

美国对华科技的“灰色地带”竞争战略

韩秋明

(中国科学技术发展战略研究院, 北京 100038)

摘要: 大国之间的“灰色地带”竞争日渐引发智库界、学术界和政策界的高度关注。经分析得出,美国对华科技“灰色地带”竞争存在3个特点,包括选择双方利益和能力不对称的领域作为切入点,违背科研规律和国际规范,呈现出从“I”到“C”再到“O”的渐进性打压路径等。深入探讨美国对华科技“灰色地带”竞争的5个表现,包括控制关键科技产品对中国可用性,在关键地缘政治地点或重点领域开展竞争,在前沿领域展示科技力量,减少中国对关键矿产、海底光缆等重要科技资源的控制权,制造不利于中国科技发展的舆论环境等。最后提出加强科技预警、寻找与美国共同利益点加强合作、利用多边渠道主动发声,塑造有利舆论等思考。

关键词: “灰色地带”; “灰色”竞争; 中美科技博弈; 科技预警

中图分类号: G323; G359.3 **文献标识码:** A **DOI:** 10.3772/j.issn.1009-8623.2024.04.005

近年来,“灰色地带”(Grey Zone)一词在美国智库界、学术界和决策者中持续引发关注。尽管该概念的内涵外延尚未得到统一,但社会各界普遍认为,未来数十年大国之间的“灰色地带”竞争将成为全球竞争格局的主要阵地。其中科技竞争是“灰色地带”竞争的主要内容之一,分析研究美国科技“灰色地带”竞争将有助于理解和判断下一步美国对华科技战略发展走向和态势,为中国采取有效应对措施提供决策支撑,具有现实意义。

1 美国将对华科技竞争作为重要的“灰色地带”竞争手段

1.1 美国对“灰色地带”的理解

“灰色地带”并非近年才有的新词,早在20世纪末,美国战略界和决策层就已将与“灰色地带”相关的挑战^[1]列为讨论热点。2015年以来,以智库为代表的智囊机构相继出版专题著作或报告,如兰德公司出版《掌控“灰色地带”:理解冲突的变化时代》^[2]、战略与安全研究中心(CSIS)出版《完

全击败:重新获得“灰色地带”的战略优势》^[3]等,将“灰色地带”由战略理念推到决策层面。特别是2023年3月,兰德公司发布报告《理解和应对中国“灰色地带”战术的新框架》^[4],特别提出美国要对中国实施“灰色地带”竞争战略。

“灰色地带”不是传统的物理空间概念,而是大国之间竞争的一种战略博弈举措,是一种隐性、非常规、相对模糊以及使用非战争手段的竞争性互动,其综合运用政治、经济、科技、外交、舆论和网络等工具,通过长期、渐进的模式改变现状或制造紧张局面,蚕食、规制和消耗竞争对手,塑造有利于己方的环境态势,是一种极具胁迫性和诱导性的战略手段。

1.2 美国对华开展科技“灰色地带”竞争的特点

美国智库研究^[3]认为,“灰色地带”战略竞争具有利益和能力上的非对称性、信息和规范上的模糊性以及行为方式上的渐进性等显著特征。从这个角度来看,美国对华科技竞争与上述特点较为吻合。

作者简介:韩秋明(1984—),男,博士,副研究员,主要研究方向为科技政策、技术评估。

收稿日期:2023-11-03

1.2.1 选择双方利益和能力不对称的领域作为切入点

非对称即以己之长击彼之短。近年来，中国科技创新取得了快速发展，美智库信息技术与创新基金会^[5]研究表明，在10个重大战略领域中，中国有7个位居领先地位，涉及计算机和电子产品、化学品、机动车和金属制品等。可以看出，美国占据优势的技术已逐步减少。

在此情况下，芯片领域是美国为数不多的相对优势领域。特朗普任总统时，决定在这一领域打击中国，以对华为的制裁为代表。自2014年以来，华为一直是全球最大的电信设备制造商。在2019年美国对其实施制裁之前，华为在电信运营商市场、企业市场和消费者市场都处于领先集团，特别是在具有颠覆性的5G领域，华为拥有的专利数量排名全球第一位，其主导力推的PolarCodes（极化码）也成为5G控制信道编码标准。但从另一方面来看，华为的各类信息设备产品中都安装了大量芯片，包括能够实现数字信号处理技术的芯片（DSP）、现场可编程门阵列（FPGA）、专用集成电路芯片（ASIC）、光纤接口芯片和射频前端模块等。美国芯片行业发达，现代芯片行业的基石如晶体管、集成电路都是由美国人最先发明和实现商用的。当前美国也在半导体领域的基础材料、知识产权方面占据显著优势，即使不在美国注册的晶圆厂如台积电等，也大量使用了美国技术。可以看出，芯片是中美双方利益和能力明显不对称的领域，对华在芯片领域进行打压是典型的美国选择己方最擅长的方面，在中国科技薄弱环节施加压力的“灰色地带”竞争手段。

1.2.2 美国对华科技打压违背科研规律和国际规范

科学理论和科技产品是全人类的共同财富。面对气候变化、新冠疫情、能源危机和经济衰退等事关全人类生存发展的共同挑战，没有国家能够独自应对；同时，没有国家能够独享科技创新成果，每个重大科技产品都需要全球化的创新链和产业链。无国界、无障碍、无歧视的开放科学精神和理念，科学知识交流和技术创新合作的互惠共赢，这是国际科技创新发展的共识。

美国不断对华科技打压遏制，但是目前看效果不佳，且美国自身业受到“反噬”。在芯片方面，对中国中兴、华为等企业进行出口限制，而高通、

AMD和英伟达等美国芯片公司也因此营业额大幅减少，股价大跌，许多科技企业开始大规模裁员。在人才方面，美国从2018年开始启动“中国行动计划”，旨在打击“间谍”，防止美国科技被中国“盗窃”，但并未收到预期效果。相关案例表明，美国对华科技遏制不符合科研规律和国际规范。此外，就芯片、光刻机等出口限制，中国有关部门已向WTO提起诉讼，美国明显的贸易保护主义做法破坏国际经贸秩序，违反国际贸易规则，将对全球和平发展利益造成不利影响。

1.2.3 对华科技打压呈现出从“T”到“C”再到“O”的渐进性打压路径

在美国对华科技打压早期，特朗普政府将中国视为对立面，多次在公开场合将中国与俄罗斯描述成“对手（Adversary、Rival或Enemy）”，并采取“301”调查、重点企业出口管制、舆论抹黑（新冠溯源、知识产权“盗窃”等）、政府官员制裁等针对性强的措施，对中国发起猛烈攻击和严重挑衅，这种战略可被视为将双方对立起来的“T”型战略。

拜登上台后采取联合盟友的对华遏制策略，一方面与欧洲盟友联合采取行动，建立跨大西洋伙伴关系，成立美欧贸易和技术委员会；另一方面扩大其在亚洲的影响力，推行美国印太战略，将美国与东盟关系升级为“全面战略伙伴关系”^[6]，发展电动汽车生态系统等；还与新加坡、日本、韩国和澳大利亚等^[7-10]国家建立网络、清洁能源和先进制造等技术伙伴关系或开展创新对话。这种战略可被视为“C”型半包围战略。

近期，针对中国在非洲的影响力，美国通过与新冠疫苗全球获取机制（COVAX）、非洲疫苗采购信托基金的合作，向撒哈拉以南非洲国家捐赠了超过1.94亿剂疫苗（不到中国捐赠的10%）。此外，美国政府时隔8年后再次启动美国—非洲领导人峰会，就全球卫生安全、粮食安全和气候变化等问题开展磋商，电池材料等也是此次峰会的焦点之一，目的是摆脱关键矿产对中国的依赖。美国在“C”形战略的基础上加强与非洲的合作，希望对华形成美国、欧洲、亚洲、非洲协同的“O”形全面包围圈。

2 美对华科技“灰色地带”竞争的主要表现

美国兰德公司2022年3月发布报告《“灰色

地带”的竞争》^[11]，总结了数十种“灰色地带”竞争策略，包括在国际地缘政治方面，使用政治、经济和军事手段支持目标国家的手或敌对国家；在双边方面，减少特定货物的贸易或流动，并针对目标政府开展网络攻击；在基层方面，在敏感领域或关键地缘政治区域进行舆论战等。

与上述竞争策略对比可以发现，美对华科技“灰色地带”竞争主要表现在以下几个方面。

2.1 控制关键科技产品对中国的可用性

2022年10月7日，美国商务部工业安全局（BIS）发布半导体出口管制新规，明确将非平面晶体管结构16 nm或14 nm或以下（即FinFET或GAAFET）的逻辑芯片、半间距18 nm或以下的动态随机存取存储器（DRAM）存储芯片、128层或已上的NAND闪存芯片等先进和高性能计算芯片及含有此类芯片的计算机商品加入《商业管制清单》（CCL），对运至中国的最终用途为超级计算机或半导体开发或生产的物项增加新的许可证要求。中国军事实体被美国明令禁止参与《芯片与科学法案》授权的有关项目，如果半导体公司（美国本土或其他盟友国家）在中国或其他可能“不友好”的国家建设或扩建先进的半导体制造工厂，这将使得该公司无法获得相应的补贴和研究资助。该法案还将禁止与中国有教育合作关系的大学（如孔子学院）等获得研究资金。

此外，半导体出口管制新规突破了原有规则下以“物项管控”为基础的传统监管逻辑，将“美国人”参与中国境内半导体开发、生产活动，列为与需严格监管的“境外参与核、生化、导弹扩散活动”等行为等同，都将对之进行全面监管。同时，“美国人”的定义十分宽泛，包括美国的公民、永久居民、庇护民、依照美国法律设立的法人实体（包括中国在美的分支机构），以及位于美国境内的人士等。违反美国《出口管理条例》（EAR）的规定，可能会受到民事或刑事处罚，包括25万~100万美元的罚金和最长20年的监禁，二者可以单处或并罚。

这是典型的控制或减少中国关键科技资源的“灰色地带”竞争手段。人才的限制会给中国半导体发展带来一定冲击。据《华尔街日报》报道，在16家中国上市半导体公司工作的高级管理人员中，

至少有43人是美国公民^[12]。《日经亚洲》引述分析师的推估，在半导体中企任职的美籍高管应有数百人^[13]。上市招股书信息显示，多家中国顶级芯片设备和材料公司的创始人和高管为美籍华人或持有绿卡。相关限制为中国半导体产业发展的人才基础带来一定影响。

2.2 在关键地缘政治地点或重点领域开展科技竞争

台积电是全球最大芯片代工制造商，也是全球有能力生产最尖端芯片的三家顶级公司之一。2020年5月美国商务部工业与安全局发布的《外国直接产品规则》（FDPR）要求全球任何厂商只要使用了美国的技术或设备，在向中国提供半导体芯片时都必须得到美国政府的出口许可证。作为全球最大的芯片供货商，台积电受影响较严重。同时，美国政府持续向台积电施压，要求其在美设厂，并将技术、设备、人才等半导体开发资源一并带到美国。

2022年8月美国通过《芯片与科学法案》，主要内容包括向半导体行业提供约527亿美元的资金支持，为企业提供价值240亿美元的投资税抵免，鼓励企业在美国研发和制造芯片。同时美国也是全球最重要的半导体市场之一。台积电原本对赴美设厂犹豫不决，原因在于成本过高，美国芯片制造人才短缺，也缺乏原材料、IC设计、封装测试等上下游业者，但面对美国新实施的策略以及地缘政治的影响，其仍决定在美国投资400亿美元建厂。2022年12月6日，台积电在亚利桑那州新厂区举行移机典礼，美国总统拜登出席。美国对台积电的战略，符合在关键地缘政治地点或重点领域开展科技竞争这一“灰色地带”竞争的手法。

2.3 在前沿热点领域展示科技力量

在人工智能方面。2022年11月，美国开放人工智能研究中心（OpenAI）推出ChatGPT（GPT-3.5版本）大语言模型^[14]，产品上线后仅2个月时间月活跃用户过亿，成为历史上增长最快的消费应用；并于2023年3月更新GPT-4版本，在办公、科研、编程、搜索引擎和服务机器人等领域得到广泛应用和传播，并引发全球对大语言模型关注的热潮。除此之外，美国科研机构或公司不断推出ProGen，Notion AI，DALL-E2，Stable Diffusion和Midjourney等生成式人工智能（Generative AI）工具，

广泛被世界各国使用，这展示了美国仍在引领人工智能的主要技术创新。

在国防科技方面。美国国防部于 2022 年 12 月对外公开新一代的 B-21 隐形轰炸机，这是美国 30 余年来开发的第一款大型无人驾驶隐形轰炸机，也是美国对其核打击力量的 3 个支柱进行现代化改造的一部分，其他还包括核弹道导弹发射井和潜舰核弹头等。美国国防部宣称其隐身性能由于采用了最新技术和材料而得到更大的提升，“开放式工程结构”为吸收未来更先进的技术搭建了框架，它将成为美国应对中国“威胁”的一件战略武器。此外，2023 年 10 月，美国国防部宣布研发新一代核重力炸弹 B61-13，威力可能将达到 40 万 t 以上，是当年在广岛爆炸的“小男孩”原子弹的 26 倍。

在核聚变方面。2022 年 12 月，美国能源部宣布其下属劳伦斯利弗莫尔国家实验室（LLNL）在国家点火设施（NIF）进行了历史上第一次可控核聚变实验，实现了“核聚变点火”（Fusion Ignition），该反应产生的能量超过所消耗的能量，并称这一突破将永远改变清洁能源和美国国防的未来。这一成就在 2023 年 7 月底再次得到实现。该技术虽然距离要实现商业核聚变发电还有一段距离，但已经是里程碑式的成就，其实用化的脚步也正在提速。2023 年 5 月，美国氦核能源公司与微软签署了历史上第一份核聚变能源商业合同，这将于 2028 年为微软提供至少 50 MW 的电力。

因此，美国在相关领域的技术突破是在向世界展示其仍然在前沿性颠覆性技术方面领先全球，旨在对所有竞争国家进行科技宣言。

2.4 减少中国对关键矿产、海底光缆等重要科技资源的控制权

世界各国都在追求“双碳”发展目标，这直接造成了锂、铜、钴、镍和锌等关键稀土元素的供应紧缺。这些稀土元素是生产可再生能源技术的重要组成部分，如电动汽车的电池、风力涡轮机叶片等。此外，稀土元素在半导体和其他电子产品的制造过程中也发挥关键作用。西方国家各个地区采矿业的社会和环境成本在不断增加，而非洲则是稀土矿产的重要生产区域，具有强大的矿业潜力。在第二届美国—非洲领导人峰会期间，美国重申并扩大了与非洲国家政府、民营行业、社会组织以及慈

善机构的持久伙伴关系，表明非洲将在应对全球面临的时代最大挑战之一——气候变化中发挥关键作用，并宣布为科特迪瓦提供 100 万美元资助其建立生物质电厂，提供 85.7 万美元用于在塞拉利昂实现清洁水力发电，提供 100 万美元用于在赞比亚开发电池能源储存技术，与摩洛哥启动太阳能 10 项全能非洲设计挑战，与肯尼亚落地热能空气直接捕获等^[15]。相关绿色技术的投资，主要是为了重新恢复停滞了 8 余年的美非关系，并企图遏制中国在非洲的影响力，争取在非洲发展美国可控的关键矿产产业，降低对中国的依赖。

海底光缆是全球信息互联互通的重要基础设施，承载 95% 以上的国际互联网流量。特别是随着云计算、大数据和元宇宙等技术的发展，海底光缆的作用愈加彰显，其建设方竞争也成为大国博弈的重点，如连接十几个国家、跨越三大洋的东南亚—中东—西欧 6（SeaMeWe—6）光缆，原本已明确由中国企业建设，但美方向光缆沿线国家的电信公司提供总价值 380 万美元的培训补助金，同时通过使领馆开展外交游说（如美其名曰“这是与美国建立经贸合作和获得相应援助的起点”）和施压（如美国即将把中国承建公司列入实体清单，相关工程会无法收尾，前期投入损失等）^[16]，要求相关国家电信公司放弃中国企业，转而支持美国企业。最终美国实现了其目标，中国企业被替代，美国企业用比中国高 3 倍的成本承建了这一重要基础设施。

2.5 将中国视为头号对手长期开展“网络战”

美国长期以来将中国视为网络攻击的主要对象。2021 年 7 月，中国国家互联网应急中心发布报告，2021 年上半年中国捕获计算机恶意程序样本数量主要来自美国，占比达 49%^[17]。2022 年 3 月，三六零安全科技股份有限公司（以下简称“360 公司”）发布的《网络战序幕：美国国安局 NSA（APT—C-40）对全球发起长达 10 余年无差别攻击》报告指出，美国国家安全局针对中国、英国等 47 个国家开展长达 10 余年的网络攻击活动，并利用“量子攻击”技术（一种针对国家级互联网专门设计的先进网络流量劫持攻击技术）对中国社交软件发起攻击^[18]。2022 年 6 月，中国国家计算机病毒应急处理中心和 360 公司披露美国国家安全局下属一款网络攻击武器“酸狐狸”^[19]，持续对中国发起猛烈的

网络攻击，该平台是美国计算机网络入侵行动队（CNE）的主战装备。2022年9月，中国国家计算机病毒应急处理中心和360公司发布报告指出，美国国家安全局特定入侵行动办公室（TAO）对中国网络目标实施了上万次的恶意网络攻击，控制了相关网络设备（网络服务器、上网终端、网络交换机、电话交换机、路由器和防火墙等），疑似窃取了高价值数据，同时还利用其控制的网络攻击“武器”平台长期对中国的手机用户进行无差别的语音监听，并单独针对西北工业大学发起上千次网络攻击活动^[20]。

除了网络攻击外，美国还希望组建专门网络部队开展网络战。2022年6月，美国《陆军时报》报道^[21]，美国国防部正将工作重心转移到为未来与精通技术的对手作战做准备，希望美国陆军现役网络战部队到21世纪20年代末规模可以扩大一倍，其中特别提到，美国国防部认为中国是美国目前的“头号威胁”。2023年3月，前北约最高军事长官、美国塔夫茨大学弗莱彻法律与外交学院名誉院长詹姆斯·斯塔夫里迪斯（James Stavridis）^[22]撰文呼吁，美国需要建立一支新的独立军种——网络部队（Cyber Force）对包括中国在内的国家开展网络空间角力^[21]。保卫民主基金会网络与技术创新中心总监马克·蒙哥马利（Mark Montgomery）也是倡导成立美国网络部队的主要人员之一，他表示美国国会现今特别关注来自中国的威胁，因此能提高美国对抗中国能力的事务将被优先部署，而成立网络部队绝对是值得考虑的举措^[23]。

2.6 制造不利于中国科技发展的舆论环境

中国“一带一路”倡议凭借平等、互利共赢的合作理念得到了众多国家的认可，持续吸引更多国家的加入。为了削减中国的影响力，美国不断对此进行舆论渲染，宣称“一带一路”的实施缺乏明确的环境准则、安全标准，与1700多个至关重要的生物多样性地域以及265个受威胁物种的分布范围交叠，对水质造成了不良影响，污染了周边土地，破坏了脆弱的生态系统，可能会导致“永久性的环境退化”^[24]。美国媒体还使用“中国债务陷阱”这一词形容中国在亚洲、非洲和拉丁美洲等地区进行的投资建设，指控中国用庞大的债务套住了许多发展中国家^[25]。

美国还以“数字威权主义”等阻碍中国和技术

标准制定方面的发展。美国妄称中国借助政治影响力，试图为包括电信、电力传输和人工智能在内的各种前沿技术制定标准，利用欧洲等盟友在数据隐私、技术主权等问题上的警惕感，不断宣扬所谓技术窃密、人权和伦理风险等，制造所谓“技术民主国家”和“技术专制国家”之间的分立。相关报道颠倒黑白，不分是非，意图制造不利于中国科技发展的舆论环境。

3 启示

美国对华科技打压遏制不择手段，在“全政府、全社会、全领域”和“出口管制、小院高墙、技术联盟、投资审查、人才遏制”等手段的基础上，持续开展“灰色地带”竞争。这也进一步提醒中国科技界，只有坚持科技自立自强，掌握关键核心技术，才能从根本上保障国家经济安全、国防安全和其他安全。面对美国各类打压手段，中国应坚持底线思维，按照“预警评估，以我为主，多边推进”的原则，精修“内功”，提升科技总体实力，同时主动出击，利用多边渠道积极拓宽反科技遏制阵线的应对策略。

一是加强科技预警，提升应对“灰色地带”竞争能力。继续对美国等西方国家的相关科技政策、涉华科技法案等最新动向进行动态监测，对中国科技政策走向进行预判并制定相关预案。开展技术预警与科技安全前瞻研究，对来自外部持续累加、迭代升级的风险，以及科技垄断与反垄断、竞争与反竞争等方面进行研判，避免对中国科技安全造成长期性、持续性损害。充分发挥新型举国体制优势，推动在AI、量子、核能、下一代通信网络和高科技武器等关键技术领域取得突破，对冲美国不断发布创新引发的国际影响。

二是寻找共同利益点，主动加强与美国的合作。面对美国的科技打压，中国不仅要坚持底线思维，积极应对，还应以2023年11月中美元首会晤为契机，主动作为，与美国积极开展合作。一方面从面对全球共同挑战和互利共赢出发，推动中美合作互动。中美科技交流合作作为应对气候、环境、生态、能源和疾病等全球性问题提供解决方案，携手推进世界稳定繁荣发展。另一方面可着眼于在一些非敏感领域，如农业、科技金融和交通等进行合作，中美之间各有优势，根本利益冲突少，可实现优势

互补。此外，还可在科研诚信、科技伦理和新技术应用对社会影响等重大问题上加强协同治理和政策协调，尝试制定共同的道德规范和行业规则。

三是利用多边渠道主动发声，塑造有利舆论。利用多边平台旗帜鲜明反对“科技脱钩”与“科技冷战”，用好联合国、G20等多边机制，“《区域全面经济伙伴关系协定》、10+1（东盟十国与中国）、10+3（东盟十国与中国、日本、韩国三国）”等现有区位优势，通过各种方式向国际社会表明美国对中国科技打压遏制的实质，指明美国相关措施背离国际准则、破坏国际规则，在全球形成避免滥用科技制裁的强大舆论环境。

四是深入推进科技外交工作。以开放换开放、以市场换市场，使科技交流成为增进战略互信、促进互利共赢的重要途径，营造有利于自身科技发展的良好外部环境。继续推进多边科技合作，在已参加的国际组织中，就科学技术创新议题提供“中国方案”。利用“一带一路”发展的历史契机，秉承“共商、共建、共享”原则，将科技合作作为公共产品，解决发展中国家关心的贫困、气候变化和污染等全球性问题。■

参考文献：

- [1] FISH J M, MCCRAW S J. Fighting in the gray zone: a strategy to close the preemption gap[EB/OL]. [2024-01-20]. https://www.globalsecurity.org/military/library/report/2004/ssi_fish-mccraw-reddish.pdf.
- [2] MAZARR M J. Mastering the gray zone: understanding a changing era of conflict[EB/OL]. [2024-01-20]. <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1427&context=monographs>.
- [3] FREIER N. The darker shade of gray: a new war unlike any other[EB/OL]. [2024-01-20]. <https://www.csis.org/analysis/darker-shade-gray-new-war-unlike-any-other>.
- [4] LIN B, GARAFOLA C L. A new framework for understanding and countering China's gray zone tactics[EB/OL]. [2024-01-20]. https://www.rand.org/pubs/research_briefs/RBA594-1.html.
- [5] Information Technology and Innovation Foundation. The Hamilton Index, 2023: China is running away with strategic industries[EB/OL]. [2024-01-20]. <https://itif.org/publications/2023/12/13/2023-hamilton-index/>.
- [6] The White House. ASEAN-U.S. leaders' statement on the establishment of the asean-u.s. comprehensive strategic partnership[EB/OL]. [2024-01-20]. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/12/asean-u-s-leaders-statement-on-the-establishment-of-the-asean-u-s-comprehensive-strategic-partnership/>.
- [7] U.S. Department of State. The inaugural U.S.-Singapore cyber dialogue[EB/OL]. [2024-01-20]. <https://www.state.gov/the-inaugural-u-s-singapore-cyber-dialogue/>.
- [8] U.S. Department of Commerce. Joint statement: U.S. Department of Commerce and Singapore ministry of trade and industry celebrate inaugural U.S.-Singapore partnership for growth and innovation annual dialogue[EB/OL]. [2024-01-20]. <https://www.commerce.gov/news/press-releases/2022/10/joint-statement-us-department-commerce-and-singapore-ministry-trade-and>.
- [9] U.S. Department of State. U.S.-ROK joint symposium on countering DPRK cyber threats to cryptocurrency exchanges[EB/OL]. [2024-01-20]. <https://www.state.gov/u-s-rok-joint-symposium-on-countering-dprk-cyber-threats-to-cryptocurrency-exchanges/>.
- [10] U.S. Cyber command public affairs. CYBERCOM concludes CYBER FLAG 23 exercise[EB/OL]. [2024-01-20]. <https://www.cybercom.mil/Media/News/Article/3209896/cybercom-concludes-cyber-flag-23-exercise/>.
- [11] LIN B, GARAFOLA C L. Competition in the gray zone[EB/OL]. [2024-01-20]. https://www.rand.org/pubs/research_reports/RRA594-1.html.
- [12] 华尔街日报. 中国芯片公司的美国高管因美国出口禁令陷入两难[EB/OL]. [2024-01-20]. <https://cn.wsj.com/articles/%E4%B8%AD%E5%9B%BD%E8%8A%AF%E7%89%87%E5%85%AC%E5%8F%B8%E7%9A%84%E7%BE%8E%E5%9B%BD%E9%AB%98%E7%AE%A1%E5%9B%A0%E7%BE%8E%E5%9B%BD%E5%87%BA%E5%8F%A3%E7%A6%81%E4%BB%A4%E9%99%B7%E5%85%A5%E4%B8%A4%E9%9A%BE-11665989706>.
- [13] 日经亚洲. 中国“海龟”科技高管陷入困境[EB/OL]. [2024-01-20]. <https://asia.nikkei.com/Business/Tech/Semiconductors/China-s-sea-turtle-tech-executives-stranded-by-U.S.-crackdown>.

- [14] OpenAI. Introducing ChatGPT[EB/OL]. [2024-01-20]. <https://openai.com/blog/chatgpt>.
- [15] The White House. U.S-Africa partnership in supporting conservation, climate adaptation and a just energy transition[EB/OL]. [2024-01-20]. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/13/fact-sheet-u-s-africa-partnership-in-supporting-conservation-climate-adaptation-and-a-just-energy-transition/>.
- [16] BROCK J. U.S. and China wage war beneath the waves-over internet cables[EB/OL]. [2024-01-20]. <https://www.reuters.com/investigates/special-report/us-china-tech-cables/>.
- [17] 国家互联网应急中心. 2021年上半年我国互联网网络安全监测数据分析报告[EB/OL]. [2024-01-20]. <https://www.cert.org.cn/publish/main/upload/File/first-half%20%20year%20cybersecurity%20report%202021.pdf>.
- [18] 360 政企安全集团. QUANTUM 量子攻击系统：美国国安局（APT—C-40）黑客组织高端网络攻击武器技术分析报告[EB/OL]. [2024-01-20]. <https://www.anquanke.com/post/id/270813#h2-9>.
- [19] 新华网. 美“酸狐狸”对中国发起网络攻击[EB/OL]. [2024-01-20]. http://www.xinhuanet.com/mil/2022-06/30/c_1211662321.htm.
- [20] 360 政企安全集团. 关于西北工业大学发现美国 NSA 网络攻击调查报告[EB/OL]. [2024-01-20]. <https://360.net/about/news/article631563158774d7005a02ad96>.
- [21] Army Times. US Army to double cyber corps strength as focus shifts from counterinsurgency[EB/OL]. [2024-01-20]. <https://www.defensenews.com/cyber/2022/06/13/us-army-to-double-cyber-corps-strength-as-focus-shifts-from-counterinsurgency/>
- [22] STAVRIDIS J. The US military needs to create a cyber force[EB/OL]. [2024-01-20]. <https://news.bloomberglaw.com/privacy-and-data-security/the-us-military-needs-to-create-a-cyber-force-james-stavridis>.
- [23] JASPREET G. Lawmaker ‘definitely’ considering value of independent cyber force[EB/OL]. [2024-01-20]. <https://breakingdefense.com/2023/02/lawmaker-definitely-considering-value-of-independent-cyber-force-but-wants-more-study/>.
- [24] 美国驻华大使馆和领事馆. 中国破坏环境的行为[EB/OL]. [2024-01-20]. <https://china.usembassy-china.org.cn/zh/chinas-environmental-abuses/>.
- [25] 新浪财经. 美国出资制造“债务陷阱”谣言，诋毁中国“一带一路”倡议[EB/OL]. [2024-01-20]. <https://finance.sina.com.cn/wm/2022-07-05/doc-imizirav2067963.shtml>.

“Grey Zone” Competition Strategy of United States Against China’s Technology Development

HAN Qiuming

(Chinese Academy of Science and Technology for Development, Beijing 100038)

Abstract: The grey zone competition between major powers has increasingly attracted great attention from think tanks, academia and policy makers. This paper summarizes the three characteristics of the grey zone competition in science and technology implemented by the United States against China, including choosing areas where the interests and capabilities of both parties are asymmetrical as the entry point, violating the laws of scientific research and international norms, and showing the progressive containment path from “I” to “C” to “O”. This paper also provides an in-depth analysis of five manifestations of the U.S.’s technological grey zone competition with China, such as controlling the availability of key S&T products to China, competing in key geopolitical locations or key areas, demonstrating technological strength in frontier areas, reducing China’s control over important S&T resources such as key minerals and submarine optical cables, creating public opinion that is not conducive to China’s S&T development, etc. It finally puts forward some thoughts including strengthening scientific and technological early warning, finding common interests with the United States, and using multilateral channels to shape favorable public opinion.

Keywords: grey zone; grey competition; Sino-U.S. science and technology game; science and technology early warning