2.1 核心网智能韧性体系构想

ITU-R 已明确 6G 六大典型场景，包括沉浸式通信、超大规模连接、极高可靠低时延通信、AI 与通信融合、通感一体和泛在连接。多场景、多网络、多技术之间的融合，使得 **6G 网络系统构成了一个复杂巨系统。该系统涉及人与人、人与物、物与物之间的感知、计算、通信及控制过程**。系统网络安全风险也面临

着多样性、复杂性和不可预见性。作为移动网络的大脑，核心网长期以来面临着高稳、高效和业务创新使能等挑战。因此，6G 核心网韧性的重点是防御未知的未知网络攻击并保障业务连续性。其本质是由威胁和风险问题而引起的对网络、系统、业务健壮性的体系化思考。目的是保障网络面临攻击或其他不利情况（如：设备故障、自然灾害、战争）时，具备预测、承受等能力以维持基本网络服务，具备恢复、自适应等能力以重新达到网络系统最佳水平。

6G 核心网智能韧性体系将重点围绕六大典型场景，**针对三种威胁（开放环境高级持续威胁、云化网络功能失效威胁、多域流转隐私泄露威胁），从三个维度（点、线、面），构建四种韧性能力（多维感知、灵活包容、动态修复、迭代更新），达成四项韧性目标（预测与智能优化、抵抗与故障容错、恢复与快速响应、自适应与自演化），构建可测试、可评估的 6G 网络智能韧性体系。**内容如图 1 所示。

图 1 6G 核心网智能韧性体系构想

6G 核心网智能韧性体系综合考虑了 6G 网络的各个关键要素，包括：物理基础设施、虚拟化网络资源、网络服务编排与管理，确保从单一网络功能到整个网络系统的全面韧性。同时从三个维度进行综合防护：网络功能、网络流程和链

路、以及网络架构，也即点、线、面。通过实施负载均衡、冗余设计、动态切换、意图识别和智能协同等措施，构建一个冗余、异构、自监督、自适应和自生成的6G核心网智能韧性体系，并促进形成一个具备多维感知、灵活包容、动态修复和迭代更新能力的网络系统。系统横向层面能够与传统的外挂式安全防护技术或体系融合，形成协同防御机制。纵向层面能够与智能网联基础平台之上的其他技术体系融合，形成韧性自治的能力。通过这种全面的方法，6G网络将能够更好地预测潜在的安全威胁、抵御未知的未知网络攻击、快速从灾害故障中恢复、灵活自适应不断变化的网络环境和威胁态势。此外，这种综合的韧性体系不仅限于技术层面的提升，还涵盖了流程和测试方法的演进，确保6G核心网在面对未来挑战时，能够以可测试、可评估的方式保持服务的连续性和可靠性。

2.2 应对三种安全威胁

随着6G网络基础设施的云化、网络功能的服务化、网络服务的开放化和网络组件的开源化，这些由多供应链供给的网络组件无法避免的存在因软硬件固有的不可信性导致的随机错误、失效和故障等问题，同时开放的云原生平台和服务大大提升了被主动攻击的可能性。在网络产品设计过程中，安全问题往往容易被忽视，尤其是在功能鲁棒性或功能韧性的设计中，设计者往往没有充分考虑到未知的未知网络攻击可能带来的破坏性影响。这种疏忽可能导致严重的后果，因为现代网络攻击日益复杂和隐蔽，它们不仅能够破坏服务和泄露数据，还能对物理世界造成直接的影响。因此，6G核心网韧性的设计必须从根本上解决这一问题，致力于在即使遭遇“未知的未知”等网络攻击时仍能有效避免损失，仍能维持核心功能提供有效服务，从而实现从“恢复”到“免疫”的跃迁。需应对开放环境高级持续威胁、云化网络功能失效威胁、多域流转隐私泄露威胁导致6G网络服务功能、性能下降的问题，以保持网络可用性、可靠性和可信性。

开放环境高级持续威胁：是指那些针对网络基础设施漏洞的攻击导致6G网络服务中断或性能下降的威胁。在6G网络中，这些威胁包括但不限于恶意软件攻击、分布式拒绝服务（DDoS）攻击、APT攻击、零日漏洞攻击、中间人攻击、跨域攻击等。可能性包括网络边界中的接入点、远程访问技术的使用，进入组织网络基础设施的受感染文件。如：在云网融合场景下，攻击者利用基础设施软硬件漏洞致使运行其上的网络服务不可用，造成大量严重网络事故。为了解决这些

问题，6G 核心网韧性需预防和响应这些威胁，确保网络服务的可用性。

云化网络功能失效威胁：是指软硬件设施由于自身不可信、缺陷或操作错误导致网络故障而引起 6G 服务功能障碍的威胁。在 6G 网络中，功能安全问题可能导致服务中断、数据丢失或不正确的数据传输。例如，NRF 的故障可能影响核心区域内的所有网元通信，而软件缺陷可能导致网络管理功能失效。为了解决这些问题，6G 核心网韧性需要实现高容错能力，通过冗余设计和故障转移机制来确保关键任务服务的可靠性。

多域流转隐私泄露威胁：是指由于用户数据隐私泄露被攻击者利用而导致 6G 服务功能受损或性能下降的威胁。在 6G 网络环境下，数据在不同管理域间的复杂流转可能引发一系列安全问题，尤其是用户数据的泄露、未经授权的访问以及数据在传输过程中的完整性受损。以混合组网场景为例，若子网中的用户信息遭到泄露或篡改，不仅可能导致合法用户被拒绝访问企业园区网络，还可能涉及用户权限等级的非法变更，造成非授权的高级访问权限，进而威胁到整个网络的安全性。为了解决这些问题，6G 核心网韧性需提高对信息安全威胁的防御能力，确保整个网络系统的可信性。

2.3 具备三个维度防护

在 6G 网络的设计和实施过程中，确保网络韧性至关重要，关系到网络在面临不断演变的安全威胁、技术故障、以及不可预测的外部事件时的稳定性和可靠性。网络韧性机制的设计需要从微观到宏观的多个层面进行细致的考量，包括单个**网络功能的鲁棒性、网络连接的冗余性，以及整体架构的灵活性和适应性。为了实现这一目标，需从点（网络功能）、线（网络流程、链路）、面（网络架构）**三个维度出发，全面构建 6G 核心网韧性能力。

点：指提高 6G 网络功能的韧性能力。依据动态异构冗余 DHR 架构设计 6G 网元（虚拟化或实体），当系统发生故障时，冗余配置的部件可作为备援，及时介入并承担故障部件的业务，避免因单点故障而造成业务停滞的情况。当设备受到攻击后无法保持正常工作状态时，可切换到最小业务系统保障核心业务的连续性。当网络面临突发流量时能够自动伸缩以保障业务的 QoS。对网络功能的监控也至关重要，这包括实时监控设备的运行状态，及时发现并响应异常情况，以及定期进行安全审计和性能评估，确保网络设备能够在各种情况下保持最高水平的

可用性。此外，还应实施有效的故障恢复策略和灾难恢复计划，以便在发生严重故障或攻击时，能够迅速恢复服务，减少对用户的影响。以上作用于网络功能的措施，可以显著提高 6G 网络的鲁棒性，确保网络功能稳定性。

线：指在网络链路和流程上保证 6G 网络韧性。通过链路冗余、逃生路径、韧性选路等方式，当网元受到非法攻击时，网络可以主动将其旁路或进行业务迁移或切换，确保网络服务的可用性。通过不同类型的网络备份（如固定网络、移动网络或卫星网络），当受到攻击或自然灾害时，可继续保障业务的稳定运行。通过智能检测、自动清洗，防范大流量、突发、间歇型的 DDOS 攻击；通过国际认可的 RPKI 和 BGPSEC 等技术改进 BGP 协议，增加路由协议安全机制，提高网络韧性。同时，3GPP 定义了多会话承载机制，支持冗余的用户面路径，实现双 PDU 会话资源配置，确保网络业务的高可靠。

面：指在架构上保证 6G 网络韧性。云网融合环境下，设备规模及网络组成较为复杂，涉及到多设备、多系统、多网络的协同工作，风险暴漏面增加。借鉴动态异构冗余 DHR 的构造思想，使用多设备、多系统、多网络改变现有业务目标的相似性、单一性，在业务系统受到攻击或故障时能灵活改变业务的承载设备、系统类型和网络路径，保持业务稳定运行，提供可靠的服务。同时，6G 网络将支持分布式自治网络（DAN）架构，由分布式微云单元（SCU）及其相关协议组成，这些单元可以支持在网络中分布式部署，具备自包含和自治能力。这种分布式的设计有助于提高网络韧性，因为即使某个部分受到攻击或发生故障，其他部分仍然可以独立运行，从而保证网络服务的连续性。

2.4 构建四种网络韧性关键能力

2.4.1 多维感知

6G 网络业务处理伴生海量数据，构建网络韧性能力的关键是对这些数据进行多维度感知。多维感知包括横向感知、纵向感知和时空感知。横向感知关注于业务的全生命周期，包括从终端用户到服务提供者的所有环节，要求网络能够收集和分析来自 6G 链中不同参与者的数据，以便及时发现和响应潜在的安全威胁或性能问题；纵向感知则关注分布式网络架构下的运维数据，包括云基础设施状态和多供应链开源组件漏洞信息等，以确保网络的各个功能在虚拟化平台正常工作；时空感知则关注环境感知，包括社会环境和自然环境，并进行时间维度上的

推演，最终实现对如天气变化、热点事件、空间状况等复杂模型或小概率事件的反演或精确分析。

空天地一体化实现 6G 网络的立体覆盖，通过多维感知可提供更广泛的服务范围和更高的服务质量。在智能驾驶场景中，多维感知能力可以通过云边端的实时协同，就近提供边缘智能服务；在低空经济场景中，多维感知可以实时监控无人机的飞行路径、速度、方位，以优化无人机的航线规划，避开禁飞区和空中交通拥堵区域，确保货物按时安全送达；在远程医疗或工业控制场景中，多维感知可以监控业务的 QoS 或 QoE，实现超可靠低时延通信保障。

2.4.2 动态修复

网络故障或性能下降可能会迅速发生并扩散，因此，动态修复能力的关键在于快速识别问题并智能化、自动化的触发恢复措施，以维持核心功能提供有效服务，从而避免网络中断造成的损失。这个过程涉及：意图识别、智能决策、自动修复。其中修复的方法包括：负载均衡、弹性伸缩、流量重定向、动态轮换、微隔离、重配置或者替换故障组件等。

动态修复能力是 6G 核心网韧性的核心，它通过整合分布式自治、跨域协同及人工智能等先进技术，实现了网络资源的高效利用和自动化的资源分配与优化，增强了网络在面对流量高峰、网络攻击或自然灾害等挑战时的适应性和恢复力。如，6G 网络能够自动检测并重定向服务节点故障，迅速识别并防御网络攻击，以及在基础设施受损时快速部署新的网元或跨云协同，确保关键通信服务的连续性。这些特性确保了 6G 核心网韧性能力从被动、间歇性向主动、持续性发展，使网络具备一定的与生俱来的防御能力，以及通过后天学习得来的经验式修复能力，且具备被动防御已知攻击，主动抵御已知但无法克服和新型未知攻击的能力，保障系统超稳态运行。

2.4.4 迭代更新

6G 核心网韧性还需要包含迭代更新的能力，即网络能够不断地学习和适应新的威胁和挑战。迭代更新的能力体现在两方面，一是优化业务服务质量，二是调整网络状态或集成新技术，以适应新的外部环境或抵御新的漏洞威胁。迭代更新可通过在数字世界中对物理实体或过程进行模拟、验证、预测和控制，获得物理世界的最优状态，从而实现从“恢复”到“免疫”的跃迁。

6G 网络利用机器学习算法分析控制面或数据面流量模式，以实时更新入侵检测系统（IDS）和入侵防御系统（IPS）的规则库，自动识别并阻止新型攻击或异常网元访问。通过持续的网络管理和优化，AI 算法可以根据实时数据学习和进化，自动调整网络参数，预测并防止网络拥塞，优化能源消耗，提高网络效率。6G 网络还能够根据用户反馈和行为分析，不断更新服务，提升用户满意度。例如，网络可以自动识别用户习惯和偏好，提供个性化和优化的用户上网体验。此外，6G 网络的设计支持快速集成新技术并通过迭代更新网络协议和接口，确保与新兴技术的兼容性和互操作性。如：集成区块链和量子加密技术，以增强对信息安安全威胁的防御能力；集成 DHR、MTD、零信任技术，以增强对网络安全或功能安全威胁的防御能力，确保网络的长期稳定性和安全性。迭代更新使 6G 网络能够持续进化，以应对未来可能出现的诸多问题。

2.4.2 灵活包容

6G 网络作为一个复杂巨系统，在技术层面需要兼容不同的技术，在业务层面需要满足差异化韧性需求。这就要求 6G 网络是一个高度可扩展、可编程和模块化的系统，能够支持各种新兴技术和服务的快速部署和演进，实现网络韧性能力的按需定制、动态部署和弹性伸缩。

一方面，通过网络功能 API 和标准化接口允许第三方开发者以新的方式与网络互动；另一方面，可编程能力不再局限于控制平面，而是引申到数据平面。开放性可编程的程度取决于网络部署和连接的能力、网络资源编排管理能力、服务和应用提供能力，这些能力由不同的框架支持着，包括：3GPP CAPIF（Common API framework，通用 API 框架），作为一个安全且可互操作的 API 管理器，对于支持网络在部署、管理和应用层面的开放性至关重要；ETSI SDN（软件定义网络）控制器框架，提供逻辑网络作为服务（LNaaS），支持更丰富的连接拓扑，对服务进行控制和管理，以支持更好的用户体验，实现整体资源利用和网络性能；ETSI NFV 框架，其 Os-Ma-nfvo 参考点可被用来创建“意图引擎”，允许运营支持系统/业务支持系统（OSS/BSS）控制网络服务和网络切片的完整操作及利用人工智能（AI）/机器学习（ML）算法根据最终用户的意图自动化服务管理；基于 P4 的可编程框架，允许定义数据平面的行为，灵活实现各种网络协议，同时保持数据平面的高性能，支持从小型网络到大规模数据中心网络的扩展，允许在

数据平面实现安全策略，提高了网络的韧性。

2.5 达成四项网络韧性核心目标

2.5.1 预测与智能优化

预测是网络韧性的第一道防线，它基于多维感知能力实现对潜在威胁的前瞻性认知和评估，并对威胁可能发生的时间、地点和方式进行预测。在 6G 核心网智能韧性体系内，预测能力至关重要。它基于对历史安全事件的深入分析、用户行为的分析、系统漏洞的评估、网络状态趋势的监测以及异常流量模式识别，确定网络哪个环节最有可能成为攻击的目标，并确保这些节点得到适当的保护。通过在数字世界中对攻击过程进行模拟、验证，网络可以不断优化其预测能力，确保能够及时发现并响应新的威胁。

6G 核心网韧性将达成预测与智能优化的强大目标，以抵御已知的已知、已知的未知、未知的未知安全威胁挑战。为了提高预测的准确性，网络运营商需要与全球的安全社区合作，共享威胁情报，以便更快地识别出新的攻击模式和漏洞，降低安全事件的可能性和潜在影响，确保关键任务和业务功能的持续性和安全性。此外，网络还应具备自动化的响应机制，一旦预测到威胁，能够立即采取行动，如隔离可疑的网络流量或加强受威胁节点的保护。

2.5.2 抵抗与故障容错

抵抗与故障容错是网络韧性的第二道防线，它通过对攻击影响的控制和限制或对攻击者行动的遏制，能够在一定程度上保持关键服务的质量和性能。这涉及到对硬件故障、软件错误、网络问题等各种异常情况的处理。常见的容错机制包括冗余备份、数据镜像、错误检测与纠正等。6G 网络通过有效的防御体系和冗余机制，可以提高自身的鲁棒性，实现对威胁的承受和容错能力。

6G 网络的“抵抗”和“故障容错”能力确保了其在面对潜在的网络攻击、硬件故障、软件缺陷或自然灾害等多种挑战时，能够维持关键功能的连续性和数据的完整性。通过集成先进的加密技术、入侵检测系统、动态访问控制以及智能化的网络设计，6G 网络能够实时监测和响应外部威胁及异常行为，及时调整流量，重新路由通信，或隔离受感染部分，以保持网络稳定性和可靠性。同时，借助内置的冗余机制和自愈能力，6G 网络能够自动检测和响应故障，快速重新配

置资源，修复受损服务，确保用户体验的无缝性和业务运营的持续性，从而在实现故障容错方面取得了重要进步。

2.5.3 快速响应与恢复

快速响应与恢复是6G核心网韧性的核心要求，它基于动态修复能力在业务遭受攻击带来的最小化影响后快速恢复。为了实现快速有效的恢复，网络必须制定详尽的灾难恢复计划和业务连续性计划，这些计划应包括数据备份策略、系统恢复点的创建、关键业务功能的优先级排序以及恢复时间目标（RTO）和数据恢复点目标（RPO）的设定。6G网络韧性涵盖多个相互交织的实现策略，这些策略共同构成面临不断变化的网络威胁和挑战时能够自我监督、自我保护、自动适应并迅速恢复的全方位防御体系。

6G核心网韧性体现在网络能够持续稳定地提供可信赖的高质量服务，并能够对各类人为和非人为因素造成的网络扰动和破坏做出实时的自动化响应，在受到扰动和破坏后，网络能够迅速恢复到新的稳态，确保服务的连续性和可靠性。为了提升响应速度，6G网络可以利用自动化工具，例如安全信息和事件管理（SIEM）系统，自动化地收集、分析和响应安全事件。还包括使用自动化脚本和工具来加速恢复过程，如系统映像的自动恢复或虚拟机快照的回滚。6G网络还需要从每次事件中学习，通过事后分析来识别恢复过程中的不足之处，并根据这些经验来改进恢复计划。这种持续的改进和适应确保了网络的恢复能力随着时间的推移而增强，更好地应对未来的攻击或中断。此外，网络应定期进行恢复演练，验证恢复计划的有效性，并确保所有相关人员都了解他们在恢复过程中的角色和责任。

2.5.4 自适应与自演化

自适应与自演化是网络韧性的最终目标，它基于网络的迭代更新能力实现网络的自学习和进化，以适应不断变化的威胁格局，确保其长期的可持续发展。自适应网络不仅能够根据历史数据和实时威胁情报，自动调整其安全配置和策略，以更好地抵御新的攻击手段，还能识别出新的威胁模式，并自动更新防御措施。自适应能力还要求网络能够快速响应新的用户需求。这可能涉及到软件更新的自动化部署，以及对网络设备的自动配置。通过这种方式，网络不需要手动干预，实现零接触网络目标。

6G 核心网韧性系统的演化范式是一个动态的、自监督、持续进化的过程，它涉及到从单个设备到整个网络生态系统的各个层面。通过模仿生物进化的原理，6G 网络能够更好适应不断变化的环境。在生物进化中，细胞分化成组织，组织通过连接构成有机体，有机体基于环境进化从而形成生态系统。同样地，6G 网络韧性系统的演化范式也应该是从基本的构建块开始，逐步发展成一个复杂的、高度互联的网络生态系统。在这个系统中，各个组成部分能够相互协作，共同适应外部环境的变化，从而确保整个网络的稳定性和安全性。在这个生态系统中，网络不仅能够抵御外部攻击，还能够适应内部变化，如技术升级、业务扩展和用户需求变化。通过这种持续的进化和适应，6G 网络能够保持其长期的稳定性和安全性，为用户和企业提供持续的价值和创新。

2.6 满足可测试可评估属性

6G 核心网韧性需要满足可测试、可评估属性，在此基础上提供定性、定量的网络韧性指标。在网络韧性测试方法方面，针对网络所面临的不同威胁，可以相应地使用不同的测试方法。

针对“已知的已知”威胁，即对于可以提前预想到的网络系统故障，可以采用混沌测试这一测试方法。混沌测试是通过主动向系统中引入异常状态，制造故障场景，并根据系统在各种压力下的行为表现，确定优化策略的一种系统测评手段。这种方法有助于提前探知系统风险，通过架构优化和运维模式的改进解决系统风险，从而实现韧性架构，提高故障免疫力。例如，在 6G 核心网中，随机或人为地使部分网元失效，在此情况下检查系统、业务整体运行情况是否受到影响。

针对“已知的未知”威胁，典型的是在网络安全场景下，对于系统中当前存在的漏洞点未知，且可能被攻击者利用的情况，可以采用模糊测试这一测试方法。模糊测试是一种通过向系统输入异常数据以发现潜在漏洞和错误的方法，它通过模拟攻击者可能使用的技巧，对网络协议、接口、服务等进行压力测试，以检验其在非标准条件下的行为。这种方法不仅关注安全性，还评估网络在异常流量下的性能表现，确保即使在面对攻击或系统故障时，网络仍能维持关键服务的稳定性。同时，模糊测试还能用于评估网络系统预测攻击的能力。

针对“未知的未知”威胁，可以采用内生安全白盒测试方法。内生安全白盒测试是一种破坏性的评估方法，用于评估基于架构的内生安全设备与系统的功能

安全和网络安全能力。这种方法通过开放部分可重构执行环境给攻击者，测试攻击者是否能够对整个设备或系统实施有效攻击，从而评估系统在面对“未知的未知”网络攻击时的网络韧性能力。

6G 核心网韧性评估度量需要建立网络韧性指标，现有的国标《信息安全技术 网络弹性评价准则》中定义了对网络弹性的基本评价准则。针对 6G 愿景，6G 网络韧性指标需要在此基础上进一步扩充。除了强化带宽、延迟、丢包率等传统网络服务质量（Quality of Service, QoS）指标，还要考虑 6G 泛在连接下空天地一体多接入方式的协同工作能力、人工智能驱动网络自治的可靠性、通感融合服务的准确性等。同时，还需要考虑在 6G 不同业务场景下，根据服务重要程度和复杂性等具体情况使用相对灵活的韧性指标。

在评估方法上，面向 6G 的韧性能力量化测试与评估方法基于系统架构的网络韧性评估，重点关注系统架构能力，通过定义网络韧性系统架构关键性质、核心能力和主要指标，对系统架构的网络韧性能力进行评估。具体的 6G 核心网韧性评估方法包括高层次定性评估、结合定性和半定量的覆盖式评估和详细定量的评分评估。这些评估可以通过混沌测试、模糊测试及内安安全白盒测试获得。系统架构网络韧性能力评价要素综合反映了系统所具备的网络韧性能力基线。若系统架构的某一评价要点得分过低，则表明系统即使在其他方面应用再多韧性技术，也难以从根本上提升系统对基本业务的网络韧性保证水平。

3. 6G 核心网智能韧性参考架构

6G 核心网的设计必须全面兼顾高动态性、高可靠性、高可用性和高质量的性能需求。在网络原生 AI 的加持下，6G 网络将突破传统移动网络的刚性防护理念，迈向一种更为灵活和稳定的电信级可靠性新范式。这一新范式将建立在冗余、异构、自监督、自适应和自生成等核心原则之上，通过在系统结构层面的创新，实现一种“构造即安全”的网络韧性。

6G 核心网智能韧性参考架构致力于在云网融合的环境中开辟一条增强网络韧性的新路径。随着云网融合的不断深化，6G 网络的规模和构成变得日益复杂，这要求多设备、多系统和多网络之间能够协同作业。为了构建一个韧性十足的网络解决方案，网络和服务提供商必须确保在空间、技术和供应链层面实现多样性。

如图 2 所示，参考架构将动态性、异构性和冗余性作为其设计的核心，同时整合了包括安全检测、威胁感知、意图识别、信任评估在内的多种先进安全技术。通过运用多设备、多系统和多网络的协同效应，该架构能够打破现有业务目标的单一性，使得在网络遭受攻击或出现故障时，能够灵活地调整承载设备、系统类型和网络路径，从而提供韧性服务。此外，该架构通过一个持续的循环过程，实现了对安全威胁的细致、多角度、实时的动态分析。这一过程基于四个核心阶段：预测、防御、检测和响应。在这个循环中，架构能够自动适应网络环境和威胁态势的不断变化，并持续优化其防御机制，确保网络的持续安全和稳定。

参考架构分为四层，包括：异构基础设施层、韧性使能层、韧性网络功能层，以及应用与开放层。异构基础设施层提供多类型基础资源供给（频谱、终端、站点、承载网、计算、存储）；韧性使能层包含：安全态势收集器、安全分析引擎、意图分析引擎、韧性控制器、安全编排器、VNF 超市、异构分析引擎、信任评估器等核心模块，这些模块之间通过协同以确保网络的韧性服务；韧性网络功能层承载韧性使能层智能编排的差异化韧性网络能力，从而为不同的 6G 场景服务；应用与开放层满足多样化应用场景需求，如：工控场景、车联网场景、远程医疗场景等。其中，韧性使能层是整个参考架构的关键，下面详细介绍其核心组件的能力，以及各组件之间交互的过程。

安全态势收集器：基于数据采集插件实时收集各类数据，包括但不限于网络性能数据、网络流量数据、系统日志、网络设备状态信息等，并将采集到的数据传输至数据汇聚中心，支持存储、检索和回放，同时支持可视化呈现。

安全分析引擎：包含入侵检测模块、风险研判模块、安全响应模块、底层算法库。入侵检测模块主要基于模型预测或基于三方知识融合进行预测；风险研判模块主要进行数据关联分析，包括归因分析和时序分析；安全响应模块负责安全分析结果的推送，以及对遭受安全威胁时的攻击溯源；算法库包括 CNN、LSTM、BERT 等常见的 AI 模型。

意图分析引擎：由意图解析模块、编排策略模块组成。其中，意图解析模块负责识别用户需求或当前网络状态，并将意图转化为具体的安全策略（如：DHR 构造、防止未授权访问、检测和响应 DDoS 攻击、CPU 预测等），在网络中自动部署和执行，同时监控网络事件，实现快速响应。意图分析可以实现零接触式

动态编排与控制，大大提高业务韧性的同时降低运营成本。

韧性控制器：承载 NFV 管理和 SDN 控制器能力。安全编排模块集成各种防御策略能力（包括拟态防御、移动目标防御、防火墙等），其根据决策层安全部署请求，将面向用户的韧性服务转为动态调度、随机迁移、冗余管理、安全策略等，如网络、软件参数的动态调整，等价功能异构体的管理、轮换策略等，然后把任务下发到编排器中；编排器负责新建一个子网络（Sub Network），并在虚拟资源上生成若干 NF（如果是拟态防御策略，则包括 VNF 的异构副本，网络功能级的拟态裁决器），在 SDN 控制器的协助下，根据韧性要求完成这些 NF 链路连接、路由规则下发及自动化部署等，然后把子网络已生成的信息反馈给韧性控制器，完成一个子网的生成。

安全编排器：基于标准的 ETSI NFV 架构，包含虚拟化网络基础设施（NFV Infrastructure，NFVI）、虚拟网络功能与网元管理（Element Management，EM）、管理与编排器（Management and Orchestration, MANO）和运营支持系统/业务支持系统（Operational Support Systems/Business Support Systems, OSS/BSS）四个模块，模块内组件和各模块间通过参考点进行通信。负责 VNF 的生命周期管理和跨云协同管理。

VNF 超市：负责各种不同虚拟化网络功能的管理。VNF 超市是一个开放的空间，任何符合条件的厂家都可以将自己的网络能力发布到里面。VNF 超市为不同的网络需求打包满足条件的 VNF 列表，并配合意图驱动引擎和安全编排器完成对应的网络实例化。

异构分析引擎：多供应链提供不同的网络组件，网络组件之间异构度越大则可认为发生共模漏洞或同时出现功能故障的概率越小。异构分析引擎则负责对同种功能不同厂商的网络组件异构度进行分析，为冗余方案提供可靠性最大的组件集合。

信任评估器：包括静态和动态评估。静态评估是基于代码的静态扫描信息进行信任评估，包括识别软件漏洞、代码质量、开源供应链安全识别等信息；动态评估则基于历史数据对网络设备进行评估，以选择最佳状态的网络设备作为 6G 网络服务的提供者。

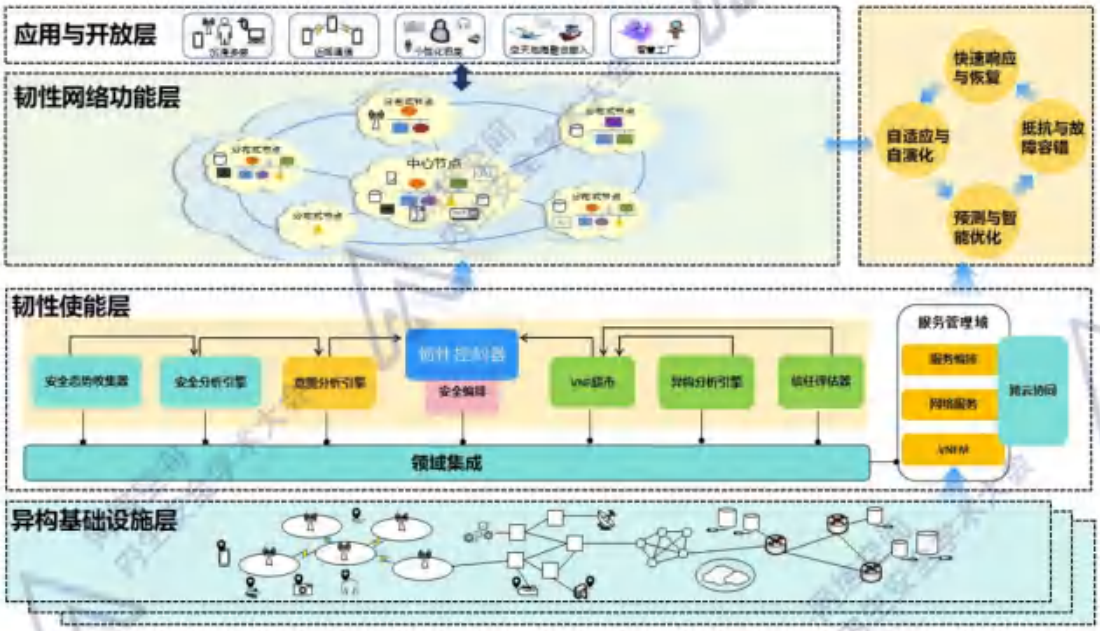

图 2 6G 核心网智能韧性参考架构

上述参考架构的关键能力与第二章四项网络韧性核心目标的对应如表 1 所示。该框架包含差异化韧性能力构造和零接触式韧性管理两个关键流程，两个流程不断循环，以达到网络状态最优。

1）差异化韧性能力构造。用户输入韧性网络需求，意图分析引擎解析用户意图并将其转化成对应的意图元组（意图元组指示符合用户韧性需求的网络拓扑结构和韧性策略）。韧性控制器根据意图元组去 VNF 超市获取对应的网络资源。异构分析引擎和信任评估器会提供 VNF 超市中的网络资源的评估信息，韧性控制器根据评估信息通过安全编排器实现差异化韧性能力构造。

2）零接触式韧性管理。安全态势收集器会采集网络各类数据，并进行存储和可视化。安全分析引擎基于采集的数据集通过 AI 算法进行分析和预测，并将分析的结论传递给意图分析引擎，意图分析引擎识别网络运行态语义信息，并下发调整策略至韧性控制器，如果需要更换 VNF 或冗余备份 VNF，韧性控制器会去 VNF 超市获取对应的网络资源，韧性控制器最终通过安全编排器实现韧性自适应能力。

表 1 参考架构关键能力与网络韧性核心目标对应表

使能器名称	能力概述	支撑的关键能力	支撑的韧性目标
安全态势收集器	数据采集	多维感知	预测
安全分析引擎	安全分析 威胁预测	多维感知 迭代更新	预测与智能优化
意图分析引擎	智能分析 意图识别	动态修复 迭代更新	自适应与自演化
韧性控制器	动态调度 韧性控制	动态修复	抵抗与故障容错
安全编排器	隔离、可定义	灵活包容 动态修复	快速响应与恢复
VNF 超市	多供应链	灵活包容	故障容错
异构分析引擎	冗余/异构	多维感知	抵抗与故障容错
信任评估器	信任评估	多维感知	预测与智能优化

4. 6G 核心网智能韧性使能关键技术

4.1 架构类技术

4.1.1 DHR 技术

如图 3 所示，动态异构冗余（Dynamic Heterogeneous Redundancy，DHR）架构核心在于引入基于策略裁决的动态反馈控制和运行环境结构加密机制，以实现高度韧性和快速恢复能力。尤其针对 6G 网络面临的硬件和软件故障、恶意及意外攻击、以及自然或人为灾难等多方面安全威胁，DHR 技术提供了一种新视角。它将广义不确定摄动或扰动转化为 DHR 构造内部的差模或共模扰动问题，使攻击者难以识别目标、难以评估攻击效果、无法继承攻击经验、难以复现攻击场景，从而有效抑制“未知的未知”网络威胁，大幅提高 6G 网络空间的韧性。

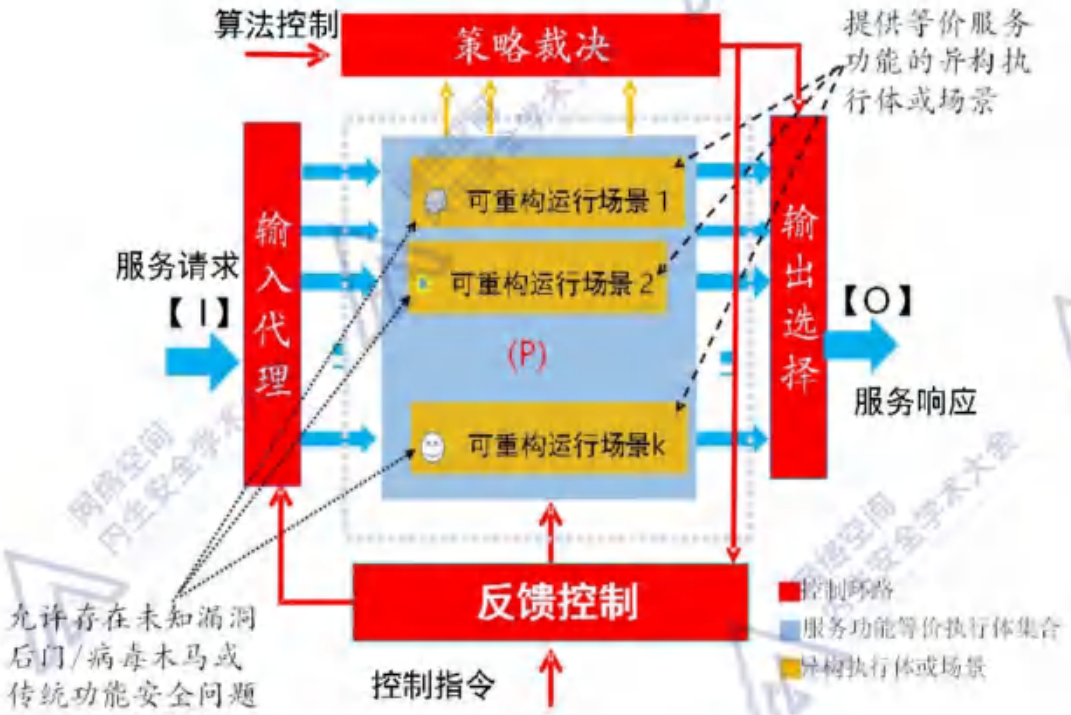

图 3 DHR 构造架构图

DHR 对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**DHR 的异构性（设备、操作系统、底层硬件）减少了 6G 网元设备因同种漏洞攻击导致服务不可用概率，其冗余性减少了网络功能因不可靠或自然灾害导致的服务不可用，基于大数的裁决机制避免了网络信息或数据被篡改的风险。因此，DHR 可有效应对开放环境高级持续威胁、云化网络功能失效威胁、多域流转隐私泄露威胁引起的 6G 服务功能或性能下降的问题。
- **防御维度：**DHR 通过结构构造来保证 6G 核心网韧性，主要体现在其架构的冗余和动态的特性。6G 核心网系统可采用动态异构冗余（DHR）构造技术，使用多设备、多系统、多网络的复杂性来改变现有业务目标的相似性、单一性，在网络受到攻击或故障时能灵活改变网元的承载设备、系统类型和硬件环境，在架构上实现网络的高可靠、韧性服务。
- **提升的关键能力：**DHR 技术为 6G 核心网韧性构建提供一种新的视角，强调在持续变化的多样化安全威胁面前，通过动态和智能的策略实现网络的持续稳定和安全，保证了网络韧性的动态修复、迭代更新能力。
- **支撑的核心目标：**DHR 基于对系统整体和局部资源的智能识别与动态调配，

实现从静态到动态的安全保障机制，从而大幅提升网络系统的适应性和恢复速度。通过实时监控网络状态和安全事件，DHR 技术能够迅速激活局部动态冗余机制，以最小的资源实现最快速的恢复和防御，确保 6G 核心网在各种复杂环境下的超稳态运行。

4.1.2 ZSM 技术

如图 4 所示，零接触式网络服务和管理（Zero-Touch Network and Service Management，ZSM）技术通过实现网络服务的全自动化管理，包括自我配置、监控、修复和优化，利用 AI/ML 技术进行智能决策，以及跨域协同管理，显著提升了 6G 网络的韧性，确保了服务的连续性和快速迭代，从而为 6G 网络的高效、稳定运行提供了强有力的支持。

ZSM 架构对 6G 核心网韧性的提升体现在以下方面：

- **可应对威胁：**ZSM 搭载零接触式闭环控制技术的自动化和智能化减少了人工干预，能够降低人工失误造成的配置错误和策略更新不及时导致的服务不可用概率，有效应对网络配置错误导致的网络功能故障失效威胁。
- **防御的维度：**零接触式闭环控制技术通过网络智能自治来增强网络韧性，主要体现在其自动化运维特性上。网络通过点面配合，自动感知预测预防故障，及时处理故障并恢复网络，实现“自愈”。
- **提升的关键能力：**零接触式服务管理通过机器学习增强网络的多维感知能力，实现环境变化的快速适应。全流程自动化运维减少了人为干预，缩短了故障恢复时间，提升了网络的动态修复和自我优化能力。这种管理方式减少了对人工的依赖，提高了网络的智能化水平，确保了 6G 核心网在面对不断变化的环境和挑战时的持续迭代更新。
- **支撑的核心目标：**通过自动化的故障检测和恢复机制，零接触式闭环控制技术确保网络在遇到故障或攻击时能够迅速恢复正常运行，提供高可靠的服务，保证了在高度复杂网络的韧性运行能力。同时。对于攻击造成的故障和性能下降，零接触闭环控制系统能够根据系统状况动态及时灵活调配系统资源，以保证关键服务正常运行。并且可以根据环境变化自适应优化网络配置，高效利用网络资源，为关键业务提供可靠保障，为用户提供透明化的网络韧性服务。

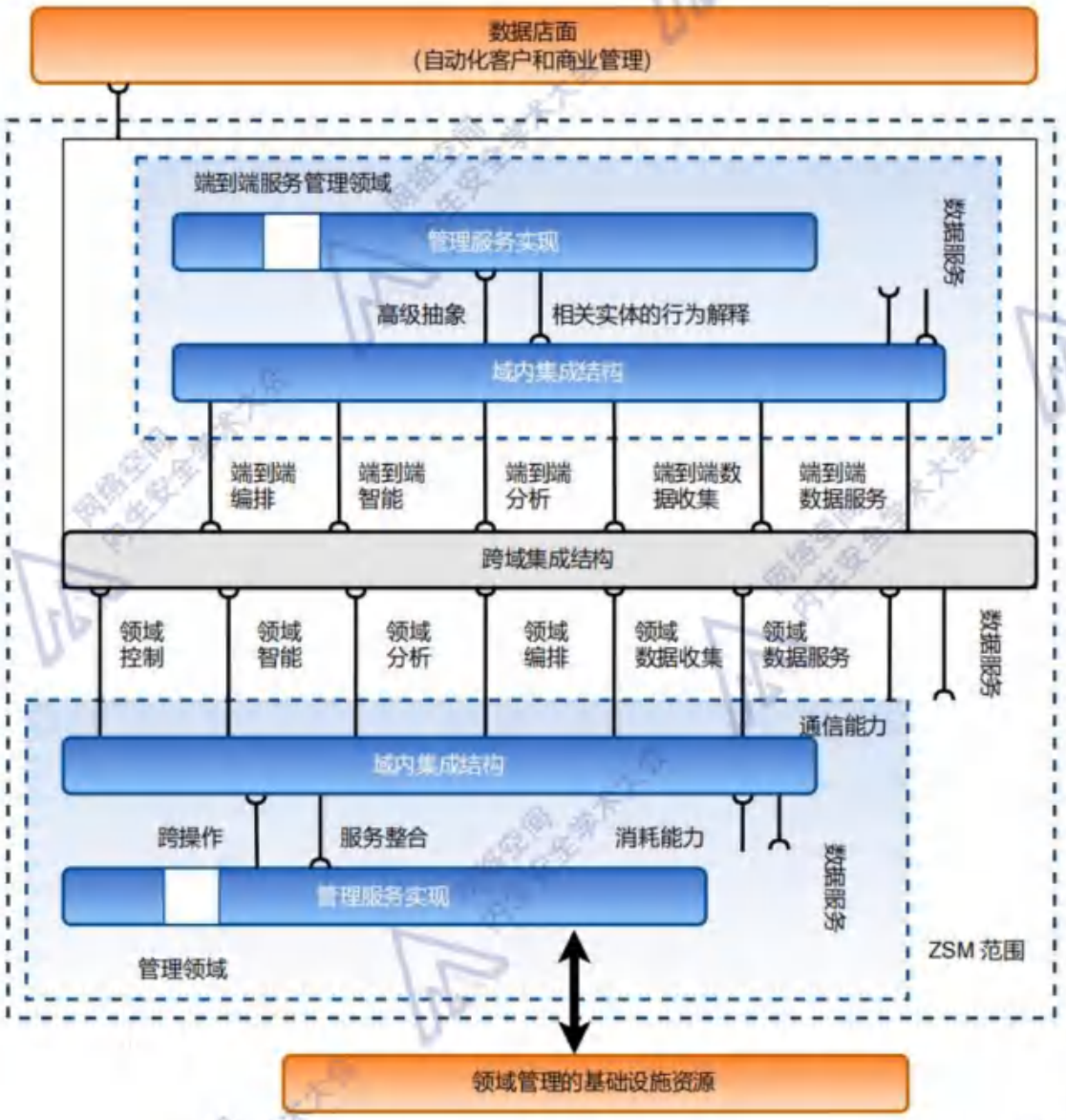

图 4 ZSM 框架参考图

4.1.3 零信任技术

如图 5 所示，零信任（Zero-Trust，ZT）是一种安全框架，其核心思想是“永不信任、始终验证”。零信任网络架构认为所有的网络流量都应该被视为潜在的威胁，需要基于访问主体身份、网络环境、终端状态等尽可能多的信任要素对所有用户进行持续验证和动态授权。此外，零信任将访问目标的权限细化到应用级、功能级、数据级，只对访问主体开放所需的应用、功能或数据，极大地收缩了潜在的攻击面。网络韧性和零信任共享关于网络威胁的假设。然而，在有争议的网络环境中，网络韧性是由任务保证驱动的，零信任的重点是防止对数据和服务的未经授权访问。

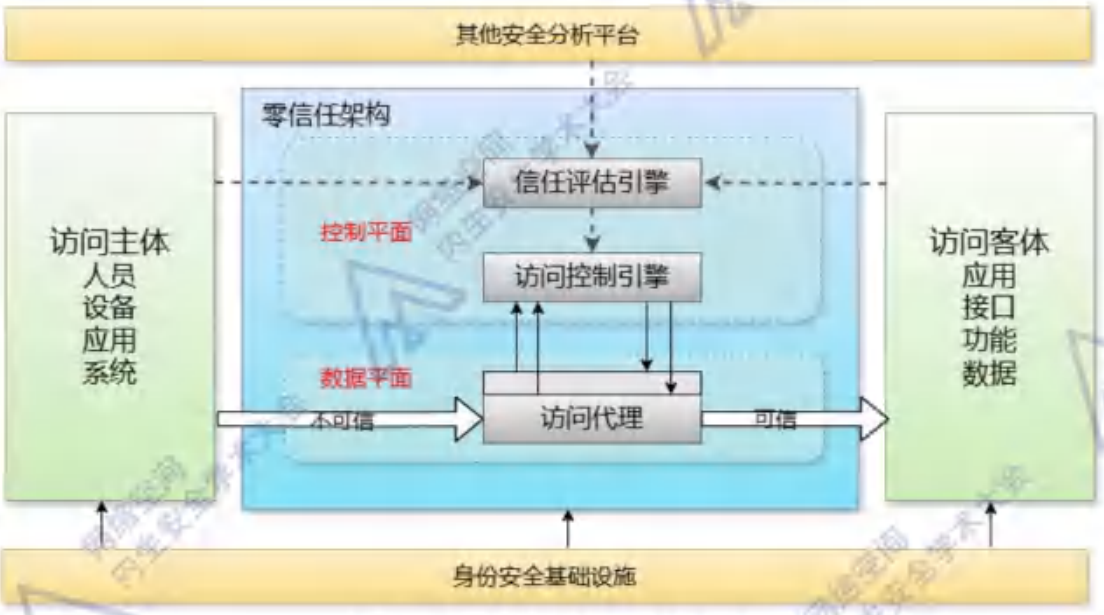

图 5 NIST 零信任架构总体框架图

零信任架构对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**零信任技术的实施，通过精细化的访问控制和动态授权，减少了因单一漏洞攻击导致服务不可用的概率。其持续验证的特性，确保了整个访问过程中用户身份的合规性，实时管控访问过程中的违规和异常行为，有效应对开放环境高级持续威胁、多域流转隐私泄露威胁引起的服务功能或性能下降的问题。
- **防御维度：**在零信任模型中，网络被划分为多个小的、隔离的区域，每个区域都实行独立的安全策略和访问控制。这种微分段策略限制了潜在的攻击者在网络中的横向移动，即使攻击者成功侵入了网络的某个部分，他们也无法轻易地访问其他部分，从而降低了整个网络受到损害的风险。
- **提升的关键能力：**零信任技术通过持续的多维感知、精细化的访问控制和自动化的响应机制，显著增强了网络的弹性，特别是在动态修复方面，能够实时检测和响应安全威胁，快速调整访问策略以隔离或限制可疑活动，从而保护网络免受攻击和故障的影响。同时，它也支持网络的灵活包容和迭代更新，使网络能够适应不断变化的威胁环境和业务需求。
- **支撑的核心目标：**零信任通过对终端风险、用户行为进行实时分析，同时结合安全控制策略，综合考虑访问主体、目标客体、环境属性（终端状态、网络风险、用户行为等）进行权限动态判定，实现对应用访问、功能使用、数据交互等多维度控制，能够为 6G 核心网提供更为坚实的安全保障。零信任

模型强调持续监控和实时分析网络活动。通过使用先进的分析工具和机器学习算法，系统能够识别出异常行为和潜在的安全威胁，并迅速采取措施进行响应。这种自动化和智能化的监控机制大大提高了网络对攻击的检测和响应速度，增强了网络的自适应能力。

4.1.4 网络数字孪生技术

如图 6 所示，数字孪生技术通过集成物理模型、传感器数据和历史运行数据，创建实体装备的虚拟映射，反映其全生命周期。它是一个数字映射系统，超越现实，实现物理网络实体与虚拟孪生体的实时交互。数字孪生网络的核心要素包括数据、模型、映射和交互，利用这些要素，可以对物理网络进行全生命周期的分析、诊断、仿真和控制。这种技术优化了网络应用的部署，降低了成本，提高了效率，减少了对现网的影响，推动了网络的极简化和智慧化运维。

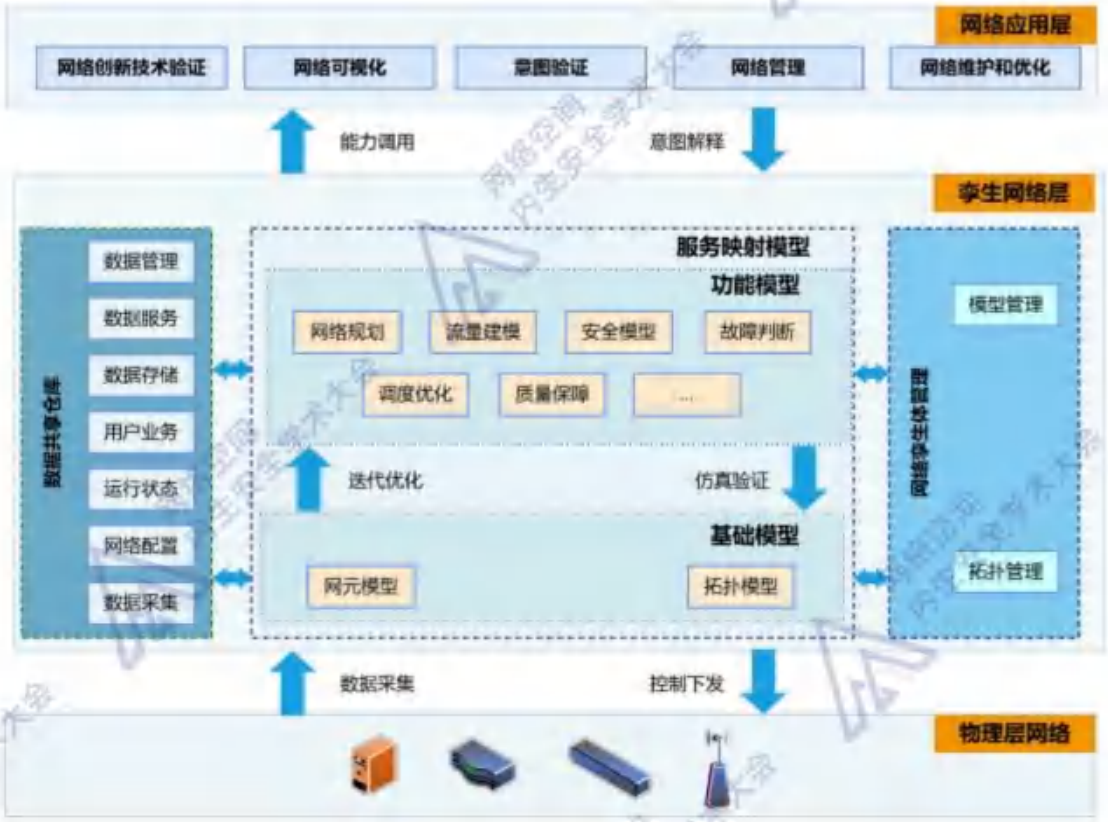

图 6 网络数字孪生技术框架图

网络数字孪生技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**网络数字孪生技术能有效应对开放环境高级持续威胁和多域流转隐私泄露威胁。它通过在虚拟空间中创建网络的精确映射，模拟攻击和数

据流转，预测潜在风险，测试防御策略，从而在不影响实际网络的情况下优化安全措施。这种方法有助于提前识别和防御 APT 攻击，同时监控和预防隐私数据泄露，增强网络的整体安全性和韧性。

- **防御的维度：**网络数字孪生技术在网络韧性的点、线、面三个维度上提供全面防护。在点维度，它通过模拟网络功能测试安全策略；在线维度，它监控网络链路和流程，及时发现威胁；在面维度，它构建网络架构的虚拟映射，预测攻击影响，优化防御策略。这种技术通过虚实映射和动态交互，增强网络的预测、抵抗、响应和自适应能力，提升网络的安全性和韧性。
- **提升的关键能力：**网络数字孪生技术通过创建物理网络的精确数字副本，实现了多维感知，能够模拟和预测网络行为，增强了网络的感知能力。它提供了一个灵活包容的平台，允许在不影响实际运行的情况下测试和优化网络策略。此外，网络数字孪生技术通过在虚拟环境中的模拟，支持动态修复网络问题，并能够迭代更新网络配置以适应不断变化的环境，从而提升了网络的韧性和适应性。
- **支撑的核心目标：**网络数字孪生技术通过建立物理网络的数字映射，实现对网络动态变化的实时监控。这项技术能够模拟、优化和预测物理实体的行为和性能，从而实现网络的智能优化。通过在虚拟环境中的模拟和预测，网络可以在实际发生故障前预测并准备相应的容错措施，这增强了网络的抵抗能力和故障容错性。此外，网络数字孪生技术还允许在虚拟环境中测试和验证新的网络策略，然后将其实施到实际的物理网络中。这种能力使网络能够自适应地响应外部环境的变化，并实现自我演化和优化。

表 2 给出了各架构类技术与 6G 核心网韧性能力的对照表。优良的系统架构能够确保网络系统适时感知威胁风险、稳健抵抗威胁攻击、控制威胁在最小范围内、及时应对化解系统扰动并在可接受时间内恢复其功能，并根据威胁变化智能调整适应的能力。

表 2 架构类技术韧性使能对照表

技术名称	6G 核心网韧性能力													
	可应对威胁			防御维度			提升的关键能力				支撑的核心目标			
	开放环境高级持续威胁	云化网络功能失效威胁	多域流转隐私泄露威胁	点	线	面	多维感知	灵活包容	动态修复	迭代更新	预测与智能优化	抵抗与故障容错	快速响应与恢复	自适应与自演化
DHR	√	√	√	√		√			√	√		√	√	
ZSM		√		√		√	√		√	√	√		√	√
零信任	√		√	√		√	√	√		√		√	√	√
数字孪生	√		√	√	√	√	√		√	√	√			√

4.2 能力类技术

4.2.1 AI Agent 技术

如图 7 所示，AI Agent 技术是一种先进的人工智能系统，能够在极少的人工指导下执行复杂任务并做出决策。与传统的自动化工具不同，AI Agent 具备独立思考、适应环境和自主执行任务的能力。它们通过感知外部环境、分析数据并根据预设目标进行决策，展现出强大的灵活性和智能性。

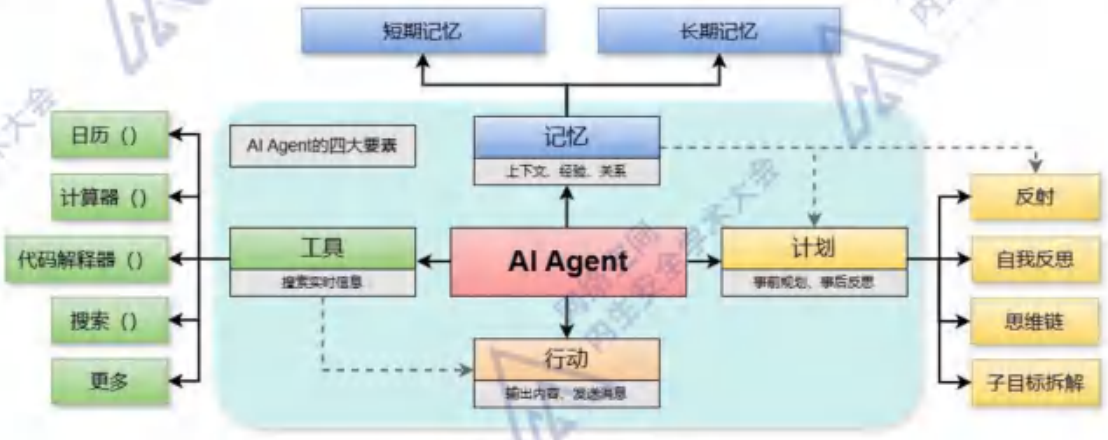

图 7 AI Agent 框架图

AI Agent 技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**在 6G 网络中，AI Agent 通过自动化安全防御和智能故障预测与恢复来抵御网络威胁和功能威胁。对于网络安全威胁，AI Agent 能够实时分析网络流量和行为模式，主动识别并响应潜在的攻击，如 DDoS 攻击或恶意软件传播，并通过持续学习新的攻击手段动态调整安全策略。针对功能威胁，AI Agent 利用历史数据预测设备故障和服务中断，提前采取措施，如重新配置路由路径或激活备用资源，从而减少服务中断时间并维持高质量的服务。
- **防御维度：**AI Agent 从点和面两个维度为保证 6G 网络韧性发挥作用。在单个节点层面，每个接入点配备的 AI Agent 可以独立感知环境变化、提供定制化服务，并快速进行自我修复，确保局部服务的连续性和稳定性。在面层面上，AI Agent 通过全局视角进行动态资源调度，设计冗余路径以提高抗毁性，并促进不同地理位置的 AI Agent 之间的协作，共同维护整体 6G 网络的稳定性和安全性，从而实现整个 6G 网络系统的高可靠性和自适应能力。
- **提升的关键能力：**AI Agent 技术通过跨域智能协同能力显著提升 6G 网络韧性，使多个 AI Agent 能够根据环境反馈和历史数据独立进行推理与决策优化，并在不同地理区域或网络节点间共享信息、协调资源分配及故障恢复策略，从而实现更高效的服务质量保障和自动化的网络管理，减少对人工干预的需求。
- **支撑的核心目标：**AI Agent 利用先进的机器学习算法从历史数据中学习模式，提前识别潜在的网络故障或安全威胁，并自动采取预防措施，从而增强系统的预测能力。面对动态且不可预测的环境，AI Agent 能够迅速调整策略，确保即使在网络组件遭受攻击或出现故障时，整个系统仍能保持关键服务的连续性和数据完整性，提升网络的承受能力。一旦发生异常情况，AI Agent 会立即启动自动化故障检测与恢复机制，如重新配置路由路径或激活备用资源，实现快速恢复。此外，持续的学习和适应过程使得 AI Agent 不断优化其执行策略，提高应对新挑战的效率和效果，增强了 6G 网络的自适应性，确保在各种复杂场景下都能提供可靠且高质量的服务。

4.2.2 可持续的意图管理技术

如图 8 所示，可持续的意图管理技术是一种创新的网络资源管理和配置方法，结合网络意图与能源效率，通过动态反馈控制和自动化调整机制，实现网络的高度自适应性和快速恢复能力。面对现代网络的复杂配置、频繁变更及安全威胁，此技术利用网络意图优化行为，确保网络自动适应变化、自我修复并抵御安全威胁，同时关注能源效率，全面提升网络韧性和安全性。通过将战略意图转化为具体指令，该技术促进资源高效利用与动态调整，减少人为错误，利用智能算法在不影响服务质量的前提下寻找最优配置方案，以最低能耗提供最佳服务效果，并通过持续监控网络状态和性能指标，及时响应异常，迅速恢复服务，确保网络在各种挑战下高效稳定运行。

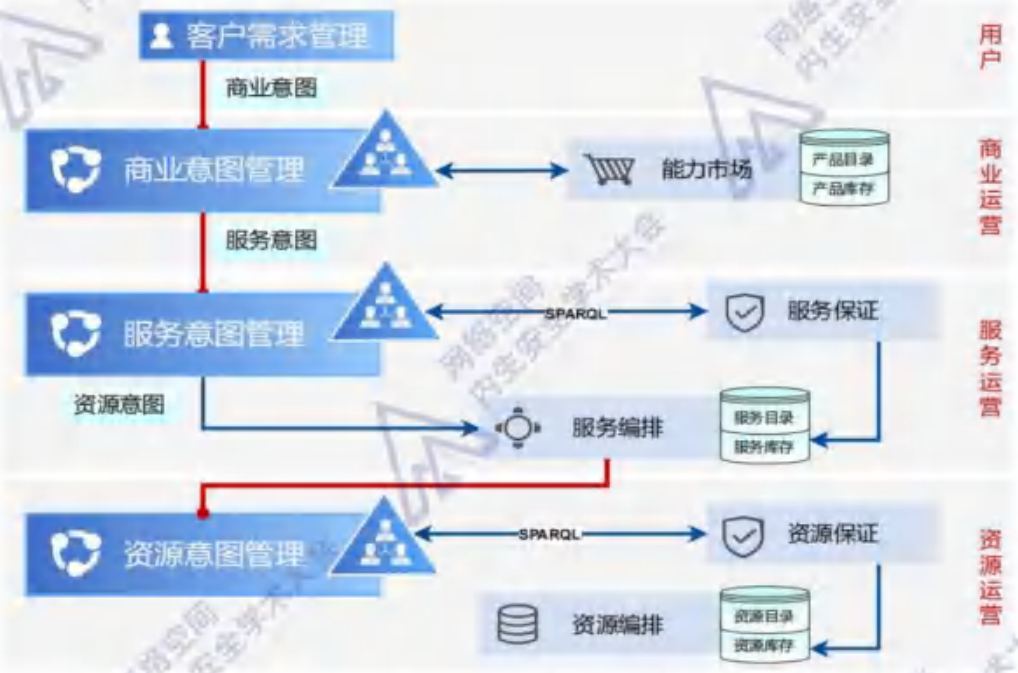

图 8 可持续意图管理原理框图

可持续的意图管理技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**可持续的意图管理技术在 6G 网络韧性环境下，通过其高度自动化和自适应性，能够有效应对网络威胁和功能威胁。对于开放环境高级持续威胁，该技术能够实时监控网络状态和流量模式，快速检测出异常活动如 DDoS 攻击、恶意软件传播等，并即时启动预定义的应对措施，如自动隔离受影响节点、调整流量路径，以减轻攻击影响，确保网络的稳定性和可用性。针对云化网络功能失效威胁，通过持续验证网络意图，确保所有网络功能和

服务按预期运行；当检测到任何偏离预期的行为时，能够自动执行恢复操作，比如重服务实例或重新分配资源，以维持服务的连续性和质量。

- **防御维度：**通过意图驱动的管理，确保每个网络功能都按照预定的意图和策略运行，减少误配置和潜在的安全风险。检测到某个网络功能出现问题时，自动重新分配资源或启动备用功能，以最小化服务中断。利用 AI/ML 技术进行全局优化，以实现在不同网络域之间平衡负载和资源，提高整体网络的抗攻击能力和故障恢复能力。
- **提升的关键能力：**通过持续监控和分析网络流量、性能指标和日志数据，AI/ML 模型可以识别出异常行为或潜在的攻击，增强网络的感知能力。根据网络负载和业务需求动态调整资源分配，确保网络在面对变化时能够灵活响应。通过意图驱动的管理，网络可以自动根据预定义的策略和意图进行配置，提高对新服务和新需求的适应性。在检测到网络故障或性能下降时，系统可以自动执行预定义的修复策略，如重新路由流量、启动备用服务或调整资源分配。AI/ML 模型可以根据新的数据和经验不断学习和优化，以适应网络环境的变化，提高网络管理的效率和效果。
- **支撑的核心目标：**在预测方面，利用机器学习并结合网络意图，预测未来趋势，提前调整资源分配和优化系统性能。在承受方面，通过多层安全防护和快速故障恢复，基于意图的自动化机制确保网络在故障或异常情况下快速恢复。在恢复方面，系统具备自愈能力和自动化恢复机制，通过意图驱动的故障检测和修复，快速响应各种变化，保证系统稳定性和可用性。在自适应方面，通过实时监控和自适应控制算法，结合网络意图动态调整系统参数和资源分配，提高系统性能和效率。这些措施确保 6G 网络在复杂多变的环境中保持高效、稳定和可靠的运行。

4.2.3 DFP 技术

如图 9 所示，DFP（Dynamic Function Placement，动态功能放置）是 6G 架构中的关键技术，它允许在不同领域（从最终用户到中心云）之间灵活部署和迁移网络功能，以实现服务的差异化和连续编排。DFP 需要跨领域操作，要求各领域共享资源和 API 以支持服务发现，并确保不同云实例之间的网络功能能够高效、技术无关地互联互通。DFP 的核心职责包括功能实例的重新

定位和运行时上下文的转移，与 NFV 的生命周期管理（LCM）的传统功能紧密相关。DFP 和连续体编排在 6G 架构中相辅相成，两者共同支持 6G 网络在提供高可靠性和韧性服务方面的能力。

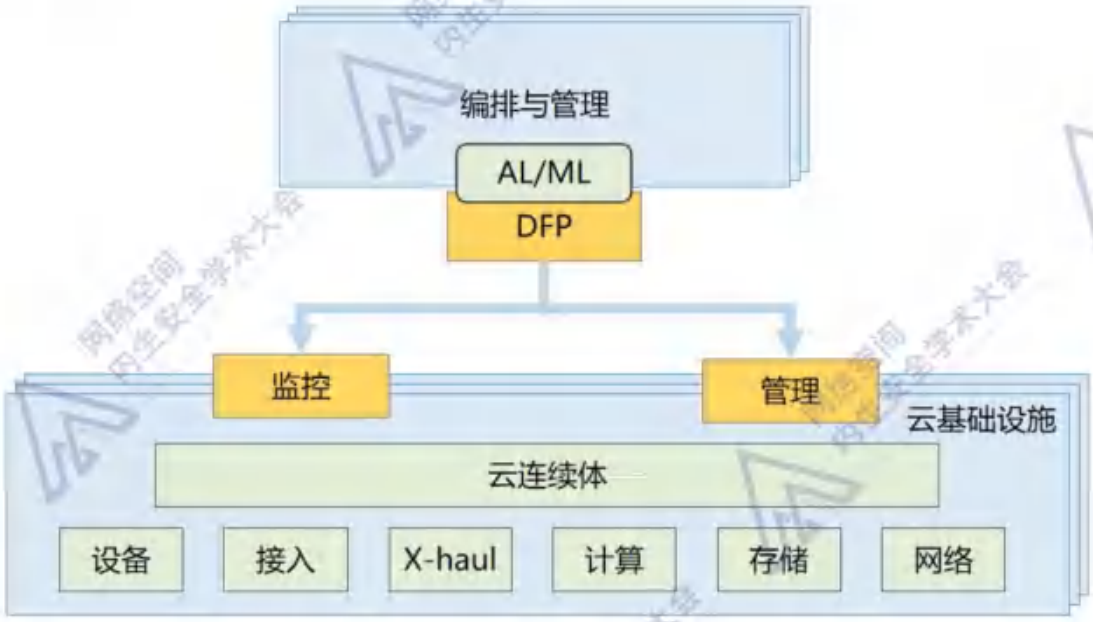

图 9 基于 DFP 实现云连续体编排架构图

DFP 技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**DFP 通过在不同网络域之间动态部署网络功能（或多个位置部署功能副本），降低了单点故障的风险，增强了网络对抗恶意攻击的能力。在面对分布式拒绝服务（DDoS）攻击或其他网络层攻击时，DFP 能够快速重新定位服务，以维持网络服务的连续性。DFP 支持数据在不同网络域间的安全迁移，通过与加密技术结合，DFP 能够在数据传输过程中保护数据不被未授权访问或篡改。
- **防御维度：**6G 网络面临的挑战不仅仅是常规的网络故障，还包括更加复杂多变的安全威胁及高强度的服务需求。DFP 通过在网络中创建功能副本，实现了架构层面的冗余，为网络提供了在遭受攻击时的备份（备用网络功能和路径）。DFP 允许网络根据实时威胁情况动态调整资源分配和功能部署，使网络能够灵活应对不断变化的安全威胁。DFP 还支持跨不同网络域的服务编排，使得网络能够在更广泛的范围内实现协同防御，提高了整体网络的防御能力。DFP 实现 6G 网络韧性全局可感、可控、可防的能力。其防御的维度包含点、线、面。

- **提升的关键能力：**DFP 允许网络运营商和第三方开发者通过编程方式自定义和部署网络功能，以适应特定的韧性服务需求。DFP 结合意图驱动的编排可以自动执行网络配置和管理任务，减少人工干预，提高网络韧性管理的效率和准确性。在多域环境中，DFP 确保服务可以在不同网络域之间无缝迁移，即使在某个域发生故障时也能保持服务的连续性。DFP 结合 AI 和 ML 技术，能够预测潜在的安全威胁，并主动调整网络配置以防御这些威胁。在遭受攻击或故障时，DFP 可以快速重新部署网络功能，实现网络服务的快速恢复，增强网络的韧性和鲁棒性。
- **支撑的核心目标：**DFP 在 6G 网络中通过预测与智能优化实现资源的高效管理，通过抵抗与故障容错增强网络的安全性和可靠性，通过快速响应与恢复确保服务的连续性，以及通过自适应与自演化能力使网络能够持续进化以适应不断变化的环境和需求，从而为未来的通信网络提供灵活、高效、安全和可靠的服务。

4.2.4 MLOps 技术

如图 10 所示，云原生技术的基本框架包括容器化技术、容器编排、微服务架构、持续集成与持续部署（CI/CD）以及 DevOps 文化与实践等方面。这些技术和框架相互配合，共同构成了云原生应用的开发、部署和管理体系。MLOps（机器学习运维）是一种实践方法，它结合了机器学习（ML）、开发运营（DevOps）和数据工程的概念，旨在简化机器学习模型和工作流程的开发、部署以及持续维护过程。MLOps 的核心在于将机器学习模型的整个生命周期进行管理，从数据收集、模型创建、软件开发生命周期、持续集成/持续交付，到编排、部署、健康、诊断、治理和业务指标。

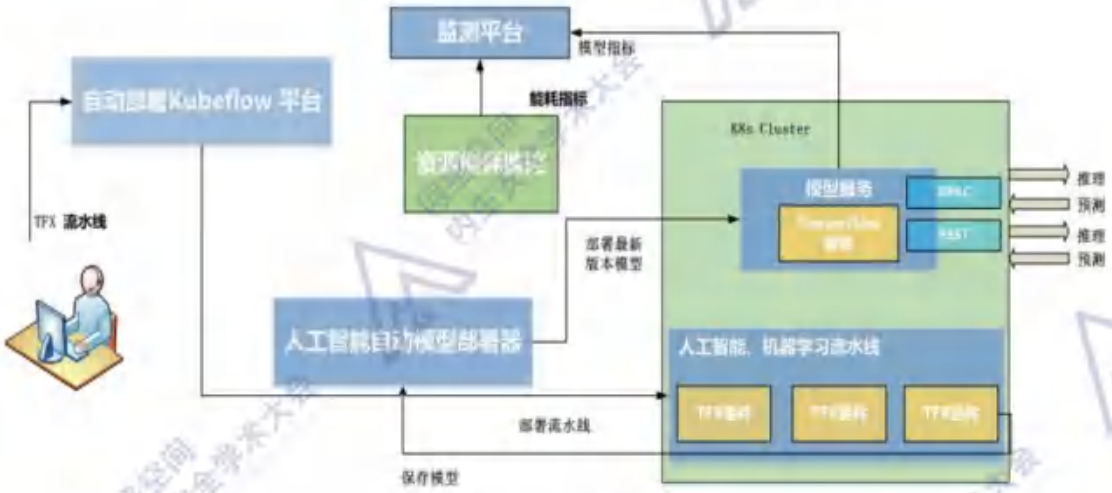

图 10 MLOps 架构图

MLOps 技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**微服务架构将复杂的 6G 网络应用细分为更小、更灵活的服务单元，每个服务单元都能够独立进行开发、部署、扩展和维护，使得整个系统更具韧性和可伸缩性。在面对复杂多样的 6G 网络安全威胁和需求时，这种功能分割方案显著减少攻击面和数据外泄的可能性，负载均衡和冗余备份机制减少了网络威胁中的云化网络功能失效威胁。
- **防御维度：**容器化是云原生技术的另一个核心要素，通过将应用程序及其运行环境打包成容器，容器化技术提供了一种轻量级、一致性和可移植的解决方案，使得海量异构的 6G 网络应用能够在不同的计算环境中无缝运行。当 6G 网络的某个区域受到攻击或发生故障时，容器化技术可以快速重新部署受影响的服务到安全区域，从而最小化服务中断时间，确保关键业务的连续性不受影响。此外，容器化的微服务架构还支持对网络资源的细粒度管理，能够根据实时需求动态分配资源，从而优化性能与成本效率，增强网络在面对资源压力和环境变化时的韧性表现。
- **提升的关键能力：**CI/CD 作为云原生技术的第三个核心功能，通过自动化的软件开发流程，实现从代码提交到部署的快速迭代和连续交付，确保 6G 网络海量服务和应用能够迅速响应韧性需求的变化。此外，CI/CD 支持对 6G 网络配置和服务进行持续的优化和调整，维持高度可靠性和安全性的同时，提供高效、灵活、优化的网络韧性服务，满足 6G 网络对于连续、可靠、安全的韧性需求。

- **支撑的核心目标：**通过持续集成和持续部署（CI/CD）流程，MLOps 能够快速迭代模型，以适应网络环境的变化，实现预测性维护和优化。MLOps 强调自动化和监控，有助于提高系统的容错能力。通过自动化测试和智能监控模型，MLOps 可以快速发现并响应模型故障，减少系统故障的影响。MLOps 支持模型的持续训练，使得智能模型能够根据新数据进行自我更新和演化。这种能力使网络能够自适应地响应外部环境的变化，实现自我演化和优化。

4.2.5 MTD 技术

移动目标防御（MTD）通过不断变化网络或系统的配置来提升安全性，使攻击者难以找到稳定的攻击点。MTD 的核心在于增加系统的不可预测性，通过定期更改关键参数如 IP 地址和端口，以及采用随机化技术，让攻击者难以构建有效的攻击策略。这种防御策略还具备自适应能力，能够自动调整防御措施以应对新的威胁。MTD 在设计时注重防御的深度，通过多层次的变化提高攻击者的攻击成本。在实施 MTD 时，需要综合考虑安全性、成本、性能和可管理性，确保在不牺牲用户体验的前提下，实现动态且有效的安全防护。

MTD 技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**MTD 技术通过动态变化网络配置，如随机化 IP 地址、端口号和路由策略，增加了攻击者识别和利用系统弱点的难度。在 6G 网络中，这种不断变化的环境使得攻击者难以找到一个稳定的攻击点，从而有效提高了网络应对开放环境高级持续威胁能力。
- **防御维度：**MTD 技术可以通过随机化机制来保护网络功能层面的安全。可以通过 IP 地址跳变、端口跳变、动态路由等手段，增加网络链路和流程的不确定性，改变网络架构的静态特征，增加攻击者分析和攻击网络架构的难度，从而提供对整个网络架构的动态防护，实现网络的高可靠、韧性服务。
- **提升的关键能力：**MTD 技术通过动态改变系统配置，如 IP 地址跳变、端口跳变等，为网络提供了灵活的防御策略。MTD 技术的核心在于动态地改变系统的攻击面，这种动态变化使得攻击者难以维持对网络的控制。当网络遭受攻击时，MTD 可以通过快速变化攻击面来隔离受损部分，从而实现动态修复和恢复。
- **支撑的核心目标：**MTD 技术通过随机化和多样化减少攻击者攻击成功的可

能性，以此限制攻击者的攻击，大大缩短攻击者的攻击周期或使攻击者难以完成攻击任务，而提高系统的抵抗能力。MTD 框架可以根据目标系统的安全状态自适应地变换攻击面，这种适应性体现在能够根据网络安全状态和系统自身的安全状态来调整防御策略，实现自适应的能力。

4.2.6 TEE 技术

可信执行环境（Trusted Execution Environment，TEE）是一种硬件辅助技术，它通过在处理器中创建一个隔离的执行区域，确保在该环境中运行的代码和处理的数据的安全性。这种隔离机制使得即使在多任务操作系统和虚拟化环境中，敏感数据也能在加密状态下安全处理，从而保护数据免受恶意软件和未授权访问的威胁。TEE 技术主流的实现方案是在硬件设备上提供一个独立的区域进行存储和运算，以保证在该区域内的代码和数据安全可信。所以 TEE 功能与各个芯片厂商的芯片紧密相关。目前主流的可信执行环境技术产品主要有：ARM 公司的 TrustZone、Intel 公司的 SGX（Software Guard Extensions）和 AMD 公司的 SEV（Secure Encrypted Virtualization）。

TEE 技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**TEE 通过提供一个隔离的执行环境，确保敏感操作和数据处理在这个受保护的环境中进行。这种隔离性减少了因系统漏洞或恶意软件攻击导致的数据泄露概率，其安全性不依赖于外部操作系统的完整性。因此，TEE 可有效应对开放环境高级持续威胁、多域流转隐私泄露威胁。
- **防御维度：**TEE 提供了一套机制来验证软件的完整性，确保在安全环境中运行的软件设备没有被篡改。6G 可针对不同场景将该重要网络功能放置 TEE 环境实现高等级安全防护。TEE 技术通过硬件辅助的隔离机制来保证网络功能的安全性，使用独立的执行环境来处理敏感数据和操作，从而实现网络数据的高安全性和隐私保护。
- **提升的关键能力：**在 6G 网络中，TEE 可以用于支持联邦学习，允许多个设备共同训练一个模型，同时保持数据的隐私和安全，提升网络分析的韧性。TEE 提供了一个隔离且安全的环境，可以在网络遭遇攻击或故障时，快速切换到备份路径或备用节点，从而实现动态修复。TEE 支持在安全隔离的环境

中进行软件和固件的更新。同时支持在安全隔离的环境中进行软件和固件的更新。

- **支撑的核心目标：**TEE 通过提供一个隔离的环境，保护关键的安全和加密操作免受主操作系统的干扰和潜在攻击。这种隔离性增强了系统的抵抗能力，即使在外部攻击或内部故障的情况下，TEE 内的代码和数据仍然安全，确保了关键功能的容错性。在网络攻击或故障发生时，TEE 内的安全监控和响应程序可以迅速触发，执行预定义的恢复策略。

4.2.7 SRv6 技术

SRv6（Segment Routing over IPv6）是一种网络技术，它结合了 Segment Routing（SR）的灵活性和 IPv6 的普遍性，旨在提高网络的可编程性、可扩展性和效率。SRv6 允许网络运营商通过在数据包的头部插入一系列的“段”来定义数据包的路径，每个段代表网络中的一个指令或操作，从而实现对数据流的精确控制。SRv6 技术的核心优势在于其路径编程能力，它允许网络管理员或自动化系统根据实时网络状况动态调整数据流的路由。这种灵活性使得 SRv6 成为提升网络韧性的关键技术之一。

SRv6 技术对于 6G 核心网韧性的提升表现在以下方面：

- **可应对威胁：**SRv6 技术支持多路径传输，使得数据流能够通过多个不同的路径在网络中传输，这样在链路或节点发生故障时，能够迅速重新路由流量，减少单点故障的影响。SRv6 可有效应对网络路径在遭遇开放环境高级持续威胁、云化网络功能失效威胁引起的服务功能或性能下降的问题。
- **防御维度：**SRv6 的快速故障恢复能力确保了网络在面临中断时能够即时切换到备用路径，最小化服务中断时间，从而显著提高了 6G 网络的韧性和可靠性。SRv6 通过多路径和结合网络编码技术保证了网络链路的韧性。
- **提升的关键能力：**SDN 实现网络的控制面和数据面分离，使其能够全局感知网络状态，SRv6 通过结合 SDN 技术，实现了网络链路状态的实时感知。同时，SRV6 的三层可编程性大大提高了网络数据面的灵活性。SRv6 能够在网络中实现路径的动态修复，确保在链路或节点发生故障时，流量可以快速重新路由，从而提高网络的可靠性和稳定性。
- **支撑的核心目标：**SRv6 技术配合 SDN 技术可以实现网络路径的智能优化，

同时，SRv6 通过与多路径技术结合可以抵抗和容忍单点故障。灵活的路径选择和策略实施，增强了 6G 网络对不同网络条件和需求的自适应能力。这种适应性不仅体现在对故障的快速响应上，还体现在对网络拥塞和性能波动的实时调整上，使得 6G 网络能够更加灵活地应对各种挑战。

表 3 给出了各能力类技术与 6G 核心网韧性能力的对照表。能力类技术作为架构类技术的有力补充，在 6G 网络中发挥着至关重要的作用。它深入渗透至链路层和功能服务层，为网络链路和网络服务提供了强大的韧性保障。这种技术能够及时响应并阻止网络链路或功能故障，确保网络的连续性和可靠性。通过持续集成尖端的能力类技术，6G 网络架构可实现更高效、更灵活、更智能的韧性控制。

表 3 能力类技术韧性使能对照表

技术名称	6G 核心网韧性能力													
	可应对威胁			防御维度			提升的关键能力				支撑的核心目标			
	开放环境高级持续威胁	云化网络功能失效威胁	多域流转隐私泄露威胁	点	线	面	多维感知	灵活包容	动态修复	迭代更新	预测与智能优化	抵抗与故障容错	快速响应与恢复	自适应与自演化
AI Agent	√	√		√		√			√	√	√			√
TEE	√		√	√					√	√		√	√	
MTD	√	√		√		√	√		√			√	√	√
DFP	√	√		√		√	√	√	√		√	√	√	
SRv6		√			√		√	√	√			√	√	
IBN	√			√			√		√		√		√	
MLOps		√		√					√				√	

5. 总结

6G 网络的发展不仅仅是对速度和连接性的提升，更是对网络韧性和安全性的全面革新。本蓝皮书探讨了网络韧性在 6G 时代的重要性，以及如何通过多样化的技术策略和架构设计来实现这一目标。网络韧性确保了 6G 网络在面对不断演变的威胁和挑战时，能够保持稳定性和可靠性，同时为用户和企业提供持续的服务。通过实施先进的防御机制、强化安全协议、以及采用自动化和智能化的响应措施，6G 网络将能够抵御各种潜在的安全威胁，从而保护网络和关键基础设施免受损害，并确保数据的完整性和隐私。

未来，6G 网络的韧性将成为衡量其成功的关键指标之一。随着技术的不断进步和创新，6G 网络将具备更高的自监督性、自适应性、自组织性和自我修复能力。此外，随着人工智能和机器学习技术的融合，6G 网络将能够预测和应对未知的未知安全威胁，实现更加智能化的安全防护。

我们期待全球范围内的合作和协调，以确保 6G 网络韧性的全球一致性和互操作性。通过跨学科的研究和产学研合作，6G 网络将能够实现其在网络韧性方面的全部潜力，为全球用户带来更加安全、可靠和可持续的数字未来。

总之，网络韧性在 6G 网络中的重要性不容忽视。它不仅是技术进步的体现，更是对未来网络环境的一种前瞻性投资。随着 6G 网络的逐步实现，有理由相信，一个更加强大、智能和安全的网络时代即将到来。

参考文献

[1] 邬江兴. 内生安全赋能网络弹性工程[M]. 科学出版社, 2023

[2] NGMN. 6G Trustworthiness Considerations[R]. 2023

[3] Beyond 5G Promotion Consortium. Beyond 5G White Paper: Message to the 2030s[R]. 2022.03

[4] Open6Ghub. Organic 6G Software-Based Networks: Adaptability, Flexibility, Simplicity, Reliability and Openness at the System Level[R]. 2024.07

[5] SNS JU. SNS Journal 2024[R]. 2024

[6] Next G Alliance. Next G Alliance Report: Roadmap to 6G[R]. 2022.02

[7] Next G Alliance. Next G Alliance Report: Trust, Security, and Resilience for 6G Systems[R]. 2022.07.

[8] Nokia Bell Labs. Security and trust in the 6G era[R]. 2021

[9] Ericsson. 6G – Connecting a cyber-physical world[R]. 2022.02

[10] NIST. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach[S]. 2021.12

[11] ITU-R. Framework and overall objectives of the future development of IMT for 2030 and beyond[S]. 2023.06

[12] National Science Foundation(NSF) . Resilient & Intelligent NextG Systems (RINGS)[EB/OL]. https://www.nsf.gov/pubs/2021/nsf21581/nsf21581.pdf

THE 4th
ACADEMIC CONFERENCE
ON **CYBERSPACE**
ENDOGENOUS
Safety & Security

THE 7th
"QIANGWANG"
INTERNATIONAL ELITE
CHALLENGE
ON **CYBER MIMIC**
DEFENSE