数字孪生在网络安全领域应用的研究及建议

来源：CCIA

作者：联盟秘书处

数字孪生

数字孪生也可以应用在网络安全领域，通过运用数字孪生对网络环境和安全状况进行数字定义、建模和展示，完善对网络空间安全状况的认知，同时通过交互和服务接口，持续进行网络空间的安全评估、预测性防护、攻防演练等，扩充网络安全态势感知的范围，促进网络空间安全方案的改进。

数字孪生（Digital Twin），是具有数据连接的特定物理实体或过程的数字化表达，该数据连接可以保证物理状态和虚拟状态之间的同速率收敛，并提供物理实体或流程过程的整个生命周期的集成视图。数字孪生最早应用在航空航天领域，随着大数据、云计算、人工智能等新一代信息技术的发展，目前已被广泛应用于电力、工业制造、城市管理等行业。

数字孪生也可以应用在网络安全领域，通过运用数字孪生对网络环境和安全状况进行数字定义、建模和展示，完善对网络空间安全状况的认知，同时通过交互和服务接口，持续进行网络空间的安全评估、预测性防护、攻防演练等，扩充网络安全态势感知的范围，促进网络空间安全方案的改进。

一、技术发展情况

“Digital Twin”一词在2010年美国国家航空航天局（NASA）的技术报告中被正式提出。2016年至2019年,Gartner连续四年将“数字孪生”列为“十大战略科技发展趋势”之一。

数字孪生尽管在用途、范围和功能方面存在千差万别，但在其功能方面符合软件设计模式。数字孪生是一个动态软件模型，它依赖于互动操作和其他的数据来了解其实现的业务模型及当前状态，部署资源并响应以满足预期的客户价值。

数字孪生技术发展重点在于：

模型的稳健性，重点关注如何支持特定的业务成果；

与现实世界的链接，可能用于实时监控和控制；

应用大数据分析和人工智能推动新的商机；

能够与其互动并评估“假设”情景。

近几年，国内外安全企业、研究机构和咨询机构开始陆续提出将数字孪生的概念应用于安全领域。2020年，美国《空军杂志》报道提及，美国空军正在使用GPS IIF卫星的数字孪生模型来检测系统的所有网络安全问题。但总体来说，数字孪生在网络安全领域的应用仍处于概念阶段。

二、发展难点分析

2011年，美国密西根大学Michael Grieves教授在《几乎完美：通过PLM驱动创新和精益产品》给出了数字孪生的三个组成部分：物理空间的实体产品、虚拟空间的虚拟产品、物理空间和虚拟空间之间的数据和信息交互接口。

数字孪生发展的重点在于提高自身收集和可视化正确数据的能力，应用正确的分析方法，并有效地响应业务目标。

数字孪生要应用在网络安全领域从目前的技术现状来看，该技术应用的发展难点主要有：

（1）网络空间的智能数字建模

网络物理系统环境、系统上下文、配置和任务方面具有高度的动态性。网络空间建模是将网络空间实体的动态数据通过虚拟实体建模展现，涉及到资产识别、网络拓扑识别、通信拓扑识别、网络策略统一管理等各项技术，存在一定的技术难度。

（2）网络空间实体与孪生体之间的数据和信息交互

网络数据的信息量巨大，依靠现有的大数据技术和人工智能技术在孪生体与网络空间实体之间建立数据传输通道会存在明显的延时问题和准确性问题，如何做到及时准确地反馈网络空间实体的变化，是数字孪生在网络安全领域应用必须解决的问题之一。

（3）安全态势推演

数字孪生在网络安全领域的应用，要求实现网络安全态势的智能推演，支持在孪生体中进行完整的威胁分析，并推演出威胁的影响范围和防护措施。涉及到的技术领域包括：网络渗透、威胁分析、脆弱性分析、场景建模、智能策略等，需要在智能推理方面产生革命性技术突破。

三、产业落地情况

在国外，2016年成立于意大利的Haruspex网络安全公司,提出构建并应用数字孪生来模拟攻击者的行为，从而以经济高效的方式将风险降到最低。Haruspex推出了相关产品来实现对网络空间的完整威胁评估、预测性防护、安全取证等。奥地利的萨尔茨堡研究中心的网络物理系统的可信赖IoT4CPS研究项目，通过设计数字孪生模型以及机器学习，来进行行为分析，以及安全性、隐私和安全措施的预测。

在国内，一些已有的安全技术其本质上也可以认为是数字孪生在网络安全领域应用中某个演进过程的技术实现。如：蜜罐技术，可被认为是基于类似数字孪生的思想去做的攻击欺骗；网络审计，可被认为是对网络环境的智能建模尝试（如，“立思辰安全监测审计系统”）。当然，这些探索仍然处于起步阶段，如果希望真正地将数字孪生的理念落地，应该是将“定义（建模）、展现、交互、服务、进化”等演进过程逐步实现，进而在网络建模、态势感知、攻击欺骗、攻防演练、趋势预测等多个方面强化网络安全。

四、意见和建议

数字孪生在网络安全领域的应用，可以有效提高网络安全防护水平，与工业行业数字孪生应用的结合可以进一步提高国家基础设施的安全，具有重大意义。目前数字孪生在国内外均处于起步阶段，需要国家和主管部门机构从战略层面加以引导和规范，各企事业单位在执行、建设层面积极配合，共同推动数字孪生在网络安全领域的快速应用和发展。

在战略层面，建议开展顶层设计，制定明确的数字孪生技术在安全领域应用的战略和目标。

在执行层面，依托产业生态力量，充分发挥生态体系下各专业力量的优势，加紧突破大数据、人工智能、虚拟现实等支撑技术核心壁垒，加快构建具备安全业务特点的产业生态。

在建设层面，建议按照从推动既有安全产品的整合、建设基于数字孪生理念的核心安全平台，以及开展基于平台策略的安全智能应用等三个阶段分批安排建设阶段和内容。

数字孪生在安全领域的应用在理论研究和应用探索方面仍需主管机构、产业界和学术界持续推动，注定将是一个长期持续的过程，要选择适应长期、可持续建设要求的技术、建设模式和运作模式，最终建立起符合数字孪生要求的安全数字孪生平台。