数字时代国家安全困境与网络空间命运共同体构建

郎 平

【内容提要】以互联网、大数据、人工智能为代表的数字技术加速创新应用和融合发展，国际社会由网络时代迈入数字时代。在这一时代，网络、数据和人工智能安全风险相互叠加交织，国家行为体面临更加复杂和不确定的安全环境，表现为不安全感加剧、安全概念泛化和滥用以及在对外关系中统筹发展和安全的难度加大等特点。国际社会只有同舟共济、携手构建网络空间命运共同体，才能有效应对数字时代的国家安全困境，实现普遍安全和发展，推动人类社会走向和平与繁荣的未来。

【关键词】数字时代　国家安全　网络空间命运共同体　人工智能

纵观人类社会发展历程，每一次重大技术革命都会给国家安全带来新挑战。在以互联网为代表的信息技术革命影响下，网络安全成为关乎全局的重大问题，而大数据、云计算等数字技术创新加持下的数字智能革命则进一步拓展了网络安全的内涵和外延，其涵义已等同于数字时代的国家安全。当下，数字空间已经成为大国博弈的竞技场，面对数字时代高度不确定的安全威胁和风险，国际社会是携手共治还是对抗分裂，将在很大程度上决定人类发展的未来。

数字时代的国家安全环境

伴随着数字技术加速创新应用和融合发展，数字化、网络化和智能化革命正在世界范围内展开，数字经济成为世界经济增长和产业变革的新动能新引擎。同时，数字技术的广泛应用也带来更多更广泛的安全风险，国家安全环境在不断演进的技术发展中面临更大的不确定性和复杂性，这一方面表现为网络攻击和网络犯罪等恶意网络活动持续肆虐，另一方面数据安全和人工智能安全风险迎面而来并与网络安全风险相互交织叠加。数字时代的国家安全环境也由网络时代迈入数字智能化时代。

在网络时代，国家主要面临来自技术层面和社会层面的两类安全威胁。技术层面的安全威胁可以出现在网络空间系统的各个环节，通过对计算机系统和网络系统的攻击，造成诸如计算机系统资源被非法入侵，信息内容和数据被非法修改、破坏和窃取，网络接入和网络服务被中断，关键基础设施无法有效运转等危害。社会层面的安全威胁主要表现为网络犯罪、网络恐怖主义、个人信息和隐私被侵犯、信息操纵背景下的舆论战和信息战等，它们往往被某些行为体（个人、组织或国家）以代码或信息内容为工具和武器，通过扰乱一国的政治经济社会秩序，从而实现其商业或政治目的。网络时代的国家安全风险主要来源于互联网自身的技术漏洞以及网络空间应用层和内容层被人为利用或武器化，也就是说，一国的信息化程度越高，其对网络设施的依赖程度越大，所面临的安全风险也就越高。美国是互联网的缔造者并且拥有全球最强大的网络实力，虽然先后出台了“前置防御”“持续交手”“分层威慑”“前出狩猎”等进攻性网络安全策略，但同样面临诸多网络安全威胁。

近年来，在互联网浪潮的助推下，大数据、云计算、物联网、人工智能等数字技术取得重要进展，数字经济与实体经济深度融合，网络空间由此迈入数字智能化时

代。这个时代的重要特征就是数字技术融合生态的出现，每一项技术创新都有其他技术突破作为支撑，无论是万物互联的前景还是人工智能的广泛应用，都需要依托强大的互联网基础设施、大数据技术和算力的不断提升。但作为硬币的另一面，网络空间的安全威胁也出现了融合性的新特征。例如，攻击者利用人工智能技术，可以高准确度猜测、模仿、学习甚至是欺骗检测规则，挑战网络防御的核心规则；与既有攻击手段融合，在网络攻击效率、网络攻击范围、网络攻击手段等方面加剧网络攻防长期存在的不对等局面；人工智能与区块链、虚拟现实等技术结合还可催生出新型有害信息，形成有针对性的传播目标，衍生有害信息传播新模式，并加大数据和用户隐私全面泄漏的风险。无论是网络攻击工具的变异升级还是攻击效果和影响范围的扩大化，供应链安全、数据安全、人工智能安全既关系到国家的产业和经济安全，更渗透到国家政治、经济、社会、军事等领域的方方面面，可谓牵一发而动全身。

人工智能特别是生成式人工智能取得重大突破，标志着人工智能技术从弱人工智能向强人工智能的飞跃。尽管生成式人工智能会创造非凡的增长机遇，但其所带来的安全风险已经引发国际社会高度关注。美国政治风险咨询公司欧亚集团总裁、政治学者伊恩·布雷默指出，生成式人工智能的迭代升级速度超乎想象，国家试图控制人工智能并使其为己所用，但远远跟不上人工智能的升级和普及速度；这一技术很有可能威胁民族国家作为世界地缘政治主体的地位，并将引发全球权力结构和平衡的根本转变。[1] 美国纽约大学斯特恩商业与人权中心副主任保罗·巴雷特等认为，生成式人工智能应用软件能回答晦涩问题、编写计算机代码、创作诗歌和进行可怕的人类对话，将带来一系列风险，包括为散布虚假信息和发动网络攻击提供便利、激化种族和性别偏见、侵犯个人隐私和扩散网络虚假信息等。[2] 俄罗斯联邦内务部社会委员会主席阿纳托利·库切连纳教授认为，人工智能在军事领域的应用可能导致对“绝对武器”的追逐，引发规模远超冷战时代的军备竞赛，还可能完全操控人类的生活，并给教育体系带来难以想象的混乱。[3]2023 年 7 月，联合国安理会首次以“人工智能给国际和平与安全带来的机遇与风险”为主题召开高级别公开会议，联合国秘书长安东尼奥·古特雷斯表示，尽管人工智能工具越来越多地被联合国用于识别暴力模式、监测停火以及帮助加强维和、调解和人道主义努力，但使用人工智能的网络攻击已经开始针对关键基础设施和维和行动，生成式人工智能的出现很可能成为虚假信息和仇恨言论现象的“决定性时刻”。此外，人工智能系统出现故障以及人工智能与核武器、生物技术、神经技术和机器人技术之间的密切关联也会带来相应风险，国际社会迫切需要对这一变革性技术进行全球治理。[4]

2021年5月7日，美国最大燃油运输管道运营商科洛尼尔管道运输公司遭黑客攻击，被迫关停供应网络。图为5月12日弗吉尼亚阿灵顿一处燃油售罄的加油站。（中新社图片）

数字安全困境下的国家行为体

数字时代不断演进累积的安全风险成为当今时代之变的重要特征，而大国力量对比的深刻调整则导致大国竞争加剧，两者相互叠加交织，不仅成为数字时代国家安全困境的根源，也成为撬动数字时代国际关系演变的重要支点。对处于世界无政府状态下的国家行为体而言，安全始终是其最根本的利益，使国家免受重大安全威胁和消除安全恐惧是其参与国际互动的最根本需求。为此，西方主要国家纷纷制定或调整国家安全战略，以维护国家主权、安全和发展利益。

2023 年 3 月，拜登政府发布新版《国家网络安全战略》，明确描述了新的战略环境变化并对其网络空间战略作出重大调整。[5] 第一，重新定义网络空间的战略目标，从狭义的网络空间安全和繁荣转向更能体现美国未来战略目标的数字生态体系，并且描绘了美国在下个十年的新蓝图 ：从智慧电网到万物互联再到实时的全球合作，宣称美国继向世界提供互联网这一公共产品之后，将为世界提供能够“促成各种科学发现以及其他超乎想象的公共产品”。第二，美国政府对网络空间的战略定位出现重大转变，互联网从全球公共产品再度成为美国实现战略目标的国家权力工具。例如，白宫明确指出 :“在今后决定性的十年里，美国将把网络空间重新构想为一种工具，以反映我们价值观的方式实现我们的目标 ：经济安全和繁荣，尊重人权和基本自由，对我们的民主和民主化制度的信任以及多样化的社会。”[6] 第三，对华战略定位从“长期竞争对手”转向“最大威胁”，并诬称中国“对美国政府和私营机构的网络构成了最广泛、最活跃和最持久的威胁”。在美国看来，中国对美国的威胁已经不仅仅局限在某个领域，而是一个既有“重塑国际秩序意愿”又具备经济、外交、军事和技术实力推动实现这一目标的大国。

作为数字主权理念的提出者，欧盟也进一步强化了其数字发展战略中的安全考量，并提出“去风险”策略。2023 年 6 月，欧盟委员会发布《欧洲经济安全战略》，针对当前欧盟面临的一系列经济风险，在既有政策和工具的基础上，设计出一套包括评估、提升、保护与合作的整体架构，从而达到全方位“去风险”的目标。[7] 欧盟认为，新冠疫情、乌克兰危机以及地缘政治紧张局势加剧凸显欧洲经济的脆弱性，而深刻的技术变革正在增加安全挑战的复杂性。在这样的背景下，欧盟主要面临四类安全风险 ：供应链弹性风险、关键基础设施的物理和网络安全风险、技术安全和泄漏风险以及经济依存武器化和经济胁迫的风险。对此，欧盟强调要建立欧盟经济安全的共同战略框架，最大限度地发挥经济开放的优势，同时最大限度地减少相互依存带来的安全风险。主要路径是提升自身经济实力以降低风险，加强自我保护以防范风险，建立更广泛的经贸联系以分散风险。美国战略与国际研究中心学者费德里科·斯坦伯格和艾米丽·本森认为，《欧盟经济安全战略》的发布是欧盟将经济安全和外交政策联系起来的重要一步，该战略总体上试图勾勒出对欧盟经济安全构成威胁的各类情形，并进一步强调地缘政治风险已开始渗透到几乎每个政策领域 ；虽然在对华政策上存在差异，但欧盟的经济安全战略与拜登政府的新经济学说基本保持一致。[8]

显然数字时代的国际环境变化正在对国际体系中的国家行为产生影响。首先是国家的不安全感加剧。一般认为，安全是指国家感到不受威胁或免于恐惧的状态，其中既包含了外部威胁的客观态势，也包括行为体对威胁的主观认知，


（新华社图片）

而后者与自身维护国家安全的能力直接相关。在国家力量对比发生深刻调整的当下，数字技术创新和应用的快速迭代成为大国综合国力提升的重要引擎，但也会导致国家陷入该领域安全能力缺失的真空，增加国家的不安全感，并且加剧对他国特别是对手国实力快速提升的恐惧。例如，2023 年 6 月，德国发布首份《国家安全战略》，内容涵盖外交、警务、国际发展、网络安全和供应链等，标志着德国国家安全理念在数字时代呈现明显的泛安全化转向。

其次是大国竞争背景下国家安全概念泛化和滥用。二战结束后，随着经济全球化进程的加速，经济安全等非传统安全的重要性开始逐渐上升，但其关注的内容主要是经济层面产业链供应链的安全。然而，随着地缘政治冲突和大国博弈加剧，一些国家开始将经济相互依赖所赋予的权力当作强制其他国家行为的地缘政治工具。特别是在数字技术朝着融合生态体系发展的背景下，人为将数字领域的科技合作、投资贸易往来甚至是相关人文交流安全化，系统性地将遏制措施从某些技术公司扩展至整个产业链，国家之间经济、社会等诸多领域的交往活动均被置于所谓“国家安全”的管控之下，不仅导致全球产业链供应链碎片化，极大降低了全球经济生产效率，而且推高了相关国家维护安全的成本，增加了陷入安全困境的风险。

2023年4月18日，爱沙尼亚首都塔林，北约举行年度“锁盾”网络防御演习，来自38个国家的3000余名安全专家参与演习。

最后是对外关系中平衡安全和发展的考量。长期以来，维护国家安全和发展利益是国家对外关系的一体两面，国际经济合作与安全议题也相对独立。然而，随着国家在数字时代的不安全感日渐上升，安全概念不断泛化，越来越多的对外经济活动被认为与国家安全紧密相关而被采取限制措施。考虑到数字智能化技术的通用性以及军民两用特性，对一国来说，数字领域是采取开放还是限制策略既事关本国相关产业的市场利益和国家经济发展，也关系到本国的国家安全风险是否可控，典型例子如供应链安全和跨境数据流动。近年来，无论是欧美等从最初的对华“脱钩论”转向所谓的“去风险化”，还是美国在“小院高墙”策略的推进过程中希望尽可能缩小范围，划出一条线，聚焦真正的对华“卡脖子”技术，其本质都是谋求在对华发展经贸关系时确保自身发展利益最大化，以保持对华绝对竞争优势为基础维护其核心安全利益。

携手打造网络空间命运共同体

面对数字智能化时代更加复杂和不确定的因素及挑战，国际社会是任由地缘政治对抗和竞争升级还是同舟共济携手应对，是摆在所有国家特别是大国面前的重大问题。如果选择前者，人类社会恐将进入不可控的时代，科技发展带来的将是大规模冲突、对抗和文明倒退。如果选择后者，国际社会将以共享共治为基础，共同应对数字技术带来的安全威胁和挑战，为世界带来和平、繁荣和文明进步。

就当前网络空间国际体系而言，国家间的合作模式大致可以分为三类：依附型合作、大国竞争和充分合作。依附型合作模式以主导国和依附国的不对等合作为特征，主导国可以在很大程度上利用依附国的资源发展数字经济，同时为依附国提供安全保护，但是这种合作

（新华社图片）

2023年7月18日，在位于纽约的联合国总部，中国常驻联合国代表张军（左一）在人工智能与安全问题高级别公开会前和与会代表交谈。

模式容易形成“中心—外围”的数字霸权体系，进而固化并加剧全球数字经济发展的不平等。大国竞争模式常常发生在领先国与崛起国之间，它们在数字空间展开全面的竞争，不过这种模式很容易使彼此陷入“安全竞赛”困境，占用大量经济发展的资源。充分合作模式则以共享共治、互利共赢为特征，更有助于各方在均衡安全的基础上实现共同发展。

从理论上看，中国提出的携手构建网络空间命运共同体的倡议与充分合作模式相互吻合，基于主权平等、和平安全、开放合作的对外战略可以充分发挥技术、数据和安全的公共产品属性，通过协调各国利益和促进各方合作，有助于在全球层面实现数字经济高质量发展与高水平安全的动态平衡。那么在实践中，面对无政府状态的国际社会，特别是数字时代不可控风险持续加大的国家安全环境，应如何推动构建网络空间命运共同体？

第一，国际社会应充分认识到共同安全才是应对数字安全困境的有效路径。回顾互联网诞生以来半个多世纪的发展历程，互联网在创新人类生产生活方式的同时，其面临的安全风险还在持续扩大，由于国家间缺少有效合作，网络空间的安全赤字和治理赤字不断加剧。在强烈的不安全感驱动下，一些国家通过增加自身安全投入并采取攻击性的单边安全举措来追求狭隘的自身安全，但由于网络空间安全风险跨越国界和多领域融合的特点，只会导致更加不安全。数字人工智能时代的到来如同一枚潜在威力巨大的风险“放大器”，在网络空间失序的情况下，很可能给人类带来难以估量的巨大安全风险。联合国秘书长古特雷斯在 2022 年《联合国气候变化框架公约》第二十七次缔约方大会上指出，“我们只有一个选择 ：要么合作，要么灭亡”。现在的网络空间或许也到了这样的时刻。如果说科技的发展并不必然带来人类文明进步，人类历史总是在进步与倒退之间循环，那么能够摆脱倒退转向进步通道的首要条件就是各国都要树立共同安全的观念。

第二，公正合理性是网络空间国际秩序建立的基本要求。公正性主要表现为尊重各国的网络主权，主权平等原则是现代国际关系的基本行为准则，也是构建网络空间命运共同体的前提和基础。由于国际合作的本质是主权让渡，因而网络空间国际秩序只能建立在国家自愿服从的基础之上，否则就不能体现国家间的主权平等。合理性主要表现为国家的权责平衡，权利与责任平衡对

等是一项公认的国际法原则，对当前网络空间国际秩序的构建尤为重要。由于网络空间是一个以技术为基础的人造空间，有些国家凭借先行者的绝对优势掌控了巨大的权力，那么在技术生态日趋融合而数字鸿沟持续扩大的当下，理应承担更大的国际义务。从网络时代到数字人工智能时代，各国在网络空间筑起一道道主权边界的“篱笆”以维护国家安全。正如西方谚语“好篱笆造就好邻居”所言，主权边界就像网络空间的“篱笆”，但只有公正合理的权责分配才称得上“好篱笆”，才是网络空间命运共同体建设得以持续推进的保证。

第三，行动的有效性是推进落实网络空间命运共同体建设的重要考量。大道至简，实干为要。基于共同安全的理念和公正合理的原则，构建网络空间命运共同体的关键在于促成有效的集体行动。迄今为止，联合国打击网络犯罪公约谈判是国际社会在网络安全领域最有成效的协作。尽管美西方认为于 2001 年在匈牙利首都布达佩斯缔结的《网络犯罪公约》已经成为打击网络犯罪的国际规范，但他们愿意重新开展谈判的重要原因是合作的预期收益超越了利益分歧。相比之下，各国在网络战、网络空间负责任行为规范、国际法适用等诸多问题上始终未能达成一致，这一方面是由于各国对网络空间安全的战略认知存在差异，另一方面也是因为网络空间安全威胁的严重程度还不足以让各国放下利益分歧而共同应对。强人工智能时代的到来或将成为网络空间安全发展史上的重要节点。面对人工智能可能带来的安全失控甚至是人类灭绝的风险，国际社会应该同舟共济，以有效的集体行动将网络空间命运共同体理念落到实处。

这是2022年11月7日拍摄的《携手构建网络空间命运共同体》白皮书。

（新华社图片）

本文是国家社科基金重大项目“网络空间国际规则博弈的中国主张与话语权研究”（项目批准号：20&ZD204）的阶段性研究成果

作者系中国社会科学院世界经济与政治研究所研究员

[1] Ian Bremmer, “The AI Power Paradox: Can States Learn to Govern Artificial Intelligence—Before It’s Too Late?” *Foreign Affairs*, August 2023, https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox.

[2] Paul M. Barrett and Justin Hendrix, “Safeguarding AI: Addressing the Risks of Generative Artificial Intelligence,” June 2023, https://bhr.stern.nyu.edu/tech-generativeai#:~:text=By%20Paul%20M.%20Barrett%20and%20Justin%20Hendrix%20VIEW,the%20AI%20harms%20right%20in%20front%20of%20us.

[3] Анатолий Кучерена, “Чем грозит человечеству неуправляемый искусственный интеллект - Российская газета,” April 2023, https://www.rg.ru/2023/04/11/elektronnyj-apokalipsis.html.

[4] The UN, “International Community Must Urgently Confront New Reality of Generative, Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards,” July 2023, https://press.un.org/en/2023/sc15359.doc.htm.

[5] 在该战略中，美国重新定义了美国社会的数字发展愿景，围绕构建“既先天就更容易形成防御能力和网络弹性又契合美国价值观”的新数字生态体系这一战略目标，提出五大支柱以及具体 27 项举措。参见 The White House, “National Cybersecurity Strategy,” March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf。

[6] The White House, “FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy,” March 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[7] “Joint Communication to the Eruopean Parliament, the European Council and the Council on European Economic Security Strategy,” June 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2023:20:FIN.

[8] Federico Steinberg and Emily Benson, “Evaluating Europe’s Economic Strategy,” July 2023, https://www.csis.org/analysis/evaluating-europes-economic-security-strategy.