伊朗网络安全能力建设及成效评估

文｜西北大学中东研究所 曹峰毓 刘芳芳

伊朗独特的地理位置与资源禀赋使其在国际政治中具有举足轻重的地位。然而，伊朗与美国、以色列等国在核问题、地区影响力等方面存在深刻矛盾。这些矛盾不可避免地延伸至网络空间，使伊朗成为网络攻防的前沿阵地。值得注意的是，伊朗面临的网络安全威胁已突破单纯的技术对抗范畴，呈现出与能源设施攻击、金融系统瘫痪等传统安全议题深度交织的特征。当网络武器与实体基础设施破坏形成共振时，其破坏效能将呈指数级增大。这种网络安全事件与传统安全风险的杂糅效应，直接威胁中东地缘政治平衡，还可能通过网络武器扩散、攻击链跨国传导等方式波及其他地区，进而对全球安全格局产生连锁反应。同时，伊朗网络安全能力建设的经验与教训，也为其他发展中国家提供了可借鉴的经验。深入研究伊朗的网络安全问题，不仅有助于理解其自身在网络时代的应对策略，更能为推动全球网络安全治理体系的完善提供有益的启示。

一、伊朗面临的网络安全形势

伊朗面临的网络安全威胁呈现国家行为体与非国家行为体双重发难的复合型特征。该国紧张的地缘政治形势使其成为网络攻击的重点目标，而关键基础设施的网络脆弱性则进一步加剧了潜在的安全风险。国家行为体层面的攻击主要由政府或准政府机构发动，目标通常聚焦战略核心领域，如核设施、能源系统及军事网络，其驱动因素是地缘政治竞争与战略威慑。此类攻击具有国家战略级破坏意图，旨在通过瘫痪关键基础设施削弱对手综合国力，而非国家行为体层面的攻击则更多由黑客组织或个人发动，目标转向民生领域与社会稳定，其驱动因素包括意识形态冲突、获取经济利益等方面。

（一）国家行为体层面的网络攻击

伊朗遭受了大量来自国家行为体的网络攻击。其中，以色列对该国发动的网络攻击对其造成严重损害。根据赛门铁克（Symantec）公司 2020 年 1 月发布的报告《W32.Stuxnet 档案》（W32.Stuxnet Dossier），2010 年 6 月，伊朗纳坦兹核设施遭受“震网”（Stuxnet）蠕虫病毒攻击。这是全球首次针对工业控制系统的国家级网络攻击。该病毒利用移动存储设备潜入核设施内部网络，并利用至少四个零日漏洞通过 Windows 系统进行自我传播。其目标是感染西门子 WinCC/PCS 7 工业控制系统控制软件中的项目文件。此次攻击造成了伊朗纳坦兹核设施约 1000 台离心机报废，使该国核计划推迟至少两年。“震网”病毒的出现迫使伊朗将网络安全提升至国家安全战略核心层面。

在“震网”病毒事件后，以色列针对伊朗核设施的网络攻击有增无减：2011 年 11 月，伊朗布什尔核电站检测到结构与“震网”相似的“毒区”（Duqu）蠕虫病毒，该病毒的功能是窃取核设施设计图纸等敏感资料；2021 年 4 月，伊朗原子能组织（AEOI）称，纳坦兹核设施电力系统遭网络攻击，部分离心机损坏。伊朗指控此次攻击为以色列所为，并宣布将铀浓缩水平提升至 60%。这加剧了该地区核危机。

同时，以色列对伊朗的网络攻击也逐渐由核设施扩展至对该国经济至关重要的石油设施。2020 年 5 月，伊朗重要石油出口港口阿巴斯港的沙希德拉贾伊（Shahid Rajaee）码头计算机系统遭到攻击，导致航运服务瘫痪数日。

除了以色列，美国等西方国家也曾对伊朗发动多次网络攻击。2012 年 5 月，美国向伊朗石油部及石油公司网络大规模植入“火焰”（Flame）病毒。该病毒具备窃取文件、记录键盘输入等复杂功能。为防止进一步破坏，伊朗被迫断开关键石油设施的网络连接，导致该国的石油生产和出口受到极大影响。2012 年 6 月，伊朗情报部部长海达尔·莫斯莱希（Heydar Moslehi）称，该国网络受到由美国、以色列和英国实施的“擦除器”（Wiper）病毒攻击。

（二）非国家行为体层面的网络攻击

伊朗还遭受来自非国家行为体的分散性安全威胁。近年来，各类黑客组织对伊朗关键民生领域的攻击愈加频繁。2021 年 11 月，黑客组织曾对伊朗的燃料分配系统发动网络攻击，导致约 4300 个站点受到干扰。黑客组织还劫持了伊斯法罕的广告牌，上面写着“哈梅内伊！我们的汽油在哪里？”等标语，目的是进一步破坏伊朗政府形象。2023 年，伊朗第一副总统穆罕默德·礼萨·阿雷夫（Mohammad Reza Aref）透露，该国的燃料分配系统在当年又遭受了两次网络攻击，约 70% 的加油站受到影响。其中一次袭击确信是由一个名为“掠食性麻雀”（Predatory Sparrow）的黑客组织发动。2025 年 3 月 18 日，伊朗反政府黑客组织“紧闭的双唇”（Lab Dookhtegan）宣布，已成功破坏两家与伊朗政府有关联公司的 100 多艘油轮的所有通信。

据美国有线电视新闻网（CNN）报道，2025 年 6 月 17 日至 18 日，“掠食性麻雀”组织对伊朗的金融系统展开了大规模攻击。其中，伊朗赛帕银行（Bank Sepah）的核心系统被破坏，客户服务严重受阻，进而导致系统瘫痪，银行服务全面中断，甚至还波及了该国的加油站系统。伊朗最大加密货币交易所 Nobitex 也成了其攻击目标。该组织通过入侵 Nobitex 系统，窃取并销毁了价值约 9000 万美元的加密货币。同时，伊朗国有电视台也遭到网络攻击，黑客播放了煽动民众反抗伊朗政府的视频。面对此次攻击，伊朗被迫采取全国断网、封锁境外应用及号召卸载 WhatsApp 等强硬措施加以应对。

二、伊朗网络安全能力建设的实践

伊朗的网络安全能力建设是一个逐步发展和完善的过程。在相当长时间，伊朗未能对网络攻击的潜在威胁给予足够重视，互联网管制以审核、过滤敏感信息为主。直至遭遇“震网”病毒等严重网络袭击后，伊朗才真正开始重视网络安全治理架构的构建，通过增设网络安全部门、增加网络安全投入、注重网络安全人才培养以及提升公众网络安全意识等多方面举措，不断提升自身网络安全能力，逐步建立起网络安全防护体系。

（一）互联网监管

互联网进入伊朗初期，伊朗政府的相关管理比较宽松。该国较为系统的互联网监管始于 2001 年。当年 12 月，伊朗文化革命最高委员会颁布了一系列法令，规定伊朗国内的互联网服务提供商需依据政府制定的网站名单，对不符合规定的网站进行屏蔽处理。2002 年，伊朗哈塔米政府颁布了名为“Takfa”的国家信息化计划，力争在 2008 年实现电子政务和电子商务的大规模运用。然而，内贾德总统上任后却将“Takfa”计划中止，并在 2006 年颁布新的互联网管理条例，规定伊朗国内的互联网服务供应商要将用户的网速限制在 128KB/s 以内，试图以此唤起伊朗民众“回归对伊斯兰文化的热爱”。鉴于伊朗法律对互联网的管理较模糊，伊朗宪法监护委员会在 2009 年核准了议会通过的《计算机犯罪法》（CCL）。依据该法，伊朗的立法、行政以及司法三大部门需要就互联网管理相关事宜展开集体决策与协同行动。此外，相关法律还明确指出，由伊朗政府负责裁定互联网上应被屏蔽的内容对象。

（二）网络安全治理架构

伴随“震网”病毒之后愈加严重的网络袭击，伊朗意识到网络空间已经成为国家安全的新疆域，开始重视网络安全治理架构的构建，主要体现在以下方面。

第一，增设网络安全部门。2010 年 11 月，伊朗成立了网络防御司令部（Cyber Defense Command）。该司令部隶属于阿特什（Artesh）被动防御组织，负责在伊朗境内从事与网络安全防护相关的活动。同年，伊斯兰革命卫队成立了“网络电子司令部”（IRGC-CEC），主要负责网络攻击和防御，逐渐成为伊朗网络战的核心力量。伊朗在 2011 年设立网络警察（Cyber Police），负责打击网络犯罪、监控互联网内容、防范网络间谍活动。该部门曾多次逮捕涉嫌网络攻击的嫌疑人。随后，伊朗又在原网络警察部队的基础上组建了“费塔警察”（FETA Police），专门处理互联网犯罪，并承担打击“政治犯罪和安

全犯罪”的任务。2012 年 3 月，根据伊朗最高领袖哈梅内伊的命令，伊朗正式成立了网络空间最高委员会（Supreme Council of Cyberspace）。该委员会成员包括伊朗总统、议会议长，以及情报、司法、电信、文化和科学部长等国家高级权力机关的实权人物，主要职责包括制定网络政策、强化网络安全、协调各相关部门等。网络空间最高委员会的成立标志着伊朗在网络安全治理上迈出了重要一步，也标志着伊朗将网络安全提升到国家战略层面，同时打破了以往各部门在网络事务上各自为政的局面，实现了从分散管理到集中统筹的转变，提高了协同效率。除了协调行动，该部门还有着高达 4000 万美元的初始预算，用于支持网络安全相关活动的开展。伊朗革命卫队下属的巴斯基（Basij）准军事组织虽然在成立之初便担任辅助警察和群众运动的职能，之后逐渐活跃在网络监控与防御领域。在监测预警体系方面，伊朗还设立了“计算机应急响应小组协调中心”（CERT），整合网络流量监控、漏洞扫描与威胁情报分析，形成覆盖政府、军事与民用领域的多层级预警机制。

第二，增加网络安全投入。伊朗还大幅增加了在网络安全领域的资金投入，并有针对性地开发相关技术。自鲁哈尼任总统后，伊朗显著增加了在网络安全领域的投入。在 2013 年至 2016 年期间，相关领域的支出实现了倍数级增长。其中，伊朗通过网络防御司令部针对性地开发了工业控制系统（SCADA）防护系统，强化了核设施、能源系统等关键基础设施的网络安全隔离与实时监控。在 2012 年“火焰”病毒攻击石油部时，该系统通过主动切断网络连接遏制了病毒扩散。2019 年 10 月 29 日，伊朗信息和通信技术部长穆罕默德·贾瓦德·阿扎里·贾赫罗米（Mohammad Javad Azari Jahromi）宣布，伊朗的“数字堡垒”（Dajfa）网络安全项目在 2018 年成功拦截了超 3300 万次网络攻击，成为该国网络安全建设的标志性成果。同时，伊朗在以量子加密为代表的新兴安全技术领域也取得了阶段性突破。伊朗 2018 年启动了量子纠缠与量子密钥分发（QKD）相关研究。2020 年，AEOI 宣布完成了 300 米距离量子通信测试。2024 年，伊斯兰阿扎德大学（Islamic Azad University）提出“混合混沌量子密钥分发”（CQKD）模型，通过混沌矩阵与量子行走技术将密钥空间扩大至 10^{124} 量级。同期，伊朗量子技术中心（ICQT）在偏振控制领域取得突破，利用粒子群优化算法稳定光纤链路偏振状态，有效解决了量子密钥分发系统长期存在的信号漂移问题。CQKD 模型通过将混沌理论与量子密钥结合，大幅提升了密钥的复杂度，使其更难被破解；粒子群优化算法则通过模拟鸟群觅食行为，精准调整光纤中光粒子的偏振状态，减少信号传输误差。根据 2024 年引文数据库 Web of Science 的数据，伊朗在量子技术所有领域的科研成果已位居伊斯兰国家首位，尤其是在量子遥感技术领域，位列全球第八、伊斯兰国家第一。

第三，网络安全人才培养。伊朗通过高校与军事机构协同培养网络安全人才，例如，在德黑兰大学等院校开设网络安全专业，联合“马赫信息安全中心”（Mah Information Security Center）开展实战化教学，课程涵盖恶意代码分析、加密技术等领域。巴斯基宣称拥有 12 万名网络战志愿者，通过高校培训计划将学生纳入预备技术队伍，形成学术研究—军事应用的人才输送链条。伊朗本土 IT 企业如搜索引擎“Parsijoo”、移动应用商店“Cafe Bazaar”则兼顾民用服务与技术储备，为网络安全领域提供市场化人才出口。

第四，提升公众网络安全意识。伊朗政府通过“国家互联网项目”推广“清洁互联网”，鼓励使用本土社交平台与搜索引擎（如 Yooz），减少对西方技术的依赖，引导民众参与网络安全防护。媒体宣传则侧重案例警示，如公开报道以色列网络攻击企图，强调网络战是国土安全的延伸，推动社会形成对政府监管措施（如 VPN 限制、内容审查）的支持。然而，政府对网络的长时间管控加剧了民众对政府的疏离感。2024 年 12 月，伊朗总统马苏德·佩泽希齐扬（Masoud Pezeshkian）宣布解禁 WhatsApp 和 Google Play 两个平台。同时，伊朗官方还强调这是“一系列分阶段放松举措”的第一步，未来可能会逐步解除更多平台禁令。解禁措施旨在缓解民众对网络管

控的不满，为引导公众主动参与安全防护创造条件。

三、伊朗网络进攻力量的组织与实践

在遭遇大量攻击后，伊朗意识到不仅需要发展网络防御力量，更需要积极地开展网络进攻，并将其作为针对西方的非对称反制手段。该国的网络进攻力量主要由两个方面组成。其一是伊斯兰革命卫队网络战分支等军方的正规网络战部队，其二是半官方乃至民间的黑客组织。为了规避国家责任，后者相较于前者往往更加活跃，其中较有影响的黑客组织包括马布纳研究所（Mabna Institute）、“高级持续性威胁 33 组织”（APT33）、“复制小猫”（Copy Kittens）、“钻井平台”（Oil Rig）、“剁肉刀行动”（Operation Cleaver）与“污水”（Muddy Water）等。近年来，“博学狮鹫”（Educated Manticore）、“网络复仇者”（Cyber Av3ngers）、“马利克小队”（Malek Team）、“汉达拉黑客”（Handala Hack）和“国土正义”（Homeland Justice）等新兴黑客组织也日趋活跃。

值得强调的是，根据以色列网络安全公司捷邦（Check Point）发布的《2025 年网络安全状况报告》（The State of Cyber Security 2025），除传统手段外，伊朗正积极将人工智能工具集成到网络攻击之中，包括漏洞研究、侦察、代码开发和攻击执行优化，明显提高了攻击的效率和规模。例如，名为“风暴-0817”（STORM-0817）的伊朗网络攻击者被观察到使用 OpenAI 模型辅助开发监控工具和恶意软件，包括调试安卓间谍软件代码、编写 C2 服务器程序、开发社交媒体爬虫工具和翻译用于情报收集的专业资料。

第一，美国是伊朗网络攻击的主要对象。“巢穴”（Ashiyaneh）组织声称曾在 2010 年对美英法千余家网站发动过网络攻击。在 2011 年至 2013 年期间，伊朗黑客对美国 47 家银行和金融机构发动持续的分布式拒绝服务（DDoS）攻击，致使这些银行的客户一度无法正常访问网站。2013 年，黑客试图控制纽约市郊一座小型水坝的洪水闸门，但由于在攻击时水坝已因例行维护而断开连接，未能成功。针对这次袭击，美国司法机构于 2016 年正式对 7 名“与伊朗政府存在关联”的黑客提起指控。2019 年 10 月，微软威胁情报中心（MSTIC）指出，伊朗黑客组织“磷”（Phosphorus）企图入侵与美国大选相关方、政府官员以及媒体记者所使用的邮件账户。近年来，与伊斯兰革命卫队有关联的组织如“网络复仇者”利用人工智能工具升级了对美国关键基础设施的攻击。例如，2023 年，该组织入侵了美国宾夕法尼亚州阿利奎帕市水务局的可编程逻辑控制器（PLC）系统。OpenAI 公司称，相关组织使用大语言模型（LLM）建立了自动化攻击流程，包括查询工业设备软件漏洞、优化攻击脚本、在公开工具中混淆恶意代码等环节，提高了其网络攻击的效率和规模。

第二，以色列是伊朗网络攻击的另一个重点国家。2018 年 7 月，伊朗黑客组织“魅力小猫”（Charming Kitten）曾被指控企图通过仿冒以色列网络安全公司“ClearSky”的网站，以此窃取用户信息。工业网络安全公司奥托里奥（OTORIO）的研究人员诺姆·埃文（Noam Even）2024 年 7 月 9 日在 OTORIO 官网发布的文章《我们从 12 月 1 日以色列水库袭击事件中学到了什么》（What We've Learned From The Israeli Reservoir Attack on Dec 1st）透露，2020 年 12 月，伊朗对以色列水处理设施进行了网络攻击，但未造成任何损害。2021 年 10 月发布的《2021 年微软数字防御报告》（Microsoft Digital Defense Report 2021）显示，在 2020 年 11 月至 12 月伊朗黑客组织“Pay2Key”曾成功渗透并攻击了 80 家以色列企业，其中不乏航空航天等高科技企业。在 2023 年 11 月至 2024 年 1 月巴以冲突期间，伊朗黑客扫描暴露公网的工业控制系统（ICS），利用其设备默认密码 / 空口令及默认传输控制协议（TCP）端口，入侵全球以色列制可编程逻辑控制器和人机界面（HMI）系统，致使美国水务、能源、医疗等数十家关键设施遭到渗透。此外，伊朗还将宗教意识形态与网络战相结合，在“圣城日”（Quds Day）等重要节日组织黑客对以色列发起象征性攻击，既展示技术能力，又强化反以共识。捷邦公司 2025 年 6 月发布的安全报告《2025 年网络安全状况报告》显示，与伊朗伊斯兰革命卫队有关

联的黑客组织“博学狮鹫”曾对以色列记者、知名网络安全专家和计算机科学教授发起过大规模网络钓鱼活动。同一份报告还显示，与伊朗情报和安全部（MOIS）有关联的黑客组织“虚空狮鹫”（Void Manticore）则向以色列关键基础设施和私人组织部署了“No-Justice”等擦除型恶意软件。“网络复仇者”组织同样将人工智能工具网络武器化，并用于针对以色列关键基础设施的攻击，包括利用 ChatGPT 等工具研究工业控制系统漏洞、调试脚本错误、创建专用脚本，并开发代码混淆技术。根据捷邦公司在 2024 年 11 月发布的名为《恶意软件聚焦：WezRat 的深入分析》（Malware Spotlight: A Deep-dive Analysis of Wezrat）的专题文章，“博学狮鹫”组织还利用人工智能工具生成虚假消息，通过冒充科技高管或研究人员的虚构助理，经由电子邮件和 WhatsApp 消息与目标接触，并将其引导至伪造的 Gmail 登录页面或 Google Meet 邀请页面，体现了攻击的隐蔽性和社交工程技巧的升级。

第三，中东亲美国家也成为伊朗网络攻击的目标。为震慑中东亲美国家并在与相关国家的地缘政治竞争中占据主动，伊朗也对沙特等阿拉伯国家发动网络攻击。据美国特雷利克斯网络安全公司（Trellix）2024 年 9 月 19 日发布的《伊朗的网络能力》（The Iranian Cyber Capability）专题报告，在 2012 年与 2016 年，沙特阿美石油公司两次遭受“沙蒙”（Shamoon）病毒攻击，黑客组织利用恶意软件永久擦除或破坏数据，导致总共 3.5 万台计算机数据被销毁。据称，此次网络攻击是由伊斯兰革命卫队网络战分支实施。2019 年，伊朗黑客还袭击了阿联酋、卡塔尔和科威特等海湾邻国的多家私营企业，旨在窃取公司机密并清除计算机数据。此次攻击还波及了全球 200 多家石油和天然气及重型机械公司，数千人受到影响。

四、伊朗网络安全能力建设的成效评估

伊朗虽然试图通过综合手段改善其网络安全态势，但不断遭受大规模网络袭击的事实表明，伊朗的网络安全建设仍存在较为明显的不足。目前，已经有多个组织尝试对伊朗的网络安全建设的成效进行量化评估。其中，英国智库国际战略研究所（IISS）2021 年 6 月发布的《网络能力与国家力量的总体评估》（Cyber Capabilities and National Power：A NetAssessment）报告显示，伊朗的网络能力在 15 个参评国中位列第三梯队，被认为在网络能力建设上存在显著缺陷。2022 年 9 月，哈佛贝尔弗科学与国际事务中心（Belfer Center for Science and International Affairs）发布的《2022 年国家网络空间能力指数》（National Cyber Power Index 2022）报告显示，伊朗的网络能力有了明显提高，总体排名在 30 个国家中位列第 10，但这主要是源于该国在网络监视与网络攻击领域的较高得分。该国网络防御能力仅位列第 28。国际电信联盟（ITU）发布的《全球网络安全指数 2024》（Global Cybersecurity Index 2024）显示，伊朗网络安全指数位于第三层级，表明其总体仍处于网络安全体系建设的基础阶段，并在技术、能力建设、协同合作领域存在明显短板。这些不同机构的评估结果虽存在差异，但都揭示了一个核心问题，即伊朗在网络监视与网络攻击方面具备一定优势，却在网络防御体系、制度建设与协同能力上存在明显短板。这些短板不仅体现在模型分析中，还多次体现在安全事件中。这些不足主要体现在政策体制与技术条件两个层面。

第一，在政策层面，伊朗目前尚未颁布国家级别的网络安全战略且政府各部门间协作效能低下。虽然伊朗已经成立了以网络空间最高委员会为代表的领导部门，但 14 个网络相关部门包括革命卫队、情报部、网络警察等都缺乏统一指挥链，导致协同失效；国家网络防御中心（NCDC）协调能力有限，实战指挥权模糊。在具体部门的分工上，伊朗的网络安全职能分散在伊斯兰革命卫队、情报部、“费塔警察”等多个机构中。这些机构存在明显的职能重合，大幅降低了伊朗对网络突发威胁的反应速度。

第二，在技术层面，伊朗的网络能力存在深层次的系统性缺陷，主要体现在三大相互关联的维

度。一是在技术自主性方面，伊朗面临严重的硬件与核心技术依赖困境。其网络战硬件约 90% 依赖西方进口，因遭到制裁被迫通过黑市获取二手设备，导致供应链存在后门风险。同时，伊朗被彻底排除在全球先进芯片供应链之外，7nm 以下制程芯片几乎无法获取。时至今日，伊朗的民用设备仍严重依赖 Windows 系统，而军用操作系统则多基于修改版 Linux，因此易受定向攻击。同时，尽管伊朗在量子加密领域取得关键突破，但其实际进展也存在一定程度的虚假宣传。例如，该国 2023 年被曝出重大技术造假，其声称的世界首个“量子处理器主板”实为 Zynq-7000 开发主板。二是攻击能力呈现初级化与低效特征。攻击手段多集中于钓鱼邮件、DDoS 等低阶方式，缺乏高级可持续威胁（APT）能力；自研恶意软件主要利用已知漏洞，被检测率高，实际攻击效果有限。近年来，伊朗大规模使用人工智能网络攻击工具，在一定程度上提升了其网络攻击的规模、速度和隐蔽性，但其高度依赖已知漏洞的技术路径仍未发生质变。同时，其对人工智能工具的使用也为防御方进行溯源分析和干扰提供了关键切入点。三是关键基础设施防护尤其薄弱。其中，伊朗的工业控制系统的物理操作网与办公互联网未进行有效隔离的问题尤为突出。这一致命弱点已被以色列等地缘对手反复利用，多次对伊朗发动攻击并对其造成巨大损失。

五、结语

作为中东地缘政治的关键参与者，伊朗的网络安全态势呈现出防御能力滞后与进攻性反制并存的复杂局面。长期以来，伊朗因有争议的核计划以及与美以等国的地缘政治冲突，成为网络攻击的重要目标。在“震网”等攻击事件后，伊朗成立网络空间最高委员会、网络防御司令部等机构，并通过“数字堡垒”项目强化技术防御。然而，因受制于技术代差、部门协同低效、量子加密等前沿技术工程化滞后及供应链安全风险等因素，伊朗网络防御存在显著漏洞，在高级持续性威胁应对方面处于被动地位。

伊朗在防御的同时，也积极发动网络反击，导致网络安全问题外溢，对地区乃至全球安全构成潜在威胁。在中东层面，伊以网络对抗呈现“物理—网络”混合战争趋势。人工智能工具在攻击中的大规模应用成为新特点。同时，伊朗黑客组织对沙特阿美、阿联酋私营企业的攻击，加剧海湾国家对“伊朗威胁”的认知，推动阿拉伯国家与以色列深化网络安全合作，进一步固化地缘对立格局。

从信息安全技术与政策实践的核心视角观察，伊朗案例深刻揭示了地缘政治冲突如何成为网络攻防的催化剂。一方面，持续的地缘政治压力迫使伊朗在技术受限的条件下，通过逆向工程与本土化创新发展非对称网络战能力。其针对工业控制系统的防护技术与攻击手段均带有鲜明地缘博弈色彩。当前，伊朗正积极将人工智能工具武器化，提高攻击效率和规模。尽管这并未解决其基础技术代差问题，但仍标志着其网络战能力进入了一个新阶段。另一方面，伊朗与美以等国的网络攻防实践暴露出当前国际网络安全治理的碎片化特征，如攻击溯源困难、责任认定模糊等问题，且人工智能的融入进一步加剧了这些问题。

伊朗的实践为全球网络安全治理提供了双重警示。一是技术自主性是发展中国家抵御地缘政治驱动型网络威胁的基础，但单纯依赖逆向工程难以弥合与先进国家间的代差，需通过国际技术合作与知识共享构建可持续防御体系。在新的技术态势下，防御方在强化基础技术自主可控的同时，也必须加速发展人工智能赋能的主动防御、威胁狩猎和深度伪造检测能力。二是国际社会亟须建立基于地缘政治平衡的网络空间规则框架，明确攻击溯源、责任认定与冲突升级的量化标准，防止网络武器成为地缘冲突中“非对称战略武器”。该框架必须前瞻性地考虑人工智能技术融入网络战带来的新风险，制定相应的行为规范、技术验证和问责机制。唯有将技术治理与地缘政治现实相结合，才能避免网络安全沦为大国博弈的牺牲品，真正实现全球网络空间的稳定与安全。【本文系国家社会科学基金青年项目“海上恐怖主义及其治理研究”（项目编号：21CGJ009）阶段性研究成果】

（本栏编辑：王丹娜）