新兴技术对全球安全治理的结构性影响

复旦大学国际问题研究院教授、博导　蔡翠红

摘　要：新兴技术凭借基础性、架构性、程序性和渗透性四大特质，逐渐演变为重塑全球安全治理的结构性力量。这种力量并非以外在冲击的方式显现，而是通过治理工具、治理对象和治理环境中的多重嵌入，逐步改变治理体系的运行方式，使技术成为制度结构的一部分。当结构性力量积累到足够程度，便在治理逻辑、治理权威与治理秩序三个维度上引发系统性变迁，推动全球安全治理从以主权与领土为中心的单域体系，转向跨域、多层、拼贴式的新型治理结构。

关键词：新兴技术　结构性力量　全球安全治理
【中图分类号】D815　　【文献标识码】A
DOI:10.16619/j.cnki.cn10-1264/d.2026.04.012

新兴技术的快速迭代与跨领域扩散，正以前所未有的方式重塑全球安全格局。无论是国家间的战略竞争、国际制度的适应性压力，还是跨国风险的链式蔓延，其背后均呈现出一个共同特征：安全问题的生成、传播与治理，日益依赖技术体系本身的结构特性。人工智能、卫星系统、网络基础设施、数据流动体系等关键技术，已不再是传统安全议题的外部变量，而成为影响安全秩序演化方向的深层动力。当新兴技术逐渐演变为塑造安全结构、行为体能力基础，以及治理制度运行方式的底层条件时，其影响已超出传统意义上工具性或议题性的范畴，从而具有一种能够设定治理可能性、约束行为选择并重构权力关系的结构性力量。理解这种力量的来源、逻辑与后果，是解释全球安全治理何以正在发生深层变迁的关键。

新兴技术作为结构性力量的生成机制

理解新兴技术为何能够推动全球安全治理发生深层变迁，必须首先将技术视为一种具有“结构性力量”的分析对象，而不是一般的治理要素。借鉴国际政治经济学的经典论述，本文将“结构性力量”界定为能够塑造行为体选择范围、重新配置权威关系、设定制度运行边界的基础性权力。不同于传统的“关系性权力”，结构性力量并不通过强制、交换或威慑体现，而是通过构建他者所必须依赖的制度性与物质性环境来实现影响力。[1]我们可以从基础性、架构性、程序性和渗透性四大主要特质，理解其何以从全球安全治理体

系所运用的客体与手段，演变为该体系不可或缺的主体与结构组成部分，从而成为一种塑造全球安全秩序的结构性力量。

基础性。技术之所以具备结构性力量，首先在于它已成为治理体系运行的基础资源。无论是跨国威胁监测、军事力量部署、供应链安全评估，还是网络防御和数据流动管理，其运作都依赖于高度技术化、可编程化的基础设施。治理行动并非仅被技术增强，而是根本无法脱离技术体系本身。没有全球导航卫星系统就无法进行精确打击，没有数据分析与人工智能系统就无法开展快速风险评估，没有通信网络就无法维持跨国协同治理。新兴技术正是通过这种基础性嵌入，在全球安全治理中获得设定行为边界的能力。

架构性。技术标准、协议和基础设施，共同构成数字时代全球安全治理的操作系统。一方面，标准即规则，5G、人工智能伦理、数据跨境等标准，预先设定治理的可能范围与方式；另一方面，技术基础设施，如海底光缆、卫星网络、根服务器等，构成全球安全治理的新疆域，且无论是技术标准、基础设施协议，还是频谱配置、轨道资源分配和人工智能模型底层架构等，都具有高度的先占性和惯性。一旦某一技术体系成为跨国治理的默认框架，就会形成锁定效应，其后进入者在制度、成本与兼容性约束下难以改变既有路径。技术架构由此预先设定治理行为的边界和规则，行为体在全球安全领域的活动，首先发生在由技术架构划定的“空间”内并受其约束，技术因此成为先于具体治理行动的结构性框架。

程序性。技术被深度内嵌于治理决策与执行的流程，成为全球安全治理的程序性依赖对象。治理不再单纯依赖制度框架，而是在技术体系的程序性逻辑中运作。随着人工智能、卫星网络、数据基础设施和通信系统成为跨国安全治理的常规配置，威胁监测、情报生成、风险评估、决策支持与执行协调等关键环节，越来越依赖技术体系的程序逻辑、处理路径与交互结构。治理流程不再自由地在制度空间中展开，而是在技术系统预设的节奏、接口与兼容性框架中被组织、限定与运行。一旦基于特定技术系统建立起安全治理的流程，如自动化核指挥系统和金融监控网络，因其高效和惯性，这一系统往往难以被替换或逆转。当技术从辅助工具转变为决策流程中不可或缺的环节时，其将获得塑造治理结果的能力。治理的程序正义和实质结果便开始受到技术运行逻辑的影响，技术由此成为治理结构的内在组件。

渗透性。结构性力量不是存在于单一的结构中，而是存在于各不相同但互有联系的结构中。[2]新兴技术并不隶属于单一安全领域，而是涉及军事安全、经济安全、社会安全与认知安全等各方面。这是一种“系统级”而非部门性影响。例如，人工智能可在军事上改变决策速度，在经济上重塑供需结构，在社会上改变舆论传播机制，在认知空间中改变信息真实性的判断基础；卫星遥感既是军事、经济与气候治理的关键基础，又与地缘政治博弈直接相关；网络体系更是横跨所有治理议题的底层空间。新兴技术由此成为连接不同安全子系统，并驱动其耦合的关键节点。这种跨领域渗透意味着，即便某一国家或主体试图在单一领域降低技术依赖，也无法真正脱离技术体系的整体运作。

综上，新兴技术之所以具有结构性力量，不在于其具有更强的工具效能，而在于其基础性、架构性、程序性和渗透性四大特质，共同构成一种能够设定治理可能性、约束行为选择并重塑权力分布的深层结构条件。当技术兼具这些特质时，将超越“在治理结构中使用的工具”这一角色定位，作为治理结构必须依赖的基石、必须遵循的框架、必须经过的流程以及必须应对的议程生产者，从而成为一种结构性力量。

新兴技术作为结构性力量对全球安全治理的多重嵌入

新兴技术具备成为结构性力量的必要条件，但结构性力量并不会凭空显现。要使技术真正影响全球安全治理，其需要进入治理体系的实际运行逻辑之中，并对治理能力、治理议程与治理空间产生实质性影响。这一路径可概括为“多重嵌入”，即技术通过嵌入治理体系的不同层级，使其潜在的结构性力量得以转化为实际的操作性影响。这一过程不是技术单纯地附加于治理体系，也不是治理对技术的简单适应，而是一种双向塑造关系的展开，使治理的运行条件、行动模式和可能性边界被技术逻辑重新组织。

工具嵌入：新兴技术作为治理手段。技术首先以工具的形式进入治理体系，这是结构性力量得以显现的初级形式，但其影响远远超出“提高效率”的传统理解。人工智能分析、机器学习预测、卫星遥感监测、自动化识别系统等技术不再是治理过程的辅助性组件，而逐渐成为治理能力的前提。当安全风险的识别、决策与响应必须依赖这些技术时，技术便获得“设定行动可能性”的权力。例如，人工智能风险分析系统决定哪些威胁能够被识别，卫星系统决定哪些区域具备可视性，跨境网络协议决定哪些攻击行为能够被追踪。治理行为者不是基于主观意愿采用技术，而是在一个技术定义的能力框架内开展治理。

更为重要的是，治理的节奏、尺度与决策逻辑也随之发生结构性变化。人工分析需要数日甚至数周的情报流程，如今可以实现毫秒级完成；网络攻击以极快速度传播，迫使治理者进入技术节奏控制的响应模式；卫星图像实时更新，使得治理从周期性管理转向持续性监测。技术决定了治理路径，而不是治理者通过制度安排决定行动方式。这意味着技术嵌入已经改变治理实践的基本结构，使得治理能力本身在技术体系中被定义，工具嵌入由此成为技术结构力量最直观、最具可见性的表现方式。

对象嵌入：新兴技术通过议程设定进入治理体系。当技术从治理手段转变为治理对象时，其结构性力量便进入到治理议程层级，影响治理内容本身。新兴技术不断生成新的安全议题，而这些议题往往具有不可回避性，从而迫使治理体系围绕技术逻辑进行再组织。例如，致命性自主武器系统（LAWS）推动国际人道法面临责任归属与伦理结构的重构；生成式人工智能驱动的深度伪造危机，使信息治理进入全新的风险时代；商业卫星在俄乌冲突中的广泛应用，迫使国际法重新界定民用技术的战略属性。在这些案例中，治理者关注的不是传统意义上的政治冲突或军事风险，而是由技术体系自身产生的连锁效应。这意

味着治理不仅处理外生的技术议题，而且必须从技术的逻辑出发构建议程。

议程结构的重塑，进一步影响治理主体的构成。传统的安全治理以国家、国际组织与条约体系为中心，但技术相关议题无法仅靠国家解决，也无法通过传统外交体系消化。科技企业、跨国工程组织、标准化机构和全球开源技术社区在许多关键议题中的角色甚至超过国家。例如，人工智能安全规范的制定离不开大型科技企业；网络治理依赖平台架构与协议控制；太空安全议题涉及私营航天公司；数据治理议题取决于跨国企业的数据中心布局。技术议程的出现推动治理权威从国家主导转向多主体分布，并使议程设置权成为新的权力来源。技术力量在这一层级的嵌入表现为，治理体系的内容与结构被技术所引导，而非由传统政治逻辑所主导。

环境嵌入：新兴技术成为治理空间。技术嵌入的目的不是成为工具或议程，而是构成治理活动发生的环境。传统的全球安全治理以领土地理范围作为基本空间框架，但技术扩展了治理的可能空间，使网络空间、外层空间和数据空间成为新的治理场域。在这些空间中，治理不再以国家边界为组织原则，而是以技术基础设施和系统逻辑作为运行条件。[3]这些治理活动并不是在技术之上进行，而是在技术体系内部展开。

网络空间是典型的治理环境之一，互联网协议体系、平台算法、数据路由结构和流量分配系统构成新的政治空间，其权力关系并不遵循传统地缘政治规律，而是受制于技术拓扑结构。例如，域名系统（DNS）与边界网关协议（BGP）的控制权，影响全球网络治理的基本秩序；社交平台算法，影响信息扩散的速度与范围，从而改变政治稳定性；跨境数据流动路径，决定国家对公民数据的实际控制能力。

外层空间是治理环境扩展的重要方向。轨道资源、卫星通信网络和高分辨率遥感体系，构成国家能力投射和信息控制的基础，使得治理空间从“地理领土”转向“轨道地理”；在数百颗卫星以集群方式运行的背景下，掌握轨道资源的行为体在事实上拥有重塑治理空间的权力。

数据空间的形成，进一步拓展安全治理环境。数据量、数据密度与数据可访问性，决定治理能力边界；数据主权论争，反映国家如何试图在技术构成的空间中重新定义边界；人工智能的训练数据，构成技术治理风险与能力的基础，使得治理者的权力与数据体系密不可分。在这些情境下，技术不是治理使用的要素，而是治理依赖的存在条件。

虽然工具嵌入、对象嵌入与环境嵌入可以单独分析，但它们并不是三个独立过程，而是在实践中层层叠加并相互强化，最终形成治理体系整体技术化的累积效应。工具嵌入改变治理能力，迫使治理者关注技术生成的风险，从而推动对象嵌入；对象嵌入进一步推动治理空间的技术化，使治理从传统地理空间转向技术空间，从而完成环境嵌入。环境嵌入反过来又进一步强化行为体对技术的依赖，使工具嵌入更为深入。技术的结构性力量决定治理者能够看到什么、操作什么、控制什么，以及治理在何种空间中展开。随着多重嵌入的累积，治理体系逐渐呈现出“技术性结构”，即治理运行的前提条件、规则逻辑与权力关系均在技术基础上展开。

新兴技术嵌入下全球安全治理的三维重构

新兴技术之所以能够深刻影响全球安全治理，不在于其工具属性或议题属性本身，而在于其通过多重嵌入机制获得结构性力量，从治理体系的外在变量，转变为治理秩序的生成条件，使得治理的逻辑、权威与空间基础被重新定义。这意味着，治理活动在何种逻辑下运转、由哪些行为体发挥关键作用、又在何种空间中展开，均因技术体系的存在而发生系统性变化，全球安全治理正在经历一种深层次重构。

治理逻辑的重构：从行为者逻辑到系统逻辑。在传统安全治理框架中，威胁识别、权力平衡与威慑机制构成治理的基本逻辑，即“行为者逻辑”，建立在威胁来源可以被归因，意图可以通过战略分析予以判断，力量可以通过部署与对冲实现均衡的假设之上。然而，新兴技术的出现使这些前提遭遇根本性动摇。技术驱动的风险不来自特定行为者，而来自系统结构本身：算法的不透明性、网络攻击的匿名性、卫星系统的链式脆弱性、数据泄露的非线性扩散，使得传统意义上的“敌意—意图”范式难以有效捕捉安全威胁的生成机制。[4]在这种环境下，各国越来越依赖技术预警系统、大规模数据监测框架和风险预测模型来识别潜在威胁。治理逻辑从控制确定性威胁转向管理不确定性风险，从对行为者行动的威慑与约束，转向对系统脆弱性的监测、调节与缓释。全球安全治理由此呈现出一种“系统逻辑”，强调预见性、风险化与敏捷性三者的结合。治理焦点从“谁会发动攻击”转向“系统在何处可能失稳”；从“控制行为”转向“控制系统的脆弱性暴露”；从“应对威胁”转向“持续监测和适应性调整”。

这种逻辑变化具有结构性意义，其既改变治理模式，又改变行为者在治理体系中的角色与责任。国家被要求持续维护系统稳定性，而非仅在危机爆发时采取行动；国际制度必须适应技术环境的高速变化，而不能依赖缓慢的条约谈判；企业与平台因掌握关键数据与模型，被纳入风险治理结构之中。治理逻辑的重构，由此成为技术结构性力量在治理体系中最先显现的转型维度。

治理权威的重构：国家的治理权必须通过与技术节点的互动实现。技术的结构性力量对治理体系最直接的冲击，是对治理权威来源的重塑。传统上，全球安全治理主要依靠主权国家展开。大国凭借军事、经济与外交资源占据治理中心，小国则围绕其制度安排展开行动。然而，当治理能力的基础由技术体系决定时，权威不再主要源于领土或主权，而是源于对关键技术节点的掌控能力。这意味着，技术节点成为新的治理中心。掌握全球云计算资源的企业、控制太空基础设施的商业航天公司、主导人工智能模型开发的研究机构、运营全球信息平台的技术巨头等，都在事实上拥有对治理过程产生影响的能力。它们能够决定数据流向、算法规则、空间访问权限和通信路径，因此在某些领域对治理进程的重要性超过传统国家行为体。治理权威由此从“政治位阶”转向“节点位阶”，呈现出以技术能力而非主权地位为中心的等级体系。

这一变化体现在国家—企业之间的权力再分配，也体现在国家内部权力结构的重新

排列。技术能力强的国家在治理网络中的位置不断上升，而技术基础薄弱的国家则面临被排除在关键治理协商之外的风险。权威关系因技术节点分布，而产生新的结构性差异，国际制度也随之发生结构重组。在数据治理、网络安全、外空管理与人工智能安全部门，治理不再依赖单一条约或统一机构，而是由多个技术节点构成跨主体网络共同调节。国家仍然是重要行为体，但其治理权必须通过与技术节点的互动实现。这种由技术驱动的权威重构，体现结构性力量在治理体系中的深度渗透，即谁控制技术节点，谁就能控制治理结构的运行条件。

治理秩序的重构：从单域秩序到跨域多层秩序。技术作为结构性力量对全球安全治理的影响，最终集中体现在秩序层面的深刻重构上。[5]秩序并非权力分布的简单映射，而是国际系统运行的底层组织逻辑，涵盖规则生成的原则、协调机制的运作方式以及稳定性的来源。在威斯特伐利亚体系长期塑造的国际结构中，全球安全治理秩序建立在单一空间与单一原则之上，国家主权是唯一合法的规则来源，领土构成治理边界，条约与力量均衡共同支撑秩序的稳定结构。这种“单域秩序”得以维持，是因为国际互动主要发生在地理空间，治理工具以政治和军事手段为主，边界清晰、层级分明。然而，当技术成为治理体系的结构性力量后，秩序得以运行的基础条件开始发生系统性变化。技术改写的不是某一项制度或某一类行为者，而是改写秩序形成的环境和秩序得以成立的前提。治理秩序的组织原则、协调方式与稳定机制因此出现复合化与跨域化的趋势，整体呈现出一种多层叠加的新型结构。

一方面，秩序的规则生成原则，正在从主权原则转向机制性多样化。在技术驱动的治理环境中，许多直接影响安全互动结构的关键性规则并非由国家制定。例如，互联网协议决定信息流动路径，数据互操作标准影响跨境风险暴露方式，算法治理框架影响模型误差传播及风险管理方式。这些技术性规则虽然没有形成新的中央权威，却通过设定行动可能性边界、塑造行为逻辑、定义系统运行条件，在事实上承担秩序组织功能。另一方面，秩序的协调机制，正在从条约体系转向制度拼贴。传统秩序依赖条约与国际组织来实现协调，治理过程以明确的层级和程序为基础。然而，在技术驱动的安全场景中，风险呈现高度跨域、即时和复杂的特征，使得条约体系的反应速度、灵活性与专业性难以满足需求。因此，治理协调机制呈现出“制度拼贴”的结构。技术标准组织、平台公司和技术联盟等成为规则制定的重要平台。这些机制之间不存在统一的权威层级，而是以并置、重叠和竞合的方式共同运作，使秩序的运行方式从线性、集中式转向分布式、复合式，这正是技术时代治理秩序的重要标志。

构建具备敏捷性、韧性与协同能力的新型治理体系

通过将“新兴技术”置于全球安全治理的深层结构之中，可以看到其影响力并非来自技术作为工具的直接效用，而是源于对治理体系底层逻辑的改变。技术之所以具备塑造国

际体系的能力，是因为其凭借基础性、架构性、程序性和渗透性的特质，形成了足以改变行为边界与制度结构的“结构性力量”。这种力量并非以外在冲击的方式显现，而是通过治理工具、治理对象和治理环境中的多重嵌入，逐步改变治理体系的运行方式，使技术成为制度结构的一部分。当结构性力量积累到足够程度，便在治理逻辑、治理权威与治理秩序三个维度上引发系统性变迁，推动全球安全治理从以主权与领土为中心的单域体系，转向跨域、多层、拼贴式的新型治理结构。

新兴技术驱动下的治理转型并非渐进式调整，而是一种范式层面的重构。未来全球安全治理面临的主要挑战，不在于如何控制单项技术的风险，而在于如何在高度耦合的技术体系中维持系统性稳定；不在于如何在传统条约模式下寻找共识，而在于如何协调多种机制、多层主体与多域空间之间的运行逻辑；不在于简单修补旧有制度，而在于构建能够适应技术速度、复杂性与不确定性的治理体系。在此意义上，全球安全治理应强调敏捷性、韧性与跨域协同，形成面向系统风险的新型治理能力。当技术成为世界结构的一部分，治理的首要任务便不再是应对技术，而是学会在一个被技术重新构造的国际体系中思考、行动与共存。

【本文系国家社科基金重大项目“科技革命、产业革命对世界格局的影响塑造和前瞻性应对研究”（项目编号：25&ZD277）的阶段性成果】

注释

[1][2][英]苏珊·斯特兰奇著、杨宇光等译，《国家与市场》（第2版），上海：上海人民出版社，2006年，第21页、第22页。

[3]丁迪：《数字科技驱动下全球治理的范式转变与中国方案》，《社会主义研究》，2025年第4期，第154—163页。

[4]苏若林、贾开：《跨越核技术类比陷阱：人工智能的国际安全风险及管控》，《国际政治研究》，2025年第3期，第33—55页。

[5]王明国：《全球互联网治理的模式变迁、制度逻辑与重构路径》，《世界经济与政治》，2015年第3期，第47—73页。

责编：周小梨 / 美编：石 玉