“网络地缘政治”视野下伊朗与以色列网络空间博弈研究*

钟　灵　孙德刚

摘　　要：在第四次工业革命的背景下，地缘政治博弈已经从传统的陆地、海洋、天空、外太空、极地和深海等物理空间拓展至网络空间，成为国家间地缘政治博弈的“新边疆”，并由此催生出地缘政治博弈的新形态——“网络地缘政治”。网络地缘政治既具有传统地缘政治的基本要素，又具有超越传统地缘政治的新特征，包括网络主权边界的模糊性、军事威慑的低效性、“进攻有利”的偏好性等。网络地缘政治延伸并反作用于传统地缘政治，日益构成了跨越物理和网络界限的地缘政治概念。本文研究表明，伊朗与以色列的网络空间博弈并未完全脱离传统地缘政治博弈的逻辑，双方都将网络空间视为改变攻防态势的重要场域，网络博弈是两国在地理空间领域攻防的延伸。伊朗和以色列的网络军备竞赛加速了中东网络空间的军事化，对中东安全格局产生了深远影响。网络地缘政治与物理地缘政治相互联动，导致中东“次级修昔底德陷阱”，“物理—网络”混合战争愈演愈烈。

关 键 词：网络地缘政治；网络空间博弈；伊朗与以色列关系；“次级修昔底德陷阱”

作者简介：钟灵，复旦大学国际关系与公共事务学院2024级博士研究生（上海 200433）；孙德刚，博士，复旦大学中东研究中心、国际问题研究院研究员（上海 200433）。

文章编号：1673-5161（2025）03-0103-31
中图分类号：D815
文献标识码：A

* 本文系2023年度国家社科基金重点项目“大国在中东博弈的新动向与中国中东战略研究”（23AGJ011）的阶段性成果。感谢《阿拉伯世界研究》匿名评审专家提出的宝贵修改建议，文责自负。

伊朗和以色列作为中东地区的战略竞争对手,存在结构性矛盾。自 1979 年伊朗伊斯兰革命以来,因意识形态矛盾尖锐和安全利益难以兼容,伊以双方长期处于敌对状态。伊朗和以色列通过代理人战争乃至直接攻击对方本土,开展激烈的地缘政治博弈,以维护本国利益与安全。近年来,这一针锋相对的势头逐步从物理空间向网络空间蔓延。2010 年,以色列和美国联合使用“震网”(Stuxnet)蠕虫病毒攻击伊朗的核基础设施并使其瘫痪,导致 1,000 台离心机受损,严重延缓了伊朗的核计划进程,暴露了伊朗网络安全防护能力的脆弱性。伊朗随即启动本国网络能力建设,加强与以色列在网络空间的攻防互动。2020 年 4 月下旬,伊朗对以色列的供水和污水处理基础设施发动网络攻击,其间控制了运行水泵系统的密码,致以方蒙受重大损失。同年 5 月,以色列随即予以回击,对伊朗的沙希德·拉贾伊(Shahid Rajaei)港口实施网络攻击行动,致使港口的航运和货物装卸业务中断。从伊以你来我往的网络攻击事态来看,双方似乎将网络空间视为同物理空间博弈平行的战场,在网络空间进行博弈较量。网络战被双方视为是物理地缘博弈的延伸。如何理解网络空间与物理空间的关系?伊以双方的网络空间博弈与物理地缘博弈是平行关系,还是被包含的关系?双方互动的基本逻辑是什么?在网络空间日益重要的新时期,伊以网络空间博弈对理解中东安全的发展有何启示意义?本文尝试回答上述问题。

长期以来,地缘政治是国际政治领域的重要研究议题。地缘政治的本质是政治行为体通过对地理空间的控制和利用来获得权力、追求利益和实现安全,并借助地理环境展开相互竞争与协调的过程及其形成的空间关系。① 随着时代的发展,地缘政治学先后衍生出海权论、陆权轮、空权论和天权论等理论流派。如今,技术的进步和迭代推动了互联网的快速发展,互联网在短时间内实现了与人类社会全面且深入的融合,推动了一个不同于传统客观实在的新质态的网络空间的诞生,并逐步向智能物理空间演进发展。② 随着网络与现实同构社会的到来,基于互联网形成的网络空间已经成为与海、陆、空、天并行的“第五空间”。③

① 陆俊元:《地缘政治的本质与规律》,北京:时事出版社 2005 年版,第 86 页。

② Zhang Hang, Liu Bo and Wu Hongyu, “Smart Grid Cyber-Physical Attack and Defense: A Review,” *IEEE*, January 28, 2021, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9352761, 上网时间:2024 年 10 月 9 日。

③ 美国国防部最早提出网络空间是“第五空间”的概念。

尽管有人认为网络空间是“全球公域”,无法应用于地缘政治的概念,但“斯诺登事件”的发生、世界主要国家网络安全战略的相继出台、国家间开展网络攻防以及各国试图掌握网络空间规则制定权等一系列行为,无不揭示着网络空间的地缘属性,地缘政治概念正在被应用于网络空间的研究当中。本文首先阐释网络地缘政治概念的起源和内涵,再梳理网络地缘政治与传统地缘政治之间的关系逻辑,在此基础上分析伊朗与以色列网络空间博弈的行为模式、利益考量和对中东安全的潜在影响。

一、“网络地缘政治”概念的缘起

“网络地缘政治”概念的提出源于经典地缘政治理论对现实的解释不足。经典地缘政治理论认为,地缘政治学是一门研究国家如何利用其地理空间要素以维护国家权力、利益和安全的学问。① 随着科学技术水平的不断提高,人们所能触及的空间范围逐步扩大,对地理要素的理解也呈现出阶段性和日益多样化的特点。然而,这些变化总体上并未脱离物理空间的框架,也没有脱离地理要素具有明显主权边界的理论基点。网络空间的出现及其发展则对传统地缘政治的理解提出挑战。一方面,网络空间的虚拟性和无界性模糊了国家边界,淡化了主权概念,这使得网络空间作为一种空间概念难以适用于地缘政治的视角。另一方面,网络空间虽然本质上是虚拟存在,但它与物理空间产生日益密切的联系,呈现日渐融合的趋势,仅看到网络空间的虚拟性质是片面的。网络空间在经历了由技术社群主导的“乌托邦”与资本主导的“创世纪”后,累加了巨大的风险和脆弱性,造就了可能“失控的世界”,于是呼吁主权国家的强势“回归”②。伴随全球网络空间治理从“非国家化”向“再国家化”演进,各国围绕网络空间权力展开博弈,这种空间—权力的关系亟需从理论中找到解释。

总体而言,网络空间仍然具有较强的地缘属性,这首先源于网络空间构成架

① 参见陆俊元:《地缘政治的本质与规律》,第 86 页;Iabal Ramadhan, “The Implication of Cyberspace Towards State Geopolitics,” *Journal Ilmu Politik*, Vol. 3, No. 2, 2021, pp. 161-184。

② 封帅:《数字空间的政治秩序建构:数字权力、主体累加与多位面互动进程》,载《国际观察》2024 年第 2 期,第 80-84 页。

构的国家化及其内在的地理属性。网络空间的定义繁多,但从其构成来看,网络空间是物理和虚拟物品或财产的结合。① 网络空间由四个层级组成,分别是物理层、逻辑层、信息层和人类活动层暨社交层。② 其中,物理层是支撑网络空间运行的硬件设备和基础设施,包括海底和陆地光缆、路由器、光纤等物理设备;逻辑层指软件、协议和代码;信息层包括数据和信息的储存、传输和处理;社交层则指人与人之间的互动和社交网络。域名、根服务器和信息等资源是由国际社会共享,具有非排他性和非竞争性的特征,赋予了网络空间一定的"公域"性质。但是,网络空间基础设施需要依托物理空间铺设,并受相应国家的维护和管理,归属国家的主权范围;信息层的数据生成、接收和储存等行为也需要遵守国家的法律规范;而人类活动层中网络信息、内容的生产者及其消费者具有特定的国籍,其行为活动更是受到其所属国家的司法管辖。因此,网络空间仍然无法脱离主权国家而存在,其本质是全球公域和国内私域的混合场域③,体现出明显的主权和地缘属性。

网络空间的地缘属性还源于主权国家对其工具化和武器化以服务自身地缘战略目标的实践。④ 当前,人类社会对信息和通信技术(Information and Communications Technology, ICT)基础设施的日益依赖带来了显著的互联互通性,在技术便利日常生活的同时,这种依赖使得国家安全暴露在巨大的网络和技术漏洞当中,网络攻击作为网络技术演变的延伸品基于"利用逻辑",给民众的经

① Martin C. Libicki, "Cyberdeterrence and Cyberwar," *RAND*, October 21, 2009, p. 6, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf, 上网时间:2025 年 1 月 8 日。

② Marjory S. Blumenthal and David D. Clark, "The Future of the Internet and Cyberpower," in Franklin D. Kramer, Larry K. Wentz and Stuart H. Starr, eds., *Cyberpower and National Security*, Washington, D.C.: National Defense University Press, 2009, pp. 206-240.

③ 张晓君:《网络空间国际治理的困境与出路——基于全球混合场域治理机制之构建》,载《法学评论》2015 年第 4 期,第 53 页。

④ 参见 Mostafa Esmaeili, Amir Abbas Rokni, Seyed Reza Hosseini, "Cyber Geopolitics at the Crossroads of Power: An Analysis of US Cyber Hegemony in Confrontation with China," *Foreign Relations Quarterly*, Vol. 15, No. 4, Issue 60, Winter 2024, pp. 267-296; 蔡翠红:《网络地缘政治:中美关系分析的新视角》,载《国际政治研究》2018 年第 1 期,第 9-37 页。

济安全和国家的设施安全带来严重的安全风险。① 在此背景下,国家主权凭借对暴力手段的垄断权以及对国家资源的分配权,不仅以“维护安全”的名义强势介入网络空间,而且利用国家机器从事网络攻击,意图威胁和削弱地缘对手的安全。②

此外,国家对网络空间的依赖导致各国存在程度不一的脆弱性和敏感性,这使得网络空间本身就成为权力的重要源泉。处于网络空间关键节点处的国家利用自身能力、技术等先发优势,武器化他国对自身的依赖,服务自身战略利益。例如,伊拉克战争期间,在美国政府授意下,伊拉克顶级域名“.iq”的申请和解析工作被中止,导致所有以“.iq”为后缀的网站从互联网上被移除,直接影响了伊拉克网站的可及性和民众的网络访问。③ 网络强国的先发优势还具有累积效应,通过垄断技术、掌握网络空间的规则制定权,网络强国得以维持其对网络空间的主导权,并对他国网络空间产生巨大影响。鉴于网络空间对国家权力竞争的重要性,当前世界各国围绕网络资源、网络规则主导权的争夺已然展开,网络空间的地缘政治张力日益凸显。④

基于网络空间内在的和实践中日益凸显的地缘属性,学界提出了“网络地缘政治”这一概念,认为网络地缘政治是继海权论、陆权轮、空权论和天权论之后的一套新的地缘政治理论体系。网络地缘政治强调网络空间作为一个独立的空间

---

① 参见 Aisha Adeyeri and Hossein Abroshan, “Geopolitical Ramifications of Cybersecurity Threats: State Response and International Cooperations in the Digital Warfare Era,” *Information*, Vol. 15, No. 682, 2024, https://doi.org/10.3390/info15110682, 上网时间:2025 年 4 月 3 日。

② 封帅:《数字空间的政治秩序建构:数字权力、主体累加与多位面互动进程》,第 84 页。

③ 《从网络大国走向网络强国》,中央网络安全和信息化委员会办公室,2014 年 6 月 24 日,https://www.cac.gov.cn/2014-06/24/c_1111279634.htm?from=groupmessage,上网时间:2025 年 3 月 30 日。

④ 参见 James Wood Forsyth Jr., “What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace,” *Strategic Studies Quarterly*, Vol. 7, No. 1, 2013, pp. 93-113; Garrett Potts, “Cyber Leadership in the Era of the Great Power Competition,” in Adib Farhadi, Ronald P. Sanders and Anthony Masys, eds., *The Great Power Competition*, *Volume 3*, *Cyberspace: The Fifth Domain*, Cham: Springer, 2022, pp. 3-26; 江天骄:《中美网络空间博弈与战略稳定》,载《信息安全与通信保密》2020 年第 9 期,第 11-17 页;沈逸:《中美战略博弈下的网络安全与网络空间治理新秩序》,载《信息安全与通信保密》2019 年第 8 期,第 16-17 页;鲁传颖:《网络空间治理的力量博弈、理念演变与中国战略》,载《国际展望》2016 年第 1 期,第 117-134 页。

体系而成为地缘政治博弈的新场域,网络空间的互动具有灵活性、快速性、非对称性和普及性等特点,其理论核心是在讨论网络空间技术与国家地缘政治权力的关系。在网络地缘政治博弈的诸要素当中,除空间和技术本身外,还包括网民数量、数字经济规模、网络军事力量等要素。相较于传统的地缘政治中国家着力提高利用物理空间海陆空水等要素的能力,网络地缘政治则强调国家利用网络空间的能力,包括利用网络技术优势、建立网络规范、参与网络治理等。网络地缘政治的基本逻辑是通过占据网络空间技术制高点,掌握主动权以服务国家自身发展和利益,即抢占“制网权”。

二、“网络地缘政治”与传统地缘政治的关系

本文将传统地缘政治界定为依托海、陆、空、天等物理空间的地理资源进行地缘博弈的理论学说和实践。在第四次工业革命的背景下,网络空间作为人为构造的虚拟空间,从根本上改变了传统地缘政治思维对地理要素的理解,开辟了国家间权力博弈的全新边疆,并对战争与冲突的形态产生了深远影响,是对传统地缘政治理论的突破。与此同时,随着网络空间与物理空间趋于同构的社会形态的出现,网络空间又日益对以自然地理空间为依托的传统博弈思维和局面产生深刻影响。从这个意义上讲,网络地缘政治与传统地缘政治既有区别,又有联系,本部分将着重讨论两者之间的关系,揭示网络地缘政治的复杂性及其对传统地缘博弈格局的影响,进而为分析伊朗与以色列在网络空间的互动提供分析框架。

(一) 网络地缘政治是传统地缘政治的反映

网络空间被视为数字世界对物理空间的映射,在技术基础上增加行为体、行动以及制度和规范等人类在物理空间中的活动范式,物理空间中的政治、经济、社会、文化、军事、科技等活动都被映射到网络空间当中。[①] 就这个意义而言,网络地缘政治可被理解为国家传统地缘博弈在网络空间的映射,国家在现实空间与他国的博弈状态势必也要通过网络空间表现出来。

网络空间本身是传统地缘政治发展的衍生物,丰富了传统地缘政治的手段,

① 周宏仁:《网络空间的崛起与战略稳定》,载《国际展望》2019 年第 3 期,第 23 页。

可以作为权力工具服务于传统地缘政治目标,[①]构成国家传统地缘政治博弈战略的一部分。互联网的最初起点“阿帕网”(ARPANET)的产生便源于美国冷战期间为加强军事连接,取得对苏联博弈优势的需要。尽管网络空间至今历经巨大发展,但网络技术与现实空间的日益融合非但没有改变其服务于传统地缘政治的工具属性,反而因为网络空间具有的经济、军事和安全潜能,成为传统博弈中日益倚仗的地缘博弈工具。以信息网络技术为支柱的网络能力已经成为国家实力的重要组成部分,诸如5G、人工智能、半导体等前沿高科技产业已经成为国家经济竞争力的主要来源,大国在上述领域展开了激烈竞争。同时,各国积极推动网络技术在军事领域的应用,通过为武器赋能,帮助国家在现实战场中取得先发优势,网络空间对地缘博弈的作用日益突出。正如任职于美国空军部队的研究人员罗伯特·李(Robert M. Lee)指出,网络力量对现代战争的作用与以前空中力量同样具有革命性意义。[②]

如前所述,网络空间的产生最初源于冷战时期大国间传统地缘博弈的需要,因此网络地缘政治天生地与传统地缘政治共享诸如主要行为体、国家实力、权力与安全等基本概念框架。尽管技术社群、私营部门和个体在网络空间获得前所未有的话语权和影响力,但主权国家在当前仍然是网络空间最重要的行为体。国家在其中遵从相似的行为逻辑,即国家利益决定国家行为与互动。国家不断推动自身的网络技术发展,加强网络基础设施建设,完善法规和政策框架,旨在提升其利用网络空间的能力、抢占网络空间技术制高点和把握网络空间规范规则制定权,获得和增强国家的网络空间权力,为自身的经济发展、国家安全、政治稳定和意识形态安全等目的服务。

此外,网络地缘政治关系很大程度上可以反映传统地缘政治的权力结构和动态。传统地缘政治中的敌友关系、博弈手段等在很大程度上同态映射在网络空间当中。当前,美、中、俄、欧构成网络空间的四支主要力量,这与现实地缘的权力分布相吻合。其中,美欧等发达国家与中俄等新兴大国在参与网络空间全球治理中形成相互竞争的两大主张,前者支持多利益攸关方的治理模式,并倾向

① 蔡翠红:《网络地缘政治:中美关系分析的新视角》,第16页。

② Robert M. Lee, “The Interim Years of Cyberspace,” *Air & Space Power Journal*, Vol. 27, No. 1, January-February 2013, p. 58.

于保留由自身主导的既有网络空间治理机制,后者则坚持应在联合国框架内推动建立具有包容性和代表性的治理机制。2022 年美国拜登政府发布美国国家安全战略,将中国界定为最大的地缘政治挑战。2023 年 6 月欧盟峰会通过涉华决策的决议,重申对华政策的多面性并坚持“伙伴、竞争者和制度性对手”的“三重定位”,双方在传统地缘博弈中采取脱钩、构建地区盟友体系,以期抑制中国的发展。这一策略也延伸至网络空间领域,美国同样将中国视为网络空间的竞争对手,并强调要在网络安全议题上加强与盟友和伙伴的政策协调,建立一个广泛的网络联盟,以“人权”为旗号共同维护既有的有利网络规范,①以应对中国在数字领域的崛起。

(二) 网络地缘政治是对传统地缘政治的突破

网络空间自互联网诞生时起就被认为是一个全新的、独立的空间,引发了空间概念内涵和外延的巨大变化。网络空间自身的独特运作逻辑使得其突破传统地缘政治博弈的基本假设,与传统地缘政治博弈的特点相区分,并推动地缘政治理论的重新思考。

网络空间地缘博弈超越了传统的主权边界,拓宽了国家博弈的疆域。传统地缘政治以国家的领土为基本单位,各国的行动通常受到明确的地理和边界约束。然而网络空间的虚拟性和瞬时性,使得行为体行动不受物理边界约束,可以在全球范围内行动和互动。尽管国际社会承认国家具有网络主权,联合国信息与安全政府专家组(Group of Governmental Experts, GCE)多次在其发布的报告和文件中强调“尊重各国在网络空间的主权”②,但围绕如何明晰国家的网络空间主权边界的争论不止。传统国家主权的权力边界、职责功能及工具偏好都出现明显变化,传统地缘博弈中的主权概念受到冲击。相比较而言,主权对外的活动范围被拓宽,甚至可以说技术所及之处都可以成为国家活动的范围。主权作为传统地缘博弈的理论基点,其内涵的改变意味着网络空间博弈的内容、形式和逻辑都将有所创新。

网络地缘政治主权基点的变化推动了与传统地缘政治博弈逻辑截然不同的

① 凌胜利:《霸权护持与拜登政府的议题联盟》,载《和平与发展》2024 年第 2 期,第 29 页。

② Hao Yeli, “A Three-Perspective Theory of Cyber Sovereignty,” *The Fifth Domain*, Vol. 7, No. 2, 2017, pp. 108-115.

新型博弈模式的出现。首先,地理位置和资源的重要性被大大削弱。在传统地缘博弈中,国家通常将领土内的地理和资源优势转化为经济和军事实力,从而在博弈中取得对他国的相对优势。然而,在网络空间中,由于网络技术的普及和网络设施的可及性,行为体可以超越距离和资源的限制,仅凭借网络信号、网线等设施即可精准地实施重大网络攻击,威胁他国网络和现实基础设施安全,并在全球范围内投射影响力。地理优势和国家实力的泛对称关系得到扭转,将导致国家能力和实力的重新分配。

其次,传统地缘博弈强调防御性逻辑,核心目标是保护国家安全和主权,通过修建防线和强化防御能力抵御外部威胁,并依靠武器性能与数量的可量化与可比较性实现对外部的有效威慑。但网络空间的进攻容易、防守困难、归因困难等特点,使得以进攻为主的博弈逻辑逐渐形成。网络武器的延迟性、一次性和可复制性等特点,使得其性能难以预测和量化,进而影响网络威慑的有效性。

网络空间博弈的创新和突破之处还在于新的政治博弈目标即获取“制网权”。当前对制网权仍存在多种理解①,但总体而言可视为是一国在网络空间施加控制和影响力的能力,其核心是一国依托技术在网络空间维护自身安全,并确保国家利益实现的能力。其主要可视作以下几方面的合力:一是网络空间基础设施。国家在网络基础设施中占据主导地位,通过控制关键基础设施对全球网络运行施加控制力。二是网络军事能力建设。国家通过加强网络军事能力的建设,确保在发生网络冲突时拥有先发制人的战术主动权,同时降低自身脆弱性、提高网络韧性和复原力。三是技术领导力和规范制定权。在技术革命的背景下,国家增强自身的网络技术竞争力,进而掌握网络技术标准的制定权、话语权和主动权,使得相关的网络制度和规范能尽可能地反映本国的立场和观念,从而在全球网络治理中占据有利位置。

(三) 网络地缘政治对传统地缘政治具有反作用

网络地缘政治对于传统地缘政治的反作用并非指网络博弈服务于传统地缘

① 参见 Daniel T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in Franklin D. Kramer, Larry K. Wentz and Stuart H. Starr, eds., *Cyberpower and National Security*, pp. 24-42; 张耀:《网络空间安全视阈下的制网权释义》,载《经济与社会发展》2018 年第 2 期,第 39-44 页。

政治的目的,而指的是网络地缘博弈具有相对独立性,行为体在其中的互动会对物理空间的政治博弈产生意料之外的作用和影响。

首先,网络空间中影响传导的全球化特征,使得国家在网络空间中更容易产生特殊的共同利益,并产生诸多要求合作的公共性议题,这对国家在传统地缘政治中的分歧起到弥合或稳定作用。以网络犯罪议题为例,自互联网诞生以来,依托网络进行诈骗、勒索和赌博等犯罪活动屡禁不止,给世界各国造成巨大经济损失。在未来几年,全球网络犯罪的成本将以每年 15%的速度增长,预计到 2025 年网络犯罪将给世界造成 10.5 万亿美元的损失。① 网络犯罪来源具有多样性、匿名性和跨域性,单个国家难以对犯罪行为体实施有效威慑,因此国际合作就成为实现本国安全的一种手段。② 在地缘政治竞争加剧、联合国团结面临撕裂,传统国际组织效力面临质疑的情况下,各国依然在联合国框架下推进打击网络犯罪的议题合作,共同商议起草了《联合国打击网络犯罪公约》。③ 该公约草案在 2024 年 8 月 8 日得以顺利通过,显示出大国地缘竞争下的合作方面。

其次,网络空间的独特性质促使国家的网络地缘利益与传统地缘利益相比既有继承也有不同,国家在网络空间的利益分歧也对传统地缘中的合作关系起到分化作用。在当前网络空间治理机制的主要力量较量中,欧美与中俄因网络空间能力、权力大小、网络文化等差异④客观上形成了相对立的“多(利益攸关)方主义”和“多边主义”两种主张,但是仍无法断定就此形成了两大阵营的格局。当前美欧内部围绕信息主权、隐私权的分歧依然剧烈,以市场开放为基础和以行业自律为准则的“美国模式”与以事前预防为基础和以强制性规范为准则的“欧盟模式”之间长期存在分歧与矛盾。2016 年欧盟颁布《通用数据保护条例》

① Steve Morgan, “Cybercrime to Cost the World $10.5 Trillion Annually by 2025,” *Cybercrime Magazine*, February 21, 2018, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, 上网时间:2024 年 7 月 19 日。

② 刘宁、郎平:《不同议题下的中美网络安全关系:合作、竞争与冲突》,载《战略决策研究》2017 年第 2 期,第 3-19 页。

③ 《联合国打击网络犯罪公约》全称是《打击为犯罪目的使用信息和通信技术行为的全面国际公约》(*A Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*)。

④ 鲁传颖:《试析当前网络空间全球治理困境》,载《现代国际关系》2013 年第 11 期,第 48-54 页。

(*GDPR*),早在决议草案审议时,美国前驻欧盟大使就曾表示,该法案将有损跨大西洋间的数据流动及贸易。①

最后,国家网络地缘政治博弈的不同模式对传统地缘政治的稳定性具有两重作用。一方面,当前国家间在网络空间中(in cyberspace)开展的一系列地缘活动,如网络间谍、攻击网络防火墙、入侵系统等网络行动,部分地替代了传统军事冲突。由于其烈度较低、且损失往往可逆,国家在利用网络行动传达国家意志、实现国家利益的同时,能较为有效地进行冲突管理。特别是在多方形成默契即将网络攻击的烈度控制在现实武装攻击的门槛之内时②,其对现实空间的地缘博弈会起到一定的稳定作用。但另一方面,通过网络空间(through cyberspace)发起的、针对一国物理空间,旨在瘫痪或破坏关键基础设施建设的攻击,则可能直接导致冲突在现实空间的跨域升级,破坏传统地缘政治的稳定状态,对现实秩序形成冲击。2012 年时任俄军总参谋长马卡罗夫(Nikolai Makarov)曾表示,针对一国实施的网络攻击可被视为开战,既可以采取对等的网络攻击,又可以使用传统的军事手段予以反击。③ 而网络空间的全球化特性和多领域融合的特点,使得一国的行动可以迅速扩散到其他国家和领域,促使原本局限于特定国家和区域间的冲突扩散到全球,带来不可预测的连锁反应和风险。研究指出,网络空间的不安全性使得核战略稳定具有脆弱性;危机上升的不确定性加剧了核战略平衡被破坏的风险。④

在当前国际和地区大国的地缘博弈实践中,网络地缘政治与传统地缘政治的边界呈现出加速融合的趋势,逐步构建起一个跨越物理和虚拟界限的复合地

① 方芳、刘宏松:《政策环境、外部冲击与欧盟个人数据保护政策形成》,载《世界经济与政治》2023 年第 5 期,第 135 页。

② Carly E. Beckerman, “Is There a Cyber Security Dilemma?,” *Journal of Cybersecurity*, Vol. 8, Issue. 1, 2022, pp. 1-14.

③ Elizabeth Gibney, “Where Is Russia’s Cyberwar? Researchers Decipher Its Strategy,” *Nature*, March 17, 2022, https://www. nature. com/articles/d41586-022-00753-9, 上网时间:2024 年 10 月 2 日。

④ 门洪华、丁迪:《脆弱制衡还是韧性共存——网络空间战略稳定模式探索》,载《社会科学》2023 年第 6 期,第 107-121 页;刘杨钺、张旭:《网络空间武器化的发展态势以及对战略稳定的影响》,载《信息安全与通信保密》2019 年第 9 期,第 107-121 页;Pavel A. Karasev, “Cyber Factors of Strategic Stability: How the Advance of AI Can Change the Global Balance of Power,” *Russia in Global Affairs*, Vol. 18, No. 3, 2020, pp. 24-52。

缘政治形态。

网络空间与地球和太空的地理特征共同影响世界政治、经济、军事和社会。[①] 权力作为一种控制力，既强调对海、陆、空、天等自然地理要素和资源的控制，也强调对网络空间信息流、数据流等要素的控制。物理空间中的地理要素能够帮助塑造有利的网络空间“地形”，如通过掌控关键的数字基础设施获得网络空间的阻断性权力；而网络技术的发展也促使物理空间的诸多领域围绕数字通信技术重组，网络能力嵌套进物理空间，从而优化和重塑物理地形。总体而言，“网络地缘政治”形态意味着物理空间与虚拟空间的深度互嵌，是硬件设施与技术要素的结合，其核心在于通过硬件设施、技术要素及规则体系的综合博弈，重构全球地缘秩序。未来，地缘竞争的核心不仅限于领土与国界，而是如何实现多领域、多维度的有效协调，以应对国际竞争和参与国际合作（见表 1）。国家参与地缘竞争势必需要具备更加全面、系统的思维，将自然禀赋、经济发展、军事能力、信息技术和全球治理等方面纳入战略思维和部署框架。

表 1　传统地缘政治与网络地缘政治的异同点

	传统地缘政治	网络地缘政治
竞争场域	物理空间	虚拟空间+物理空间
战略目标	保卫国家领土、扩大势力范围、维护国家利益、维护全球影响力	综合运用地理资源和技术要素，控制信息流、获得技术主权、打击敌对网络基础设施、维护国内基础设施安全
竞争要素	领土、地理资源、地理位置（地理影响政治）	海、陆、空、天、太空地理资源要素；信息流、数据流等数字资源（技术影响政治）
主权边界	清晰	模糊，没有国家宣称放弃网络主权
追求权力	是	是
零和博弈	是	是
互动逻辑	防御为主、对称逻辑、防御有利论	攻防二元性、非对称逻辑、进攻有利论
威慑类型	对等原则、报复性战略威慑	拒止威慑、纠缠威慑、跨域威慑
威慑效力	强	弱

资料来源：作者自制。

① Gazmend Huskaj, “Digital Geopolitics: A Review of the Current State,” *International Conference on Cyber Warfare and Security*, Vol. 18, No. 1, 2023, p. 153.

需要强调的是,部分国家因为资源禀赋、经济发展水平、技术能力和安全关切不同,未能充分挖掘和发挥网络空间的潜力。在此背景下,“网络地缘政治”尚未发展为一种普遍形态。当前,数字技术发达的国家将首先构建网络地缘思维,旨在最大化其技术优势带来的战略收益;而数字技术落后的国家短期内仍然会以传统的地缘博弈思维为主。但随着这些国家面临的网络安全和数字技术威胁日益加剧以及第四次工业革命推动技术的不断扩散,这一形态未来有望实现在更广泛国际范围内的扩展。

三、伊朗与以色列的网络空间博弈及其内在地缘政治逻辑

从地缘上看,尽管以色列受到阿拉伯国家包围,伊朗处于阿拉伯国家的边缘地带,但第三次中东战争结束后,伴随着阿拉伯世界在中东地区影响力的整体下降,伊朗和以色列这两个非阿拉伯国家逐步崛起,并在地区事务中发挥日益重要的作用。1979 年伊朗伊斯兰革命以来,伊以关系转瞬直下陷入敌对状态,围绕伊核问题、军事对抗和地缘政治影响力等议题展开斗争。2010 年以色列与美国共同研发了“震网”病毒用于针对伊朗的网络攻击,破坏了伊朗纳坦兹(Natanz)核材料浓缩设施的工业控制系统,由此拉开了以伊在网络空间博弈的序幕,形成了物理空间和虚拟空间并行的双轨斗争。多年来,两国的互动推动了地区敌友阵营的分化和重组,深刻塑造了中东地区的地缘格局。随着两国的互动延伸至网络空间场域,厘清双方网络空间博弈的逻辑对理解中东地缘政治有重要意义。基于网络政治博弈和传统地缘博弈的关系,可以对双方互动的态势和逻辑做出以下解读。

(一) 传统地缘政治利益构建伊以网络空间安全思维

伊朗和以色列在传统现实博弈中的核心利益、战略思维和原则指导着双方网络空间安全思维的形成。网络安全思维虽然不属于国家网络互动的范畴,但却指导着国家在互动中的策略和行动选择,研究国家的网络安全思维有助于理解国家在网络空间的行动逻辑。总体而言,伊以的网络安全思维未脱离两国在传统地缘博弈中的利益诉求,是双方物理空间博弈状态的反映。

以色列建国后历经了五场中东战争,并逐步确立了安全至上、武力至上、自

助至上的基本国家安全原则。[①] 以色列认为在群敌围绕、战略纵深缺失和人力资源有限的安全环境中应当持续强化自身军事实力和装备性能,对周边国家形成军事威慑,并谋求与大国(主要是美国)结盟,以实现生存和绝对安全的目标。[②] 在该原则的指导下,以色列的网络空间思维和行动始终围绕解决“维护生存安全”“提高技术优势”“威慑潜在攻击者”“与大国展开合作”等几项核心问题展开。

以色列是世界上推动网络空间军事化进程最早也是最快的国家之一,以此确立对邻国的网络军事优势。网络空间军事化表现为出台明确网络威胁的网络安全战略、制定网络空间的军事学说和政策,以及建立执行网络攻防任务的军事或准军事机构。[③] 2009 年以色列国防军就提出网络空间是战略性和可操作的作战地带。2010 年以色列发布《2010 国家网络倡议》,明确表示以色列应当在五年内成为全球前五的网络强国。2017 年以色列发布《以色列国防军战略》,明确将网络空间视为一个军事领域,要求以色列在战略、战役和战术层面发展防御和进攻能力;[④]同年,以色列发布首份《以色列国家网络安全战略》,强调以色列的国家网络防御体系由市场韧性、操作响应和国家防御三个独立层级构成,其目标是推动军民合作,以网络科学与工业生态系统为基础,确保以色列在网络领域始终保持技术和操作上的优势,从而应对面临源自对手的日益复杂

① 吴昊昙:《安全、武力与自助:以色列的国家安全研究》,载《国际政治研究》2022 年第 3 期,第 72 页。

② Dan Meridor and Ron Eldadi, “Israel’s National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine, Ten Years Later,” *Memorandum*, No. 187, February 2019, p. 22.

③ 参见杨楠:《网络空间军事化及其国际政治影响》,载《外交评论》2020 年第 3 期,第 69 页;Opeoluwa Adisa Oluyemi, “Militarization of Cyberspace and Its Implications on National/International Security,” *International Journal of Social Science Research and Review*, p. 3; Miguel Alberto N. Gomez, “Arming Cyberspace: The Militarization of a Virtual Domain,” *Global Security and Intelligence Studies*, Vol. 1, No. 2, Spring 2016, p. 48。

④ 桂畅旎:《以色列国家网络安全防御体系建设及启示》,载《中国信息安全》2022 年第 7 期,第 103 页。

的网络威胁。① 以色列也积极建立与域外网络强国的合作关系。2016 年,以色列与美国签署《网络防御合作协定》,组建“美国—以色列网络安全行动小组”,促进两国在网络空间技术交流、情报共享领域的合作。与此同时,以色列还与日本、北约等建立合作联系以增强自身的网络能力,显示出传统地缘政治利益、思维与策略的延续。

伊朗具有独特的战略文化。在帝国辉煌大业的大国心态、源于屈辱历史的受害者心态②等多重政治心理长期影响下,伊朗形成了层层递进的国际战略观念。③ 受独特的战略文化和面临的地缘现实影响,伊朗逐步确立了自身核心利益,即确保政权的生存、抵御外部大国(尤指美国)的压力。伊朗的战略具有鲜明的防守性,同时试图通过加强网络空间的应用,扩大其在地区事务中的影响力。伊朗在 2010 年受到美国和以色列联合发起的“震网”攻击后才开始迅速发展和提升自身网络攻击和防御能力。2012 年 3 月,伊朗最高领袖哈梅内伊宣布成立最高网络空间委员会(Supreme Council of Cyberspace, SCC),下设国家网络空间中心(National Cyberspace Center, NCC),主要职责包括保护国家免受网络攻击,显示出鲜明的“防守性”战略色彩。伊朗在网络空间中也常以进攻的姿态来实现战略上的防御目标,这与其传统地缘博弈的策略相符合。2012 年 8 月,伊朗利用“沙蒙”(Shamoon)病毒发起对沙特阿美公司的网络攻击,作为对“震网”攻击的回应。④ 2020 年,伊朗伊斯兰革命卫队圣城军指挥官卡西姆·苏莱曼尼(Qassem Soleimani)遭美国无人机的定点暗杀,面对美国无视自身主权的侵略性行径,伊

① State of Israel Prime Minister's Office National Cyber Directorate, *Israel National Cyber Security Strategy in Brief*, September 2017, p. 5, https://en-cyber. tau. ac. il/sites/cyberstudies-english. tau. ac. il/files/media _ server/cyber% 20center/cyber-center/Israel% 20Cyber% 20Security% 20Strategy%20-%20Brief%20-%20English%20-%20Book%20-%20Final%20-%202017. pdf, 上网时间:2025 年 2 月 18 日。

② 金良祥:《评估伊朗对于美国极限施压的反制》,载《现代国际关系》2019 年第 11 期,第 24 页。

③ 田文林:《伊朗对外行为的战略文化分析》,载《阿拉伯世界研究》2016 年第 4 期,第 76-86 页。

④ Risk and Resilience Team, *Hotspot Analysis: Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions*, ETH Zürich: Center for Security Studies (CSS), May 2019, p. 13, https://css. ethz. ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev. pdf, 上网时间:2024 年 11 月 26 日。

朗随后通过发射弹道导弹与开展网络侦查活动加以反击报复,[①]试图以此彰显保卫国家利益的意志和决心。2022 年 2 月,以色列空袭伊朗境内无人机基地后,以色列遭受了迄今为止规模最大的一次网络攻击,多个政府网络陷入瘫痪,这被广泛认为是伊朗发起的行动。

同时,伊朗也将网络空间视为展示自身实力、扩大影响力、塑造抵抗西方列强形象的重要途径。伊朗多年来加强对拉丁美洲和撒哈拉以南非洲非穆斯林国家的反帝国主义网络外交,提高自身作为反帝国主义力量的声誉。[②] 2023 年 10 月 7 日,新一轮巴以冲突爆发后,伊朗加大了针对以色列和美国的网络行动力度,并在社交媒体上冒充以色列民众发起批评以色列总理的舆论攻势[③],以巩固自身的反美反以形象和伊斯兰世界领导力。上述行为体现了伊朗战略文化与地缘政治动机的结合,揭示了其地缘战略在网络空间的连贯性。通过此类战略部署,伊朗得以维护其地区安全环境,并在全球舞台上展示其网络能力和战略意图。

(二) 网络行动是伊以改变双方传统博弈中被动状态的重要依托

在以色列与伊朗长期的地缘政治博弈中,双方在战略缓冲空间、传统军事和经济力量呈现出不同程度的不对称性,这驱使双方各自寻求传统领域以外的方式和手段,弥补自身劣势并争取战略主动。网络空间以其无界性、成本收益的不对称性等特质,成为伊以双方改变被动状态的重要依托。

对以色列而言,网络空间弥补了以色列战略纵深缺失的短板。以色列领土面积狭小,建国后一直处于周边阿拉伯国家的包围当中,有限的战略缓冲空间使以色列长期缺乏安全感,因此始终将发展先进的预警能力以弥补战略纵深缺失

① "The Iranian Cyber Threat," *United Against Nuclear Iran*, June 2024, https://www.unitedagainstnuclearіran.com/sites/default/files/UPDATE% 20-% 20The% 20Iranian% 20Cyber% 20Threat.pdf, 上网时间:2024 年 11 月 28 日。

② Pierre Pahlavi, "Iran's Cyber Influence Strategy Poses Formidable Challenges for the West," *The National Interest*, March 9, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/iran%E2%80%99s-cyber-influence-strategy-poses, 上网时间:2024 年 12 月 1 日。

③ "Report: Iran Cyberattacks Against Israel Surge After Gaza War," *VOA*, October 15, 2024, https://www.voanews.com/a/report-iran-cyberattacks-against-israel-surge-after-gaza-war/7823577.html, 上网时间:2024 年 10 月 17 日。

作为发展重点。从这一角度来说,网络空间的无界性与以色列的战略需求高度契合。[①] 网络空间突破了传统地理疆域的限制,拓展了以色列的行动空间,有效消除了国土面积和国家实力之间的泛对称性。通过利用其网络技术优势,以色列不仅能够克服疆域和资源的限制,还具备了实施远程打击的能力。同时,网络空间也使以色列能够更有效地监控和防范来自境内外的威胁,并在战时状态下迅速收集情报、分析数据并做出应对。这种快速反应能力为以色列提供了更多的战略灵活性,增强了其应对突发事件的能力。

自 1948 年建国至 20 世纪 70 年代初,以色列为改变缺少战略纵深和缓存空间的劣势而注重发展军事能力,并依靠其核武器形成对伊朗等地区国家的威慑。但随着伊朗核计划的持续推进,以色列领导人普遍认为,伊朗获得核武器似乎只是一个时间问题,一旦伊朗实现核武装,地区均势就会被打破。特别是以色列缺少可以在现实斗争中对伊朗形成干扰的地区代理人,而一个可能拥有核武器、在地区中拥有众多代理人的伊朗,将会使其在传统地缘政治博弈中陷入极其被动的状态。届时,伊朗的代理人将更加肆无忌惮地向以色列发射火箭,或实施其他“恐怖行动”。[②] 为此,以色列高度重视利用其在网络空间的技术优势,尝试通过发起网络攻击延缓伊朗的核计划,争取战略主动。2010 年,在以色列和美国的主导下,“震网”病毒攻击并成功瘫痪了伊朗的核设施,据称这一行动使得伊朗核计划要推迟十余年。2022 年 6 月,时任以色列总理塔利·贝内特(Naftali Bennett)在接受英国《经济学人》杂志采访时表示,“我们不再对付触角,对付伊朗的代理人,我们已经通过网络攻击直击要害,创造了新的博弈方式”[③],显示出网络空间对于以色列的战略意义。

与此同时,以色列也加强了对伊朗及胡塞武装、真主党等代理人的网络间谍活动,通过发动网络攻击以挫败敌对方在现实中针对以色列的攻击企图。例如,

① 桂畅旎:《以色列国家网络安全防御体系建设及启示》,载《中国信息安全》2022 年第 7 期,第 101 页。

② 汪舒明:《大屠杀记忆、以色列战略文化与伊朗核危机》,载《外交评论(外交学院学报)》2013 年第 2 期,第 137 页。

③ “Israel's Prime Minister Explains His New Approach to Iran,” *The Economist*, June 8, 2022, https://www.economist.com/middle-east-and-africa/2022/06/08/israels-prime-minister-explains-his-new-approach-to-iran, 上网时间:2024 年 10 月 17 日。

以色列多次依托网络间谍所提供的情报优势,使其在复杂的加沙地道系统和黎巴嫩的山地地形中精准定位目标,通过精确制导空袭予以打击。①

伊朗在与以色列的传统博弈中的被动状态源于其与以色列的物理层面的军事、经济和科技实力差距,这一差距因为美以之间的特殊盟友关系以及美国对伊的制裁日渐扩大。伊朗国防和地区政策的核心之一是非对称打击②,伊朗领导层认为要能够与以色列匹敌、与之抗衡并制止它,伊朗就必须在一个更加平等的领域与之较量,而网络空间攻防的成本收益不对称性使之成为伊朗与以色列博弈的理想场域。

从行为体的进攻能力而言,发动网络攻击的低门槛性以及部分技术的可及性,使得伊朗即使面临广泛的武器禁运和经济制裁,依然能够获得网络作战能力。战略与国际研究中心(Center for Strategic and International Studies)的研究发现,当前伊朗用以发动网络攻击的网络武器大多是在黑市购入的经过修改的恶意软件,这些武器并不具备更先进的网络武器的破坏力③。此外,在网络空间推动技术迭代和提升武器性能所需要的时间及成本,远低于在物理空间提升动能武器(kinetic weapons)性能的时间和成本,且效率更高,伊朗在网络空间追赶以色列的技术水平相对容易实现。伊朗推进网络安全治理能力建设和网络空间军事化起步相较于以色列更晚,但仍在短时间内实现了技术的突破增长。当前伊朗已经成为第二梯队网络强国之首,并成为少数几个不仅有能力开展情报收集,还有能力实施具有破坏性的网络攻击的国家之一。④ 从这一意义上看,伊朗在网络空间与物理空间相比处于一个更加平等的位置。

从地缘政治对手防御成本的角度来看,网络防守的成本远高于发动网络攻击的成本,网络攻击可以做到“一击即溃”,而网络防御必须确保万无一失,因此

① Lior Tabansky, “Offensive Cyber Operations as a Tool of War,” *The Jerusalem Strategic Tribune*, January 2024, https://jstribune.com/tabansky-offensive-cyber-operations-as-a-tool-of-war/, 上网时间:2024 年 12 月 4 日。

② 吴冰冰:《伊朗为什么能顶住美国的极限施压?》,载《文化纵横》2022 年第 1 期,第 8 页。

③ James Andrew Lewis, “Iran and Cyber Power,” *Center for Strategic & International Studies*, June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power, 上网时间:2025 年 2 月 2 日。

④ “Part 2: Iran's Cyber Strategy, Institutions, and Capabilities,” in Chuck Freilich, ed., *The Iranian Cyber Threat: The Institutions and Praxis of Iran's Cyber Strategy*, Tel Aviv: The Institute for National Security Studies, January 2024, p. 26.

面临巨大压力。① 尽管伊朗在网络技术和经济上与以色列及其盟友美国存在一定差距,但以色列在面对伊朗的针对性攻击时仍然处于高风险状态,这迫使以色列投入额外资源以加强其网络防护,这种情况在以色列对数字空间的依赖日益深入的背景下尤其如此。② 根据伊朗发动网络攻击的历程,当前伊朗已经具备攻击以色列民用和关键基础设施的能力。2020 年 4 月,伊朗成功对以色列的几处水处理设施发起网络攻击,其间控制了运行水泵系统的密码,试图提高自来水的氯含量。以色列国家网络局局长乌纳(Yigal Unna)认为,“这是首次旨在对现实生活造成损害而不是对信息技术或数据造成损害的攻击行为……倘若未能及时发现,将造成灾难性后果”,③并坦言需要投入更多资源以加强本国网络防御能力。以色列国家网络防御局首席执行官加比·波特诺伊(Gabi Portnoy)也表示,伊朗的袭击不一定是复杂的,但确实有效,以色列需要做好更充分的准备,才能阻止伊朗的袭击。④ 可见,伊朗仍然凭借其现有的网络能力对以色列进行打击并造成对方损失,一定程度上策应其在物理空间与以色列的地缘博弈,显示出网络空间和物理空间的日益融合。

(三) 网络空间频繁接触代替现实热战,形成现实地缘的消极脆弱稳定

本文将地缘稳定定义为两国之间不会发生战争的一种状态。⑤ 消极脆弱指的是稳定建立在相互威慑、相互制衡而非合作、共治等正向共同利益的基础上;同时也意味着尽管双方不存在全面战争,但具有滑向全面战争的风险,稳

① John B. Sheldon, “Deciphering Cyberpower: Strategic Purpose in Peace and War,” *Strategic Studies Quarterly*, Vol. 5, No. 2, 2011, p. 98,转引自江天骄:《全球网络空间的脆弱稳定状态及其成因》,载《世界经济与政治》2022 年第 2 期,第 134 页。

② David Siman-Tov and Shmuel Even, “A New Level in the Cyber War between Israel and Iran,” *The Institute for National Security Studies*, June 3, 2020, https://www.inss.org.il/publication/iran-israel-cyber-war/, 上网时间:2024 年 12 月 16 日。

③ “‘Cyber Winter Is Coming,’ Warns Israel Cyber Chief After Attack on Water Systems,” *The Times of Israel*, May 28, 2020, https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/, 上网时间:2024 年 11 月 3 日。

④ Matan Wasserman, “The Cyber War Against Israel Has Escalated: How Much Is It Costing Us?,” *The Jerusalem Post*, June 27, 2024, https://www.jpost.com/brandblend/article-807889, 上网时间:2024 年 11 月 3 日。

⑤ [美]托马斯·芬加、樊吉社:《中美关系中的战略稳定问题》,载《外交评论》2014 年第 1 期,第 44 页。

定缺乏制度保障。伊朗和以色列长期处于敌对状态,但两国在现实战场中总体上保持“斗而不破”、激烈但有节制的状态。迄今为止,伊以矛盾尚未爆发到全面战争的程度,无论是以色列和伊朗,抑或美国与俄罗斯等域外大国,各方都不愿意冒全面开战的风险。虽然双方在传统地缘博弈中形成了脆弱的稳定状态,但却在网络空间中热战,企图通过网络空间的频繁接触来代替现实中的全面战争。

具体来看,网络空间的持续交手对传统地缘形成消极脆弱稳定的作用主要有两方面。

第一,网络攻防双方均将网络空间视为与传统地缘空间平行的战场,试图通过持续交手,构建一个既独立于现实环境、又能在保持对抗烈度可控的前提下长期运作的战略空间。网络攻击引发的损害相对有限且潜在可逆,攻击方通常能对行动的后果、影响范围具有较为清楚的预估。此外,网络攻击通常不会直接导致人员和物理设施的毁灭性伤害,可以减少目标对象国和国际社会的舆论压力。另一方面,网络攻击的时机和规模常常难以追溯,使得被攻击方在政治话语上具有操作空间以服务政治利益的需要。被攻击方既可以将本国的网络脆弱性和安全事故解读为对方网络攻击的结果,也可以在面对国内舆论压力的情况下,适当模糊来源,控制局势。正是基于网络攻击这两项优势,伊以将网络攻击视为是博弈的重要工具和手段,能够在不引发全面战争的情况下,仍通过网络手段进行敌对行为。

2020 年 4 月,以色列公开报道本国水设施受到袭击,但并未正式公开指责,避免了直接指责伊朗。① 同年 5 月,伊朗的港口受到以色列的网络攻击,导致货物运输中断数日,最初伊朗声称是技术故障导致,但随后承认是网络攻击所致。伊以对于对方的网络行动在话语和叙述上保持一定的灵活性,这一策略有助于避免事态升级,维护现实的地缘稳定。2023 年 10 月新一轮巴以冲突爆发以来,冲突外溢导致伊朗和以色列之间罕见地出现直接的回合式打击,但双方都表现出克制,并未将局势升级为全面战争。同时,双方在网络空间则展开热战,以色

① Gil Baram, “How the Cyberwar Between Iran and Israel Has Intensified,” *The Washington Post*, July 25, 2022, https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/, 上网时间:2024 年 8 月 18 日。

列国家网络局(Israel National Cyber Directorate, INCD)2023 年年度报告显示以色列受到的网络攻击较上一年增加了 43%,其中 68%的攻击与加沙冲突同时发生,并强调伊朗和黎巴嫩在这其中的作用。① 2024 年 10 月 12 日,伊朗报告其司法、立法和行政部门都遭受了严重的网络攻击,大量信息泄露。此外,伊朗核设施和燃料配送网络、市政网络等基础设施也成为了网络攻击的目标,②这一轮攻击发生时正值以色列宣称要报复伊朗对其的导弹袭击。以色列前副国家安全顾问查尔斯·弗雷利希(Charles Freilich)表示:“伊朗和以色列似乎都认为网络攻击升级的风险低于动能攻击,双方得以在发动网络攻击的同时预期对方的反应较小。”③

第二,网络攻防双方企图通过持续的交互产生威慑作用。威慑通常通过影响对手对其行为与收益的计算,进而改变其决策心态,以达到阻止其采取某种行动的目的。成功的威慑具备几个前提条件:一是威慑方应当具有实力,并具有使用实力让对手付出代价的意志。二是对手必须要知道自己应该避免什么行为,并对自身行动的成本具有清晰认识。伊以网络攻防经历表明,伊以都尝试通过发动网络攻击以展示自身的进攻意图和网络实力,传递军事和政治信号,从而阻止对方在网络中和现实中的行动。

以色列在网络空间积极奉行累积威慑理念,该理念被视为是“惩罚性”与“拒止性”的统一,依重视程度可分为“重惩罚”(deterrence by punishment)、“重拒止”(denial deterrence)和“惩拒并进”(deterrence by punishment and denial)三种形态。④ 2010 年,以色列和美国凭借“震网”病毒瘫痪了伊朗核设施;2021 年

① *Annual Summary 2023: In the Midst of the “Iron Words” War*, Israel National Cyber Directorate, p. 8, https://www.gov.il/BlobFolder/news/booklet_yearly_summary_2023/en/booklet_yearly_summary_2023_eng.pdf, 上网时间:2025 年 3 月 31 日。

② “Iran Hit By ‘Heavy Cyberattacks’ Targeting Its Nuclear Facilities Amid Middle East Tensions,” *News 18*, October 12, 2024, https://www.news18.com/world/iran-hit-by-heavy-cyberattacks-targeting-its-nuclear-facilities-amid-middle-east-tensions-9083699.html, 上网时间:2024 年 10 月 14 日。

③ Rishi Lyengar, “The Next Israel-Iran Fight Could Be in Cyberspace,” *Foreign Policy*, April 16, 2024, https://foreignpolicy.com/2024/04/16/iran-israel-conflict-missile-attack-cyberattacks-warfare/, 上网时间:2024 年 10 月 14 日。

④ 陈曦、葛腾飞:《以色列安全战略中的累积威慑析论》,载《西亚非洲》2024 年第 1 期,第 102 页。

4 月,恢复履行伊核问题协议进入关键节点,伊朗纳坦核设施的电力系统遭到网络攻击,导致一部分离心机损坏。伊朗随即指责以色列是此次攻击的实施方,[①]而以色列并未对此予以否认。通过这次网络攻击,以色列有针对性地向伊朗传递了其在关键节点直接干预伊朗核计划的能力与决心,从而释放出明确的威慑信号。除利用网络空间对伊朗的现实行动形成威慑,以色列还通过跨域威慑(cross-domain deterrence)阻止伊朗及其地区代理人对以色列网络空间发起攻击。2021 年 5 月,以色列对哈马斯的军事情报网络设施空中打击,以报复后者发起的网络攻击[②],展示出将类似目标置于危险之中的能力。以色列期望以此产生警示效应,表明如果伊朗及其代理人持续开展此类网络行动,以色列将以高昂的报复作为回应。相对应的,2020 年 4 月,伊朗针对以色列水设施的网络攻击被广泛认为其意在向以色列传达不允许以在网络战线上挑战伊朗。[③] 以色列和伊朗多年来还通过不断完善自身网络防御,提高网络攻击的门槛来实现劝阻目的。

(四) 伊以网络空间博弈影响和改变地区地缘博弈重点和格局

伊以之间的网络空间地缘博弈日益加剧,对两者的地缘政治博弈重点、博弈力量格局等起到了反向塑造的作用。这主要表现为制网权竞争推动了两国网络空间军事力量建设,引发军备竞赛,加剧地区安全困境。

---

① 陈瑶:《伊朗与以色列网络空间冲突的演进、动因及影响》,载《西亚非洲》2024 年第 3 期,第 132 页。

② Erica D. Borghard and Jacquelyn Schneider, "Israel Responded to a Hamas Cyberattack with an Airstrike," *The Washington Post*, May 9, 2019, https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/, 上网时间:2025 年 1 月 5 日。

③ Gil Baram, "How the Cyberwar Between Iran and Israel Has Intensified," *The Washington Post*, July 25, 2022, https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/,上网时间:2025 年 4 月 1 日;《以色列和伊朗在隐蔽的网络空间公开开战》(波斯语),2020 年 6 月 13 日, *irdiplomacy*, http://irdiplomacy.ir/fa/news/1992183/جنگ-آشکار-اسرائیل-و-ایران-در-فضای-پنهان-سایبری, 上网时间:2025 年 4 月 1 日;"Iran Cyberattack on Israel's Water Supply Could Have Sickened Hundreds — Report," *The Times of Israel*, June 1, 2020, https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/,上网时间:2025 年 4 月 1 日。

网络威慑的概念在学理上借鉴了核威慑的理论框架。[①] 然而,与传统的核威慑相比,网络空间威慑的建立十分困难。核威慑建立的基础在于两方面:其一,多方对核武器能对生存构成绝对性威胁的风险存在共识;其二,拥核国家普遍具有一次打击和二次打击的能力,即一方优先使用核武器后,另一方能够实施有效报复,从而形成核战争无赢家的博弈局面。但在网络空间中,网络攻击杀伤力有限,加之攻击难以溯源,极大削弱了一国通过威慑劝阻对手使用网络武器的能力。[②] 正因如此,尽管伊以都尝试划定红线以限制对方的攻击行为,但现有互动表明,双方都未能确立足够可信的威慑。相反,两国陷入了相互报复的恶性循环,推动了双方攻防能力的持续演进。双方都在加强自身网络军备建设,并希望通过升级自己的网络攻击强度来改变对方的行为,追求绝对安全,由此形成了网络空间军备竞赛。

2010 年,内塔尼亚胡政府推出的国家网络倡议确立了以色列成为网络强国的目标。多年来,在纲领性文件的指导下,以色列不断加大投资,发展先进的网络空间技术,研发了包括“震网”“杜库”(Duqu)等具有巨大破坏力的病毒攻击软件,并将其付诸针对伊朗的实战当中。以色列还推动了融合大数据、人工智能等先进技术的“网络铁穹”系统的研发,以防范潜在的网络安全威胁。伊朗也不甘示弱,在受到“震网”冲击后,2012 年伊朗成立最高网络空间委员会,负责制定国家网络政策,初始预算为 4,000 万美元。鲁哈尼担任总统后,伊朗的网络安全支出急剧增长,三年内增长了 1,200%以上。[③] 大量资金除用于信息通信技术研发外,还大量投入至网络专业人才的培养以及民间黑客组织的支持,赞助了包括马布纳研究所、“伊朗网军”、APT33、“复制小猫”(CopyKittens)、“石油钻井平台”(OilRig)、“剁肉刀行动”(Operation Cleaver)、“污水”(Muddy Water)等在内的一系列网络行动代理人。在这一过程中,伊朗从最初的运用钓鱼软件发动网络攻击,逐渐发展到可以实施网络间谍活动、网络假消息宣传、分布式拒绝服务攻

① 参见 Joseph S. Nye Jr., “Deterrence and Discussion in Cyberspace,” *International Security*, Vol. 41, No. 3, 2017, pp. 44-71。

② 鲁传颖:《重新理解战略稳定:构建网络——核稳定机制》,载《同济大学学报(社会科学版)》2023 年第 4 期,第 54 页。

③ Veronika Netolická and Miroslav Mareš, “Arms Race ‘in Cyberspace’ — A Case Study of Iran and Israel,” *Comparative Strategy*, Vol. 37, Iss. 5, 2018, p. 419.

击和入侵关键基础设施网络的水平。[①] 2020 年初,以色列宣称其网络防御体系保护以境内关键基础设施免遭攻击。但仅数月后,当年 4 月以色列水设施就受到了源自伊朗的攻击。深受冲击的以色列宣称“网络寒冬已经来临”[②],随即于 2021 年宣布一项建立网络安全总部的计划,旨在协调各方,强化自身网络能力以应对伊朗的网络攻击。

军备竞赛往往与现有安全困境相互加强。尽管伊朗和以色列之间存在明确的敌意,双方不满足安全困境的成立条件,但中东地区作为一个高度关联的安全复合体,地区国家间的主要安全关切彼此交织,各国安全无法置身于其他国家的安全考虑之外。因此,伊朗与以色列的网络军备竞赛具有显著的传导效应,不仅引起地区国家的普遍警惕,也直接刺激了其他行为体效仿其网络安全与军备建设的步伐,地区各国网络空间安全化和军事化的历程由此开启。2017 年沙特成立国家网络安全局(National Cybersecurity Authority),旨在为沙特实现有效的网络治理、管理网络风险和加强网络攻防能力提供框架;[③]2018 年阿联酋发布首份国家网络安全战略,强调预防潜在的网络攻击、建立网络安全隐患的响应和恢复体系,以及培养网络相关人才的重要性;[④]阿曼于 2020 年建立了综合电子防御中心;巴林、卡塔尔于 2021 年分别建立了国家网络安全中心。

伊朗和以色列在网络战中所展现出来的进攻性和技术优势,强化了海湾国家的“伊朗威胁认知”,推动了阿拉伯国家与以色列关系的改善,这构成阿拉伯国家与以色列的和解的重要动因。事实上,过去十年,海湾国家与以色列已经在网络空间悄然开展合作,2007 年阿联酋就与以色列人马蒂·科查维(Mati Kochavi)的“4D 安全解决方案”(4D Security Solutions)公司接洽,希望后者帮助升级其能源设施的防御系统,并在阿布扎比建立名为“猎鹰之眼”(Falcon Eye)的全市智能监控系统;2012 年沙特阿美公司在受到大规模网络袭击后便向以色列寻求网络

① 龚汉卿、张运雄、郝志超:《伊朗网络战能力研究》,载《信息安全与通信保密》2021 年第 4 期,第 37 页。

② “‘Cyber Winter Is Coming,’ Warns Israel Cyber Chief After Attack on Water Systems”.

③ 《沙特国家网络安全战略》(阿拉伯文),沙特国家网络安全局,https://nca.gov.sa/ar/national-cybersecurity-strategy/,上网时间:2025 年 1 月 5 日。

④ “National Cybersecurity Straategy,” *Telecommunications Regulatory Authority*, https://tdra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf, 上网时间:2025 年 1 月 5 日。

安全援助,以修复攻击造成的伤害;2017 年以色列公司还与沙特公共投资基金(Public Investment Fund)进行秘密谈判,讨论以何种方式参与“未来新城”(NEOM)的开发。①

阿以关系持续改善的高峰是 2020 年《亚伯拉罕协议》的签署。阿联酋、巴林、摩洛哥和苏丹与以色列实现关系正常化,并形成以《亚伯拉罕协议》为基础的合作框架,网络安全其中的重要合作议题。② 2021 年,摩洛哥成为《亚伯拉罕协议》缔结国中第一个与以色列签署双边网络防御协议的国家;2022 年,摩洛哥、以色列、阿联酋和巴林的网络安全负责人出席在巴林举行的首届跨地区网络峰会,共同讨论如何应对源自“共同敌人”的威胁。③ 这一合作的隐含意义在于,通过依托以色列在网络能力和技术领域的领先地位,为相关国家提供保障,以保护其关键基础设施免受伊朗的潜在威胁。④

可见,伊朗和以色列当前的地缘博弈已经由传统的以军事实力竞争意图抢占地理空间优势为主,转向以网络技术与军事竞争并重,呈现出“物理+虚拟”结合下的地缘政治形态。在新的地缘博弈态势下,伊朗和以色列都将提升信息技术和科技水平视作新的战略制高点,不仅通过增强自身的网络攻击和防御能力获取优势,还在以网络技术赋能关键基础设施控制、舆论信息传播和情报信息收集等方面,构建起一个多维度、跨领域和立体的竞争体系。

---

① Nima Khorrami, “One Year On: Israel’s Cybersecurity Cooperation with the GCC States,” *Insights*, No. 266, 2021, p. 4, https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf, 上网时间:2023 年 2 月 13 日。

② “Insight 266: One Year On — Israel’s Cybersecurity Cooperation with the GCC States,” *Middle East Institute*, September 14, 2021, https://mei.nus.edu.sg/publication/insight-266-one-year-on-israels-cybersecurity-cooperation-with-the-gcc-states/, 上网时间:2025 年 3 月 31 日;“S. 1777 — Abraham Accords Cybersecurity Cooperation Act of 2023,” *Library of Congress*, https://www.congress.gov/bill/118th-congress/senate-bill/1777/text, 上网时间:2025 年 3 月 31 日。

③ “The First Regional Cyber Summit: Israel, Morocco, Bahrain, and the United Arab Emirates Gather in a First of Its Kind Meeting,” *Israel National Cyber Directorate*, December 14, 2022, https://www.gov.il/en/pages/meeting_union, 上网时间:2023 年 2 月 13 日。

④ Ahmed El-Masry, “The Abraham Accords and Their Cyber Implications: How Iran Is Unifying the Region’s Cyberspace,” *Middle East Institute*, June 9, 2021, https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace, 上网时间:2024 年 4 月 17 日。

四、伊以网络空间博弈的影响与启示

对伊朗和以色列在网络空间的互动逻辑分析,既有助于理解伊以行为的本质,也有助于以小见大,理解中东地区安全现状和发展趋势,把握中东安全治理的现实需求。总体而言,伊以的网络空间博弈对于理解当前中东安全治理的启示主要有如下几点。

(一) 地缘思维向网络空间延伸加深信任赤字,增加地区不稳定

伊朗与以色列在网络空间的互动显示出地缘思维向网络空间的延伸和扩展,在网络地缘政治的背景下,网络空间的新特性进一步加深了既有的信任赤字。网络威胁的泛在性和扩散性使得国家间形成前所未有的深度相互依存,单一国家无法孤立自保,必须在更广泛的共同利益基础上寻求合作,这要求更新传统的治理思维和认知理论。然而,由于既有的思维定式和深层次的信任赤字,中东国家仍倾向于依据传统的地缘政治视角来解释网络行为,突出表现为海湾阿拉伯国家基于对伊朗威胁的恐惧和疑虑加强与以色列的网络合作。

尽管 2023 年沙伊达成和解,促使阿拉伯世界与伊朗实现关系缓和,但由于网络互动的匿名性和意图的不明确性以及主体的复杂性,以伊朗、以色列、沙特为代表的地区大国在本国出现网络空间事故时,仍然会受到认知相符[①]的影响,优先将其解读为来自地缘博弈对手的网络攻击。同时,由于网络攻击难以溯源和核查,国家间的认识和归因难以证实或证伪,易形成错误认知并激发敌意,破坏国家间正在建立的信任,因此本文认为网络空间博弈会为本轮地区缓和添加不确定性和不稳定性。但伴随沙特和伊朗推进两国高层互访、加强军事交流和合作,两国希望减少误判可能性,这有助于巩固和解进程。

(二) 巴以冲突凸显混合战争新趋势,强化国家对威胁不可预测性的担忧

混合战争指的是国家或非国家行为体结合常规与非常规战术、军事与非军

① 认知相符指人们在理解和认识客观世界时会保持自己原有认识的趋向,当接收新信息时,总是下意识地使新获得的信息与自己原有的认识保持一致,而回避、抵制与原有认识不一致的信息。参见[美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,秦亚青译,上海:上海人民出版社 2015 年版,第 127-147 页。

事手段以及秘密或公开行动的战争形式。尽管各国政府和公众已经认知到网络空间作为一种战术和战略资源的广泛应用,但将传统的动能战(kinetic warfare)与网络战(cyber warfare)深度整合的实例在现代战争史上仍相对罕见。在新一轮巴以冲突中,以色列和哈马斯以及双方的支持者借助网络空间实现各自的战略目标,旨在发挥网络行动的协同效应。2023 年 10 月 27 日,以色列中断加沙地区的电信服务持续 34 小时,导致“救护车都无法到达伤者身边”①,冲突期间以色列的黑客组织对巴勒斯坦国家银行和电信公司的目标发动攻击。与此同时,来自沙特阿拉伯、巴基斯坦、土耳其、也门等伊斯兰国家的黑客组织也联合发起了代号为“反以色列”(OpIsrael)的系列网络行动,对以色列国家电力局、《耶路撒冷邮报》、以色列国家档案馆等目标发起网络攻击,并散布虚假警报意图引起以色列民众恐慌。② 上述行为使地区各国对潜在“动能+网络”混合战争的到来形成更为具象的认识,激发地区国家发展自身网络能力的紧迫性。

更重要的是,2024 年 9 月 17 日和 18 日,在以色列远程控制下,黎巴嫩先后发生了大规模传呼机爆炸,造成大量人员伤亡,这意味着通讯设备“武器化”成为以色列在现代高科技作战背景下采取的一种新型作战方式,也意味着现代战争无处不在,安全风险已经嵌入到生活的方方面面。③ 以色列的行动模糊了战场与日常生活场域的边界,促使各国对智能手机、电子产品和其他高科技产品被用作武器产生疑虑。这也强化了地区政府和民众在现代性社会中的“组织化不确定性”,陷入本体和物理不安全的状态之中。

(三) 域外与域内地缘竞争联动,引发“次级修昔底德陷阱”疑虑,阻碍地区

① Leer en Espanol, “34 Hours of Fear: The Blackout That Cut Gaza off from the World,” *The New York Times*, October 29, 2023, https://www.nytimes.com/2023/10/29/world/middleeast/gaza-blackout-internet-israel.html?auth=login-google1tap&login=google1tap, 上网时间:2024 年 5 月 16 日。

② Lauren Menzie, “The Role of Cyber Operations in Middle East Conflict,” *Teneo*, October 21, 2024, https://www.teneo.com/insights/articles/the-role-of-cyber-operations-in-middle-east-conflict/, 上网时间:2024 年 11 月 1 日。

③ 孙德刚、钟灵:《黎以冲突将引发多重危机》(阿拉伯文),约旦新闻报纸网,2024 年 10 月 1 日,https://jornews.com/post/99830https://jornews.com/post/99830, 上网时间:2024 年 10 月 3 日。

网络治理机制建设

“修昔底德陷阱”指的是一个新兴崛起的大国挑战现存霸权国时,因权力转移带来的不确定性,容易引发崛起国和守成国之间的战争。本文将“次级修昔底德陷阱”界定为大国间权力竞争在地区性冲突中的投射,这将导致域内国家间的竞争更加剧烈。伊朗和以色列在地区中的地缘冲突及地缘思维在网络空间的延续,本质上是受到生存安全和意识形态对立驱动。然而,随着美国在世界范围内推广“修昔底德陷阱”叙事,并主动将大国战略竞争推向中东,在地区推行对立和冲突性话语,这将促使伊朗和以色列的网络和现实对抗中形成“次级修昔底德陷阱”,进一步导致地区地缘政治呈现复杂化和碎片化趋势,最终阻碍地区网络治理的合作,加剧地区安全赤字。

有学者将伊朗、以色列和沙特在地区的对抗解读为是地区“修昔底德陷阱”①,但无论是从相对实力差距还是斗争意图来看,伊朗和以色列的地缘博弈仍然与该理论具有本质区别。修昔底德陷阱理论通常聚焦于崛起国与守成国之间相对实力差距的缩小,以及由此引发的权力转移过程中产生的结构性矛盾。从两国实力上看,以色列在网络技术、情报能力和军事能力等方面始终对伊朗保持着绝对优势。尽管伊朗不断增强自身的网络攻击和军事实力,但更多是在追赶而非挑战和威胁以色列。从意图上看,伊朗和以色列长期以来在网络空间的地缘对抗的根本动力都聚焦生存安全和意识形态的对立,反以是伊朗伊斯兰革命和政权的重要合法性之一,而以色列也将伊朗的敌意及其实践视作是对国家安全和生存的重大威胁。在此背景下,伊朗积极提升能力并借助代理人策略以削弱以色列的战略空间,以色列也通过军事、经济手段等遏制伊朗,这一态势延伸并反映在网络空间中,双方推动网络空间军事化,并竞相以“遏制”与“反制”的模式缠斗。

然而,伊朗和以色列的地缘博弈性质因大国战略竞争加剧而进一步复杂化。当前,以色列在网络空间与美欧密切协作;伊朗由于受到西方制裁和孤立,技术

① 参见 Betty Bassett, “The Thucydides Trap in the Middle East: Saudi Arabia’s Geopolitical Dilemma,” *Medium*, November 19, 2023, https://medium.com/@bettybassett63/the-thucydides-trap-in-the-middle-east-saudi-arabias-geopolitical-dilemma-by-betty-bassett-45b9a9be0992, 上网时间:2024 年 10 月 3 日。

和经济发展受到限制,也主动加强了与中俄的网络空间技术合作,意图实现技术自主和自强。然而,美国致力于在全球范围内推广以大国战略竞争为核心的叙事,因此将这一叙事与其对伊朗的遏制政策相结合,从阵营对抗的角度解释中俄伊的网络合作,认为中俄伊结成所谓的“威权阵营”挑战美欧以的“民主阵营”①,将伊朗和以色列的地缘冲突纳入大国博弈框架。由此,原本局部性的地区安全对抗被赋予了大国竞争的象征性意涵,促使双方陷入“次级修昔底德陷阱”。双方的地缘博弈既受到各自的生存考虑驱动,又受大国战略博弈的影响,因而具有了域内国家对抗和大国战略竞争的双重性质,这将使得伊朗和以色列之间的网络能力竞争和网络空间对抗更加难以调和。

“次级修昔底德陷阱”还集中表现为美国将以色列作为地区战略支点,利用地区阿拉伯国家对伊朗的安全焦虑,实现化敌为友,搭建起以伊朗为防范对象的网络安全合作框架,并试图以此与中国开展制度竞争,分化和削弱阿拉伯国家与中国构建地区网络安全治理机制的效力。近年来,中东国家加紧安全合作“向东看”,以应对美国从地区战略收缩带来的不确定性。中国也积极回应地区国家诉求,2021 年与阿盟共同签署《中阿数据合作安全协议》,2022 年正式启动中伊《25 年全面合作计划》,将网络安全合作列为重点领域。同时,中俄推动上合组织向中东扩员,并将网络安全合作列为重要合作方向,这些行动旨在与各方加强数据安全合作,共同应对网络威胁,实现区域的共同安全和合作治理。

这本可以作为开启建立地区网络治理机制的开端,但美国将大国战略放在首要位置,认为其中东战略就是联合以色列、阿拉伯国家和土耳其等,遏制中国—俄罗斯—伊朗所谓“修正主义战略三角”②。美国首先采取“胡萝卜加大棒”

① 参见 Simon Handler, “The 5×5 — The State of Cybersecurity in the Middle East,” *Atlantic Council*, June 15, 2021, https://www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-in-the-middle-east/; David Klepper, “Cyber Criminals are Increasingly Helping Russia and China Target the US and Allies, Microsoft Says,” *AP News*, October 15, 2024, https://apnews.com/article/microsoft-russia-china-iran-israel-cyberespionage-cyber-d3a22dd2dcea32615ac15ed4fb951541, 上网时间:2024 年 12 月 30 日。

② 孙德刚、杨影淇:《论当前美国中东政策中的折衷主义》,载《国际观察》2024 年第 4 期,第 72 页。

政策,施压或拉拢地区国家疏远与中国的技术和安全合作,如美国以对英伟达 H100 等关键器件实行出口管制为理由,胁迫阿联酋数字巨头 G42 停止与中国的技术协作,导致后者于 2024 年年初中断与华合作。同年 9 月,美国与阿联酋领导人发表联合声明,重申将加强网络安全合作,维持地区稳定。① 美国还以帮助沙特发展核能以换取沙特放弃与华的高科技合作。随后,美国借助以色列的技术优势,打造技术多边合作与中国开展制度竞争,以此作为由中国倡导的地区网络合作机制的替代品。2020 年以来美国促成了阿联酋等阿拉伯国家与以色列的和解,并将网络合作作为《亚伯拉罕协议》的重要内容;除此之外,2022 年美国联合以色列、印度、阿联酋打造“中东四方机制”(I2U2),声称成员国之间保持着稳固的情报共享和网络安全合作关系。②

可以预见,美以倡导的机制门槛相对较高,而地区国家间的技术水平参差不齐,上述制度对成员的容纳性有限,将导致地区国家在网络空间治理议题上的碎片化趋势。更重要的是,美国的制度供给存在明显的对抗色彩,其内在意涵是通过对合作伙伴的争夺,形成一个排除中俄伊等国家、旨在为自身私人目标服务的合作联盟。美国期望以此维持美国对互联网的掌控,维护和扩展自身的地缘利益。毫无疑问,这将导致制度互斥,其影响是带来规则的混乱和分化,强化制度的权力面孔而非治理这一公共服务职能,使得国际秩序远离以伙伴合作为基础的“规则世界”,倒退回以大国强权为基础的“丛林世界”③,严重阻碍地区网络空间治理机制的建设,加剧地区安全赤字。

五、结语

从“网络地缘政治”的视角出发,结合网络地缘政治与传统地缘政治的关

① “U. S. — UAE Joint Leaders' Statement Dynamic Strategic Partners,” *The White House*, September 23, 2024, https://www. whitehouse. gov/briefing-room/statements-releases/2024/09/23/u-s-uae-joint-leaders-statement-dynamic-strategic-partners/, 上网时间:2024 年 10 月 3 日。

② John Clabrese, “The US and the I2U2: Cross — Bracing Partnerships Across the Indo-Pacific,” *Middle East Institute*, September 27, 2022, https://www. mei. edu/publications/us-and-i2u2-cross-bracing-partnerships-across-indo-pacific, 上网时间:2024 年 10 月 3 日。

③ 李巍:《制度之战:战略竞争时代的中美关系》,北京:社会科学文献出版社 2017 年版,第 190 页。

系,本文在回顾学界提出“网络地缘政治”概念的缘由、脉络和内涵的基础上认为,网络地缘政治是传统地缘政治在网络空间的延伸和反映,但同时网络地缘政治又部分超越了传统地缘政治的逻辑,形成自己的互动逻辑和博弈范式。网络空间的特性使得网络空间可以对传统地缘政治起到重要的反作用,对传统地缘中的伙伴或竞争关系起到分化或弥合的作用,并造成潜在的不稳定性。

基于这一分析框架,本文通过分析伊朗和以色列的网络互动,发现双方的传统地缘政治利益构建了各自的网络安全思维,双方都将网络空间视为是改变自身在传统地缘博弈中被动状态的重要工具,并试图通过网络空间的频繁接触和交手维持现实的消极脆弱稳定。伊以多年来的网络空间博弈加剧了地区安全困境,并推动了敌友关系的强化。双方的博弈互动显示出网络空间与物理空间日益融合的“网络地缘政治”新形态。

伊朗和以色列的网络空间博弈对于理解中东安全治理现状具有重要启示意义。就需求端而言,地缘思维向网络空间的蔓延加深了地区的信任赤字。2023年新一轮巴以冲突爆发以来,“动能+网络”的混合战争成为现实,加剧了地区国家对技术威胁的担忧和疑虑。此外,美国在全球范围内推动对华战略竞争,与其在中东地区对伊朗和以色列的政策形成联动效应,催化了“次级修昔底德陷阱”的形成,制约了地区安全共识的构建,加剧了安全公共产品供应不足的困境。因此,亟需加强地区网络空间治理机制建设,形成网络空间治理的国际规范,跳出网络地缘政治零和博弈思维,以“网络空间命运共同体”理念为引领,共同造福中东地区人民。

(责任编辑:包澄章　责任校对:章　远)