未来启航 | 6G

6G数字孪生网络安全技术白皮书

（1.0）

中国移动通信集团有限公司 | 中兴通讯股份有限公司 | 北京触点互动信息技术有限公司

华为技术有限公司 | 库析（南京）科技有限公司

前　言

随着“数字孪生、智慧泛在”的 6G 愿景成为业界共识，数字孪生技术也将在未来网络演进中发挥重要作用。未来 6G 网络具备空天地广域覆盖、分布式自治组网、海量异构终端接入等特征，面临安全风险难识别、安全需求难统一、安全效果难评估等挑战。数字孪生技术可以为 6G 安全提供新的思路与解决方案，助力实现低成本试错、智能化安全决策、高效率安全创新和预测性安全维护，从而提升 6G 网络安全确定性、自主性和智能性。

本白皮书旨在探讨数字孪生对 6G 网络安全的推动作用以及赋能 6G 网络安全的典型场景，并提出了数字孪生网络安全框架及关键技术。期望能够为 6G 数字孪生安全研究提供可参考的需求分析和技术方向，推动业界对 6G 数字孪生安全达成共识，保障 6G 网络安全、稳定和可持续发展。

目录

1. 数字孪生概述

1.1. 数字孪生网络的发展

数字孪生概念最先为美国教授 M.Grieves 提出，由物理对象、虚拟对象和两者的交互三部分组成，并在美国国家航空航天局构建未来飞行器项目中进行应用与发展。近年来，基于数字孪生技术的应用研究成为热点，已在民航、水利、能源、教育、医疗、信息技术等多个领域开展广泛运用。2023 年 ITU 发布的《IMT 面向 2030 及未来发展的框架和总体目标建议书》中，提出数字孪生是面向 2030 及未来 6G 移动通信的重要发展趋势之一，将实现人、机、物的连接，实现物理世界和虚拟世界的实时同步。

将数字孪生技术应用于网络，创建物理网络设施的虚拟镜像，即可搭建与物理网络网元一致、拓扑一致、数据一致的数字孪生体。各种网络管理与应用可以利用网络的数字孪生体，基于数据和模型对物理网络进行高效的分析、诊断、仿真和控制，可以实现低成本试错、智能化决策、高效率创新和预测性维护，进而助力网络实现极简化和智慧化运维。

中国移动发布的《数字孪生网络（DTN）白皮书》中提出了“三层三域双闭环” 网络架构： 三层指构成数字孪生网络系统的物理网络层、孪生网络层和网络应用层； 三域指孪生网络层数据域、模型域和管理域，分别对应数据共享仓库、服务映射模型和网络孪生体管理三个子系统； “双闭环” 是指孪生网络层内基于服务映射模型的 “内闭环” 仿真和优化，以及基于三层架构的 “外闭环” 对网络应用的控制、反馈和优化。

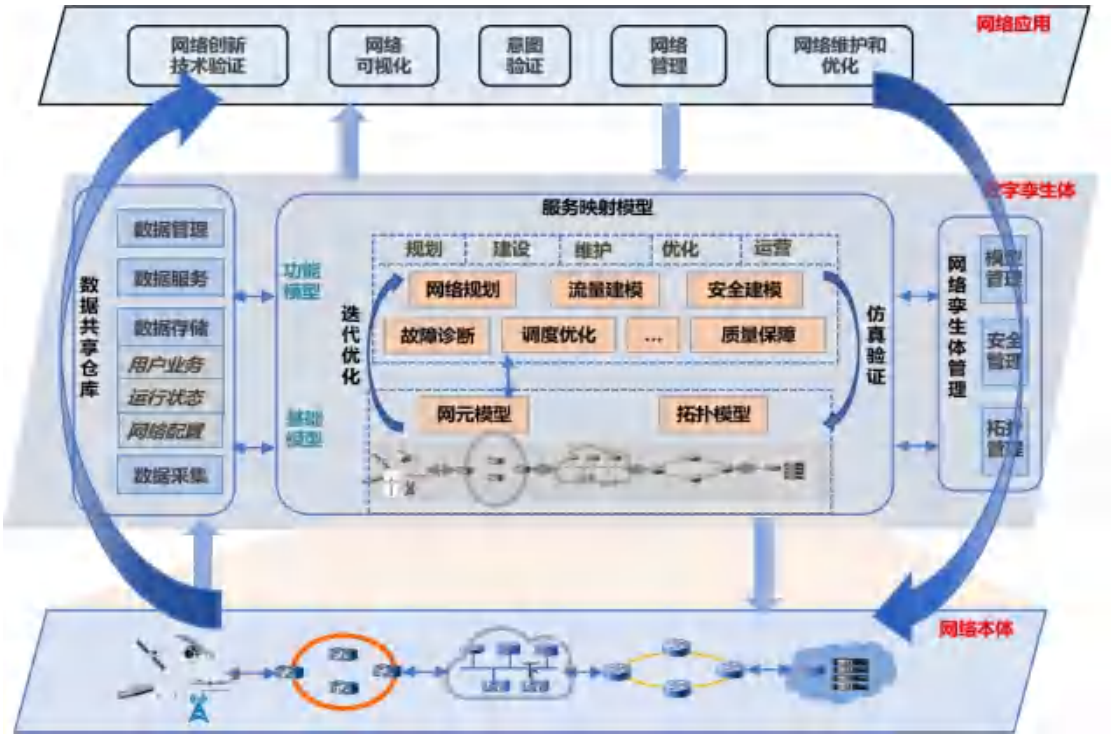

图 1 数字孪生网络“三层三域双闭环” 架构

1.2. 数字孪生对网络安全的推动作用

数字孪生技术可以为网络安全领域提供新的思路与解决方案，基于数据和安全模型对物理网络进行高效的安全分析、安全仿真和安全控制，使网络安全具备数往知来、虚实结合、由点及面的特征。

- **数往知来**

数往知来是指可以从历史数据、实时状态中探索未知的安全风险，获取未来的安全趋势，从时间维度提升网络安全分析的确定性。

在安全风险识别方面，数字孪生可以帮助实现从基于规则判定已知风险到基于数据预测未知风险的转变。通过从移动通信网络的终端、基站、核心网和网管中采集到的多源异构全量实时数据，以及对过往安全状态进行快照存档，利用数据分析和仿真推演等方式可以进行安全风险研判和趋势预测。

在安全措施制定方面，数字孪生可以帮助实现从依据经验设置措施到迭代优化探索最优策略的转变。在高拟真度的网络数字孪生环境中，能够对安全措施进行验证，使用效果评价指标对不同安全措施进行评估，基于评估结果对措施进行优化，持续循环执行上述过程以实现闭环迭代，可帮助指导安全能力部署及配置

的决策，不断逼近网络安全自治。结合对下一时刻网络的仿真和推演，可提前做出网络下一时刻的安全决策和安全规划。

- **虚实结合**

虚实结合是指数字孪生将数字和物理实体相结合，将理论、仿真和实际运行相结合，从而丰富安全分析的方法，增加安全分析结果的准确性，从程度维度提升网络安全分析的确定性。

数字孪生基于映射模型以及从实体网络空间采集的真实网络运行数据，实现对网络的高保真呈现，可以作为网络安全应用或设施的试验平台，在不影响实体网络运行的情况下得到贴近实体网络的试验结果。同时，使用数字孪生的网络管理、配置能力，根据理论假设的结果对数字孪生中的网络实体状态进行设定，比如安全风险发生的时间、概率、影响等，也可以在数字孪生体上通过仿真手段模拟安全漏洞、安全攻击等安全风险，在仿真风险后按照孪生体的网络运行逻辑运行并观察风险后果。基于概率分析、仿真风险、真实数据、数字孪生体真实运行四者的虚实结合，丰富了分析情境，减少了推演时间，贴近了真实场景，便于更充分更准确地实现对攻击效果的预测和安全策略的验证。

- **由点及面**

由点及面是指基于数字孪生可以根据需求进行单点网络风险观测或者全面安全态势感知。网络数字孪生无需也难以 100%复现物理实体网络，可根据网络安全场景需求，选择需要跟踪的对象时段、对象网络、对象过程、安全风险、安全措施、安全状态等进行建模。可用于观测单点或局部故障对网络范围内的影响，观测多个攻击对指定网元/网络的叠加影响。也可构建复杂、大型推演场景，对如 DDoS 攻击、漏洞与病毒等在大型网络环境下的破坏力、传播力等进行推演与验证，以及观测多安全措施在安全、性能、效率等多方面的表现，以此提升网络安全分析在空间维度的确定性。

2. 数字孪生赋能 6G 安全

2.1. 6G 网络安全挑战

作为关键信息基础设施，移动通信网络的安全影响国家安全、国计民生、公共利益。从 2G 到 5G 移动通信网络安全不断进化，支持更全面的数据安全和隐私保护、更丰富的认证机制以及更灵活的网络间信息保护。但现有安全防护建立在 X.805 框架的基础上，主要以分域隔离、边界防御为手段，基于已知的攻击特征和规则匹配形成被动防护，缺乏对新型威胁、未知风险的安全感知能力和应对手段，缺乏对网络攻击的主动防御能力。

6G 作为下一代数字信息基础设施，将在 5G 三大典型场景基础上继续深化和增强，拓展无线感知和泛在智能等新场景，提升网络性能、丰富服务能力，全面推动经济社会数字化浪潮，促使人类进入一个数字孪生、万物智联的全新时代。而 6G 新场景、新架构、新技术也带来新的安全挑战：

安全风险难识别。6G 网络将会引入人工智能、云计算、区块链等新技术，新技术引入提升网络性能的同时也带来了更多未知的安全风险。6G 网络架构服务化会使网络功能逐渐解耦，网络攻击路径也会呈指数级增加，6G 网络面临的安全攻击将会更加的多样性和智能化。传统的外挂式和补丁式的安全防护机制已无法对抗未来 6G 网络潜在的泛在攻击与不确定性安全隐患。

安全需求难统一。6G 网络将实现真正的万物互联，支持如卫星网络、行业网络、体域网等异构网络和海量终端，同时，沉浸式 XR、全息通信、感官互联、通感一体、智慧内生等新业务不断涌现。不同的网络、业务对安全的需求不同，6G 网络需要具备自主适应、智能协同及可扩展的安全能力，保证安全架构的健壮性和灵活性。

安全效果难评估。6G 网络架构部署将继续向异构组网和分布式网络方向演进，网络的复杂度将进一步提升。安全能力的简单叠加可能会造成网络性能下降，安全能力的多样化部署可能引入网络设计复杂、资源效率低等问题。如何选择合适的安全能力、合适的交付时机、合适的组合部署方式，来平衡安全防护效果、安全成本、安全性能是困扰客户及运营商的难题。6G 网络需要对安全效果做明

确评估，以便在此基础上持续优化安全措施，从而实现 6G 安全的自免疫。

安全风险难识别、安全需求难统一、安全效果难评估增加了 6G 安全的不确定性。如 1.2 章节分析，通过构建基于数字孪生的 6G 安全能力，可以实现 6G 安全风险自感知、安全目标自发现、安全策略效果自评价和自优化，推动移动通信网络向安全确定性、安全自治的方向演进。IMT-2030（6G）推进组发布的《6G 网络安全愿景技术研究报告》中也将虚拟共生作为 6G 网络内生安全的重要特征之一。网络数字孪生中的物理实体与虚拟孪生体能够通过实时交互映射，实现安全能力的共生和进化，进而实现物理网络与虚拟孪生网络安全的统一，提升 6G 网络整体安全水平。下述章节将介绍数字孪生赋能 6G 网络安全典型场景。

2.2. 基于数字孪生的 6G 安全典型场景

2.2.1. 安全推演评估

6G 支持多种异构网络及丰富的业务应用，安全事件的影响将更为复杂，需要系统直观的安全推演评估。通过构建网络孪生场景，对网络安全事件进行模拟，观察、记录、分析，全面解析安全事件的运行特点与可能结果。此过程可以预测潜在风险，量化其影响，并提供优化的安全解决方案，帮助优化安全资源配置，增强整体网络防御能力，平衡业务连续性与安全建设的收益，为运营人员提供智能的安全响应辅助决策能力。

在构建 6G 网络孪生场景时，将动态的资产数字化模型与静态的攻防知识模型进行关联性建模，更有效地表达网络空间特征；通过模拟多种组合的攻击行为，构建多样化的漏洞利用、病毒传播、木马植入和攻击模拟等场景来模拟攻防对抗过程，分析可能存在的攻击路径，全面评估潜在安全风险和攻击事件的影响，包括数据泄露、服务中断和恶意代码执行等多种情况，并考虑业务依赖性来分析攻击可能对当前业务系统和防护系统造成的具体影响，如潜在的业务中断广度和经济损失，利用可视化能力进行呈现，辅助运营人员全面了解安全风险与业务连续性之间的关系，从而制定更加精准安全应对策略。

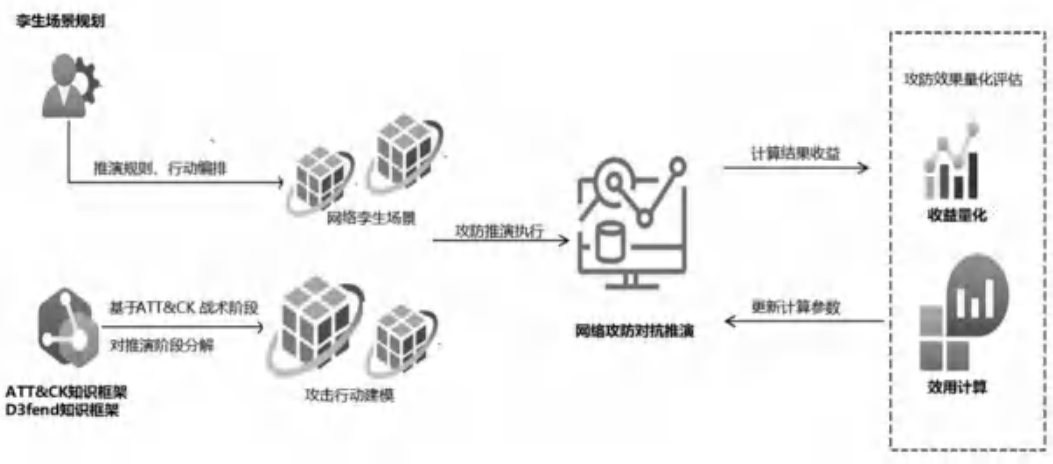

图 2 基于数字孪生的网络安全推演评估示意图

2.2.2. 差异化安全能力交付

6G 与垂直行业深度融合，将通过差异化网络支持丰富的业务场景和客户需求，需要有配套的安全措施保证网络安全运行。网络和业务的多形态需要差异化安全保障，进而需要差异化安全能力交付。利用网络数字孪生的可验证、可预测、高仿真等特性，在孪生网络上进行交付策略（如安全能力组合或安全意图解析结果）的预验证，并可对交付策略做持续优化。可充分发挥专家经验＋实施验证的优点，促进行业需求与网络安全能力及安全意图的精准匹配。

具体的，差异化网络选择的安全措施需要在满足安全要求的前提下达成性能、效率等的平衡，可在数字孪生体上对差异化的网络安全能力进行分类组合，从安全及非安全等维度进行测试验证及迭代优化，进而生成精准满足需求的交付策略。未来网络会引入意图驱动管理的能力，支撑对以安全类型、安全维度、安全能力等形式存在的意图的解析、翻译、分发和执行。在该意图驱动的网络安全配置流程中，可以在孪生网络上对意图解析后的指令进行预验证，将验证通过的指令下发给物理网络，同时也可将验证结果反馈给意图翻译系统供其优化，从而提高意图翻译的准确性。

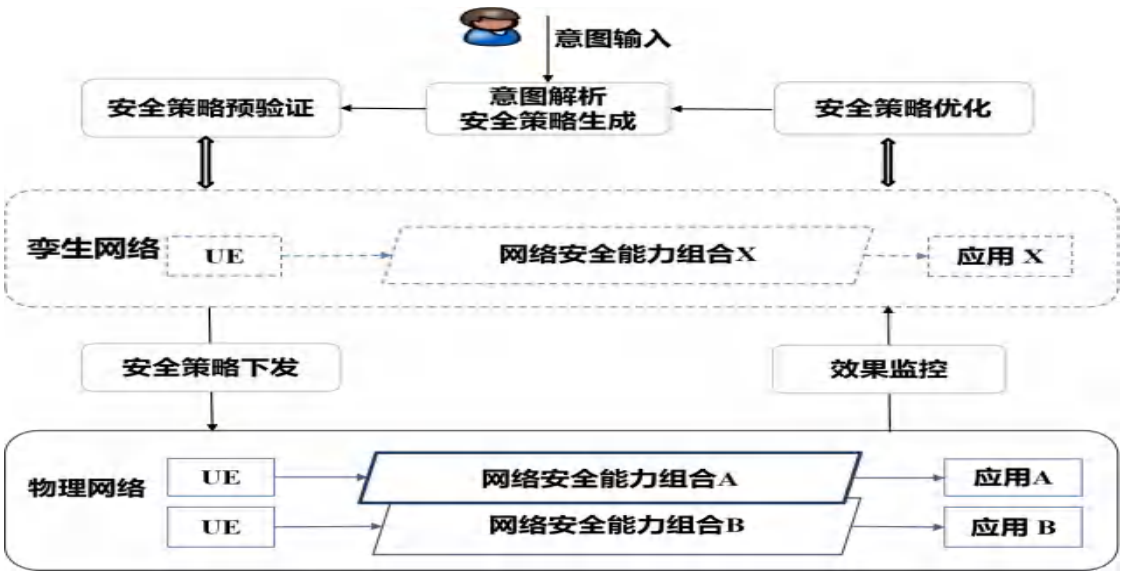

图 3 基于数字孪生的差异化安全能力交付示意图

2.2.3. 主机威胁防护

6G 由于网络容量变化，主机数量巨大，日益增长的复杂配置操作和漏洞修复给网络运维带来了巨大压力。通过跟踪和采集主机运行时行为，基于主机运行时的行为数据构建孪生体，并对孪生实体和相关模型进行学习与训练，结合 IOA 与 IOC 识别，可以快速模拟主机的运行时上下文，对用户行为、文件操作、进程跟踪、恶意提权等实现进程级行为控制，发现安全风险并实施有效阻断，使内生安全防护及检测能力下沉到操作系统内核中。

基于数字孪生的主机威胁防护场景如下图所示，包括主机实体层的行为数据采集与安全策略执行，运行时孪生层的数据模型管理与数据存储映射，用户按业务需求场景组织的安全控制应用三部分。其中，数据采集基于探针模式的操作系统内核跟踪技术，与工作负载及业务类型解耦，通过实时描述运行时应用及用户行为的黄金指标，达到对当前业务的应用上下文的深度可见，洞悉工作负载是否面临安全风险，并可以根据安全策略模型进行规则匹配或可疑推理，进行风险阻断拦截及告警。

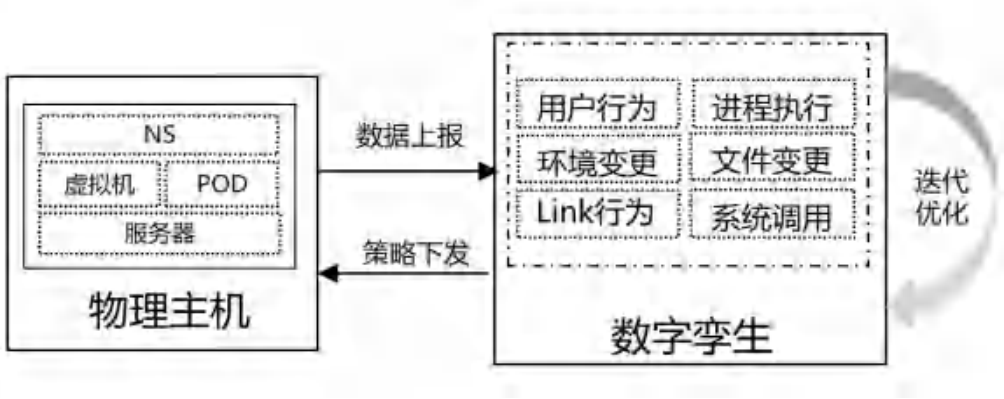

图 4 基于数字孪生的主机威胁防护示意图

2.2.4. 异常流量访问控制

未来 6G 网络架构持续演进，网络攻击路径也会呈指数级增加，针对异常流量的访问控制尤为重要。异常流量访问控制实现资源池内部东西向流量的监控，对异常流量进行分析，智能生成并执行安全策略，解决云化集中式资源池中单个网元被攻击后进行资源池内部横向攻击的场景。利用数字孪生技术，对物理网络的流量访问信息进行采集，对采集到的流量信息进行聚类分组、标签化处置，对异常流量进行检测分析处置。在孪生网络中进行异常流量预处置，包括禁用端口、隔离 VM、阻断 VM 流入流出流量等高危操作，避免在现实网络中出现异常规避导致网络中断甚至瘫痪的风险。有效降低微隔离安全策略执行时给现网带来的风险，并且可以利用网络孪生的迭代能力，持续优化形成安全策略最优解，有效提高网络的稳定性。

异常流量处置单元收到 VM 上报的异常流量及相关日志，形成安全策略。将安全策略下发至网络孪生体，网络孪生体执行安全策略，形成执行结果，评估对网络性能的影响、VM 资源占用的影响、是否出现中断或瘫痪等。基于执行结果形成安全策略优化方案，将执行结果和优化方案上报至异常流量处理单元，处理单元决策是否可以将安全策略应用至现网，或者仍需和孪生网络层交互，进一步调整安全策略。

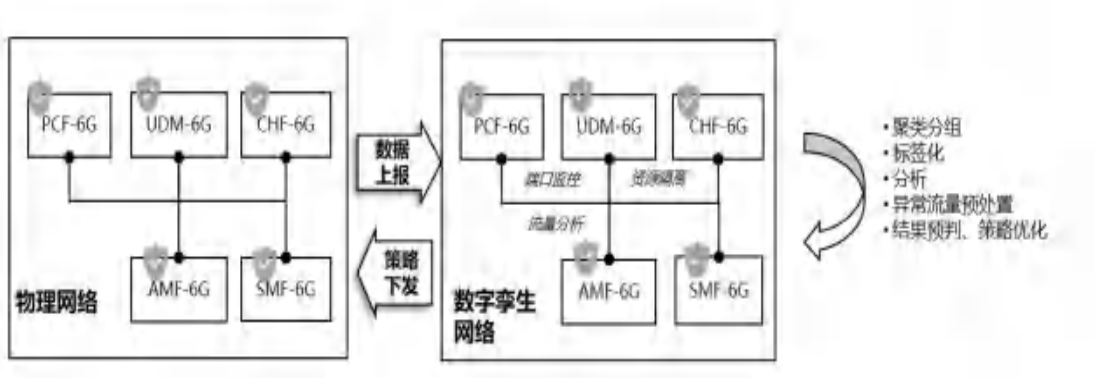

图 5 基于数字孪生的异常流量访问控制示意图

2.2.5. 安全态势感知

安全态势感知是指通过实时监测、分析和预测网络中的安全态势来主动防范潜在的安全威胁。它对于 6G 网络高度复杂和动态的环境尤为重要，能够在威胁发生前就提供预警并采取预防性措施，减少安全事件的发生，保障 6G 网络的稳定和安全。安全态势感知可以利用数字孪生技术，通过持续收集和分析网络中的各类数据，实时了解当前的网络安全状态，并结合机器学习和大数据分析技术，系统地预测潜在的安全威胁，自动触发自免疫性防护措施，以提高未来网络的内生安全能力。以高级持续性威胁（APT）防护为例，利用数字孪生技术，持续手机网络中的用户和设备行为数据，识别 APT 攻击的前期迹象，比如检测到长时间的低频率扫描活动可能预示着 APT 攻击的准备阶段；在 APT 攻击的不同阶段，基于孪生体及大数据分析评估、模型学习技术，识别和预测异常行为，及时生成预警和告警，触发防护措施中断攻击链条，阻止攻击者达到最终目标。

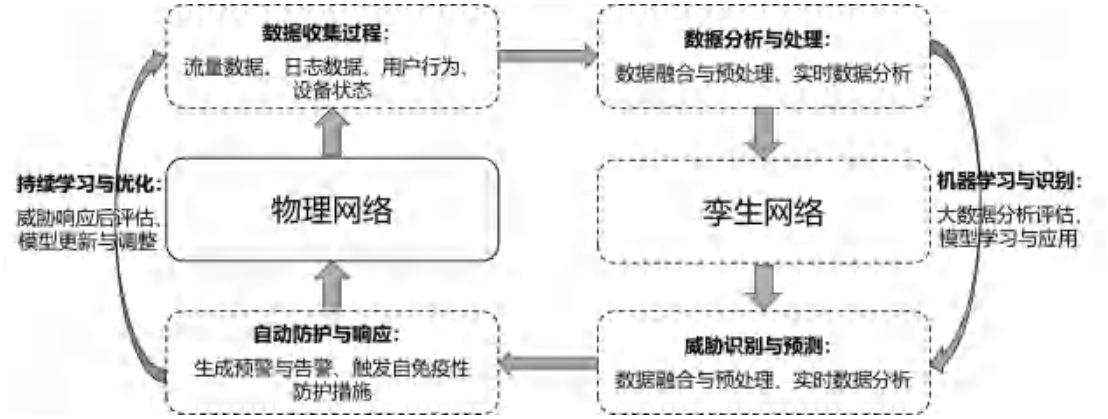

图 6 基于数字孪生的动态安全态势感知

3. 数字孪生网络安全框架

3.1. 设计原则

为了实现数字孪生赋能网络安全，在物理网络与网络安全应用之间，需要安全相关数据的深度开放与处理能力；需要网络安全映射能力来实现对网络、安全、风险的孪生；需要安全智能分析、调度能力完成闭环处置。同时，还应秉持至简、灵活设计原则进行框架设计实现平台化赋能：一方面按能力元素的类别分层分模块整合为能力集，如数据能力集、模型能力集、应用能力集等，便于对要素进行符合特征的分域管理且减少耦合；另一方面构建原子化服务化能力，支持智能化的编排管理，降低网络安全应用开发难度并能灵活自适应的部署和调整。

3.2. 总体框架

基于上述能力需求和设计原则，可以提出数字孪生网络安全基本框架和框架模块应具有的功能。该框架分为物理网络层、南北向接口、网络安全数字孪生层及网络安全应用层，框架图及模块功能基本描述如下所述。

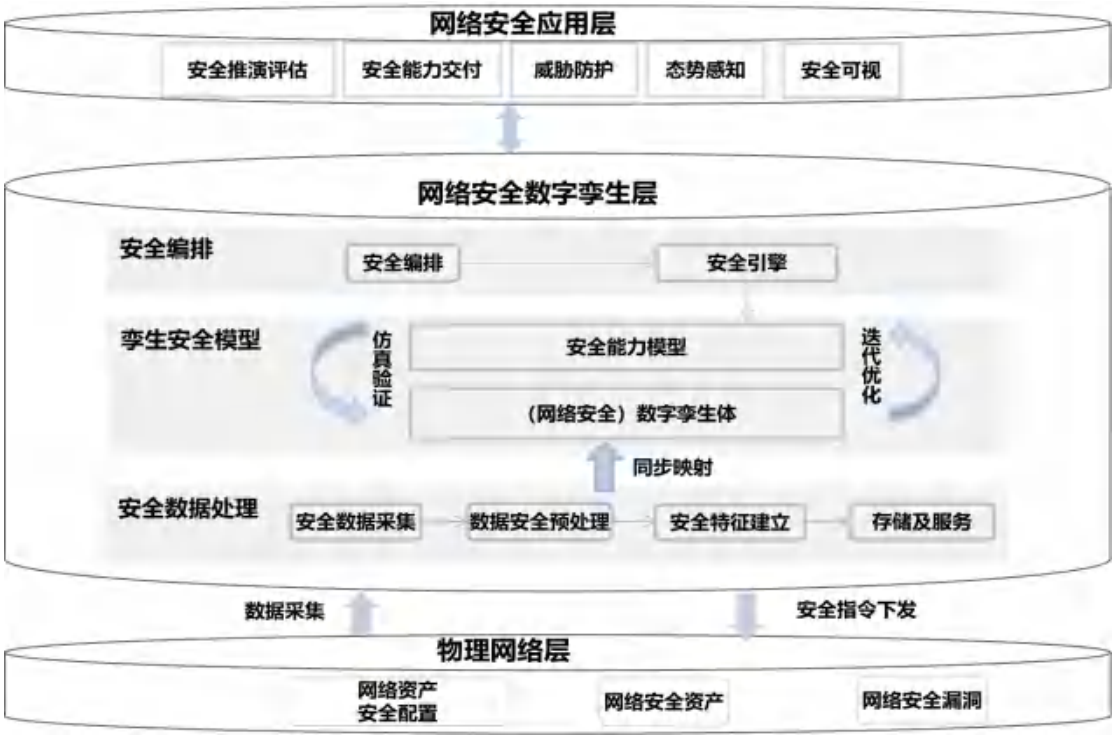

图 7 数字孪生网络安全框架

3.3. 物理网络层

物理网络空间中的各种网络资产构成了物理网络层，网络资产特别是网络安全资产、资产的配置特别是安全配置、资产的安全漏洞等是该层主要涉及的元素。物理网络实体具有不同的形态，如移动电信网、互联网、企业专网、党政军专网等，不同的安全防护需求部署针对性的安全防护资源及安全配置。此外，还包括各类内嵌式或外接式的网络资产（含安全资产）采集配置接口，支持数据采集、控制指令接收等功能。

3.4. 南北向接口

南向和北向接口负责孪生网络层与物理网络层、网络安全应用层之间孪生数据的交互、映射以及控制指令的接收、发送，包括数据采集、控制下发、能力开放和指令下发等接口功能。

3.5. 网络安全数字孪生层

网络安全数字孪生层是核心，负责处理孪生网络的数据、模型，生成及管理数字孪生体，对数据、孪生体、物理网络交互做编排和控制，以支撑实现上层网络安全应用。该层包括安全数据处理、孪生安全模型、安全编排等模块。

3.5.1. 安全数据处理

通过收集和更新各类网络实体的安全相关数据和实时运行数据，形成孪生网络的真实来源，为各类网络安全应用提供准确、完整的信息。围绕数据的处理包括：

数据采集：完成网络数据和安全相关数据的提取、转换、加载、清洗和处理，可用于支持基于 DTN 的网络安全应用。上述数据采集可以通过网络域、业务域、主机域上运行的感知设备进行数据采集，也可以通过网络自身的数据管理功能收

集数据。在 6G 时代，网络的数字孪生可以调用数据面基础服务来生成、存储、访问和传输其数字孪生体和各种安全模型。

数据预处理：包括对数据的安全预处理、安全特征建立、安全增广等。安全预处理指出于对数据的安全隐私保护所采取的数据加密、脱密等操作；安全特征建立指通过对数据的分区分类结构化处理，在建立基础数据仓库的基础上，建立安全相关主题特征数据集；安全增广指对真实数据进行增广处理，生成更多虚拟安全场景，提供多样性更好的训练数据，如漏洞分布或入侵行为等。

数据存储：针对网络数据和安全相关数据的多样化特点，采用多种数据库技术对数据进行高效存储。

数据服务：为孪生安全模型提供多种数据服务，包括快速检索、并发冲突、批量服务、统一接口等。

3.5.2. 孪生安全模型

孪生安全模型负责（网络安全）数字孪生体和安全能力模型的映射与建模。

（网络安全）数字孪生体：数字孪生体是指根据物理网络的基本配置、环境信息、运行状态、链路拓扑等信息建立的网元模型和网络拓扑模型，它是对物理网络的实时准确描述。数字孪生体可以与安全功能模型实例交互，以帮助验证和模拟安全风险或安全解决方案。数字孪生体应支持自身安全配置的更新、安全能力的操作、接口数据包捕获和修改等。

安全能力模型：功能模型是指针对特定的网络安全应用场景，充分利用数据仓库中的数据，建立安全仿真、安全预测、安全决策、安全验证、安全优化、安全规划等各种数据模型。作为网络孪生的能力源，随着安全功能模型种类的增多，基于数字孪生提供网络安全应用的能力也可以越来越强。

3.5.3. 安全编排

为了以敏捷的方式实现网络安全应用，需要在特定的孪生网络上编排所需的动作序列，包括编排所需的孪生网络、编排所需的模拟安全风险或对策、编排所

需的安全相关功能模型，这些由相应的引擎或工具执行。具体包括：对网络安全场景的解析、设定、生成、和分析等；对指定时间、范围、特征的物理网络的网元和拓扑构建模型；根据网络安全应用程序编排对风险和措施的仿真，包括指定模拟顺序、模拟时间、与风险相关的孪生实体、模拟方法和所需资源等；编排对孪生网络的安全状态，例如指定测量标准、测量时间、测量方法和所需资源等。

3.6. 网络安全应用层

网络安全应用通过孪生北向接口向网络安全数字孪生层输入需求，通过对数字孪生体、安全能力模型及孪生数据的调用，生成经过验证的安全控制指令，网络安全数字孪生层通过南向接口将控制更新下发至物理实体网络。安全推演评估、安全能力交付、威胁防护、异常流量访问控制等各种网络安全应用能够以更直观的效果、更高的效率和更小的现网业务影响快速部署。

4. 数字孪生网络安全关键技术

4.1. 数据安全采集技术

数据采集是数字孪生技术的基础，是实现数字孪生安全的关键步骤。数据采集是指从物理世界或虚拟环境中收集数据的过程，这些数据可以是 1）资产安全信息，如资产风险信息、安全设备信息等、主机基本信息、主机行为信息（如登录、进程行为、文件行为等）、主机日志信息(如攻击监控日志、恶意代码监控日志、威胁情报监控日志等）等；2）流量安全信息，如流量基本信息、攻击流量信息、网络攻击恶意代码样本信息等；3）来自网络外部的数据包括：威胁情报、专家知识库等。采集这些数据涉及多种采集技术，包括探针技术、清洗技术、标签技术等。

- 探针技术：基于网络侧镜像分光和主机层基于内核沙箱的探针技术，无需重启物理体，同时增加用户自定义数据采集，然后通过 DPI 采集技术完成采集、打时戳、去重等功能。从移动通信网络的 MANO、SDN-C、Vswitch 等接口支持的数据采集，可以使数据孪生对移动通讯网络做更精确的模拟。
- 数据清洗：对采集的网络原始数据进行数据处理、按时间分区、非结构化数据做结构化处理和 ETL 入库等操作，包含对数据的关联回填、数据清洗、数据转换、数据加密和数据加载等流程。清洗后的数据使数字孪生可以摒弃网络杂包和错包，实现网络安全数字孪生的轻量化。
- 标签技术：将探针收集到的网络实时数据按照协议层和功能加以标记、分类。如请求报文，可以在不同的协议层中标记 TCP 请求、TLS 请求、HTTP Get 等，数字孪生可以使用这类报文模拟网络风暴或者 DDoS 攻击，体现数字孪生的价值。

从孪生数据的及时性和有效性的角度来看，适配模型变化的数据采集技术在数字孪生网络安全中也非常重要，比如在事件域，当采集物理体执行的进程级信任凭据发生变化时，利用实时数据可以快速感知并处置。

4.2. 网络威胁数字化建模技术

数字化建模是将抽象的网络世界对象数字化、模型化的过程。通过数字化建模技术将抽象的网络威胁转化为计算机可以理解的数字化模型，从而可以有效理解 6G 网络的安全问题，并基于模型的编排、关联、分析来解决安全问题。

网络威胁的数字化建模需要从多个维度去融合物理域模型、认知域模型、逻辑域模型，表达网络安全特征及业务的关联性特征。孪生模型属性要有足够的灵活性用于扩展来支持不同网络空间实体表征的多样性，模型与模型之间的关联关系要有足够的科学性以反应真实网络世界，可基于现有模型构建新的模型用于表现其表征。MOF 建模方法提供了一套灵活且可扩展的框架，其核心目标是建立一个支持任意类型元数据的结构体系，并允许根据需要扩展新的元数据类型。MOF 基于经典的四层元建模体系结构，该体系结构在 ISO 等标准社区中广泛应用，确保了模型的科学性与适用性。

为了使网络威胁模型更加有效地支撑推演预测能力，模型的维度需要结合 6G 网络标准和网络攻防标准，实现 6G 网络环境下的复杂威胁分析与预测。同时，网络威胁模型具备灵活性和可拓展性，既可单独使用，也可根据具体场景需求进行组合，以应对新兴的场景建模或资源建模挑战。

4.3. 面向安全的可编程协议栈技术

可编程协议栈是网络数字孪生的关键技术之一，能够实现对网络协议的灵活定义和控制。可编程协议栈允许用户通过编程接口或图形化界面对网络协议的各个层次的字段内容进行自定义或编辑，调整和变更协议流程，以便在孪生环境中构建多种网络安全场景，模拟多种攻击和异常流程。

可编程协议栈支持将不同网络层次的协议灵活组合，例如将应用层协议与传输层协议、网络层协议进行集成和调试。这种组合可以模拟复杂的攻击链路，如从应用层渗透到网络层的横向攻击。可以通过模块化的方式设计协议栈，使得不同层次的协议模块可以灵活替换、组合或扩展。例如，可以将某个应用层协议的模块与另一个传输层协议的模块结合，测试其在不同协议组合下的安全性。可编

程协议栈支持定制协议的状态机，用户可以指定协议的状态转换规则、触发条件和对应的动作。可以模拟复杂的协议交互过程，如多步握手、认证过程等。并且可以实时调整协议的状态机，模拟协议的异常流程或攻击行为，如恶意终止连接、伪造会话等。

4.4. 网络攻防知识图谱构建技术

6G 的低延迟和高实时特性对安全威胁的快速分析、预测和响应提出了更高的要求，网络攻防知识图谱构建技术可以实现攻击路径的高效解析、跨层次攻防态势的全面展示、动态攻防对抗态势的持续更新。网络攻防知识图谱构建技术能够将单独的事件通过攻击向量等关联起来，形成一个完整的事件传播图谱，以便更好地理解攻击事件间的逻辑关系，并且可以发现原先未知的新的攻击路径。在这个过程中，通过构建攻击图和防御图，系统地研究不同攻击方式的防御弱点，分析整个攻击集合的对整体业务网络的影响范围和深度，也可以随之找到潜在的安全风险和整体防御体系的薄弱环节，制定针对性更强的防御措施。

网络威胁知识图谱构建技术可以将原本孤立的数字孪生模型建立关联关系，实现更为综合和体系化的网络风险分析。通过知识图谱能够整合多源信息，识别和分析复杂的威胁关系；将攻击路径、漏洞和安全事件进行语义关联，提升威胁检测能力；将资源、用户、网络活动在一张数字化的“网”中连接起来，进行更为广泛的网络风险评估，并借助知识图谱中定义的规则和关系，自动化识别和响应威胁，进而获得网络风险管理的主动性、实时性和可预测性。

4.5. 安全策略验证与优化技术

安全策略的验证与优化是提高网络安全防护能力的一项关键技术。通过在网络数字孪生体中实施安全策略的验证和优化，可以在不影响物理网络运行的情况下，通过不断迭代测试和反馈循环，逐步提升安全防护的全面性和有效性。

策略验证：基于对物理网络精确数字映射的孪生体进行策略验证，首先将计划实施的安全策略以及针对 6G 网络新型攻击方式的新防护措施导入数字孪生体。

接着，通过集成自动化渗透测试工具（如 Metasploit、OWASP ZAP 等）或自定义攻击脚本，执行多种模拟攻击，包括 DDoS 攻击、恶意软件感染、零日漏洞利用、内部人员威胁等，通过自动化框架执行模拟攻击，生成完整的攻击路径，并捕获攻击行为日志，分析每一个攻击步骤的执行效果。例如，通过流量分析工具（如 Wireshark、TShark）对每次攻击的网络流量进行详细捕获和分析，以评估当前安全策略的应对能力。随后，利用基于机器学习的异常检测算法（如深度神经网络 DNN 或支持向量机 SVM）对攻击路径中可能的防护薄弱点进行识别，并生成详尽的防护策略效能报告。这些技术使得攻击路径的每一个步骤都可以被精确记录、分析，进一步验证现有防护策略在不同攻击阶段的有效性。此外，为了提高验证的效率和覆盖范围，可利用虚拟化技术（如 Kubernetes、Docker）对不同的网络拓扑、流量模式进行动态编排，从而测试安全策略在各种网络条件下的表现，进一步验证其在实际网络中的可行性和可靠性。同时，在策略部署到实际物理网络之前，利用虚拟安全网关和端点防护工具进行持续的压力测试，确保策略在高负载或异常情况下的稳健性。最后，在实际网络中部署安全策略后，结合日志分析、流量监控（如 Zeek、NetFlow）、入侵检测系统（如 Snort、Suricata）等工具，可实时持续监控策略的运行效果，确保其能够有效应对各类威胁。

策略优化：根据验证过程中发现的薄弱环节及攻击路径中的关键节点，利用基于大数据分析的安全策略优化平台（如 ELK 堆栈或 Splunk）进行策略和配置的改进。优化后的安全策略和配置将再次在数字孪生体中，使用前述自动化工作做全面验证。进一步地，通过在网络数字孪生中的自动化威胁建模和反馈循环，系统能够基于实时威胁情报和网络环境变化生成动态安全策略：采用动态攻击面管理工具（如 Cortex XSOAR 或 IBM Resilient）使优化策略能够自适应网络威胁的变化，并实时调整防护措施。在实际网络中部署优化的安全策略后持续监控其运行效果，如果在部署过程中发现新策略对物理业务运行产生负面影响或未能有效防护某些攻击，可以通过预定义的应急响应机制快速回滚到之前的策略版本，或启动预定的故障恢复程序，确保网络的连续性和安全性。

4.6. 安全态势呈现技术

网络数字孪生之后，安全态势呈现技术通过可视化图形界面将复杂的网络状态和演变过程展示给用户，实现网络安全场景可视化、网络拓扑可视化、攻击流程可视化、防御策略可视化等多种能力。安全态势呈现技术不仅可以直观地展示网络安全风险，也可提高安全分析效率，帮助安全专家快速决策。

用户可以创建、选择或配置不同的场景，每个场景可能涵盖特定的攻击类型、目标区域、网络规模等参数。安全态势呈现技术提供多场景并行对比的可视化视图，帮助用户对比不同场景中的安全态势、攻击方式和防御效果。通过颜色编码、图形变化等方式直观展示场景之间的差异，特别是在防御策略调整后的效果变化。可以在时间轴上查看并控制场景的进度，观测特定时间点的安全态势演变过程。

安全态势呈现技术还能够实时展示防御策略的部署位置和范围。例如，防火墙规则的应用区域、入侵检测系统的监控范围、加密措施的覆盖范围等。直观展示防御策略与攻击路径之间的交互，用户可以看到策略在不同攻击阶段的效果，例如是否成功阻挡了攻击或延缓了攻击进展。通过热力图、影响圈等方式，展示当前防御策略的覆盖区域及其强度，帮助用户识别防御薄弱点和需要加强的区域。

4.7. 网络数字孪生安全保障技术

网络数字孪生基于孪生模型实现网络的仿真和控制，具有数字化、实时化、智能化等特点，本身面临孪生数据不可信、孪生模型不安全、控制指令不可靠等安全挑战，且基于物理网络采集海量数据也面临着数据授权及隐私保护等问题，需要利用数据安全技术和网络安全技术，实现网络数字孪生中数据全生命周期的安全保障以及网络和业务的整体统一安全。

4.7.1. 数据安全

对网络做数字孪生会产生和存储大量设备信息、用户信息、交互信息和管理信息等，这些数据对外泄漏或被应用未授权访问有可能造成用户或网络的隐私泄

露；数据在传输或存储中被篡改或破坏、采集的数据不可信等，将难以满足数据的应用和分析要求；异构网络的多级协作、跨域孪生产生数据共享的需要，也为数据安全需求的保障增加了复杂度。

因此，需要相应安全机制以保障数据的机密性、完整性、可信性、可追溯等，例如，轻量和高效的数据安全保护机制，如物理层加密技术等；数据访问授权功能，确保不同等级的数据仅能被具备权限的模型访问；数据验证机制，动态识别数据信息的真实性、发送数据意图的可靠性；数据防泄露和追踪溯源机制，通过脱敏、水印、数据流转监控等实现数据泄露的追踪溯源；隐私保护机制，实现隐私信息的全生命周期保护。

4.7.2. 模型安全

模型在不同的阶段可能面临各种安全威胁：在模型数据收集阶段，可能会遭遇数据污染攻击；模型开发或训练阶段，可能会引入漏洞和后门；而在模型部署使用阶段，则可能面临模型盗用和对抗性样本攻击的风险。这些安全问题的出现，主要归咎于以下几个方面：数据在采集、传输、使用、共享和存储过程中的管控不够严格，对攻击行为的检测不够全面等。

为了有效保护模型安全，可以采取多种措施，例如：模型训练前对数据质量进行评估和清洗，以确保数据质量；在模型开发时进行开发框架的安全检测，排除供应链潜在的安全漏洞；使用模型指纹技术来识别和验证模型的安全性，以及通过异常行为识别来监控模型的使用和运行，从而及时发现并应对潜在安全风险。

4.7.3. 指令安全

由于孪生网络可能直接对物理网络进行控制，针对数据孪生系统的攻击可能会威胁到物理世界中的人身安全、设备安全和业务安全。相比于传统网络安全风险，指令安全是数字孪生最显著的安全风险，例如向关键网元下发不恰当指令、指令隐私泄露、指令冲突等。

保障指令安全可以采取多种措施，如根据物理网络安全分域级别对指令的进

行不同控制和检验方案，对源、策略真实性、目标匹配进行多维策略验证，分层加解密实现最小化隐私设计；通过设置模型优先级、在孪生体和网元进行冲突判定和检测等手段，根据优先级指导指令执行，使得非安全类指令不能绕过安全类指令执行。

5. 总结与展望

本白皮书介绍了数字孪生技术的基本概念，探索了数字孪生赋能 6G 网络安全的典型场景，设计了数字孪生网络安全框架并阐述了关键技术，旨在推动业界对 6G 数字孪生安全达成共识，提升 6G 网络安全确定性。

当前业界对于 6G 网络数字孪生的研究还处于初级阶段，如何将数字孪生技术与 6G 网络深度融合，更好地赋能 6G 网络安全，还存在如下值得探索的关键技术问题：

- 在架构方面，如何实现数字孪生网络安全框架与 6G 网络架构的一体化设计，与 6G 网络架构新增组件如孪生体、安全面等协同交互；
- 在模型方面，如何针对不同网络安全场景设计数字孪生安全模型，构建全网通用、泛化能力高、迁移能力强的安全模型，并对安全效果性能进行量化评估；
- 在数据方面，如何实现数字孪生网络安全相关数据的可信及隐私保护，并保障异厂商接口和数据的兼容性。

6G 网络架构升级为关键信息基础设施的自主建设以及自主化安全技术的引入提供了机会和窗口期，数字孪生技术可助力 6G 安全寻求超越物理网络的解决方案，为重构和增强 6G 安全提供了新的实施路径。业界已启动数字孪生安全创新研究和标准化进程，目前已在 ITU 推进《数字孪生网络安全指南》《数字孪生用于网络安全应用的指南》《基于数字孪生的网络安全资产和安全事件可视化服务功能需求》三项标准。期望业界能够继续携手共进，加强数字孪生网络安全的技术创新和产业协作，将数字孪生赋能网络安全融入 6G 整体架构、流程及设备生产制造过程中，实现具备确定性、自适应、可评估的 6G 安全机制，为 6G 产业化及商用发展奠定安全保障基础。

缩略语

英文缩写	英文全称	中文解释
5G	5th Generation Mobile Communication Technology	第五代移动通信
6G	6th Generation Mobile Communication Technology	第六代移动通信
AI	Artificial Intelligence	人工智能
APT	Advanced Persistent Threat	高级持续性威胁
DTN	Digital Twin Network	数字孪生网络
DDoS	Distributed Denial of Service	分布式拒绝服务
DNN	Deep Neural Networks	深度神经网络
DPI	Deep packet inspection	深度数据包检测
ELK	Elasticsearch Logstash Kibana	弹性堆栈
ETL	Extract-Transform-Load	数据抽取、转换和加载
HTTP	Hyper Text Transfer Protocol	超文本传输协议
ITU	International Telecommunication Union	国际电信联盟
IOA	Indicators of Attack	攻击指标
IOC	Indicators of Compromise	入侵指标
ISO	International Organization for Standardization	国际标准化组织
MANO	Management and Orchestration	管理与编排
MOF	Meta-Object Facility	元对象机制
SDN	Software-Defined Networking	软件定义网络
SVM	Support Vector Machines	支持向量机

英文缩写	英文全称	中文解释
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全协议
UE	User Equipment	用户终端
VM	Virtual Manufacturing	虚拟机
XR	Extended Reality	扩展显示

参编单位及人员

序号	贡献单位	人员
1	中国移动	粟栗、杜海涛、王珂、闫茹、马宇威、白杰、陈璨璨、陈佳科
2	中兴通讯股份有限公司	杨春建、侯芳、顾希，刘建华
3	北京触点互动信息技术有限公司	王宇华、王航
4	华为技术有限公司	李祥军，张博，莫若，段凯旋，姜继勇
5	库析（南京）科技有限公司	董昊辰、李金鹏、林小熔

未来启航 | 6G