中国信息安全

China Information Security

“5G+产业互联网”时代数字孪生安全治理探索

贺仁龙1

(1.中国信息通信研究院华东分院,首席规划师)

数字孪生（Digital Twin），又称数字双胞胎，是对物理世界实体或系统的数字化表达，即在虚拟世界“复制”真实物理世界的事物，通过模拟物理世界的运转流程，预判趋势和风险，为决策提供依据。数字孪生被Gartner评为2019年十大战略科技发展趋势之一。Gartner估计，到2020年，将有超过200亿个连接的传感器，数字孪生将连接数十亿的实体设备。数字孪生带来的不仅仅是更便捷的创新实验、更低廉的试错成本、更精细的测量、更可靠的预测和更易于复制的经验，还升级了人们对“模型世界”的认知，打开了通过数字世界改造物理世界的窗口。然而，数字孪生发展的同时也伴随网络安全问题的逐步凸显，因此，形成全国全域感知的智慧安全指挥平台，通过安全的数字孪生技术推动智慧社会的高质量发展，才能发展现代化、数字化经济，才能构筑网络强国。

一、数字孪生是5G应用落地“强风口”

2002年，密歇根大学教授迈克尔·格里夫斯（Michael Grieves）第一次提出“数字孪生”概念。他认为，通过物理设备的数据，可以在虚拟（信息）空间构建一个可以表征该物理设备的虚拟实体和子系统，并且这种联系不是单向和静态的，而是与产品的整个生命周期联系在一起。2019年4月，我国工信部发布《关于加强质量品牌建设支撑制造业高质量发展的实施意见（征求意见稿）》，提出“推动云计算、大数据、人工智能等新一代信息技术与质量管理和技术融合，提高企业质量创新能力。推进数字双胞胎技术应用，推广可靠性仿真、质量波动仿真等模型和方法。”总体看，数字孪生可赋能各行业，整合全域感知、历史积累、运行监测等多元异构数据，集成多学科、多尺度的仿真过程，操控城市治理、民生服务、产业发展等各系统协同运转，形成一种自我优化的智能运行模式，实现“全域立体感知、万物可信互联、泛在普惠计算、智能定义一切、数据驱动决策”。

1. 数字孪生是战略科技发展的必然趋势

数字孪生通过设计工具、仿真工具、物联网、虚拟现实等各种数字化手段，将物理设备的各种属性映射到虚拟空间，形成可拆解、可复制、可转移、可修改、可删除、可重复操作的数字镜像，极大加速了操作人员对物理实体的了解，可以让很多原来由于物理条件限制、必须依赖于真实的物理实体而无法完成的操作，如模拟仿真、批量复制、虚拟装配等，成为触手可及的工具，更能激发人们探索新的途径，优化设计、制造和服务。

数字孪生是战略科技发展的必然趋势，基于“物理实体+数字孪生”的资数字孪生”的资源优化配置体系，也将成为数字化发展的终极模式。当前，数字孪生的技术应用逐步向制造、医疗、城市管理等各个领域渗透，众多企业也已在尝试利用数字孪生促进产品全生命周期管理，为远程操控、智慧城市管理、健康监测与管理等方面提供了更多可能。作为数字化发展的高级阶段，数字孪生将向综合企业数字化、信息化、智能化发展历程融合推进。

2. 数字孪生是5G赋能产业链的重要一环

4G时代的消费互联网以通信和社交为核心，实现人和人之间信息高效交互，其连接对象是人、电脑和手机。5G时代的产业互联网则将网络连接渗透到企业内部，其连接对象是人、设备、传感器等，通过5G、物联网、数据智能、机器智能等技术，实现“人机物”等生产要素的互联与制造协同。依托产业互联网，各个行业的转型升级，也将从传统产业的“独角戏”，升级为与产业互联网的协同“大合唱”。

数字孪生是5G赋能产业链上的重要一环，作为5G衍生应用，可以加速物联网成型和物联网设备数字化，与5G三大场景之一的万物互联需求强耦合。

在未来的5G时代，数字孪生能够突破传统通信技术点对点的通信模式，更多的物联网设备、工业设备将进入通信网络，进而使各行业加速融合，推动产业互联网形成。数字孪生将完全改变发现、认知和改造世界的方式，在未来世界大有可为,所带来的产业增长，也非常值得期待。

3. 数字孪生是推动工业互联网发展的助燃剂

随着工业互联网应用的推进发展，数字孪生被赋予新的生命力，工业互联网延伸了数字孪生的价值链条和生命周期，凸显出数字孪生基于模型、数据、服务方面的优势和能力，打通了数字孪生应用和迭代优化的现实路径，正成为数字孪生的孵化床。

数字孪生作为边缘侧技术，可以有效连接设备层和网络层，成为工业互联网平台的知识萃取工具，不断将工业系统的碎片化知识传输到工业互联网平台。不同成熟度的数字孪生体，将不同颗粒度的工业知识重新集成整合，通过工业App进行调用。因此，工业互联网平台是数字孪生的孵化床，数字孪生是工业互联网平台的重要场景。

“5G+产业互联网”可以实现信息流、指令流、操作流一体化，实现物质生产价值链各环节的在线远程控制，逐步实现工业数字孪生、社会数字孪生乃至整个数字孪生的世界。在工业领域，“5G+产业互联网”能够将全社会生产资源、生产过程、生产能力放置在互联网上，实现大规模海量协同的长尾效应，也服务于生产行为习惯的逐级优化、高速迭代。

二、数字孪生网络安全问题逐步凸显

5G时代，互联网将完成从消费互联网到产业互联网的时代变迁，而安全作为互联网发展的重要保障，它的主体、形态、思维都在发生重大变化。在消费互联网时代，安全保障的主体从以人为中心演变为以产业为中心；在数字世界与物理世界逐渐重合的今天，企业业务的云化和互联网化，让网络安全的边界愈加模糊，未知威胁变异加快，已有防御手段效果不佳，导致网络安全风险加剧，给企业带来巨大挑战，并阻碍业务发展、敏捷创新和运营效率的提升。从数字孪生世界的整体看，像2018年温州网约车遇害事件等系列刑事案件，都是物理世界、人类社会在数字世界的整体“全息投射”。

1. 系统性网络安全风险将集中呈现

以工业制造领域为例，数字孪生技术与智能制造的加速融合，使由封闭系统向开放系统的转变势在必行，系统性的网络安全风险将集中呈现。现代工业控制系统使工程师能够越来越依赖自动化，同时，通过企业资源计划（ERP）、制造执行、监督控制和数据采集等连接系统，保持高效率和实现资源控制。这些连接通常可以简化流程，使操作更加顺畅和高效，但是，增加网络和使用商业、现成产品会引入各种暴露点，可能会被威胁行为者滥用。2016年，德勤和美国生产力与创新能力制造商联盟（MAPI）的报告指出，三分之一的制造商从未对其工厂生产的工业控制系统进行过任何网络风险评估。

2. 未知安全问题将持续呈现上升趋势

数字时代促进了全球性互联互通供应链的发展，使企业可以很方便地发掘全球供应商及外包服务。这种连接也包括数据与网络的共享，一方面，企业通过这种连接和分析功能大大提高了效率，另一方面，这也给那些伺机而动的攻击者寻找现有网络安全漏洞打开方便之门。

网约车等新一代共享模式的出现，乘客信息安全问题、人身安全等问题在“互联网+”消费环境下进一步凸显。网约车作为典型的大数据行业，平台方掌握了海量数据和线上交易数量，如果数据脱敏不到位，很容易造成用户信息泄露。

从2018年到2019年的整体形势看，国内安全威胁事件更加普遍和严重。2018年6月，10亿条快递数据被公然在暗网兜售。这样的案例屡见不鲜。大量的用户数据被窃取后在黑产中流通，继而成为诈骗团伙的信息来源与线索。然而，安全监管工作则严重滞后于行业的快速发展，更难以有效应对不断推陈出新的网络攻击手段，未知的安全问题也将持续呈现上升趋势。

3.5G时代安全问题更加严峻

5G技术的不断成熟，将成为产业互联网的重要基础设施，这意味着毫秒级的响应要求，“掉网”可能造成严重的破坏性事件。试想，如果车联网受攻击而“怠工”，高速行驶的汽车很可能车毁人亡。5G时代来临使网络安全问题变得更紧迫、更尖锐。

“5G+产业互联网”所受到的攻击将会直接摧毁工业生产能力，以及国计民生的产业领域，一旦遭遇网络攻击，可能造成极大的社会影响和经济损失，导致个人、单位、地区、甚至国家的巨大损伤。

因此，在速度提升百倍、连接数增量十倍、响应用时仅需20%的5G时代，产业互联网安全威胁的突发性更强、破坏性更大。

三、构建数字孪生网络安全综合保障体系

总而言之，5G网络环境是一个多元而复杂的信息环境，金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全保障的重中之重，也是可能遭到重点攻击的目标。因此，迫切需要将数据孪生技术纳入网络安全综合保障体系之中，规划安全发展的整体路线。

1. 依托应用优势和产业基础统筹网络安全部署

网络安全防线是数字网络空间的国防安全线，是重要行业产业安全的生命线，也是全国安全一体化的护航产业线。加强网络安全建设，是贯彻落实国家战略、护航未来产业发展的重要举措。我国应当依托自身的应用优势和产业基础，统筹网络安全工作部署，开拓安全产业链上下游协同集聚发展的良好局面，力争打造网络安全的“桥头堡”。

2. 数字孪生治理需多层次相结合

习近平总书记在全国网络安全和信息化工作会议上的讲话中指出：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”。

如果把“数字孪生世界”比喻成海洋，那么当前的研究及应用则集中在海洋的“表层”治理与“底层”治理两个方面。“表层”治理好比清理海洋上的浮游垃圾与动植物尸体，主要表现为处理谣言、虚假信息、垃圾舆情等网络内容管理工作。“底层”治理则关注信息基础设施，例如监测网络与服务器等是否受到攻击，以及数据管理的安全防范工作。

然而，对于数字孪生世界海洋的中间层领域，譬如虚拟世界生产关系管理与协调、数字孪生世界所登记的各类产权确认与管理、甚至包含生产运营平台的法制化治理等，目前仍未有深入。综上所述，对数字孪生世界海洋中的中间层，即“水域”的安全管理与社会治理，还知之甚少，更缺乏相应的管理法规与处置手段的配套能力。因此，必须对此进行深入研究，采取有效措施，多层次结合，切实做好国家关键信息基础设施安全防护。

3. 建立全国范围全域感知的智慧安全指挥平台

5G时代，为有效推动数字孪生技术在智能制造、数字城市以及其他新兴领域的健康有序发展，必须建立全国范围全域感知的智慧安全指挥平台，实现“知、防、管、控”规范化、一体化、协同化、智能化，开展全天候全方位的感知城市网络安全和网络安全服务；实现区域维度、行业条线、跨区域协同的联动发现与联勤处置；实现全国级、大区级、省市级、地区级的层层防护能力与体系；实现“5G+产业互联网”国际空间信息安全的全面监控、最快发现、实时响应、集约指挥、协同处置的能力；打造国内首创的协作式体系化层次化智慧安全指挥平台，以更大力度、更实举措，筑牢网络安全的“防火墙”。在此，建议建立全国全域感知的智慧安全指挥平台，从“一个枢纽、三个中心、五个区域、五个层面”进行布局。

一个枢纽。建设全国区域一体化的网络安全枢纽，牵头开展全国范围内网络安全情报、态势、威胁等数据的联动共享，形成全国一体化的网络安全防线，构建新时代一体化的国家网络空间战略体系。

三个中心。建设全国范围的网络资源中心、网络安全威胁预警中心（包括工业互联网）、网络安全态势中心（包括工业互联网），打造全国一体化网络安全综合平台。在五大区域分别建设网络安全节点，提供重大事项保障和维护日常网络安全，形成多级联动效果。

五大区域。网络安全生态的建立，要从“单打独斗”变成“协同作战”。全国全域感知的智慧安全指挥平台分设中原、东部、南部、西部、北部区域平台，统筹协调组织本区域内网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

五个层面。积极净化网络安全空间，协助产业健康发展；不仅重视检查通报，同样需要重视网络安全问题解决，形成安全闭环；多方面发展网络安全产业，增强网络安全力量；形成网络安全试点示范，促进“产业+安全”；加大培养发展网络安全人才，全面支持国家网络安全建设。

4. 数字孪生打造“数字空间”全新应用形态

新一代信息技术的广泛应用，引发传统制造、生产模式的大变革。数字孪生作为新兴前沿技术，以仿真技术为基础，在智能制造、智慧城市建设等方面都将发挥较大的推动作用。通过数字孪生建立“数字空间”作为“大脑”指导物理空间，物理空间与数字空间高度融合，形成端到端的数据归集、汇聚和流动机制，建立贯穿各业务环节的、连续的、稳定的信息流，构建具备深度感知、万物互联、智慧决策、精准控制特性的全新应用形态。

四、以安全的数字孪生技术推动智慧社会高质量发展

未来，数以百亿计的事物将以数字孪生形态呈现。随着企业数字资产的不断积累，在全国全域感知的智慧安全指挥平台的管控下，利用知识自动化、专业分析算法等技术，快速洞察业务运行的内在规律，并通过机器学习等手段，实现自主学习和模型的自我进化，提升基于数据的主动服务水平和层次，推动应用从数字化、自动化向智能化迈进。加快建设数据驱动、实时感知、智能分析的新一代城市数字化治理综合基础设施，推动监管、交通、环境、治安、产业等各类数据加速汇聚、融通、挖掘、应用，助力智慧社会建设，利用汇聚的基础设施感知数据与实时脉动数据，探索构建“数字孪生社会”，形成实体城市和数字城市精准映射、虚实交互的城市发展新格局，推动智慧社会的高质量发展。

在未来的5G时代，数字孪生能够突破传统通信技术点对点的通信模式，更多的物联网设备、工业设备将进入通信网络，进而使各行业加速融合，推动产业互联网形成。数字孪生将完全改变发现、认知和改造世界的方式，在未来世界大有可为,所带来的产业增长，也非常值得期待。