

网络生物安全：大国博弈的另类疆域

□ 王小理

网络生物安全是指网络安全、网络实体安全以及生命科学与生物安全等学科间的一种新兴交叉领域，旨在理解生命医学相关网络空间、网络实体及其供应链、基础设施系统遭受恶意监视、入侵以及其他有害活动侵害过程及其状态脆弱性，并为应对此类威胁事件，开发和实施预防、防护、削弱、调查和归因机制，维持相关科技产业管理系统的安全、竞争力与稳健性。

近年来，网络生物安全融合网络安全，源于并超越生物武器、重大传染病、生物科技两用等经典生物安全框架，以一种颠覆性力量横贯生物科技创新链和产业链，并与国际网络军备、生物军控相互交融，成为影响国际战略稳定的新兴变量。对此新兴事物，宜保持清醒、放眼未来，下好先手棋。

何以可能：网络生物安全的兴起逻辑与内涵

催生网络生物安全形态的根本力量，根源于新一轮生物科技变革。当前，前沿生物科技创新，越来越依赖全球高端仪器装备（及供应链）和计算机网络。高通量测序技术、高性能基因编辑技术、生物大数据技术、合成生物学等使能工具的应用，标志着生物科技研究方法体系向自动化、信息化、智能化、工程化转型。美国科学院《21世纪的“新生物学”：如何确保美国引领即将到来的生物学革命》报告强调，“信息是新生物学的基本单元”。生物科技研发的数字化是大势所趋，网络生物安全随之兴起也是势所必然。

信息网络的安全问题渗透到生物科技领域。科研机构研发人员、企业生产制造人员、政府管理人员等使用计算机、智能设备来分析DNA序列、操作实验室设备和存储生物信息，但通常没有意识到新技术的便利通常伴随新的风险隐患。从DNA“特洛伊木马”数字攻击，到高价值的生物科技知识产权或敏感的个人健康信息被网络窃取，从关键的联网医疗仪器和设备遭受网络攻击，到“云”中共享的基因组数据完整性遭破坏和未经授权的访问等，相关的计算机系统、软件和算法自带的网络生物安全风险，一旦放在“安全放大镜”下审视，安全漏洞的发现几率将激增。特别是科技系统、卫生部门、农业部门、海关部门、商业系统的生物信息资源集成、技术与物项的监测监管信息平台，很有可能在未来成为网络生物安全的新兴风险点。

网络信息安全与生物安全互动，赋

核心阅读

近年来，网络生物安全融合网络安全，源于并超越生物武器、重大传染病、生物科技两用等经典生物安全框架，以一种颠覆性力量横贯生物科技创新链和产业链，并与国际网络军备、生物军控相互交融，成为影响国际战略稳定的新兴变量。对此新兴事物，宜保持清醒、放眼未来，下好先手棋。

予既有生物安全框架全新内涵。网络生物安全技术通过操控信息，间接操控人和技术、物项，使得虚拟生物安全与真实生物安全之间的界限正变得越来越模糊。这样使得原本用于加速生物技术研发或产业化的尖端设备、装备、生产线，也被纳入生物安全系统。如果说，传统生物安全还局限于特定的生物产品（重大烈性病原体或毒素）和前沿技术的终端应用、局部物项等范围的话，那么新兴的网络生物安全则囊括整个生物技术研发和产业链条中的每个环节，成为工具方法安全问题、过程安全问题、科技安全问题、全产业链安全问题，这使得“生物安全”概念的内涵和外延显著拓展。

战略新疆域：美国积极运筹网络生物安全

作为信息技术强国和生物技术强国，近年来美国各层级积极谋划和推动网络生物安全领域的工作。

聚焦概念本质。美国科学促进会、联邦调查局（FBI）大规模杀伤性武器部、联合国区域间犯罪和司法研究所等2014年发布的《生命科学领域大数据的国家与跨国安全影响》报告强调，利用敏感生物数据将可能对个人、组织和国家产生严重的经济、政治、健康和社会危害，生物信息（数据）安全兴起并成为国家生物安全的一部分，但其时尚聚焦在大数据及其分析技术方面，没有深层次触及次生信息的流动完整性和操控问题。2014—2016年，在FBI资助下，美国科学院先后召开三次以“捍卫生物经济”为主题的研讨会，抽丝剥茧，逐步逼近新科技变革下的生物安全新面貌实质，最终提出“网络生物安全”新概念。美国2018版《国家生物防御战略》吸纳了有关建议，隐晦指出“要防止敌对行为者为恶意目的获取或使用生物材料、设备和专业知识”。

强化理念引导。对这一新兴战略安全领域，美国国防部战略司令部2017年设立一个旨在评估生物科技基础设施安全性的研究项目，内布拉斯加大学国家战略研究所等4家单位参与，相关成果目前尚处于保密当中，但该项目涉及的两个研究方向“破坏生物学基础设施”和“制造危险生物材料”已开始得到美国学术界专家的认可。有关智库，如美国生物防御蓝丝带委员会、伍德罗·威尔逊中心、国防部大规模杀伤性武器研究中心等，围绕生物信息安全、生物实验室的连通性和智能性、生物虚拟化带来的风险等相关主题积极发声，在业界引起强烈关注。同时，2018年以来，作为美国战略科技力量，美国西北太平洋国家实验室、桑迪亚国家实验室、洛斯阿拉莫斯国家实验室、阿贡国家实验室的专家先后撰文，呼吁关注网络生物安全治理及相关科技发展。

大胆探索实践。科学模拟方面，美国安全研究人员能够用嵌入人类DNA链中的恶意软件感染计算机；在2019网络和分布式系统安全研讨会上，美国科研人员在一台常用的DNA合成仪器上展示了所谓的声学边信道攻击结果，并认为这可能会危害崭露头角的合成生物学和基于DNA的数据存储行业。引导行业加强防范意识方面，持续审视美国生物防御BioWatch计划的官方协调网站的潜在漏洞和系统缺陷，提出11条修复建议。在医疗卫生部门，美国健康主管部门于2018年先后成立网络安全协调中心、发布《健康产业网络安全实践指南》，协调整个业界的活动。

从发展角度来看，网络生物安全涉及推进和加强经济竞争力、国家安全和社会稳定，对于维持未来美国的经济实力和地缘政治非常关键。网络生物安全与美国生物科技产业战略目标密切相关。根据FBI定义，广义生物经济年创造4万亿美元价值，约占美国GDP的1/4。同时，网络生物安全增加了全球战

略稳定的新变量。网络信息安全和生物安全，属于大国战略博弈新疆域。网络生物安全横跨这两大领域，双向提升了网络空间军备控制和生物武器军备控制的重要性，使得生物安全有望成为与核安全、网络安全并行的全球战略稳定三极。鉴于大国竞争需要，网络生物安全对美国的战略价值和战略意义自不待言。

未雨绸缪：网络生物安全的未来大趋势和治理对策

网络生物安全形势可能恶化。目前，网络生物安全技术迅猛发展，全球发展不平衡问题是最大的安全问题。网络生物安全领域美国一支独大，从引领和影响世界生物科技创新和生物安全格局看，网络生物安全技术非常适合美国的科技优势和战略构想，经过3—5年的孕育，美国政府很有可能于2025年前后在网络生物安全领域开疆破土、呼风唤雨。

鉴于这一国际形势，宜积极主动，有所作为。首先，应树立崭新的生物安全观念，用长期战略框架审视网络生物安全。贯彻落实总体国家安全观，加强本领域基础理论探索和智库研究，客观评估网络生物安全态势和战略定位，在国家生物安全立法、生物安全管理条例等起草修订过程中有所体现。

其次，保持战略清醒，避免战略被挤压。认清生物安全核心装备和技术卡脖子现状，认清在生物软件、算法、数据库与国际先进水平的差距，认清网络生物安全战略技术差距，利用本领域战略机遇期窗口，谋划科技发展战略布局，凝聚一批网络生物安全领域战略人才，以便在未来发展竞争中谋取一席之地。

再次，实施外交和国家安全资源的再平衡。在网络军备控制、生物军备控制等国际既有框架基础上，启动前置性工作，加强网络生物安全政策储备、议程方案储备；在涉及国家安全与发展重大利益的网络生物安全问题上，及时发声、回应、提出反制措施，以人类命运共同体 的长远视野，维护国际战略稳定。



当前，工程技术的效益已在经济、社会等各领域得到了充分体现和展示；但与此同时，其引发的社会冲突时有发生，已成为我国社会转型时期遇到的重点难题。反思工程技术引发的种种社会冲突，不仅是因为其应用与发展过程中存在的利益冲突，而且与整个社会对工程技术的观念冲突密切相关。目前对于工程技术安全的治理侧重于强调“技术安全”，对于“价值安全”关注较低。但实际上，工程技术导致社会行为冲突的根源在于不同利益主体对工程技术的价值认知差异。因而，如何把握工程技术相关主体的价值取向，厘清工程技术中技术风险和价值风险间的关系，将是未来工程技术治理的关键所在。

工程技术的 不确定性是价值冲突的根源

工程技术本身的不确定性导致了价值认知差异。工程技术所涉及的理论是复杂的，所有的工程技术项目从理论上讲都应该是安全的，而现实的技术结果却往往呈现出概率性的、难以预测的结果。以基因编辑技术为例，伴随着其巨大经济效益的是多方面的技术不确定性。对生态系统的整体而言，基因编辑技术作物是否会对其他物种乃至生态系统产生影响还有待研究；从基因编辑技术的临床应用看，对人类细胞、胚胎细胞、功能增强等方面的应用上还未完全克服存在“脱靶”的技术障碍。这就是工程技术的不确定性会直接导致在应用上的价值争议。

工程技术认知的不确定性导致了价值认知差异。工程技术认知的不确定性源于工程技术和社会的交互关系，对于同样潜在的“现实利益风险”，不同的利益主体存在不同的认知。不同利益主体对工程技术的认识差异造成了价值观念冲突，而这种认知上的不确定性还使得冲突的观念在不对称的争论结构中互相纠缠、不断强化。

工程技术沟通的不确定性导致了价值认知差异。沟通的不确定性源于信息的不对称，不同利益主体对工程技术引发的现实风险持有不同的观点，而不同利益主体间一般仅保持着最低限度的观点交换，并没有发生观点的结合以及实质性的决策交换。

工程技术中“价值安全”治理的意义把握

工程技术的治理需要在工程技术政策决策前优先考虑社会价值，才能确保工程技术政策保持正确的价值导向。所谓工程技术中的“价值安全”治理，就是一种把价值前置的技术治理思维，就是要以价值思维引领工程技术的未来发展，以协商和互动的方式来实现对工程技术安全的有效治理。

首先，价值前置的工程技术治理提供了网格化的治理架构。网络思维将工程技术治理主体视为不同主体构成的利益共同体，将工程技术的治理结构视为由相互依赖、关系不确定的不同主体构成的网络，通过改变治理主体结构以应对技术本身的不确定性。此外，网格化的治理结构能够提供解决复杂工程技术问题的理论概念和规范起点。将技术本身的不确定性放置于工程技术决策过程背景下，通过“三方互动来参与政策的制定和执行，以形成应对工程技术安全问题的共识性规则。

其次，价值前置的工程技

未来工程技术治理的关键所在

□ 阙天舒 莫 非

术治理提供了网格化的治理工具。网格化的治理工具将不同主体协商和互动落实到新兴技术治理的博弈过程，以博弈过程体现工程技术中的不同价值观，来应对工程技术认知的不确定性。以不同利益主体对工程技术政策制定、执行的参与，来影响工程技术政策过程的演变。工程技术政策制定、执行过程中的多主体动态博弈，这种集合性思考的方式，将多个自变量结合为一个因变量，以此化解不对称争论困境中所产生的认知僵局和认知停滞。

最后，价值前置的治理方式从本质上衡量了工程技术的治理实践。信息的确定是作出有效工程技术决策的基础。在目前的工程技术治理中，难以获得不同主体一致认同的决策的原因在于工程技术的不确定性，而其中最大的负向量是信息的不确定性，所以无法产生积极有效的工程技术决策。而相关主体获取信息的程度越高，则产生有效决策的可能性越大。价值前置的技术治理方式，就是通过不同主体的协商和对话来进行决策，其协商和对话的过程就是公众参与的体现，就是不同主体了解彼此的态度、意见和建议从而共同制定最大公约化的规则和政策的过

程。综上所述，价值前置的治理方式更适合于我国现阶段的工程技术治理，其能够最大限度减少工程技术的不确定性所带来的价值冲突风险。注重工程技术中的“价值安全”治理，优先考虑工程技术的社会价值，通过多主体的参与、协商和实践来使人民意志体现于工程技术的应用之中。通过网格化的动态治理架构，将不同主体纳入协商和互动的博弈过程，以公众的参与实践来获取充分和对称的信息，促进技术安全 和价值安全的有效融合。



信息安全的本质在于技术主导权

□ 赵 刚

网络信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的技术创新领域，是全球技术创新的竞争高地。一段时间以来，西方一些发达国家，尤其是美国，以安全为理由拒绝使用华为的设备，其根本原因，就是华为在5G技术上的领先地位，给欧美发达国家带来了危机感。

信息技术一直是美国领先，第三次科技革命和产业变革主要就是信息技术的革命，在这方面美国占有绝对的优势，但以华为为代表的中国信息技术企业，依靠大量的研发投入和员工的勤劳智慧，攻克了一项又一项的技术难关，掌握了5G核心技术。

数字化时代，信息安全至关重要。它关系到国家的安全和主权，社会的安定和文化的传承，它的重要性也随着全球信息化进程的加快变得越来越重要。谁掌握了技术的主导权，谁就掌握了信息的安全，掌握了信息安全的主动权。从一个侧面可以看出来，过去所谓的信息安全，主要是

技术落后的国家，追赶型的国家，信息安全的风险最大，而发达国家，特别是美国这样的发达国家，信息安全对他们来讲只是一些技术上的改进和更新的问题，只是对一些技术漏洞进行修补的问题，不存在根本上的信息安全威胁。

随着5G时代的到来，情况发生了很大的改变。就一个国家安全来说，只要进行一定的技术防范，就不存在安全方面的隐患。例如，5G技术下，可以在发送端将信息加密，在接收端解密。也就是说，消息在被传输到达终点之前不进行解密。这样一来，即使在传输中间节点被攻击也不会造成信息泄露，除了信息加密，还可以利用信息完整性、可用性和抗抵赖性保证信息安全。由此可以看出，信息技术主导权非常重要。只有掌握了技术主导权，才能有自己国家的信息安全。

习近平总书记曾说过，高端科技就是现代的国之利器。近代以来，西方国家之所以能称雄世界，一个重要原因就是掌握了高端科技。真正的核心技术是买不来

的。正所谓“国之利器，不可以示人”。只有拥有强大的科技创新能力，才能提高我国的国际竞争力为此要努力做到以下四点。

第一，加大投入的力度，我们过去对关键核心技术，特别是卡脖子的技术，投入不足，重视不够。一些关键装备、关键零部件、核心的器件都严重依赖进口，像我们的光刻机、芯片、发动机，数控机床、触觉传感器等等，80%以上都依赖进口。

第二，攻克核心技术，我们还需要要发挥新型举国体制的优势。我们一定要集中力量办大事，统一思想，整体谋划，顶层设计。充分发挥科学家、企业家聪明才智，攻克一个一个难关，取得技术主导权。只有如此，我们才能真正获得国家的科技安全 和信息安全，以及国家的政治安全，最后才有整体的国家安全。

第三，培养科技领军人才和一流的科学家队伍。解决核心技术，掌握技术主导权，必须要有科技领军人才，要创造条件让这些科学家充分发挥聪明才智，包括制

度环境、法律环境、生活环境。只要这种创新、创造、创业的土壤具备了，领军型的科技人才就会源源不断地涌现。

第四，要加强国际合作。在全球国内整合人才、技术，整合各种创新要素和各种创新资源。近些年来，美国能源部前部长米榭文、英国皇家工程院院长安道琳、微软公司前董事长比尔·盖茨、麻省理工学院校长雷欧·拉斐尔·莱夫等一批具有很高国际影响力的国外专家，相继加入中国科学院和中国工程院外籍院士队伍。他们为我国工程科技的发展添砖加瓦，也培养了大批科技人才。外籍院士越来越多，是我国扩大国际科技创新合作、不断融入全球科技创新网络的一个缩影。

