邱耕田
马克思主义实践观视域中的理论创新
→ 6版·论苑

宋蕾
以多元市场化机制推进绿色转型
→ 7版·智库

沈卫荣
略说语文学、古典学与“中国古典学”
→ 8版·学人

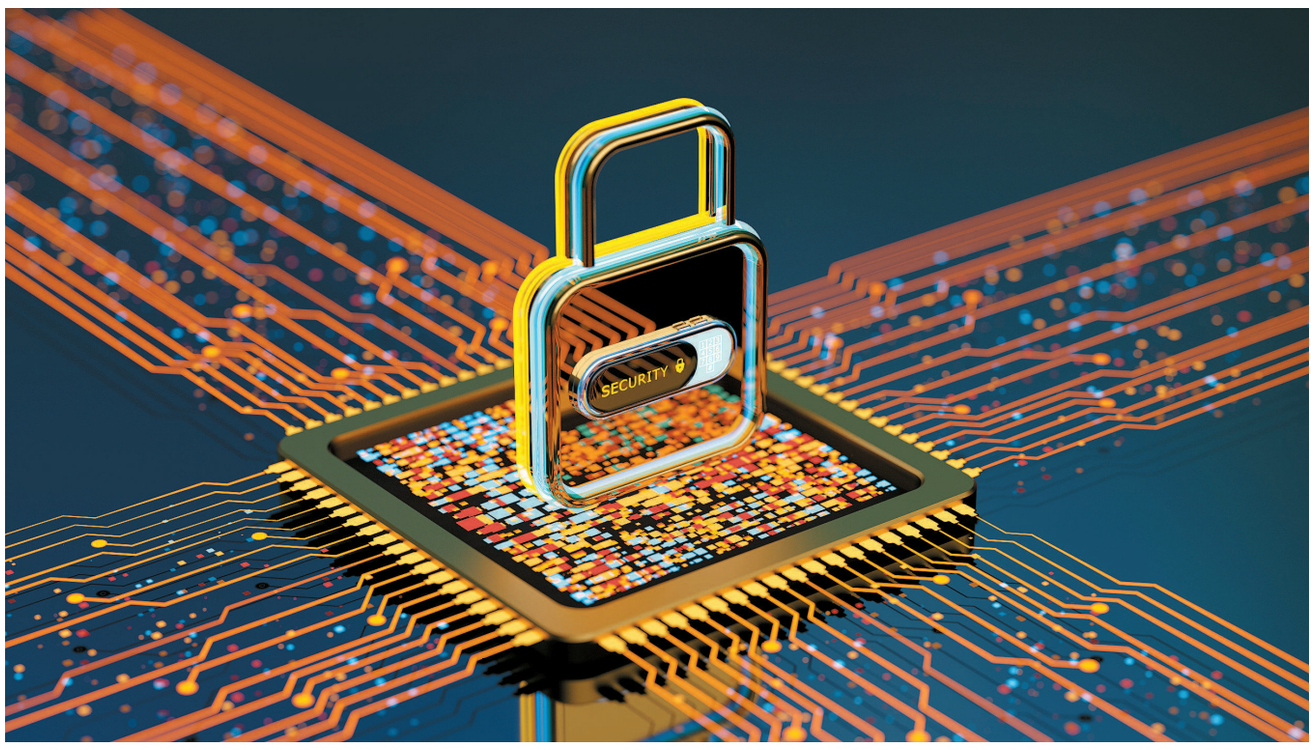
学术圆桌

网络安全和信息化是一体之两翼、驱动之双轮

筑牢网络强国的安全基石

■主持人：陈　瑜　本报记者
■嘉　宾：惠志斌　上海社会科学院互联网研究中心主任、研究员
阙天舒　华东政法大学中国法治战略研究院副院长、教授
鲁传颖　上海国际问题研究院研究员、网络空间国际治理研究中心秘书长

2024年是习近平总书记提出网络强国战略目标10周年，也是我国全功能接入国际互联网30周年。当前，随着互联网、人工智能、大数据等新技术飞速发展，国家网络安全形势日趋严峻复杂，网络安全成为关乎国计民生、关乎战略全局的一件大事。在去年召开的全国网络安全和信息化工作会议上，习近平总书记鲜明提出“举旗帜聚民心、防风险保安全、强治理惠民生、增动能促发展、谋合作图共赢”的使命任务，明确“十个坚持”重要原则，把对网信工作的规律性认识提升到全新高度。如何统筹发展与安全，筑牢国家网络安全屏障，推动网信事业高质量发展？本报约请三位专家研讨交流。



视觉中国

主持人：“没有网络安全就没有国家安全。”网络空间是国家的“第五疆域”，事关国家主权。网络安全也往往“牵一发而动全身”，对政治、军事、经济、文化、社会、科技等各领域安全产生深刻影响。今年是总体国家安全观提出十周年，如何在总体国家安全观的视域下，深刻认识网络安全的重要性？

惠志斌：统筹发展与安全是人类文明的永恒主题，也是中国式现代化建设的要求。总体国家安全观的关键词是“总体”，也对应了著名风险社会学者吉登斯所指的现代风险跨域性特征。当今世界，伴随移动互联网、物联网、大数据、人工智能等新一代数字技术集群化应用，网络空间与现实世界相生相伴，数据要素跨域跨境流动融合，网络数据安全不仅仅局限在网络空间，更是全面扩散和辐射到了政治、国土、军事、经济、文化、社会等各个领域，如网络政治安全、网络意识形态安全、网络金融安全、网络文化安全、网络恐怖主义等。没有网络安全就没有国家安全，不仅是党中央的战略判断，也是全社会的深切共识。因此，在新时代网络强国建设进程中，需要充分考虑到网络数据安全治理各要素间的系统性、整体性、协同性，着力提升治网管网用网能力水平，推进网络空间综合治理，推动形成良好网络生态。

阙天舒：互联网时代无疑带来了前所未有的机遇与红利，但网络空间安全领域正面临日益复杂且紧迫的挑战，网络安全风险问题已成为非传统安全的典型代表。总体国家安全观视域下，网络安全观与总体国家安全观不仅是包含关系，也是与其他安全观念有机统筹关系，因此，树立正确的网络安全观必须深刻理解新时代总体国家安全观的重要内涵。一方面，网络空间对于总体国家安全观的谋篇布局具有承载作用，国家安全、社会稳定及可持续发展离不开网络安全。其不仅意味着网络安全观是总体国家安全观的内涵之一，更表明筑牢网络空间安全防线对于实现总体国家安全观具有重要现实意义。另一方面，网络安全问题展现出了与总体国家安全观其他领域交织互动的特性。它远超自身技术范畴，深刻嵌入到政治安全、经济安全、文化安全等多元维度之中，并与之相互联系、作用。特别是在人工智能、信息技术等日新月异的今天，网络空间安全态势呈现出更加深层次的联动，维护网络空间安全不仅是保卫数字疆域的纯技术实践，更是维护国家综合安全利益的跨领域战略行动。

鲁传颖：网络安全不仅是总体国家安全观下的一个重要安全领域，同时，它也对其他传统安全与非传统安全领域产生了深刻的影响。这不仅包括军事、情报领域日益加大的网络安全冲突，还有金融、能源、交通、医疗等国计民生相关的重点行业面临着不断增加的网络安全风险。近年来，大国在网络安全领域的博弈不断加剧，成为国家安全领域面临最主要的风险挑战之一。在这种情况下，重视网络安全风险，提高认知程度，加大对网络安全的能力建设，成为各国政府的普遍做法。与其他安全领域相比，网络安全具有安全泛在、风险来源不确定、安全边界模糊等特点。这使得传统安全战略无法有效应对网络安全挑战。因此，不仅需要从战略高度来看待网络安全挑战，还需要应时而动，顺应技术发展趋势和网络安全特点，建立更加有韧性的网络安全体系。既要预防风险，也要树立正确的网络安全观。

主持人：当前，信息革命时代潮流与中华民族伟大复兴战略全局、世界百年未有之大变局发生历史性交汇。习近平总书记深刻指出，“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进”，“网络安全和信息化是一体之两翼、驱动之双轮”。在加快建设网络强国的背景下，如何统筹好网络安全和信息化的关系？

惠志斌：网络安全和信息化是相辅相成的。统筹发展与安全，是贯彻总体国家安全观的重要要求。我国信息化发展起步较早，但一度处于先建设应用后安全治理的状态，特别是随着移动互联网和人工智能的普及应用，网络数据安全风险日益凸显，突出表现在关键信息基础设施、数据安全和隐私保护、网络空间军事化威胁等诸多方面，直接关系到国家安全、社会稳定和人民利益。为此，我们必须着眼统筹发展和安全，坚持正确的网络安全观，深刻把握网络安全是动态的而不是静态的、是开放的而不是封闭的、是相对的而不是绝对的等重要特征，立足开放的环境，树立动态的网络安全防护理念。在实践层面，需要加大全社会的安全投入和意识教育，在实战中持续检验全社会、各行业的安全防护能力，将安全基因融入数字化转型的全生命周期，做到同步规划、同步建设和同步运营。

阙天舒：建设网络强国需要深刻理解网络安全与信息化建设相辅相成的辩证统一关系，信息化对于网络强国建设具有积极的引领驱动作用，而网络安全则为信息化建设提供坚实的安全基础与防护保障，二者一体两面、互为表里且紧密联系，应当统一部署，协同推进。第53次《中国互联网络发展状况统计报告》显示，我国互联网普及率达到77.5%。这说明网络强国战略的信息化发展规模空前，但也要注意到，网络安全需求也与日俱增。信息化发展效率受到网络安全水平制约，信息化发展速度越快，网络安全风险指数也越大，若网络安全缺位，信息化发展就会存在失控风险甚至造成灾难后果。因此，要积极探索网络安全与信息化建设协同发展及深度融合路径，在增加信息化发展投入的同时，也要关注网络安全效能的实际产出，既要推动信息化高质量发展，也要筑牢网络安全防护屏障。实践中，关键信息基础设施的布局代表着信息化发展程度与水平，应当进一步加强其防护能力，从技术、制度、人员等方面多措并举，构建监测、预警、响应于一体的安全治理体系，提升应对重大网络危机事件的整体韧性与恢复能力，从而实现网络安全与信息化发展实践的有机统一。

鲁传颖：网络安全是泛在安全，广泛存在于所有的信息系统当中，而信息化、智能化成为当今经济发展、社会治理的主要发展方向。建设网络强国离不开信息技术、数字技术的大力发展。因此，任何追求绝对安全的做法都不可取。要通过提高网络安全能力保障数字经济、信息技术的发展，就需要不断提高对于网络安全根本属性的认识。要做好安全与发展的平衡，就要做到既要重视网络安全，也要避免安全泛化，避免简单将网络安全等同于国家安全。例如，任何发生在军事领域的网络攻击都是国家安全问题，而在金融领域发生的网络攻击则需要根据损失的后果、影响面的大小来判定如何定性。网络安全风险与信息化程度总体上成正比，信息化程度越发高，面临的网络安全风险就大。因此，对于网络安全风险的接受程度也要有一个客观的认识。不能因为提升信息化程度会增加网络安全风险就因噎废食，而是要建立更大的安全格局，将发展收益纳入安全成本的考量当中。

主持人：习近平总书记对网络安全工作作出“四个坚持”的重要指示，其中之一为“坚持促进发展和依法管理相统一”。当前，新一轮科技革命和产业变革正加速演进，数字应用场景日趋丰富与复杂，如近年来生成式人工智能的大规模兴起，给网络安全带来新的挑战。在这样的背景下，如何既释动创新之翼，又夯实法治之基，筑牢数字经济发展的安全底座？

惠志斌：数字经济时代，坚持安全可控和开放创新并重，是行稳致远之道。网络空间安全需要秉持协同治理的理念，汇聚全社会的智慧和力量，因此构建一个与时俱进的网络空间法治体系尤为关键，这是保障数字经济和网络空间健康发展的基础土壤。当前，生成式人工智能、Web3.0、区块链等技术发展方兴未艾，网络空间进入代码即规则时代。因此，我们需要对这些新技术、新模式、新应用加强前瞻性的研究，科学研判可能存在的各类风险，同时让更多创新主体主动参与到新规则的设计和制定之中，推动人工智能时代的伦理构建和价值对齐，以制度的力量守护科技向善。

阙天舒：数字经济的健康发展离不开网络安全的坚实基础，而数据安全是兼顾网络安全秩序与数字经济发展活力的关键。由于技术特性的升级迭代，数字经济对于数据安全的现实需求十分迫切，数据安全不仅是保持数字经济运行稳定的安全盾，更是加速数字经济高质量发展的催化剂。数据安全治理既要强调数据流通赋能效应，更要重视数据全生命周期的安全保护。要进一步推动数据基础制度的完善，保障数据安全在数字经济发展中的创新引擎作用。因此，要从数据安全治理角度完善数字经济领域的“一典五法”制度体系建设，明确数据权利义务、主体地位、使用规范等关键要素，为数字经济发展提供坚实的数据安全法治基础。同时，数据基础制度要增强对人工智能科技要素发展的关注与采纳，根据国家数据法律法规及行业标准规范构建数据安全制度体系，推动数据可信空间架构建设，从而保障数据安全高效有序流通。

鲁传颖：法治是保障网络安全的重要手段之一。近年来，我国先后制定了网络安全法、个人信息保护法、数据安全法，出台了关键信息基础设施保护条例、生成式人工智能管理办法等法律法规。这些法律在保障我国网络安全方面发挥了重要作用的同时，也在检验着我国的司法、执法能力。网络安全相关法律体系作为一个新兴领域，执法者与合规者都面临着巨大挑战。法律条文越清晰，执法细则越明确，企业的合规成本就越低。反之，不仅会大幅增加企业的合规成本，甚至会遏制创新发展。在这一点上，要充分考虑我国数字经济、数字技术发展阶段的实际情况，不能简单照抄国外的做法。国际上有一个所谓“布鲁塞尔效应”，即欧盟制定的区域性法律法规对其他国家产生了重要影响。要充分地认识到中国作为一个网络大国、人工智能大国，有自身发展的节奏与特点，不应受到其他国家和地区的干扰。当前，网络技术、人工智能技术正处于大发展阶段，大国科技博弈日趋激烈。核心技术上能不能取得突破不仅事关网络强国建设，也事关中华民族伟大复兴。因此，网络安全、人工智能等领域的法律建设应当在战略层面考虑技术发展与法律治理之间的关系。不仅要给技术发展预留足够多的时间，也要提升对于技术的理解能力，强化能力建设，促进网络领域的法治水平。

主持人：网信工作与10亿多网民直接相连，与14亿多人民的获得感、幸福感、安全感息息相关。近年来，个人信息泄露、电信网络诈骗、网络谣言、网络勒索、恶意软件泛滥等事关人民群众切身利益的网络安全问题频现。如何持续推进网络安全综合治理，维护人民群众在网络空间中的合法利益？

惠志斌：坚持以人民为中心，是确保互联网更好服务于人民的核心原则。互联网已经深度融入经济社会各领域，成为人民群众生产生活、求知求美、创新创造的重要平台。我们要进一步抓好网络内容建设，培育积极健康、向上向善的网络文化，用社会主义核心价值观和人类优秀文明成果滋养人心、滋养社会。以时代新风塑造和净化网络空间，让正能量、主旋律始终充盈网络空间，提升广大人民群众在网络空间的获得感、幸福感、安全感。推进法治化治理，完善长效治理机制，是互联网在法治轨道上健康运行的保证。我们应把集中治理和常态化治理有机结合起来，坚持标本兼治，不断完善长效治理机制，进一步做好互联网管理基础性工作，持续为我国网络安全和信息化事业发展保驾护航，推动互联网健康稳定发展。因此，为最大化增强互联网事业发展的强大动力，需要坚持多方协同，形成治理合力。在党管网络治理的前提下，行业组织发挥好督促作用，强化行业自律意识；互联网平台主体增强责任意识，守好网络治理第一道关口防线；广大网民规范个人网络行为，增强网络鉴别能力。

阙天舒：构建风气清正、和谐共生的网络空间环境是深化网络安全综合治理、捍卫人民正当权益的根本。近年来，中央网信办开展的“清朗”系列专项行动就是针对网络生态突出问题的有力措施，其中涵盖的各类整治任务表明：首先，要强化网络安全风险的全周期监管，从源头治理网络虚假信息，切断其传播链条，并迅速启动网络辟谣行动，有效阻击网络空间中的虚假信息洪流，净化网络生态。其次，应促成网络空间安全共治的新型格局，尤其是社交媒体平台作为网络安全风险滋生、汇聚、扩散的主要场域，其运营方理应承担着不可推卸的社会责任。政府部门须引导并补足社会治理力量，携手各方共筑网络安全防线。同时，建立健全网络空间风险评估与预警机制，强化风险情报搜集与分析，精准识别潜在威胁与系统脆弱性，增强应对网络风险的前瞻性及预见性，推动网络安全综合治理的关口前移。此外，要完善并优化网络信息监督与举报机制，确保对网络不法行为的举报能迅速得到响应和有效处理，提升网络安全执法执行力与公开透明程度，切实保障人民的网络合法权益，提升大众在数字时代的获得感与幸福感。

鲁传颖：“网络安全为人民，网络安全靠人民”是我国网络安全工作的根本宗旨。随着我国信息化、智能化水平的不断提高，人民群众在享受便利的同时，也面临着越来越多的网络安全风险。网络的虚拟性、跨国性、匿名性给国家治理网络犯罪带来了巨大挑战。要做好各种形式的网络犯罪预防与打击，就需要多管齐下做好相关工作。首先，要提升公众的网络安全意识与数字素养，筑牢防范网络犯罪的第一道防线。其次，要加强国际合作，推动联合国打击网络犯罪公约尽早通过生效，杜绝犯罪分子利用不同国家之间的法律漏洞来逃避惩罚。最后，要提升网络技术的综合治理能力，更好地利用人工智能、大数据、区块链等新兴技术来应对各种形式的网络犯罪。

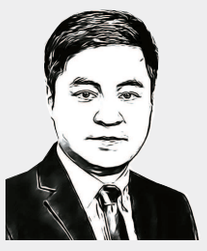
观点


惠志斌

数字经济时代，坚持安全可控和开放创新并重，是行稳致远之道。当前，生成式人工智能、Web3.0、区块链等技术发展方兴未艾，网络空间进入代码即规则时代。因此，我们需要对这些新技术、新模式、新应用加强前瞻性的研究，科学研判可能存在的各类风险，同时让更多创新主体主动参与到新规则的设计和制定之中，推动人工智能时代的伦理构建和价值对齐，以制度的力量守护科技向善。


阙天舒

维护网络空间安全不仅是保卫数字疆域的纯技术实践，更是维护国家综合安全利益的跨领域战略行动。一方面，网络空间对于总体国家安全观的谋篇布局具有承载作用，国家安全、社会稳定及可持续发展离不开网络安全。另一方面，网络安全问题展现出了与总体国家安全观其他领域交织互动的特性。它远超自身技术范畴，深刻嵌入到政治安全、经济安全、文化安全等多元维度之中，并与之相互联系、作用。


鲁传颖

网络安全是泛在安全，广泛存在于所有的信息系统当中，而信息化、智能化成为当今经济发展、社会治理的主要发展方向。建设网络强国离不开信息技术、数字技术的大力发展。因此，任何追求绝对安全的做法都不可取。要做好安全与发展的平衡，不能因为提升信息化程度会增加网络安全风险就因噎废食，而是要建立更大的安全格局，将发展收益纳入安全成本的考量当中。