伊朗与以色列网络空间冲突的演进、动因及影响*

陈　瑶

内容提要　自伊朗遭受2010年“震网”网络攻击以来，伊朗与以色列在网络空间的攻防冲突日益激烈、已进入白热化阶段，且成为双方战略对抗的新形式之一。伊、以在网络空间展开激烈的攻防能力竞赛，网络攻击增加且造成了现实破坏性结果。网络空间“进攻占优”的特性使得伊、以能够运用网络技术手段来实现各自战略对抗目标。网络冲突不会引发大规模军事报复以及缺乏国际社会监管，又有助于约束冲突烈度，促使双方不断加强在网络空间的攻防对抗。伊朗与以色列在网络空间部分地实现了对抗目标，但网络冲突加剧则促推双方战略对抗升级、深化双方之间的安全困境与对立状态；双方在网络空间冲突过程中提高了军事体系信息化水平、加强与域外大国网络合作、在地区构建网络攻防体系，增加了自身可运用的军事力量和手段。伊、以网络空间冲突与现实军事对抗相结合的“混合战争”趋势日益明显。

关 键 词　网络空间冲突　伊朗　以色列　国家安全　“混合战争”

作者简介　陈瑶，上海外国语大学国际关系与公共事务学院、中东研究所2021级博士研究生。

信息技术重塑了现代国家间的冲突和战争形态，日益加剧的网络空间冲突对传统安全和常规战争理论提出了挑战。“网络冲突”是指出于恶意或破坏性目的使用计算机技术来影响或改变国家间外交和军事的互动行为。① “网络

* 本文系2023年度国家社科基金项目“近年来伊朗面临的社会稳定挑战、政府应对及其启示研究”（23BZZ102）的阶段性成果。

① Valeriano Brandon and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in The International System*, New York: Oxford University Press, 2015, p. 32.

战”则是“网络冲突”的升级形式，指“一国渗透另一国计算机或网络以造成损害或破坏的行为”①，具有由国家行为体主导、出于政治意图、会造成现实破坏等特征。相比于现实军事冲突，在网络空间的冲突不受国家边界限制、不涉及占领领土或攫取物质资源的目标与行为，也不使用可能造成人员伤亡的暴力手段，冲突主体一般是黑客组织等非国家行为体或个人而非国家军队。总体而言，当前网络空间冲突更多是作为军事对抗的一个组成部分或军事冲突前的准备和升级阶段，兼具收集情报、干扰对手和制造轻度破坏等功能。而对网络攻击归因困难、“网络武器”向非国家行为体和个人加速扩散等问题也增加了国家间关系的不确定性。网络安全问题和军事冲突或其他非传统安全问题相互交织，形成综合性的安全挑战，深刻影响了各国的国家安全观和全球安全形势走向。网络空间冲突已经成为伊朗与以色列相互对抗的新形式。随着伊朗核问题发酵和中东地缘政治矛盾激化，伊朗与以色列关系不断恶化，双方对抗和冲突烈度有所上升。作为中东地区网络攻防能力突出的两个国家，以色列与伊朗将网络空间作为双方相互对抗的新前线。自 2010 年“震网”（Stuxnet）网络攻击事件发生以来，伊朗与以色列的网络攻防能力快速增长，双方在网络空间的攻防冲突日趋激烈，且出现了越来越多的网络攻防事件。

学界对于伊朗与以色列之间的网络空间对抗研究仍处于起步阶段，现有研究侧重梳理伊朗与以色列的网络攻防能力发展历程，解读两国的网络空间战略和介绍两国网络能力情况。② 另有部分研究者分析了伊朗开展对外网络活动的目标、手段等，但是主要关注伊朗与美国的网络空间冲突问题。詹姆斯·P. 法威尔（James P. Farwell）和达比·阿拉克利安（Darby Arakelian）认为，

---

① Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Collins, 2010, p. 6.

② See Ali Burak Daricili, “Analysis Of Iran's Cyber Security Strategy With Regard To The Attack And The Defense Capacity”, *Turkish Studies – Social Sciences*, Vol. 14, No. 3, 2019, pp. 409 – 425; Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*, Carnegie Endowment for International Peace, January 4, 2018; Michael Eisenstadt, *Iran's Lengthening Cyber Shadow*, Research Notes of the Washington Institute for Near East Policy, No. 34, July 2016; Matthew Cohen, Charles D. Freilich and Gabi Siboni, “Israel and Cyberspace: Unique Threat and Response”, *International Studies Perspectives*, Vol. 17, No. 3, 2016, pp. 307 – 321; Dmitry (Dima) Adamsky, “The Israeli Odyssey toward Its National Cyber Security Strategy”, *The Washington Quarterly*, Vol. 40, No. 2, 2017, pp. 113 – 127; 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 35 ~ 43 页；艾仁贵：《以色列的网络安全问题及其治理》，载《国际安全研究》2017 年第 2 期，第 66 ~ 89 页等。

伊朗将把进攻性网络能力作为实现其激进对外政策的工具之一。[①] 蒂姆·毛瑞尔（Tim Maurer）指出伊朗在网络空间通过“代理人”实施网络攻击，伊朗与“叙利亚电子军”之间的代理人关系属于较为松散的编配模式（orchestration model）。[②] 对于伊、以在网络空间的互动，维罗尼卡·勒托利卡（Veronika Netolická）和米罗斯拉夫·马里斯（Miroslav Mareš）则基于网络攻防能力发展情况，提出伊朗与以色列并非在网络空间进行军备竞赛，只是双方各自发展网络能力的必然过程。[③] 卢卡·罗萨（Luca Losa）运用定量分析方法，得出伊、以之间日益加剧的网络空间冲突不会改变双方目前力量平衡与对抗状态的结论。[④] 总体看，上述研究更多关注伊、以网络冲突本身，但忽视了两国在现实世界中的对抗升级才是网络空间冲突加剧的根源。人类社会由网络空间和物理空间构成，物理空间在信息化过程中向网络空间映射，网络空间也反过来影响和改造物理空间。[⑤] 因此，观察伊朗与以色列在网络空间的冲突，需要从现实的物理空间中寻求根源和探究影响。从网络空间与物理空间的互动角度分析伊、以网络空间冲突的演化、动因和影响，可为理解双方战略对抗提供新视角。此外，作为目前最显著和激烈的一对网络空间对抗关系，探讨伊朗与以色列网络冲突对中国的网络空间防御和安全治理具有一定的参考意义。

本文试图探究两个问题：一是为什么伊朗与以色列的相互对抗会向网络空间延伸并不断加剧？二是日益激化的网络空间冲突将如何影响伊、以两国的现实战略对抗？本文首先梳理自 2010 年“震网”攻击事件以来伊、以网络空间冲突的阶段性演化及特点，在分析双方战略对抗目标和特征的基础上探讨网络空间冲突成为伊、以对抗新形式的原因，最后阐述网络空间冲突激化对伊、以两国对抗的影响。由于网络空间攻防冲突具有高度的隐蔽性和复杂性，本文仅将已经被公开披露且被普遍认为是由伊朗或以色列实施的网络攻

---

① James P. Farwell and Darby Arakelian, “What Does Iran’s Cyber Capability Mean for Future Conflict?”, *The Whitehead Journal of Diplomacy and International Relations*, Vol. 14, No. 1, 2013, pp. 49 – 65.

② Tim Maurer, *Cyber Mercenaries: The State, Hackers and Power*, Cambridge University Press, 2018.

③ Veronika Netolická and Miroslav Mareš, “Arms Race ‘in cyberspace’ – A Case Study of Iran and Israel”, *Comparative Strategy*, Vol. 37, No. 5, 2018, pp. 414 – 429.

④ Luca Losa, “The Impact of Cyber Capabilities on the Israeli – Iranian Relationship”, Master Thesis, Charles University, 2020.

⑤ 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 22 ~ 23 页。

防事件作为研究样本。

一 伊朗与以色列网络空间对抗的演化

以色列和伊朗是中东地区最早接入国际互联网的两个国家，信息化水平处于地区领先地位。2010 年“震网”网络攻击事件发生后，伊朗与以色列在网络空间的冲突对抗呈现长期化和常态化特点，具体可以划分为 3 个阶段。

（一）起始阶段

“震网”网络攻击事件开启了伊朗与以色列在网络空间持续对抗的序幕。2010 年 6 月，伊朗发现境内计算机遭受“震网”蠕虫病毒攻击，超过 3 万台个人计算机被感染，多处重要的核燃料浓缩过程中使用的数据采集与监视控制系统（SCADA）设备受影响。其中，纳坦兹核设施内部约有 1 000 台离心机受损，专家估计此次网络攻击导致伊朗的核计划进度至少推迟两年。[①] “震网”病毒结构设计复杂，利用 4 个“零日漏洞”（zero - day vulnerabilities）攻击纳坦兹核设施的数据采集与监视控制系统，通过提高运转速度来损坏离心机，它标志着“网络武器”被首次使用。[②] 由此不难看出，“震网”事件是一起针对伊朗核设施有预谋、大规模的网络攻击，而只有信息技术高度发达的国家行为体才具备研发和投放“网络武器”的能力。因此，外界认为对伊朗核问题反应强烈的美国与以色列实施了此次攻击，甚至有报道称以色列曾在迪莫纳设施内试验“震网”病毒的有效性。[③]

此后，伊朗的核设施、能源部门以及战略工业部门开始频繁遭到外来网络攻击。2011 年 11 月，伊朗布什尔核电站的计算机发现感染用于窃取信息的“毒区”（Duqu）蠕虫病毒。2012 年 6 月，伊朗石油部和数家石油公司的网络系统遭到结构更为复杂、破坏性更强的“火焰”（Flame）蠕虫病毒感染，当

① Yaakov Katz，“‘Stuxnet Virus Set Back Iran’s Nuclear Program by 2 Years’”，*The Jerusalem Post*，December 15，2010，https：//www. jpost. com/Iranian - Threat/News/Stuxnet - virus - set - back - Irans - nuclear - program - by - 2 - years，2022 - 01 - 14.

② James P. Farwell and Rafal Rohozinski，“Stuxnet and Future of Cyber War”，*Survival*：*Global Politics and Strategy*，Vol. 53，No. 1，2011，p. 31.

③ William J. Broad，John Markoff and David E. Sanger，“Israeli Test on Worm Called Crucial in Iran Nuclear Delay”，*The New York Times*，January 15，2011，https：//www. nytimes. com/2011/01/16/world/middleeast/16stuxnet. html，2022 - 06 - 10.

局被迫暂时断开与关键石油设施的网络连接。由于“毒区”和“火焰”病毒的结构以及运行方式都与“震网”病毒类似，专家认为是美国和以色列再次合作对伊朗进行了网络攻击。①

“震网”攻击首次展示了数字信息技术对物理空间的破坏性影响，对于伊、以网络空间冲突乃至全球网络安全领域都具有重大意义。在此阶段，以色列与美国合作主动对伊朗发起网络攻击，企图通过网络攻击来控制伊朗核设施和关键工业设施的信息化操作系统并造成现实破坏，可被认为是以色列和美国在网络空间实施的武力行为。而伊朗此时受到网络技术和能力限制，基本无法防御、追溯和报复来自两国的网络攻击行为。

（二）升级阶段

伊朗在遭受一连串网络攻击后开始高度重视网络安全问题，迅速推进网络安全治理能力建设，与以色列展开网络能力竞赛。其一，形成以最高领袖为核心的网络安全治理架构。在受到“震网”攻击 5 个月后，伊朗政府设立了“网络防御司令部”（Cyber Defense Command）。2012 年 3 月，由哈梅内伊领导的网络空间最高委员会（Supreme Council of Cyberspace）成立，其成员都是来自议会、革命卫队和政府机构的高层人物，负责制定伊朗的网络空间政策，统筹和领导各组织的一切网络行动。其二，通过革命卫队、“被动防御组织”“巴斯基”民兵等各层级军事组织开展网络空间活动。以巴斯基为例，该组织的基层性特征②使其能够通过与高校之间的紧密联系来招募网络技术人才，该组织甚至宣称其拥有 12 万名网络战志愿者③，主要负责应对外来网络攻击和监管国内民众的网络活动。其三，增加对网络信息通信技术的资金投入。2013 年 8 月鲁哈尼总统就职后，伊朗的网络安全财政预算额大幅增长，2015 年达到 5 500 亿里亚尔（约合 1 980 万美元），较 2013 年增长超过 12 倍。④

伊朗的网络攻防能力在短时间内实现了突破性增长，成为网络空间中最

---

① Valeriano Brandon and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in The International System*, p. 26.

② 王国兵：《伊朗巴斯基民兵的历史嬗变与转型》，载《阿拉伯世界研究》2019 年第 1 期，第 35 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, 2022-01-15.

④ “Iranian Internet Infrastructure and Policy Report - Special Edition the Rouhani Review (2013-15)”, *Small Media*, February 2015, p. 7, https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb15.pdf, 2021-12-12.

活跃的国家之一。一方面，伊朗的自主网络安全防御能力进入体系化发展阶段。2019 年 5 月，伊朗首次公开用于保护公共基础设施的“数字堡垒”（Dajfa）网络安全项目，并称该项目在 2018 年就成功拦截了多达 3 300 万次网络攻击。① 另一方面，伊朗的进攻性网络能力迅速增长，有关其对外实施网络攻击的报告不断增多。其中，最突出的一起是伊朗被指利用黑客组织在 2012 年 8 月使用“沙蒙”（Shamoon）蠕虫病毒攻击沙特阿美、卡塔尔拉斯等能源公司的计算机系统，导致阿美公司销毁近 3.5 万台计算机。② 代号为“APT33”“APT34”“APT35”“APT39”等大量伊朗黑客组织开始活跃于网络空间。③ 其中，“伊朗网络军”“马布纳研究所”（Mabna Institute）和“纳斯尔研究所”（Nsar Institute）等被认为与革命卫队存在关联④，但伊朗政府从未承认上述黑客组织具有官方背景。

以色列在“震网”事件后也进一步发展了网络攻防能力，以应对日益恶化的网络安全环境，并维持对伊朗的技术优势。一方面，完善网络空间治理架构以及网络安全战略顶层设计。以色列在 2011 年通过了提高网络空间能力的决议，成立了国家网络管理局（INCD），并于 2015 年 6 月宣布建立整合各机构网络能力的网络司令部。2017 年 9 月，以色列通过首个《国家网络安全战略》，将网络安全治理行动分为稳健性（Robustness）、韧性（Resilience）和防御性（Defense）3 个层次。⑤ 另一方面，以色列在网络空间奉行“积极防御”政策⑥，继续加强网络攻防能力建设。政府、军方、企业和学术界在网络

① “Iran Foiled 33mn Cyberattacks in Past Year: ICT Min”, *Mehr News Agency*, October 29, 2019, https://en.mehrnews.com/news/151709/Iran-foiled-33mn-cyberattacks-in-past-year-ICT-min, 2022-01-13.

② Nicole Perlroth, “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back”, *The New York Times*, October 23, 2012, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, 2022-01-13.

③ “APT”组织是网络安全公司对于实施高级持续性威胁（“APT”攻击）的黑客组织的代称。“APT”攻击是指对特定目标进行持续针对性网络攻击，目的是窃取信息和实施破坏，需要长达数月或者数年的时间进行。因此，一般认为“APT”攻击是由国家行为体支持、有组织的网络攻击活动，也会认为“APT”组织受到国家政府直接或间接的支持。

④ Congressional Research Service, “Iranian Offensive Cyberattack Capabilities”, January 13, 2020, https://crsreports.congress.gov/product/pdf/IF/IF11406/2, 2022-01-13.

⑤ Israel National Cyber Directorate, *Israel National Cyber Security Strategy in Brief*, September, 2017.

⑥ 罗天宇：《以色列网络安全建设及其启示》，载《信息安全与通信保密》2022 年第 6 期，第 15~16 页。

安全信息共享、人才培养、防御行动等方面的合作，成为以色列增强网络能力的核心路径。以色列提出在网络空间打造“铁穹”系统应对日常网络安全威胁，国防军下属的指挥、控制、通信、计算机与情报（C4I）部门和网络防御部门承担防御攻击和技术人员培训任务，超过430家以色列网络安全公司①在识别和追踪网络攻击方面发挥了至关重要的作用。同样隶属于以色列国防军的“最强大脑”——“8200部队”则是该国对外实施进攻性网络活动的主体，国防军在2012年宣布将其人员规模扩大一倍，并建立了专项行动办公室。②

随着伊朗网络攻防能力的发展，伊朗开始主动对以色列实施网络攻击，双方在网络空间相互攻击和报复的频次明显上升。伊朗情报部长海达尔·莫斯莱希（Heydar Moslehi）在2012年6月称，伊朗受到由美国、以色列和英国实施的大规模网络攻击。③ 内塔尼亚胡也公开表示，以色列的电力、水利、银行等基础设施受到来自伊朗及其盟友不间断的网络攻击。④ 不过，伊朗与以色列政府都未公开承认向对方实施了网络攻击活动。在这一阶段，以色列开始单独对伊朗实施以造成现实破坏为导向的网络攻击，主要使用蠕虫病毒、木马程序等恶意软件，攻击目标依然集中在核设施、关键基础设施和政府部门。而伊朗对以色列的网络攻击活动主要使用分布式拒绝服务（DDoS）攻击⑤和勒索软件攻击，旨在使网站运行瘫痪、实现经济勒索和窃取信息；攻击的对象多样，但更多瞄准政府部门网站和企业等私营部门，鲜有攻击以色列军事

① “Cybersecurity Startup Exits in Israel Total to US $ 11.3 Billion：IVC Report”，*CISOMAG*，January 21，2020，https：//cisomag.eccouncil.org/cybersecurity-startup-exits-in-israel-total-to-us11-3-billion-ivc-report，2022-02-08.

② Richard Silverstein，“IDF To Double Unit 8200 Cyber-War Manpower-OpEd”，*Eurasia Review*，October 24，2012，https：//www.eurasiareview.com/24102012-idf-to-double-unit-8200-cyber-war-manpower-oped，2022-06-10；Yaakov Katz，“Elbit Unveils New Cyber War Simulator”，*The Jerusalem Post*，June 5，2012，https：//www.jpost.com/Defense/Elbit-unveils-new-cyber-war-simulator，2022-06-10.

③ “Iran Says Detected ‘Massive Cyber Attack’：State TV”，*Reuters*，June 22，2012，https：//www.reuters.com/article/us-iran-cyber-nuclear/iran-says-detected-massive-cyber-attack-state-tv-idUSBRE85K1EA20120621，2022-03-01.

④ “Iran Ups Cyber Attacks on Israeli Computers：Netanyahu”，*Reuters*，June 9，2013，https：//www.reuters.com/article/us-israel-iran-cyber-idUSBRE95808H20130609，2022-03-01.

⑤ 分布式拒绝服务（DDoS，Distributed Denial of Service）攻击，指借助于客户或服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动攻击，从而成倍地提高拒绝服务攻击的威力。

系统或基础设施的报告。2018 年 7 月，伊朗黑客组织（Charming Kitten）被指试图通过冒充以色列网络安全公司（ClearSky）的网站来窃取用户信息。[①] 不过，由于以色列网络防御能力突出，伊朗黑客组织的网络攻击能造成的破坏和影响相对有限。

（三）白热化阶段

伊朗与以色列相互网络攻击的对象从核设施、军事设施和政府部门扩展至民用基础设施，标志着双方在网络空间的对抗进一步激化。有报道称，伊朗在 2020 年 4 月对以色列的几处水处理设施发起了网络攻击，试图控制系统以提高自来水的氯含量，以方称在及时拦截后并未造成太大影响。作为报复，以色列被指在同年 5 月初报复性攻击了伊朗南部阿巴斯港沙希德·拉吉（Shahid Rajaee）码头的计算机系统，导致该码头的航运服务瘫痪数日。[②] 以色列国家网络安全局负责人伊加尔·温纳（Yigal Unna）称，“‘网络寒冬’即将到来，甚至比我们的设想来得更快”。[③]

伊朗与以色列在网络空间的冲突频率和烈度不断上升。以色列对伊朗的网络攻击与伊朗核问题走向高度相关。2020 年 6～7 月，伊朗纳坦兹核设施和多处重要的基础设施接连发生爆炸事故，造成核设施内部分精密仪器受损，但伊朗方面否认爆炸是由以色列网络攻击引发的说法。2021 年 4 月，恢复履行《伊核全面协议》谈判进入关键节点，伊朗纳坦兹核设施的电力系统遭到网络攻击，导致一部分离心机损坏，伊朗指责以色列实施攻击。[④] 与此同时，以色列也开始增加对伊朗民用基础设施的网络攻击。2021 年 7 月和 10 月，伊朗铁路系统和加油站的智能系统先后遭到网络攻击，而且都显示出“网络攻击 64411”的内容，而“64411”正是哈梅内伊办公室的热线号码。总统莱希

---

① Oded Yaron，“Iranian Hackers Tried to Impersonate Israeli Cyber－security Company”，*Haaretz*，July 9，2018，https：//www. haaretz. com/israel－news/2018－07－09/ty－article/. premium/iranian－hackers－break－into－israeli－cybersecurity－site/0000017f－e0cd－df7c－a5ff－e2ffcc280000，2022－01－20.

② Joby Warrick and Ellen Nakashima，“Officials：Israel Linked to a Disruptive Cyberattack on Iranian Port Facility”，*The Washington Post*，May 18，2020，https：//www. washingtonpost. com/national－security/officials－israel－linked－to－a－disruptive－cyberattack－on－iranian－port－facility/2020/05/18/9d1da866－9942－11ea－89fd－28fb313d1886_story. html，2022－01－20.

③ “National Cyber Directorate Head：Cyber Winter Is Coming”，*Israel Defense*，May 28，2020，https：//israeldefense. co. il/en/node/43267，2021－12－19.

④ Jon Gambrell，“Iran Blames Israel for Sabotage at Natanz Nuclear Site”，*AP News*，April 13，2021，https：//apnews. com/article/world－news－israel－iran－62a7aa3182992ed0f97b5486d71280c2，2022－04－18.

指责美国和以色列发动攻击旨在给伊朗制造社会混乱。[①] 伊朗黑客组织主动对以色列目标实施网络攻击的报告也有所增加。分析显示，自 2020 年 9 月以来，伊朗黑客组织平均每 6～8 周就会启动一次勒索软件攻击，目标包括美国、欧洲国家和以色列等。[②] 据报道，伊朗—黑客组织（Pay2Key）仅在 2020 年 11～12 月期间就渗透和攻击了包括航空航天工业公司在内的 80 家以色列企业。[③]

伊朗与以色列之间的网络冲突日益公开化。政府相关部门一般会模糊处理网络攻击事件，被攻击方否认遭到网络攻击或单方面指认他国实施攻击，被指控的攻击方则倾向保持沉默。现阶段，伊、以官方和媒体频繁指责对方发动网络攻击。以色列时任国防部长本尼·甘茨（Benjianin Gantz）公开指责伊朗黑客组织是“使用键盘的恐怖分子”，称伊朗每年对以色列目标进行 1 000多次网络攻击。[④] 2021 年 4 月，以色列媒体报道摩萨德对伊朗核设施发动网络攻击，军方罕见地没有审查相关内容，有观点认为这是以方承认网络攻击伊朗的信号。[⑤] 伊朗政府也开始承认遭受严重网络攻击，并强调其具备防御网络攻击和实施报复的能力。伊朗外交部发言人塞伊德·阿巴斯·穆萨维（Seyed Abbas Mousavi）称，2020 年 3 月以来对伊朗国内基础设施的大规模网络攻击都是由外国政府支持和实施的。[⑥] 伊朗媒体对网络攻击的报道增多，法尔斯通讯社（Fars News Agency）甚至在 2021 年 11 月和 2022 年 5 月先后

---

① Jon Gambrell and Nasser Karimi, “Iran's President Says Cyberattack Meant to Create 'Disorder'”, *AP News*, October 28, 2021, https://apnews.com/article/technology-business-dubai-united-arab-emirates-economy-9d2c1fc46afaec9b5b9ec7433acd4ce1, 2022-04-18.

② “Evolving Trends in Iranian Threat Actor Activity - MSTIC Presentation at Cyberwarcon 2021”, Microsoft, November 16, 2021, https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021, 2022-04-18.

③ Amitai Ziv, “Iranian Hackers Hit 80 Israeli Firms as Massive Cyberattack Continues”, *Haaretz*, December 16, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-16/ty-article/.premium/iranian-hackers-hit-over-80-israeli-firms-as-massive-cyberattack-continues/0000017f-e48b-d804-ad7f-f5fbbeeb0000, 2022-07-10.

④ David Rosenberg, “Gantz: Iran's 'Terrorists with Keyboards' Waging Cyber War on Israel”, *Israel National News*, June 29, 2022, https://www.israelnationalnews.com/news/355712, 2022-07-20.

⑤ Martin Chulov, “Israel Appears to Confirm It Carried Out Cyberattack on Iran Nuclear Facility”, *The Guardian*, April 12, 2021, https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility, 2021-12-19.

⑥ “Spokesman: Iran to Take Countermeasures Against Cyberattacks”, *Fars News Agency*, July 23, 2020, https://en.farsnews.ir/newstext.aspx?nn=13990502000376, 2020-08-22.

公布了 3 名长期针对伊朗实施网络攻击的以色列技术专家资料。[①] 双方日渐公开化的网络冲突与舆论战相结合，由此给对手制造社会恐慌、散播虚假信息和宣传意识形态的效果更为突出。

随着网络冲突日渐白热化，伊朗与以色列的网络能力竞赛进一步加剧。以色列依然是中东地区网络技术最先进的国家，但伊朗在“震网”攻击后的十年间实现了网络攻防能力的快速增长。根据英国智库国际战略研究所（IISS）对 15 个国家网络能力的排名，仅有美国属于第一梯队，以色列位于第二梯队，而伊朗则处于第三梯队。[②] 美国哈佛大学贝尔福研究中心发布的“2020 年国家网络能力指数”显示，以色列与伊朗的综合网络能力在 29 个国家中分别排名第 11 位和第 23 位；在进攻性网络能力方面，以色列排名第六，伊朗则排在第八位；在网络防御能力方面，以色列排在第 23 位，伊朗排在最后一位。[③] 虽然伊朗网络能力的发展受到信息通信设备短缺、基础设施建设滞后和西方有关制裁措施限制的严重制约，但其从外来网络攻击中不断积累技术并提高自身的网络攻防能力，这也意味着以色列在网络空间的技术优势开始呈现相对下降趋势。

二　伊朗和以色列对抗向网络空间延伸的动因

伊朗与以色列在网络空间冲突的阶段性变化与伊以关系的演进具有内在联系，即现实世界的对抗激化导致双方在网络空间的冲突加剧。需要明确的是，网络空间冲突是伊、以战略对抗的一种重要表现形式，是现实对抗在新技术领域和虚拟空间的延展，并非独立的新型对抗关系。信息技术进步和网络空间的特殊性促使伊、以战略对抗向网络空间延伸，网络冲突形式与双方战略对抗的目标和原则匹配，因此成为双方获取战略优势的新竞争领域。

---

① 《披露犹太复国主义政权高级网络间谍官员的身份和照片》（波斯文），https：//www. farsnews. ir/news/14000825000893，2022 - 07 - 20；《只能秘密生活的犹太复国主义者》（波斯文），https：//www. farsnews. ir/news/14010303000754，2022 - 07 - 20.

② The International Institute for Strategic Studies，*Cyber Capabilities and National Power*：*A Net Assessment*，June 2021，pp. 9 - 12.

③ Julia Voo etc.，*National Cyber Power Index 2020*，Belfer Center for Science and Foreign Affairs，September 2020，pp. 11 - 12.

（一）伊以战略对抗的目标与特征

1979 年伊朗伊斯兰革命后，伊朗与以色列受到意识形态和地缘政治两大因素影响，长期处于互相敌视的状态。[①] 伊朗恢复核研究活动以及对哈马斯和黎巴嫩真主党的支持，导致伊、以紧张关系进一步加剧，以色列开始将伊朗视为首要生存威胁。中东剧变以来，地区安全秩序和国家间力量对比出现重大变动，伊朗不断扩大在地区的军事存在和影响力，伊、以对抗转向战略层面。2015 年 8 月，以色列国防军首次发布官方战略文件，指出以色列需要在战略层面回应伊朗及其支持的武装组织所造成的威胁。[②]

核问题、弹道导弹和地区代理人是现阶段以色列认知来自伊朗的三大安全威胁。以色列竭力阻止伊朗获得核武器和发展核能力，一方面谋求美国及国际社会维持和增加对伊朗的制裁，另一方面通过破坏核设施、暗杀核科学家等方式来阻碍伊朗推进核计划。相比于核能力，伊朗的中程弹道导弹射程可以覆盖以色列全部重要城市，受其资助的黎巴嫩真主党和哈马斯频繁袭击以境内目标，是对以色列本土更为严重和迫切的直接安全威胁。伊朗及其代理人的武装力量介入叙利亚并向戈兰高地渗透，刺激以色列产生强烈的不安全感并开始空袭叙利亚、黎巴嫩乃至伊拉克境内的伊朗以及真主党军事目标，伊、以对抗烈度上升。由此可以看出，以色列对伊朗政策的核心是阻止伊朗现政权获取核武器，并遏制伊朗继续在地区扩张影响力和军事存在，通过限制和削弱伊朗的军事实力谋求实现自身安全最大化。

同以色列竞争是伊朗谋求地区大国地位战略的重要组成部分。虽然伊朗否认以色列的国家存在并声称要彻底摧毁后者，但更多是将反美、反以作为团结和引领伊斯兰世界的一种意识形态，希望通过坚持反犹太复国主义来确立其在伊斯兰世界的领导地位。美以特殊关系是伊朗现政权敌视以色列的原因之一，此前伊朗对以色列政策更多从属于其对美国的政策。中东变局后，伊朗通过“什叶派新月地带”“抵抗轴心”和“波斯湾文化圈”等提高在中东地区的战略地位。[③] 出于进一步提升在地区影响力的需要以及意识形态差

---

① 田文林：《伊朗与以色列对抗的根源及前景》，载《当代世界》2018 年第 8 期，第 56～59 页。

② The Belfer Center，“Deterring Terror：How Israel Confronts the Next Generation of Threats – English Translation of the Official Strategy of the Israel Defense Forces”，https：//www. belfercenter. org/sites/default/files/legacy/files/IDFDoctrineTranslation. pdf，2022 – 01 – 12.

③ 范鸿达：《伊朗提升区域战略地位的策略及前景》，载《当代世界》2020 年第 2 期，第 6～8 页。

异，伊朗对以色列采取了更加强硬的对抗态度。随着战略自主性不断上升，以色列对伊朗在地区活动的威慑和回应直接损害了伊朗的国家安全。伊朗事实上开始形成独立的对以色列政策，即在维护自身国家安全和政权稳定的基础上寻机与以色列对抗，构建相互威慑并继续扩大在中东地区的影响力。

现阶段，伊朗与以色列对抗的主要方式是构建相互威慑和追求相对战略优势，在多领域展开对抗且避免大规模直接军事冲突是两大核心原则。一方面，双方已经形成多领域、全方位的对抗格局，涉及安全、政治等高级政治层面以及经济、社会、文化等低级政治层面。[①] 其中，安全博弈是伊、以对抗的核心内容。伊朗通过发展核能力和运载工具体系构建核威慑，并依托代理人体系在地区提高政治影响力和军事存在。以色列则凭借经济资源、军事技术和以美同盟优势，通过现代化武器研发、情报获取以及与美国的安全合作来遏制伊朗核能力发展乃至影响力扩张。另一方面，双方在对抗中都意识到需要管控冲突烈度、避免陷入全面战争。伊朗与以色列的军事力量对比均衡，都不具备压倒性的战略优势。2022 年“全球火力指数”（Global Fire Power）显示，伊朗与以色列的军事实力在 142 个国家中分别排在第 14 位和第 18 位。[②] 以色列在国土面积、人口和战略纵深等方面处于劣势，伊朗则受到经济实力的限制，双方在现阶段都难以支撑长期大规模军事冲突或全面战争。摩萨德前主管埃夫莱姆·哈勒维（Efraim Halevy）曾断言，以色列对伊朗的军事打击可能将引发与伊朗几代人的战争。[③] 由此不难看出，虽然伊朗与以色列的相互对抗日益激烈，但是在短期内走向全面战争的可能性较低。

总体而言，伊朗与以色列相互对抗的战略目标和驱动力存在较大差异。以色列的对外行动出于追求国家绝对安全的考虑，在中东地区主要通过削弱对手来维持战略优势。伊朗的对抗逻辑则是服务于以攻为守、寻机对抗的地区战略，目前还处于发展实力、追求相对优势的阶段，更多通过展示潜在能力来构建威慑。由于双方力量对比较为均衡，伊、以对抗长期处于战略相持的僵局状态，都未能实现削弱或摧毁对方的目标。相反，伊朗不断提高在地

① 孙德刚：《以色列与伊朗关系评析》，载《现代国际关系》2009 年第 5 期，第 25～26 页。

② “Comparison of Israel and Iran Military Strengths（2022）”，*Global Fire Power*，https：//www.globalfirepower.com/countries-comparison-detail.php?country1=israel&country2=iran，2022-02-03.

③ Ari Shavit，“Former Mossad Chief：An Attack on Iran Likely to Foment a Generations-long War”，*Haaretz*，September 1，2012，https：//www.haaretz.com/2012-09-01/ty-article/ex-spy-chief-generations-of-war/0000017f-da84-d718-a5ff-fa8412a30000，2022-04-10.

区的影响力和军事存在，以色列与阿拉伯国家走近并形成“反伊朗”联盟。为了应对新的对抗态势，以色列前国防部长艾森科特提出通过“战争之间的行动”（Campaign Between Wars）战略来限制伊朗在地区的影响力，其中一个目标就是通过削弱和破坏对手的能力来拖延战争并威慑对手。[①] 双方转向隐蔽性更高的“影子战争”（shadow war），寻求在新技术和非常规军事领域确立战略优势并削弱对方实力，同时避免可能发生的大规模直接军事对抗，也意味着更容易滑向网络战等低烈度冲突形式。

（二）信息技术手段匹配伊朗和以色列对抗需求

网络空间本质上是从物理空间延伸和分化出来的虚拟空间，国家行为体在网络空间的互动形式由物理空间中的国家间关系主导。伊朗与以色列在网络空间对各自战略对抗目标进行了具象化和可操作化，运用网络技术手段来满足对抗需求，即通过网络攻击削弱对手实力、构建战略优势和释放威慑信号，从而影响和迫使对方改变政策和行为。

进入21世纪以来，网络空间迅速成长为继陆、海、空、太空之后的“第五大战略空间”。[②] 与物理空间中的攻防平衡不同，网络空间的“进攻占优”特性[③]事实上鼓励了国家行为体向对手实施先发制人的网络攻击，更有利于持续消耗和削弱对手实力。其一，网络攻击可以超越时空限制，“网络武器”只需要依托计算机和互联网就能实现有效投送，并且能够对他国的本土目标造成一定程度的现实破坏。其二，网络攻击还具有高度隐蔽性，病毒和木马程序甚至可以在入侵计算机系统后潜伏等待攻击指令，现有的网络防御技术在攻击开始前依然难以准确追踪，更无法干预和挫败渗透过程。其三，“网络武器”的更新迭代速度极快，虽然在遭到攻击后及时修复系统漏洞可以避免被二次攻击，但攻击方只需要修改计算机病毒的部分代码结构就可能实现绕过

① Gadi Eisenkot and Gabi Siboni，“The Campaign Between Wars：How Israel Rethought Its Strategy to Counter Iran’s Malign Regional Influence”，https：//www. washingtoninstitute. org/policy – analysis/campaign – between – wars – how – israel – rethought – its – strategy – counter – irans – malign，2022 – 02 – 03.

② Matt Murphy，“War in The Fifth Domain”，*The Economist*，July 1，2010，https：//www. economist. com/briefing/2010/07/01/war – in – the – fifth – domain，2022 – 04 – 10.

③ William J. Lynn III，“Defending a New Domain – The Pentagon’s Cyberstrategy”，*Foreign Affairs*，Vol. 89，No. 5，2010，pp. 97 – 108；Salma Shaheen，“Offense – Defense Balance in Cyber Warfare”，*Cyberspace and International Relations*，Springer，2014，pp. 77 – 93；Andrea Locatelli，“The Offense/Defense Balance in Cyberspace”，ISPI，Analysis No. 203，October 2013，https：//www. ispionline. it/sites/default/files/pubblicazioni/analysis_203_2013. pdf，2022 – 03 – 01.

防御系统识别再次攻击。这也意味着在网络空间中进攻的成本远低于防御的成本。据测算，“震网”攻击的攻防成本之比达到 1∶7.3，即攻击者每投入 1 美元进行攻击，伊朗就需要投入 7.3 美元用于防御。① 与此同时，网络攻击的破坏程度也在提高，一次网络攻击造成的平均经济损失已经高达 167 万美元。② 虽然各行为体在网络空间互动过程中会推进防御能力的增长并最终实现攻防平衡③，但是网络空间“进攻占优”的特性在短时间内不会出现根本变化。这一特性意味着伊朗与以色列只要投入相对较少的经济和军事资源，就可以达到破坏和削弱对方的目的，因此更适合双方进行长期的持续对抗。

以色列主动将与伊朗对抗引入网络空间，是为了将自身的技术优势转变为战略优势，弥补地理和人口要素的相对不足，谋求突破与伊朗的相持僵局。其一，可以通过网络攻击破坏伊朗核设施，以阻碍伊朗核计划推行。虽然以色列曾经通过大规模空袭的方式摧毁伊拉克和叙利亚的核设施，但由于伊朗的被动防御体系更加完善，且对任何攻击其核设施的行为“一报还一报”的态度非常明确④，以色列对伊朗核设施进行直接军事打击是不现实且极度危险的。因此，以色列开始寻求运用包括网络攻击在内的非常规军事手段破坏伊朗核设施，“震网”攻击就是第一次成功尝试。其二，通过网络攻击威慑伊朗收缩在中东地区旨在提升军事存在和影响力的活动。以色列国防军的安全战略文件指出，对于无共同边界的国家可以通过网络战来加强战略和战术层面的威慑。⑤ 除了攻击核设施外，以色列通过网络攻击破坏伊朗的能源、工业部门和民用基础设施，既展示了对伊朗本土实施隐蔽性直接打击的决心和能力，又能够扰乱伊朗的经济生产以及日常生活来诱发内部危机并对其进行牵制。

---

① Patrick J. Malone, *Offense – Defense Balance in Cyberspace: A Proposed Model*, Master Thesis, Naval Postgraduate School, December 2012, pp. 54 – 61.

② “Average Cost of Cyberattack Now Exceeds $1 Million”, *Security Magazine*, January 15, 2019, https://www.securitymagazine.com/articles/89734 – average – cost – of – cyberattack – now – exceeds – 1 – million, 2022 – 02 – 06.

③ Joseph S. Nye Jr., *Cyber Power*, Belfer Center for Science and International Affairs, May 2010；沈逸、江天骄：《网络空间的攻防平衡与网络威慑的构建》，载《世界经济与政治》2018 年第 2 期，第 58 ~ 61 页；左亦鲁：《国家安全视域下的网络安全——从攻守平衡的视角切入》，载《华东政法大学学报》2018 年第 1 期，第 148 ~ 157 页。

④ “Leader’s Speech at Imam Ridha’s (a.s.) Shrine”, March 20, 2012, http://english.khamenei.ir/news/1620/Leader – s – Speech – at – Imam – Ridha – s – a – s – Shrine, 2022 – 02 – 05.

⑤ The Belfer Center, “Deterring Terror: How Israel Confronts the Next Generation of Threats – English Translation of the Official Strategy of the Israel Defense Forces”.

2022 年 6 月 27 日，伊朗国内最大的 3 家钢铁公司遭到网络攻击而发生爆炸且被迫停产，被认为与以色列有关的黑客组织宣布实施了攻击并声称是对“伊朗挑衅”的回应，时任以色列总理贝内特也在次日一场网络安全会议上表示“惹恼以色列需要付出代价”。①

伊朗在与以色列的网络冲突中不断提高和展示网络能力，其意图是在网络空间构建威慑、谋求相对战略优势，并以此进行舆论宣传。伊朗发展网络能力最初是出于对“震网”攻击的被动反应和进行报复的需要，但也意识到美国和以色列仅通过网络攻击而不需要实际的军事打击就可以破坏其核设施，由此开始重视和提高网络空间的战略地位。其一，伊朗希望通过发展网络攻防能力增强长期受到国际武器禁运和经济制裁限制的常规军事力量。受到严厉的经济制裁措施和国际油价持续疲软影响，伊朗的国防开支从 2012 年的 164.9 亿美元减少至 2013 年的 120 亿美元。② 相比于常规军事能力，发展和使用网络空间攻防能力的技术门槛和经济成本更低，且受到国际社会的限制更少，也更符合伊朗的经济状况与面临的国际形势。其二，伊朗将进攻性网络活动作为突破地理限制、继续提高地区影响力的有效手段。美军长期驻扎在海湾地区，以色列近年来也持续打击伊朗及其代理人的军事活动，这使得伊朗的常规军事力量在地理边界上难以突破美国及其盟友的包围。虽然“对抗轴心”战略在叙利亚、伊拉克、黎巴嫩等国家提升了什叶派的力量，但是伊朗的地缘扩张已经到达极限。③ 网络攻击不受地理边界限制，自由度和隐蔽程度更高，有助于维系和辅助伊朗在地区扩大影响力的活动，特别是对以色列本土目标的攻击能够强化对其威慑力。其三，伊朗将加强网络攻防能力作为维护国家荣誉的重要途径④，塑造在网络空间抵抗美国和以色列进攻的英雄形象。一方面，伊朗对以色列实施网络攻击，在一定程度上可以视为对以色列本土的直接打击，既展示出伊朗在新技术领域的成就和实力，又暴露出以色列的安全脆弱性。另一方面，伊朗通过网络攻击行动来展示其伊斯兰世界利

① Emanuel Fabian，“‘Mess with Israel，You’ll Pay A Price’，PM Warns Iran，After Steel Plant Cyberattack”，*The Times of Israel*，June 28，2022，https：//www.timesofisrael.com/mess-with-israel-youll-pay-a-price-pm-warns-after-iran-steel-plant-cyberattack，2022-07-20.

② 参见斯德哥尔摩和平研究所（SIPRI）网站：https：//milex.sipri.org/sipri，2022-07-20。

③ 田文林：《伊朗与以色列对抗的根源及前景》，第 59 页。

④ Gawdat Bahgat and Anoushiravan Ehteshami，“Iran’s Defense Strategy：The Navy，Ballistic Missiles and Cyberspace”，*Middle East Policy*，Vol.24，No.3，2017，pp.89-103.

益捍卫者的形象，以获取更多支持。近年来，伊朗黑客组织在“圣城日”期间都会对以色列实施代号为“耶路撒冷行动”（#OpJerusalem）的网络攻击行动，通过使以色列网站运行瘫痪来传播反犹太复国主义信息。

可以说，伊朗与以色列的战略对抗向网络空间延伸具有一定的必然性。伊、以的多领域对抗格局决定了双方会在所有的战略空间当中竞争，特别会在涉及国家安全的新技术领域展开激烈博弈。而且，与陆、海、空物理空间相比，网络空间作为虚拟空间，具有“进攻占优”的特殊性，提高了信息技术手段与各自战略对抗目标的匹配度。因此，伊朗和以色列都将网络空间视作可能打破战略相持、确立相对优势的新领域，网络空间冲突成为双方对抗的新形式。

（三）网络冲突有助于约束对抗规模

伊朗与以色列在长期对抗中都有意识地避免与对方发生大规模直接军事冲突。低程度损害是长期维持低烈度对抗的关键所在，尽可能规避因给对手造成毁灭性破坏或严重人员伤亡而引发全面战争的风险。托马斯·里德（Thomas Rid）指出，在网络空间的破坏和间谍行为有助于减少现实世界的暴力。[①] 网络空间冲突主要通过非暴力的信息技术手段实现，直接引发伊、以军事冲突的可能性低，是能够有效约束对抗规模的低烈度冲突形式。

第一，对网络攻击的归因困难会阻碍被攻击方的报复行动。加密、转移等技术手段使得网络攻击具有高度的隐蔽性，成员的流动性和组织的分散性更使得伊朗黑客组织难以被追踪。[②] 虽然网络空间中更多强调政治归因而非技术归因[③]，通过考察地缘政治形势和经验判断可以在一定程度上解决网络攻击的归因问题，但仍需要漫长的解码和追踪过程才能最终确认真正的攻击者。这也决定了被攻击方难以在短时间内进行及时、有效的报复。而且，当前国家行为体主要通过黑客组织等“代理人”来实施对外网络攻击，被攻击方有时也难以区分个人或黑客组织是自发实施网络攻击还是受国家行为体驱使，因此国家在网络冲突的初期阶段一般会谨慎进行报复。

---

① Thomas Rid，“Cyberwar and Peace：Hacking Can Reduce Real－World Violence”，*Foreign Affairs*，Vol. 92，No. 6，2013，pp. 77－87.

② Collin Anderson and Karim Sadjadpour，*Iran’s Cyber Threat：Espionage，Sabotage，and Revenge*，p. 18.

③ 沈逸、江天骄：《网络空间的攻防平衡与网络威慑的构建》，第 64 页。

第二，国家行为体对网络攻击的报复方式和烈度具有可预见性。网络攻击基本不会造成人员伤亡，减轻了被攻击方进行军事报复的压力。而且国家间的报复行为一般遵循对等原则，即报复方式和破坏程度的对等，这意味着国家对网络攻击的报复也将限定在网络空间以内。对伊朗而言，“一报还一报”的反应策略依然是其对网络攻击进行报复的主要战略逻辑。[①] 在2020年7月纳坦兹核设施遭到网络攻击后，伊朗宣布将以同样的方式实施报复。然而，以色列军方在2019年5月空袭了哈马斯在加沙地带对以实施网络攻击的据点，标志着国家行为体首次使用实际军事力量报复网络攻击，打破了在网络空间实施对等报复的惯例和界限。不过，这只是孤例。以色列长期对哈马斯目标进行直接武装打击，且以色列与哈马斯之间的军事力量对比过于悬殊，以色列通过空袭的方式来报复哈马斯的网络攻击并不会招致大规模的二次报复。而且，哈马斯是被以色列、欧盟等认定为所谓“恐怖组织”的非国家武装行为体，以色列对哈马斯进行军事打击并不意味着主权国家之间也会出现在常规军事空间报复网络空间攻击的情况。

第三，网络空间缺乏国际法约束和国际社会监管，实施网络攻击一般不会引起外部的强烈谴责和施压。目前，网络空间秩序呈现出多中心、权力结构分散的特点，国际社会对于网络空间的规范性约束尚未形成，更遑论对实施网络攻击、使用网络武器的限制，也没有明确禁止对民用设施的网络攻击行为。因此，伊朗与以色列在网络空间的相互攻击基本上不会招致国际社会的干预甚至制裁。对于需要提升国际形象的以色列和避免更多国际制裁的伊朗而言，网络空间冲突是一种相对温和的对抗方式，更适合在承受较大外部压力的时期使用。更重要的是，网络攻击以色列目标不会触发美国对以色列的安全保障承诺，也就不会招致美国的军事打击报复，这一特征在很大程度上促使伊朗也将与以色列的对抗“战线”转向网络空间。相互实施网络攻击成为伊以战略对抗优先使用的手段之一。

可以看出，伊朗与以色列相互对抗向网络空间延伸并未脱离现有的对抗逻辑和原则。伊、以认为信息技术进步能够实现通过网络空间来削弱对方实力和传递威慑的对抗需求，网络攻击的低成本、强破坏力和超越时空限制等特点与伊、以对抗的目标相适应。网络冲突不容易引发大规模军事冲突也符

① Michael Eisenstadt, *Iran's Lengthening Cyber Shadow*, p. 6.

合双方战略对抗的基本原则，而且国际监管的相对缺失使双方可以规避外部压力。因此，网络空间冲突成为更适应双方对抗常态化和长期化的冲突形式，这也进一步刺激了伊、以强化在网络空间的对抗。

三　网络空间冲突对伊朗和以色列对抗的影响

网络空间对抗可以看作是在虚拟空间发生、对物理空间造成破坏的一种冲突形式，这意味着网络空间活动也会反过来影响物理空间。伊朗与以色列通过网络空间冲突部分地实现了各自战略对抗目标，但是都未能从根本上改变对方的政策和行为。以色列针对伊朗纳坦兹核设施的网络攻击造成严重破坏，在一定程度上阻碍了伊朗开展核活动，但是未能迫使伊朗完全放弃核计划，反而会刺激后者增加核活动。2021 年 4 月纳坦兹核设施遭到网络攻击后，伊朗的回应措施是将铀浓缩水平提升至 60%。此外，以色列对伊朗的网络攻击也未能遏制后者在地区扩张影响力的活动。伊朗在叙利亚和也门的军事存在和影响力不仅没有减少，其研发生产的武装无人机甚至进一步扩散至北非地区。伊朗在与以色列的网络冲突中既表露了维护国家安全和国家荣誉的决心，又展示了其日益增长的网络攻防能力，然而未能拒止以色列继续攻击其核设施和境外军事目标。虽然伊朗及其代理人的网络攻击会给以色列造成一定损害，但是以色列作为网络能力更先进的一方，不仅能在短时间内快速修复安全漏洞，甚至还会对伊朗境内目标进行破坏力更大的网络攻击报复行动来维持威慑。不过，从长期来看，日益加剧的网络空间冲突将在政治关系、军事能力和冲突形态三方面对伊朗与以色列战略对抗产生影响。

（一）网络空间冲突加剧伊以关系对立

网络空间冲突已经成为伊朗与以色列战略对抗的主要形式之一。伊、以网络冲突的扩大化本身就是双方对抗意愿和决心强化的表现，也会反过来诱使双方在物理空间进行更加激烈的对抗。在伊以关系持续恶化的背景下，网络冲突的频率和烈度上升会进一步加剧双方对立的紧张局势。

频繁的相互网络攻击强化了伊朗与以色列的不安全感和相互敌视。伊朗在以色列网络攻击的刺激下加快发展网络能力，不断缩小与以色列的技术差距，对外使用进攻性网络能力的行为又进一步固化了以色列对伊朗安全威胁的认知。伊、以之间本就存在的安全困境向网络空间延展并不断加剧。根据

罗伯特·杰维斯（Robert Jervis）的攻防理论，在进攻占优的情况下，安全困境深化，军备竞赛加剧，国家间更倾向于冲突和战争。[①] 由于网络空间冲突的烈度和破坏程度一般低于现实冲突，对等原则使得网络空间中的报复行为具有可预见性，主动的进攻和冲突就成为保护自身安全和构建威慑的最好方式。因此，伊朗与以色列都谋求实施先发制人的网络攻击以及破坏程度更高的报复行动，双方网络冲突的频率和烈度上升，不可避免地会在双方之间持续积累不安全感和敌意。特别是伊朗与以色列开始将对方的民用基础设施作为主要的网络攻击对象，更容易引起两国民众的恐慌情绪和相互仇视，也会影响到两国政府对网络攻击的反应策略和报复方式选择。此外，网络攻击的高度隐蔽性和有限的归因能力，使得伊朗与以色列在遭受网络攻击时存在错误归因的可能。指向错误或过度报复和冒险行为都是极其危险的，甚至可能会引发灾难性后果。[②] 在经过长期网络冲突后，伊朗通常会将网络攻击的实施者直接指向美国和以色列政府，以色列一般也认为伊朗黑客组织受命于政府或革命卫队发动攻击，然而错误的归因和报复行为很容易引发对手的强烈反应。

伊朗与以色列都已将网络空间纳入主权领域，网络攻击在一定程度上相当于侵犯主权，引发对方强烈报复的风险上升。伊朗在 2020 年 8 月发布了《网络空间防御宣言》，指出对伊朗网络空间的攻击将被视为对伊朗主权的侵犯[③]，成为首个正式将网络空间纳入主权范围的中东国家。尽管以色列官方尚未承认网络空间主权，但副总检察长罗伊·施恩多夫（Roy Schöndorf）在 2020 年 12 月的演讲中表示，国际法的主权原则适用于解释在网络空间的行动[④]，表明以色列在事实上认可网络空间属于主权领域。两国对网络空间主权的承认标志着网络空间的战略地位进一步提升，维护主权和领土安全的需求会使伊、以对网络攻击的报复决心更加坚定，使用现实手段报复网络攻击的可能性增加。伊朗官员称会使用网络和其他武器等一切方式来抵御和报复网络攻击。[⑤]

---

① Robert Jervis, "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2, 1978, pp. 167 – 214.

② 沈逸、江天骄：《网络空间的攻防平衡与网络威慑的构建》，第 70 页。

③ "Iran Armed Forces Issue Cyber Defense Manifesto", *Pars Today*, August 17, 2020, https://parstoday.com/en/news/iran – i125458 – iran_armed_forces_issue_cyber_defense_manifesto, 2022 – 03 – 01.

④ Roy Schöndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies*, Vol. 97, 2021, p. 396.

⑤ "Spokesman: Iran to Take Countermeasures against Cyberattacks", *Fars News Agency*, July 23, 2020.

以色列时任国防部长本尼·甘茨也表示，以方在网络空间内外有多种回应网络攻击的方式。①

伊、以矛盾激化后，双方都开始展示可能直接军事打击对方的意愿和决心。其一，伊、以领导人和主流媒体对相互军事对抗的表态出现了变化。以色列政府频繁释放出有意军事打击伊朗核设施的信号。贝内特曾表示将继续实施以使伊朗远离“核门槛”和限制其地区影响力为目标的战略，不希望看到伊朗在叙利亚或者以色列边界附近存在。② 伊朗《德黑兰时报》在 2021 年 12 月披露了一张计划使用导弹攻击以色列的目标地图。其二，伊朗与以色列民众对于进行相互军事对抗的意愿也有所提高。网络攻击民用基础设施对生命安全和日常生活的影响在很大程度上加剧了双方民众的恐慌和敌对情绪。以色列民主研究所在 2021 年 11 月进行的一项民调显示，51% 的受访者支持在没有美国同意的情况下对伊朗核设施进行军事打击，61% 的犹太人受访者认为伊朗是以色列的关键安全威胁。③ 伊朗德黑兰国际研究所进行的一项全国性民调显示，74% 的受访民众认为伊朗对以色列破坏行动的反应不匹配；79% 的受访民众支持伊朗对以色列的军事威胁和可能的“破坏性恐怖主义行为”采取军事对抗。④

在伊朗与以色列关系不断恶化的背景下，即便是相对温和的冲突形式也可能会招致更加危险的结果。网络攻击一般不会造成实际人员伤亡，因此不大可能成为触发全面战争的导火索，但是双方在网络空间中长期、高频的冲突互动会不断加深相互的不安全感并积累敌意，不可避免地会强化双方继续对抗甚至升级对抗的意愿。但需要注意的是，伊、以网络空间冲突加剧是导致双方对抗意愿上升的重要诱因，但并非关键因素，更非唯一因素。

（二）网络技术发展助推伊朗和以色列军力提高

近年来，伊朗与以色列频繁通过技术披露、网络安全演习、对外实施网

---

① David Rosenberg，“Gantz：Iran’s ‘Terrorists with Keyboards’ Waging Cyber War on Israel”.

② Lahav Harkov，“Prime Minister Naftali Bennett Sums Up First 7 Months Leading Israel”，*The Jerusalem Post*，January 28，2022，https：//www. jpost. com/israel - news/politics - and - diplomacy/article - 694839，2022 - 03 - 02.

③ Tamar Hermann and Or Anabi，“Does Iran Pose an Existential Threat? Israeli Voice Index November 2021”，The Israel Democracy Institute，December 8，2021，https：//en. idi. org. il/articles/36760，2022 - 02 - 20.

④ Tehran International Studies & Research Institute，“Iranian Public Opinion on Israel and Possible Future Tehran - Tel Aviv Military Confrontation”，*Special Eurasia*，January 18，2022，https：//www. specialeurasia. com/2022/01/18/iran - israel - survey - opinion，2022 - 02 - 20.

络攻击等方式展示各自的网络攻防能力。两国通过将网络攻防能力与常规军事体系结合，推进与地区内外部行为体在网络空间的安全合作，加快争夺在网络空间的战略优势。网络技术的进步和应用直接或间接地增加了伊、以在现实战略对抗过程中可运用的网络空间资源和军事手段。

第一，网络能力的提升增加了伊朗与以色列在相互对抗中可以使用的军事手段。一方面，网络能力与现有常规军事手段结合有助于进一步完善伊、以各自的军事攻防体系。随着军事系统信息化和数字化水平的提高，网络能力在获取情报信息、维护关键军事设施安全、提高军事打击精确性等方面发挥了重要作用，特别是在应对武装无人机的安全威胁上表现突出。2011 年 12 月，伊朗军方声称通过网络技术成功取得了美国一架“RQ－170”无人侦察机的控制权，并将其降落在伊朗境内俘获。① 另一方面，伊朗与以色列可以使用“网络武器”精确打击和破坏对方本土目标。现有的进攻性网络技术可以通过植入恶意软件来远程控制信息化设备的操作系统，并以修改参数等方式损坏设备或引发爆炸，理论上能够点对点打击对手的关键基础设施、战略工业部门甚至军事设施。“网络武器”增加了伊、以在打击对方本土目标时可选择的手段，造成现实破坏是伊、以网络冲突区别于其他国家在网络空间对抗关系的重要特点之一。近年来，以色列已经多次单独对伊朗核设施和关键基础设施进行网络攻击并造成严重破坏，伊朗也将进攻性网络活动作为新的对外行动方式。

第二，以色列、伊朗分别与美国、俄罗斯等域外大国加强网络安全合作，弥补了传统军事合作模式在网络空间的缺陷。传统军事合作机制在面对隐蔽、复杂和多变的网络攻击时难以提供及时、有效的防御支持，需要深化网络安全信息与技术共享、共同构建网络空间主动防御体系等合作，来提高自身在早期识别和攻击后修复漏洞的能力。因此，以色列与伊朗在现有军事合作机制的基础上加强与域外大国的网络安全合作。以色列认为伊朗是其在网络空间的“主要对手”②，美国也将伊朗列为四大网络安全威胁来源之一③，共同

① Michael Eisenstadt, *Iran's Lengthening Cyber Shadow*, p. 8.

② Yonah Jeremy Bob, “Israel Cyber Chief: Iran Has Become Our Dominant Rival in Cyber”, *The Jerusalem Post*, June 28, 2022, https://www.jpost.com/middle-east/iran-news/article-710584, 2022-07-22.

③ “National Cyber Strategy of the United States of America”, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 2022-07-22.

面临来自伊朗的网络安全挑战促使以、美加强网络合作。美国与以色列早于2016 年 6 月就签署了有关网络防御合作的协议，并在次年成立了网络安全联合工作组，以应对突发网络安全事件。2021 年 12 月，以色列国防军与美国网络司令部举行了历年来规模最大的网络防御演习。与此同时，伊朗与俄罗斯的网络安全合作也在快速推进。2021 年 1 月，伊朗与俄罗斯正式签订《网络安全合作协议》，在打击网络犯罪、技术交换、人员培训以及在有关国际组织中就网络安全问题进行协调等方面深度合作。该协议的签订被视作俄罗斯与伊朗网络安全合作项目的重要事件，以方认为这必然会增加伊朗的网络攻防能力。① 不过，相比于伊朗与俄罗斯的合作，美、以网络安全合作程度更加紧密，定期举行网络防御演习等合作机制也更加完善。

第三，伊朗与以色列在中东地区构建网络空间攻防“联盟”体系，增加了对外行动的灵活性。伊朗在网络空间沿用“代理人战略”。一方面，伊朗协助培育黎巴嫩真主党、哈马斯等组织的网络攻防能力。早在 2006 年黎以冲突期间就有真主党对以色列进行网络攻击的报告，真主党还在 2012～2015 年针对以色列等国实施了一系列被称为“爆炸雪松”的网络攻击。据称，伊朗革命卫队圣城旅在 2021 年协助黎巴嫩真主党建立了新的网络部门。② 另一方面，伊朗与“代理人”合作对以色列实施网络攻击。2013 年 5 月，为了报复以色列对大马士革郊区一个研究中心的空袭，“叙利亚电子军”在伊朗黑客组织的支持下，对以色列海法的水处理设施进行了网络攻击。③ 与此同时，以色列与阿拉伯国家开展了广泛的网络安全合作，避免后者在网络空间暴露安全短板。据悉，以色列通过本国企业或其海外子公司为海湾国家的关键民用基础设施提供网络安全保护。④ 以色列与阿联酋、巴林等国达成的《亚伯拉罕协议》中也包括了在网络安全领域深化合作的内容，并于 2021 年 7 月与摩洛哥签署了首个网络安全合作协议。可以看出，伊朗与以色列在网络空间与各自的地区盟友体系相结

① Tal Shahar，“Israel Unprepared for Cyberwar with Iran，Expert Says”，*Ynet News*，February 5，2021，https：//www. ynetnews. com/business/article/rk005B5FeO，2022－07－22.

② Eyal Pinko，“Iranians Developing the Cyber Capabilities of Hezbollah”，*Israel Defense*，March 30，2021，https：//www. israeldefense. co. il/en/node/49094，2022－07－22.

③ David Shamah，“Iran－Sponsored Cyber－Attacks Unending，PM Says”，*The Times of Israel*，June 9，2013，https：//www. timesofisrael. com/iran－sponsored－hack－attacks－unending－pm－says，2022－01－20.

④ Neri Zilber，“Gulf Cyber Cooperation with Israel：Balancing Threats and Rights”，The Washington Institute，January 17，2019，https：//www. washingtoninstitute. org/policy－analysis/gulf－cyber－cooperation－israel－balancing－threats－and－rights，2022－05－15.

合，不仅提升了自身在网络空间行动的灵活性和能力的有效投送，还增加了对方在网络空间的行动成本以及防御投入。更重要的是，随着中东地区地缘政治竞争的“阵营化”，虽然网络空间对抗并未根本改变伊朗与以色列的战略相持僵局，但可以通过提高各自“阵营”成员的网络攻防能力来追求整体的力量对比优势。

（三）伊朗和以色列间“混合战争”的冲突形态得到强化

相比于仅局限在网络空间的冲突，更需要关注到伊朗与以色列对抗走向网络冲突与现实军事冲突结合的“混合战争”趋势。霍夫曼提出“混合战争”是冲突或战争形式的融合与模糊①，主要表现为常规与非常规军事手段的混合使用以及在战争与和平的界限、参战方和技术手段等方面的模糊。隐蔽性极高的“网络冲突”作为重要的战术手段，能够充分发挥混合战争的模糊性优势。事实上，“混合战争”模式在中东地区早已出现，2006 年黎巴嫩和以色列冲突、俄罗斯在叙利亚的军事行动均被认为是其中的典型案例，而在也门和叙利亚已经出现网络空间与常规军事空间冲突相结合的迹象。

当前，伊朗与以色列之间的网络冲突与现实冲突正在同步发生。其一，在网络攻击伊朗核设施的同时，以色列依然通过暗杀伊朗核科学家和高级将领等手段阻止伊朗发展核能力。2020 年 11 月，伊朗国防部副部长、核科学家法赫德扎里在德黑兰郊区遭暗杀身亡。其二，以色列持续空袭叙利亚境内的伊朗军事目标。2019 年 1 月，以色列国防军参谋长加比·阿什克纳齐（Gabi Ashkenazi）称，自 2017 年以来以色列已对叙利亚境内超过 1 000 个伊朗军事目标进行了空袭。② 其三，伊、以在地区周边海域相互攻击对方船只。2021 年 4 月，伊朗船只“萨维兹”号在红海遭到鱼雷袭击，美国方面称以色列实施了此次攻击行动。③ 7 月，由以色列公司管理的一艘油轮（Mercer Street）在阿曼湾海域遭到无人机袭击，以色列防长称该无人机从伊朗领土起飞。④ 可

① Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington: Potomac Institute for Policy Studies, December 2007, p. 7.

② Bret Stephens, “The Man Who Humbled Qassim Suleimani”, *The New York Times*, January 11, 2019, https://www.nytimes.com/2019/01/11/opinion/gadi-eisenkot-israel-iran-syria.html, 2022-02-21.

③ Farnaz Fassihi, Eric Schmitt and Ronen Bergman, “Israel-Iran Sea Skirmishes Escalate as Mine Damages Iranian Military Ship”, *The New York Times*, April 6, 2021, https://www.nytimes.com/2021/04/06/world/middleeast/israel-iran-ship-mine-attack.html, 2022-02-21.

④ “Benny Gantz: UAV Used in Mercer Street Attack Launched from Iran”, *i24 News*, August 25, 2021, https://www.i24news.tv/en/news/israel/diplomacy-defense/1629885306-benny-gantz-uav-used-in-mercer-street-attack-launched-from-iran, 2022-02-21.

以看出，伊朗与以色列在网络空间攻防冲突加剧的同时，没有减少在现实世界的对抗，网络冲突并非两国之间唯一的冲突形式。

近年来，中东地区的“混合战争”态势明显，伊朗与以色列都有意加强网络空间对抗与现实军事冲突之间的融合程度。伊朗最高领袖哈梅内伊早在 2014 年就提出，“网络是战争形式出现的最大变革，超过 20 世纪枪支和空中力量对战争的影响……伊朗大学生作为‘网络战实施者’要做好准备”。① 由此不难看出，伊朗领导层对于网络空间冲突的战略效果给出了极高的评价。目前，地区代理人、武装无人机、海军和网络空间攻防能力已经成为伊朗“前沿防御”战略的四大支柱。② 伊朗特别注重将代理人战争、网络空间冲突与意识形态宣传等多种手段相结合，这在其介入叙利亚冲突的过程中表现突出。对于以色列而言，发挥新技术领域对军事冲突的作用是增加在未来“混合战争”中取得优势的关键。早在 2007 年以色列空袭叙利亚核设施的“果园行动”中，以方在行动前首先通过网络攻击控制了叙利亚的防空雷达和通信系统。贝内特在 2022 年 3 月公开表示，以色列国防军正在为未来在网络空间与物理空间结合的“混合战争”做准备。③

目前，伊朗和以色列已经开始尝试在战术和战略层面使用网络攻防手段，网络冲突成为双方“影子战争”和“混合战争”的重要组成部分。其一，通过网络活动为现实军事行动争取行动和战术优势，如通过网络攻击破坏对方的军事系统、窃取军事信息等。2019 年 2 月，以色列国防军网络防御部门负责人称，隶属于伊朗革命卫队的黑客组织曾试图网络攻击以方的导弹预警系统。④ 其二，将网络攻击作为对现实袭击的报复手段之一。在 2022 年 2 月空袭伊朗境内的无人机基地后，以色列遭受了迄今为止规模最大的一次网络攻

① “Iran’s Supreme Leader Tells Students to Prepare for Cyber War”, *RT*, February 13, 2014, https://www.rt.com/news/iran-israel-cyber-war-899, 2022-03-02.

② Amr Yossef, “Upgrading Iran’s Military Doctrine: An Offensive ‘Forward Defense’”, https://www.mei.edu/publications/upgrading-irans-military-doctrine-offensive-forward-defense, 2022-03-03.

③ Carrie Keller-Lynn, “Bennett Says IDF Preparing for Future of Hybrid Cyber and Physical Warfare”, *The Times of Israel*, March 3, 2022, https://www.timesofisrael.com/liveblog_entry/bennett-says-idf-preparing-for-future-of-hybrid-cyber-and-physical-warfare, 2022-07-20.

④ Yoav Limor, “IDF Cyber Chief: Iran Tried to Hack Missile-Alert System”, *Israel Hayom*, February 7, 2019, https://www.israelhayom.com/2019/02/07/idf-cyber-chief-iran-tried-to-hack-missile-alert-system, 2022-03-03.

击，多个政府网站陷入瘫痪。[①] 其三，通过网络攻击民用基础设施给对方制造社会恐慌，并谋求演变为民众对政府的不信任。2021 年 10 月伊朗加油站系统受到网络攻击，导致民众无法购买政府补贴的低价燃油而出现排队抢购燃油的情况。伊朗在 2019 年 11 月曾因油价上涨而引发大规模民众抗议，此次攻击存在诱发社会不稳定的风险。2022 年 6 月，以色列西耶路撒冷和埃拉特部分城镇的导弹预警系统被指在遭到伊朗网络攻击后发出虚假警报，引起当地居民担忧和不安。[②]

总体而言，伊、以网络空间冲突短期内将维持较高频率和烈度，且将进一步与现实冲突相结合。随着伊以关系持续恶化，通过低烈度网络空间冲突来缓解大规模军事打击压力的路径越来越难以维系。相反，网络攻击行动引发被攻击方使用低烈度手段在物理空间进行报复的可能性上升。以色列对于与伊朗在网络空间日益激烈的攻防冲突产生了高度的不安全感，未来可能通过袭击伊朗在海外军事目标、谋杀伊朗高级官员或技术人员等方式进行报复，伊朗也可能会通过“代理人”袭击以色列本土目标作为对后者实施网络攻击的报复。

四　结语

伊朗与以色列在网络空间的攻防冲突已经成为双方战略对抗的重要表现形式。以色列一直谋求成为全球性网络强国，伊朗也将网络空间主导权作为争取地区领导权的一部分，两国的网络冲突也可以看作是在争夺未来塑造中东地区网络空间秩序的主导权。由于伊以关系日益紧张，双方在网络空间的冲突已经进入白热化阶段，目前被披露的网络冲突事件只是“冰山一角”。伊朗与以色列在网络空间冲突的目标与战略对抗的目标相适应，以色列将网络空间作为打破与伊朗对抗僵局的新领域，伊朗则意图通过提升网络能力来实现地区战略目标。依托网络空间“进攻占优”、不会引发大规模军事冲突以及国际法限制缺失等特点，网络攻防手段与战略对抗的目标高度匹配。伊、以

① Yaniv Kubovich and Omer Benjakob, “Israeli Government Sites Crash in Cyberattack”, *Haaretz*, March 14, 2022, https://www.haaretz.com/israel-news/2022-03-14/ty-article/.premium/israeli-government-sites-crash-in-cyberattack/00000180-5b8b-d615-a9bf-dfdbecd30000, 2022-07-13.

② “Cyberattack Suspected behind False Siren Alerts in Jerusalem, Eilat”, *The Times of Israel*, June 20, 2022, https://www.timesofisrael.com/cyberattack-suspected-behind-false-siren-alerts-in-jerusalem-eilat, 2022-07-13.

部分实现了相互对抗的目标，但是并未从根本上突破战略相持的对抗状态，反而强化了双方的安全困境，进一步加剧伊、以紧张局势。伊朗和以色列在网络空间冲突的过程中，通过提高网络能力与常规军事手段的结合程度、加强与域外大国的网络安全合作、在地区内部构建网络空间攻防体系等路径，增加了两国在相互战略对抗中可运用的资源和军事手段。双方的战略对抗日益呈现出网络空间冲突与现实冲突相结合的“混合战争”趋势。

值得注意的是，伊、以网络空间冲突存在较高的外溢风险，对中东地区乃至全球网络安全形势形成严峻挑战。受到新一轮巴以冲突影响，伊朗与以色列在网络空间的对抗愈发激烈。以色列国家网络指挥部表示，自 2023 年 10 月 7 日以来的 3 个月内，以色列受到网络攻击 3 380 次，是往年同期的 2.5 倍①，发现 15 个与伊朗、哈马斯和黎巴嫩真主党有关的黑客组织对以实施了网络攻击②。网络攻击完全不受地理边界限制，在通过互联网渗透的过程中不可避免会导致其他国家的计算机被感染。以“震网”攻击为例，尽管该病毒是针对伊朗核设施的数据采集与监视控制系统研发的，但也感染了沙特、印尼等多国的计算机系统。伊、以网络冲突也会加速进攻性网络技术和“网络武器”在中东地区的扩散，增加非国家行为体获取“网络武器”的可能性，特别是恐怖组织利用网络空间继续进行恐怖主义活动的趋势日益明显。因此，推动国际社会制定网络空间活动的有关制度和规范日益成为全球网络空间安全治理的迫切需要。当前，中东各国也开始重视发展自身的网络攻防能力，在此过程中必然会推进国家的网络安全产业和数字经济发展，有助于提高地区整体的信息化和智能化水平。虽然中东地区内的网络冲突存在且严重，但相比于流血冲突造成的实际损害依然较小，并非当前地区国家面临的首要安全威胁。更值得注意的是，伊朗及其代理人迅速提升网络能力并与现实武装活动相结合，不仅打破了美国和以色列在地区对网络技术的垄断，也在一定程度上影响了地区力量平衡。

（责任编辑：詹世明　责任校对：史晓曦）

① Sharon Wrobel，“Cyberattacks by Iran，Hezbollah Have Tripled During the War，Says Israel Cyber Czar”，*The Times of Israel*，April 9，2024，https：//www.timesofisrael.com/cyberattacks-by-iran-hezbollah-have-tripled-during-the-war-says-israel-cyber-czar，2024-04-11.

② “‘Iron Swords’ War in Cyber Sphere：Insights，Recommendations and Mitigations’”，*Israel National Cyber Directorate*，January 7，2024，https：//www.gov.il/BlobFolder/reports/publish_2412/en/report2412en.pdf，2024-04-11.