国别研究

复杂的中间地带：海湾阿拉伯国家在网络安全规范之争中的立场与动因*

蔡翠红　张若扬

摘　　要：随着大国战略竞争加剧和全球政治多极化发展，海湾阿拉伯国家在全球网络安全治理格局中的地位逐渐不容忽视。本文考察了六个海湾阿拉伯国家在国际网络安全规范之争中的定位及其网络安全治理实践，认为海湾阿拉伯国家选择了一条符合中间地带利益的网络安全治理道路。在国际网络安全治理平台，海湾阿拉伯国家呈现出介于网络大国之间的混合性立场。在国内层面，海湾阿拉伯各国的制度框架为本国国家权力的行使保留了较大灵活性；在区域层面，非正式合作和次国家层面的对话协调机制正成为海湾阿拉伯国家区域网络安全合作的主要形式。对政治、文化和社会安全的考虑，地区竞争和冲突新形式的出现，经济和数字化转型催生的安全漏洞及对网络安全的巨大需求，以及国际层面的联盟关系及其变化，是影响海湾阿拉伯国家在国际网络安全规范之争中立场的重要因素。

关 键 词：海湾阿拉伯国家；网络安全；国际规范

作者简介：蔡翠红，博士，复旦大学美国研究中心教授（上海 200433）；张若扬，复旦大学国际关系与公共事务学院 2021 级博士研究生（上海 200433）。

文章编号：1673-5161（2023）03-0021-23

中图分类号：D815

文献标识码：A

* 本文系 2020 年度教育部重大课题攻关项目“积极参与全球治理体系改革和建设研究”（20JZD057）的阶段性成果。

随着信息通信技术的发展和应用,国际和平与安全正面临越来越多且复杂的挑战。但与此同时,网络安全领域的国际规范仍处于生成阶段。各国致力于达成一定的规范共识,但网络安全国际规范的建设进程却常常受到国家间政治博弈的影响而停滞。网络安全国际规范达成全球共识的困难主要源于网络安全治理的阵营化态势:由于不同国家在网络空间的权力结构方面存在不同优势和短板,在参与网络空间秩序博弈的过程中,各国往往围绕不同的议题领域根据各自相对优势形成相似或差异化的立场,其各自主张之间存在复杂的竞争或合作关系。这种立场差异源于国家间信息技术发展水平的差距和治理理念的差异,网络领域的发达国家作为既得利益者希望维护现有的治理模式,而发展中国家则希望打破发达国家的垄断,争取更大的话语权。这种大国之间的对立常常被描述为冷战在网络空间的复兴。①

但这种划分并不绝对,在具体实践中,各行为体在网络安全规范上的立场可能更加复杂,网络安全治理的方式也更加多样。事实上,这种简单的阵营化划分不仅掩盖了国家间在部分治理领域存在共识的可能,而且忽视了现实世界更为复杂的网络安全图景:在几个主要的网络大国之外,还有大量处于中间地带的国家在网络安全规范之争中持混合性立场,海湾阿拉伯国家便是其中的典型。② 一方面,海湾阿拉伯国家在政策、法规与参与的国际机构方面同中俄等提倡“多边主义”和“网络主权”的国家联系在一起;另一方面,它们在私营部门的网络安全合作、政府间的情报关系以及进攻性网络活动领域同欧美国家之间保持密切联系。

近年来,在大国战略竞争升级的背景下,海湾阿拉伯国家的战略地位持续提升。尽管海湾阿拉伯国家在网络安全国际治理格局中并非重要一极,但这并不意味着其在网络安全治理议题、尤其是在围绕网络安全的国际规范之争中没有重要影响。随着全球政治秩序的多极化转变和数字化转型的发展,海湾阿拉伯国家作为中东地区数字技术和数字经济的重要枢纽势,必将对国际网络安全治理格局产生更重要的影响,了解这些国家在网络安全治理问题上的立场及其成因具有重要意义。

一、问题的提出

海湾阿拉伯国家在经济、社会和数字技术的发展等方面存在广泛差异,部分

① David Ignatius, “The Cold War Is Over. The Cyber War Has Begun.,” *The Washington Post*, September 15, 2016, https://www.washingtonpost.com/opinions/global-opinions/the-cold-war-is-over-the-cyber-war-has-begun/2016/09/15/bc4ca5c0-7b87-11e6-bd86-b7bbd53d2b5d_story.html, 上网时间:2022 年 9 月 15 日。

② 本文中的海湾阿拉伯国家指海湾阿拉伯国家合作委员会六个成员国,即沙特阿拉伯、卡塔尔、阿联酋、巴林、科威特和阿曼。

海湾阿拉伯国家之间还存在深刻的政治纷争，但仍存在一些共性因素使得这六个国家在网络安全治理领域可以作为一个整体来考察。

首先，基于经济体量和互联网渗透率等因素，海湾阿拉伯国家相当于中东地区的一个数字枢纽，在网络安全规范领域重要性较高。沙特阿拉伯作为阿拉伯世界最大的经济体，也是二十国集团中唯一的阿拉伯国家。而阿联酋、卡塔尔、科威特、阿曼和巴林等海湾国家都属于富裕小国，其互联网渗透率接近百分之百。卡塔尔半岛电视台及其网站在全球拥有大量受众，且中东网站的大多数访问者都来自该地区的阿拉伯国家。近年来，这些国家积极致力于经济的数字化转型，在线活动和对数字技术的使用增长迅速。在数字化的未来，这些国家很可能成为中东地区数字服务的国际枢纽。但同时，数字化转型也增加了这些国家的网络安全风险，使其成为网络攻击和网络犯罪的重点对象。在中东地区，海湾阿拉伯国家在网络安全方面受到攻击、遭受欺诈企图最为严重。2021年至2022年，中东国家数据泄露平均成本从693万美元增长至746万美元，增幅达7.6%，远高于全球平均水平，仅次于美国，其中，沙特阿拉伯和阿联酋两国的数据泄露成本增幅尤为显著。① 海湾阿拉伯国家合作委员会（以下简称“海合会”）国家每周受到约1,200次针对企业组织的攻击，这一数字高于全球平均水平。② 据统计，仅在2021年上半年，整个海湾阿拉伯国家就遭到了超过6,200万次电子邮件威胁，超过15万次URL重定向攻击，受害者超2,800万，恶意软件攻击超700万次，含银行恶意软件攻击达2,133次。③ 这些国家的金融、石油和天然气行业，以及公共设施和交通基础设施都是网络攻击的重点对象。④

其次，从参与度来看，在数字化转型的背景下，海湾阿拉伯国家都采取了大量旨在提高网络安全能力的措施。国际电联（International Telecommunication Union，ITU）根据立法、组织、技术、能力建设和合作措施等一系列指标衡量国家的网络安全建设情况，根据2021年国际电联发布的“全球网络安全指数”（Global Cybersecurity Index，GCI），沙特阿拉伯、阿联酋、阿曼和卡塔尔在阿拉伯世界排名前五位，巴林和科威特在阿拉伯世界排名第八和第九，其中沙特阿拉伯甚至排

① “Cost of a Data Breach Report 2022，”*IBM*，July 2022，p. 10，https://www.ibm.com/downloads/cas/3R8N1DZJ，上网时间：2023年4月15日。

② “Hi-Tech Crime Trends 2022/2023，”*Group-IB*，January 2023，p. 23，https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2022/，上网时间：2023年4月15日。

③ “Attacks From All Angles：2021 Midyear Cybersecurity Report，”*Trend Micro Research*，September 14，2021，https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup，上网时间：2022年9月15日。

④ DarkMatter，*Cyber Security Report*，June 17，2019，https://www.scribd.com/document/456740035/Cyber-Security-Report-2019-DarkMatter，上网时间：2022年9月15日。

名全球第二。[①] 尽管国际电联发布的“全球网络安全指数”因其数据来源主要依赖于各国的自我评估而备受质疑,但海湾阿拉伯六国在这一指数上的地位仍显示出这些国家在网络安全领域的参与和投入要领先于其余大部分阿拉伯国家。据专家估计,仅沙特政府在网络安全方面的支出就高达 36.189 亿美元,该国网络安全市场预计将以 18.73%的复合年增长率稳定增长,至 2027 年网络安全方面的支出将达到 106.4513 亿美元。[②] 所有海湾阿拉伯国家都制定了国家网络安全战略,并在近十年来引入或修改了各自的网络犯罪和电子交易立法,一些国家还引入了国家数据保护立法。[③] 此外,这些国家都在早期的计算机应急响应团队的基础上,建立了专门的国家网络安全机构。

最后,从相似性来看,相较于中东地区其他国家,海湾阿拉伯国家同属阿拉伯世界,共同构成了一个网络安全区域。尽管阿拉伯国家间同样存在高度异质性,但就社交媒体和语言文化交流而言,阿拉伯民众在同一个平台上密切互动并形成了一个跨国的网络安全专家社区。[④] 与此同时,这些国家是在“阿拉伯之春”和《关于打击信息技术犯罪的阿拉伯公约》(*Arab Convention on Combating Information Technology Offenses*,以下简称《阿拉伯公约》)签署等一系列相似的背景和契机下开始或更深度地参与网络安全治理的,在全球网络安全治理架构中的立场也具有相似性。

值得注意的是,尽管海湾阿拉伯国家在国际多边平台同中国和俄罗斯等提倡网络主权的国家站在一起,且对美欧等国倡导的多利益攸关方模式并非持肯定态度,但美国及其多利益攸关方主义的盟友并没有像对待中国和俄罗斯一样公开谴责海湾阿拉伯国家,这与其在网络安全国际规范之争中所呈现的混合性态度是分不开的。如何理解在网络安全国际规范之争中处于中间地带的海湾阿拉伯国家所持的混合性立场?在实际的网络安全治理实践中,海湾阿拉伯国家又呈现出何种行为规范?这一系列立场和规范形成的原因是什么?本文尝试对上述问题进行深入探讨。

---

① ITU, *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity*, 2021, p. 29, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf, 上网时间:2022 年 9 月 15 日。

② “Saudi Arabia $9.84 Bn Cybersecurity Markets, Analysis, Competition, Forecast & Opportunities, 2026F,” *GlobeNewswire*, April 5, 2022, https://www.globenewswire.com/en/news-release/2022/04/05/2416342/28124/en/Saudi-Arabia-9-84-Bn-Cybersecurity-Markets-Analysis-Competition-Forecast-Opportunities-2026F.html, 上网时间:2023 年 4 月 15 日。

③ ITU, *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity*, pp. 69-70.

④ James Shires, *Moral Manoeuvres: Cybersecurity in Egypt and the Gulf States*, Ph.D. dissertation, University of Oxford, 2018, p. 50.

二、文献综述

目前学界对网络安全规范兴起过程的研究主要关注主要网络大国之间在具体问题上的分歧，对其余处于中间地带的国家关注不多。尽管近年来随着国际权力格局的变化和技术水平的发展，各阵营内部在利益冲撞下均出现了不同程度的离心倾向，学界对网络安全规范的研究逐渐超出了简单的二元格局，但关注重点仍是美国、欧盟、俄罗斯和中国等核心国家或行为体，海湾阿拉伯国家这类中间国家在网络安全规范建设过程中的地位没有得到足够重视。

在网络安全规范的理论研究中，不少文献都将网络大国，尤其是在网络安全治理领域拥有较高话语权的美国和被视为“规范性力量”的欧洲，视作规范生成和扩散的核心驱动力。① 在这一理论框架内，网络大国往往占据道义制高点而提出某种尚未能够为其他国家政府所接受的规范倡议，为使更多国家接受其规范倡议，网络大国可以通过规范移植、规范竞争、规范互补、规范磋商等方法帮助其网络空间的新规合法化。② 在这类理论模型中，位于中间地带的广阔国家被视作网络安全规范的客体，要么被成功说服，要么以拒绝姿态被排斥于一个形成中的规范共同体之外。而无论作出何种选择，中间地带的国家在强势的规范倡导者面前都显得有些被动，也较少有文献单独探讨这类中间国家在网络安全规范中的立场及其成因。

近年来，随着海湾阿拉伯国家在网络安全治理格局中的地位上升，有关其网络安全治理的研究也不断增多。相关研究多聚焦于海湾阿拉伯国家面临的网络安全威胁③，

---

① Hanan Mohamed Ali, “‘Norm Subsidiarity’ or ‘Norm Diffusion’? A Cross-regional Examination of Norms in ASEAN-GCC Cybersecurity Governance,” *The Journal of Intelligence, Conflict, and Warfare*, Vol. 4, No. 1, 2021, p. 27; Dennis Broeders and Bibi van den Berg, eds., *Governing Cyberspace: Behavior, Power and Diplomacy*, Lanham: Rowman & Littlefield, 2020, pp. 205-227.

② Martha Finnemore, “Cultivating International Cyber Norms,” in Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age*, Washington: CNAS, 2011; Oleg Demidov, “International Regulation of Information Security and Russia's National Interests,” *Security Index: A Russian Journal on International Security*, Vol. 18, No. 4, 2012, pp. 15-32.

③ Reem K. Alqurashi *et al.*, “Cyber Attacks and Impacts: A Case Study in Saudi Arabia,” *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 9, No. 1, January-February 2020, pp. 217-224; Ahmed A. Mawgoud *et al.*, “Cyber Security Risks in MENA Region: Threats, Challenges and Countermeasures,” in Aboul Ella Hassanien, Khaled Shaalan and Mohamed Fahmy Tolba, eds., *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2019*, Cham: Springer International Publishing, 2020, pp. 912-921; Booz Allen Hamilton, “Cybersecurity: A Growing Challenge in the Middle East,” *Banker Middle East*, Issue 185, June 2016, pp. 28-30; Nir Kshetri, *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, Cham: Springer, 2016, （转下页）

现有的网络安全政策和机制①,以及一些具体的网络安全领域,如海湾阿拉伯国家的网络犯罪立法②。针对海湾阿拉伯国家在网络安全规范议题中的立场,有学者认为,面对强势的大国所推行的网络安全国际规范,处于中间位置的地区和国家有两种可能的选择:一是选择"规范辅助"(norm subsidiarity),即国家或区域行为体通过创建规则以维护其自主性,将治理活动维持在尽可能低的水平以免受更强大的中心行为体的支配、忽视、侵犯或滥用,如东南亚国家联盟;二是选择接受"规范扩散"(norm diffusion),即国家或地区行为体将国际规范"社会化",进而接受、内化和实施,海湾阿拉伯国家便被视为是接受"规范扩散"的一个典型。③也有学者认为,海湾阿拉伯国家对大国所推行的网络安全国际规范的态度并不是简单的接受规范扩散,而是"规范挪用"(norm appropriation),即通过扩大规范的内涵使之适应于其利益偏好。这一"规范挪用"可以解释海湾阿拉伯国家在网络安全国际规范之争中的混合性立场,即一方面为了掩盖其在国内网络安全优先事项上同其国际伙伴(尤其是欧美)的差异,另一方面通过"挪用"网络犯罪领

(接上页注③) pp. 183-194; Bassant Hassib and James Shires, "Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy," *Middle East Policy*, Vol. 29, No. 1, March 2022, pp. 90-103.

① Abdulla Al Neaimi, "A Framework for Effectiveness of Cyber Security Defenses, a Case of the United Arab Emirates (UAE)," *International Journal of Cyber-Security and Digital Forensics*, Vol. 4, No. 1, 2015, pp. 290-301; Haifa Nasser Alshabib and Jorge Tiago Martins, "Cybersecurity: Perceived Threats and Policy Responses in the Gulf Cooperation Council," *IEEE Transactions on Engineering Management*, Vol. 69, No. 6, 2022, pp. 1-12; Nir Kshetri, *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*; Al Sairafi Zainab, *Cybersecurity Challenges for Human Rights Defenders in Gulf Cooperation Council (GCC) countries*, Vienna: Central European University, 2022; Shires James. *The Politics of Cybersecurity in the Middle East*, Oxford: Oxford University Press, 2022; Nadir Naveed Ahmed and Krishnadas Nanath, "Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System," *Journal of Cyber Security and Mobility*, Vol. 10, No. 3, 2021, pp. 511-536.

② Mohammed AlZain, "Cyber Attacks and Impacts: A Case Study in Saudi Arabia," *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 9, No. 1, January-February 2020, pp. 217-224; Mohammed Saleh Altayar, "A Comparative Study of Anti-Cybercrime Laws in the Gulf Cooperation Council Countries," *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, March 26-27, 2017, pp. 148-153; Aissani Rahima, "Anti-cyber and Information Technology Crimes Laws and Legislation in the GCC Countries: A Comparative Analysis Study of the Laws of the UAE, Saudi Arabia and Kuwait," *Journal of Legal, Ethical and Regulatory Issues*, Vol. 25, No. 1, 2022, pp. 1-14; Nir Kshetri, *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, pp. 119-134.

③ Hanan Mohamed Ali, "'Norm Subsidiarity' or 'Norm Diffusion'? A Cross-regional Examination of Norms in ASEAN-GCC Cybersecurity Governance," p. 27; Amitav Acharya, "Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World," *International Studies Quarterly*, Vol. 55, No. 1, 2011, pp. 95-123.

域的国际规范来限制其国内的政治反对派以及在线公共领域的言论自由。①

上述几类解释都把海湾阿拉伯国家这类处于中间地带的国家作为规范传播的客体，将其在网络安全规范领域的混合性立场视为一种大国竞争框架下的副产品，从而忽视了其在网络安全治理领域的主动性，总体上没有跳出大国竞争的框架。海湾阿拉伯国家长期以来是域外大国激烈争夺的“中间地带”，但相比于冷战时期不同国家选边站队、与美苏两大国长期结盟的“分裂的中间地带”，如今多极化格局下的海湾阿拉伯国家更多呈现出新型“中间地带”的特征：在面对域外大国竞争时，无论是立场取向还是应对措施都选择更符合自身利益的中间道路。② 因此在分析海湾阿拉伯国家在网络安全国际规范之争中所持立场的动因时，不仅要考虑域外大国的影响，还要在大国竞争的框架之外，结合其国内政治经济发展逻辑，从国际网络安全治理平台、国内网络安全治理政策、机制和法律以及区域层面的网络安全合作等角度来理解海湾阿拉伯国家在网络安全议题上的混合性立场。

三、海湾阿拉伯国家的网络安全治理实践和治理规范

在既有研究中，针对海湾阿拉伯国家在宏观层面的网络安全治理态度和特点的研究较少。一方面，海湾阿拉伯国家主动回避了一些围绕关键议题的争论，如关于武装冲突的国际法是否及如何适用于网络空间的争论；另一方面，在一些网络大国争议的核心议题，如在涉及网络犯罪的国际协定问题上，海湾阿拉伯国家的定位十分谨慎。③ 实际上，一个国家或地区在网络安全治理议题上的态度不仅表现为其在有关国际网络安全治理平台上的官方立场与表态，还体现在其国内及区域间治理网络安全的实践中，因此需要从国际网络安全治理平台、国内网络安全治理政策、机制和法律以及区域层面的网络安全合作等角度来综合理解海湾阿拉伯国家在面对网络安全治理问题时的立场和态度。

第一，在国际治理平台，海湾阿拉伯国家采取的是谨慎的混合性立场。

一方面，大多数阿拉伯国家在国际网络安全治理平台上同中俄立场相近。大多数阿拉伯国家都支持网络主权和信息安全，在涉及全球网络空间治理的问题上更倾向于支持以联合国为代表的国际机构发挥更大的作用。例如，在国际网络犯罪的治理问题上，网络大国之间在国际网络犯罪法律机制的建设方式上存在分歧：欧美等西方国家倾向于在 2001 年由欧委会制定并通过的《网络犯罪

① James Shires, *Moral Manoeuvres: Cybersecurity in Egypt and the Gulf States*, p. 6.

② 余纲正：《新型“中间地带”：俄乌冲突中的阿拉伯国家》，载《阿拉伯世界研究》2022 年第 5 期，第 71 页。

③ Bassant Hassib and James Shires, “Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy,” *Middle East Policy*, Vol. 29, No. 1, March 2022, p. 100.

公约》(*Cyber-crime Convention*,又称《布达佩斯网络犯罪公约》)的基础上将其全球化,反对另起炉灶重新制订一份全球性网络犯罪公约;而中俄等国却主张应在联合国框架下,利用联合国的现有平台谈判制订一份全球性网络犯罪公约,之所以采取这一立场,是因为《布达佩斯网络犯罪公约》存在民主性、代表性和有效性不足等问题。大部分阿拉伯国家都没有签署《布达佩斯网络犯罪公约》,截至 2023 年 4 月,在签署该网络犯罪公约的 64 个国家中只有突尼斯一个阿拉伯国家。并且,由阿拉伯联盟成员国于 2010 年 12 月签署并得到大多数成员国批准的《阿拉伯公约》,在关于网络犯罪问题的规定方面同早先的《布达佩斯网络犯罪公约》也存在显著区别。在 2019 年 12 月 27 日的第 74 届联合国代表大会上,中国等 47 国共提的"打击为犯罪目的使用信息通信技术"决议以 79 票赞成、60 票反对、33 票弃权的投票结果获得通过,这标志着在联合国框架下开启谈判制定打击网络犯罪全球性公约的进程正式启动。其中,大多数阿拉伯国家投了赞成票,沙特阿拉伯和巴林等部分阿拉伯国家投了弃权票。

在国际网络安全治理平台同中俄立场相近的同时,阿拉伯国家同欧美在国家和非国家层面也建立了网络安全合作关系。在国家层面,欧美国家同阿拉伯地区的诸多国家在网络安全领域建立了正式的官方合作关系。例如,从 2010 年起,美国每年通过一个中部地区网络安全会议与军事代表就网络安全进行讨论,涉及六个海湾阿拉伯国家,以及埃及、黎巴嫩和阿富汗。① 阿曼是英国在收集信息情报方面的重要合作伙伴,英国依赖阿曼收集也门和伊拉克的信号情报,②这一情报合作关系受到"五眼联盟"的高度重视,而作为"第三方"的沙特阿拉伯和阿联酋也被授权访问美国的一些信息情报。此外,英国还与沙特签订了"网络安全战略合作"协议。③ 美国于 2018 年同科威特签署了一项网络安全合作协议,帮助后者加强国内网络安全能力建设。④ 在非国家层面,阿拉伯国家同欧美的网络安全公司保持密切的商业网络安全合作关系。欧美私人网络安全公司向海湾阿拉伯国家的主要公司或政府机构提供广泛的防御性网络安全方案和网络安全咨

① "Middle Eastern Leaders Work to Strengthen Cyber Security by Sharing Information," *UNIPATH*, January 17, 2020, https://unipath-magazine.com/cooperative-cyber-defense/, 上网时间:2022 年 9 月 15 日。

② 《批准阿曼苏丹国政府与大不列颠及北爱尔兰联合王国政府关于持久友好和双边合作的全面协定的第 59/2019 号皇家法令》(阿拉伯文),阿曼公平与法律事务部,2019 年 5 月 22 日,https://mjla.gov.om/legislation/decrees/details.aspx?Id=1106&type=L, 上网时间:2022 年 9 月 16 日。

③ Foreign & Commonwealth Office, "United Kingdom-Saudi Arabia Joint Communiqué," *GOV.UK*, March 10, 2018, https://www.gov.uk/government/news/united-kingdom-saudi-arabia-joint-communique, 上网时间:2022 年 9 月 16 日。

④ Jennifer Aguinaldo, "Kuwait and the US Sign Cybersecurity Agreement," *MEED*, September 5, 2018, https://www.meed.com/kuwait-us-sign-cybersecurity-cooperation-deal/, 上网时间:2022 年 9 月 16 日。

询服务，与此同时，长期活跃在海湾地区的军火公司则为其提供了国家监视和攻击性网络安全能力方面的产品。这是阿拉伯国家同欧美在网络安全方面关系密切的另一层原因。例如，在2018年9月，为提升网络安全，沙特电信公司（STC）与总部位于美国的威胁情报平台供应商Anomali开展合作。据沙特电信公司介绍，新的合作项目是建立一个共享网络威胁信息平台，重点强化公司内部处理网络威胁的方法。① 海湾阿拉伯国家同美欧之间网络安全伙伴关系使其在多利益攸关方模式的支持者中也得到了较高评价，国际电信联盟在2018年公布了一项统计数据，依据国际伙伴关系、合作框架和“多利益攸关方”法律、投入等指标对各国进行排名，其中沙特阿拉伯和阿曼是阿拉伯地区在促进网络安全方面国际多利益攸关方合作排名最高的国家，其次是卡塔尔。②

第二，在国内层面，海湾阿拉伯国家的政策法律框架为国家权力保留了较大的解释空间。

网络安全战略和相关法律是反映一个国家在网络空间治理问题上立场的重要资料。某个国家的网络安全战略所设立的目标、为实现目标所制订的计划、其网络安全战略所使用的术语甚至是语言风格，都可能反映了该国对一些网络空间治理规范的态度。甚至可以说，国家网络安全战略反映了一个国家想要向其受众呈现的精心规划的网络安全治理形象。③ 而同网络安全相关的立法及其实践，则更直观地反映了一国在国内网络安全治理中的实际立场。与其在国际网络安全治理架构中的立场相对应，阿拉伯国家在国内网络安全战略制定和法律实践中也具有混合性的一面：其网络安全战略在对类似“国家安全”或是“恶意行为者”这类概念给出宽泛定义的同时，又普遍表达了对个人自由和隐私等国际网络安全规范的抽象认可；各自国内的网络犯罪法在将《布达佩斯网络犯罪公约》等国际规范视为立法参考的同时，又包含了被法律专家和人权活动家认为是打击国内反对派和侵犯个人自由的条款。

首先，针对国家网络安全战略的目标，主要阿拉伯国家的网络安全战略均给出了对“国家安全”的广泛定义。沙特阿拉伯于2017年10月31日通过国王令成立国家网络安全管理局（National Cybersecurity Authority，NCA），该机构主要任务是通过加强内部分析和法律解决方案来提高国家的网络安全，其制定的战略网络安全愿景反映了沙特阿拉伯网络安全治理的目标，即“创造一个有弹性、安

① “STC Inks Deal with Anomali to Boost Cybersecurity,” *Arab News*, September 4, 2018, https://www.arabnews.com/node/1366806/%7B%7B, 上网时间：2022年9月16日。

② ITU, *Global Cybersecurity Index 2018*, International Telecommunication Union, 2019, pp. 26-27, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, 上网时间：2022年9月16日。

③ James Shires, “Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf,” in Dennis Broeders and Bibi van den Berg, eds., *Governing Cyberspace: Behavior, Power and Diplomacy*, p. 211.

全和值得信赖的沙特网络空间,以促进经济增长和繁荣”。① 这一愿景还概括了沙特 2030 年在网络安全领域的六大优先目标,即协调全国的网络安全政策和机构、加强风险管理、保障网络环境的最佳运作、加强动态防御、加强同国际伙伴的合作关系以及推动网络空间的开发。② 卡塔尔国家网络安全战略对战略目标的表述是“建立和维护一个安全的网络空间,以维护卡塔尔的国家利益和卡塔尔社会的基本权利与价值观”③。巴林国家网络安全战略声称“为巴林王国提供一个安全可信的网络空间”④。科威特的国家网络安全战略旨在“加强各种形式的信息安全”以及“建立一个综合的、全面的和有弹性的机制来管理国家网络安全”。⑤ 在阿联酋,国家网络安全战略目标的表达更为广泛,旨在“建立一个更加安全的信息社会”,以“应对任何风险、威胁或袭击”,“保障国家信息和通讯安全”。⑥

其次,针对网络安全的对象,这些国家在国家战略中的表述也没有十分明确的指向。一些国家在战略中使用“恶意行为者”一词来描述网络安全威胁。例如,迪拜战略指出,“开放和自由的网络空间提供价值……重要的是保护这个值免受恶意活动和中断的风险……迪拜是恶意行为者的主要目标”⑦。卡塔尔则声称,“网络空间的相互关联性增加了来自各种恶意行为者的威胁”⑧。值得注意的是,形容词“恶意”有好几种翻译。在上述迪拜战略的句子中,“恶意行为者”一词被电子攻击所取代,而卡塔尔战略在上述句子中使用“有偏见的一方”,在其他地方使用“恶意/邪恶意图”来表示内部威胁。通过这种方式,这些战略将一系列网络威胁纳入了“恶意”这一英语和阿拉伯语词汇中,使得其在界定网络安全威胁

① 《国家网络安全战略》(沙特阿拉伯,阿拉伯文),沙特网络安全管理局,2022 年 12 月,https://nca.gov.sa/strategic,上网时间:2022 年 9 月 16 日。

② 同上。

③ 《国家网络安全战略》(卡塔尔,阿拉伯文),卡塔尔国家网络安全委员会,2014 年 5 月,https://www.motc.gov.qa/sites/default/files/lstrtyjy_lwtny_llmn_lsybrny.pdf,上网时间:2022 年 9 月 15 日。

④ 《巴林国家网络安全战略》(阿拉伯文),巴林国家网络安全中心,2020 年,https://www.ncsc.gov.bh/ar/national-strategy.html,上网时间:2022 年 9 月 15 日。

⑤ 《科威特国家网络安全战略(2017~2020 年)》(阿拉伯文),科威特通信与信息技术监管局,2017 年,https://citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf,上网时间:2022 年 9 月 15 日。

⑥ 《2012 年关于打击信息技术犯罪的第 5 号联邦法令》(阿拉伯文),WIPO Lex,2012 年 8 月 13 日,https://wipolex.wipo.int/en/text/316910,上网时间:2022 年 9 月 15 日。

⑦ 《迪拜网络安全战略》(阿拉伯文),迪拜电子安全中心,2017 年 9 月,https://u.ae/ar-ae/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/dubai-cyber-security-strategy,上网时间:2022 年 9 月 16 日。

⑧ 《国家网络安全战略》(卡塔尔,阿拉伯文)。

时拥有更多灵活的解释空间。① 同时，尽管在网络安全战略中没有直接提到与伊斯兰教法相关的要求和规定，但一些阿拉伯国家在网络空间的执法实践仍会依据伊斯兰教法传统。②

再次，海湾阿拉伯国家的网络安全战略也普遍包含了对一些国际网络安全规范的抽象认可，如个人自由和隐私等。沙特阿拉伯国家信息安全战略的目标是“使信息能够自由和安全地使用和共享”，而国家网络安全中心寻求“实现一个安全、开放和稳定的信息社会”。③ 阿联酋的国家网络安全战略渴望“一个自由和安全的网络世界”，声称“网络空间需要对创新和思想、信息和表达的自由流动保持开放”，尽管“应该适当考虑保持开放技术和个人隐私权之间的适当平衡”。④ 卡塔尔网络安全战略声称，该国的“网络安全价值观”是“表现出宽容和尊重”，并拥抱“思想和信息的自由流动”。⑤ 巴林网络安全战略的目的是“维护个人的权利和价值观”。⑥ 在科威特，“该战略的主要目的是促进支持安全和正确使用电子空间的网络安全文化”⑦，而卡塔尔的目标是“培育一种促进安全和适当使用网络空间的网络安全文化”。⑧ 在这种宽泛定义和抽象认可的基础上，这些网络安全战略文件对国际网络规范显示出一种混合性的取向。

这种混合性同样体现在这些海湾阿拉伯国家国内的网络犯罪立法中。网络犯罪立法在网络安全治理中发挥着重要的作用。首先，网络犯罪立法定义了哪些行为构成网络犯罪以及适用的相关制裁以界定犯罪行为。⑨ 其次，网络犯罪立

---

① James Shires, “Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf,” in D. Broeders and B. van den Berg, eds., *Governing Cyberspace: Behaviour, Power and Diplomacy*, p. 211.

② Joyce Hakmeh, “Cybercrime Legislation in the GCC Countries: Fit for Purpose?,” *Chatham House*, July 4, 2018, https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf, 上网时间：2022 年 9 月 16 日。

③ 《国家网络安全战略》（沙特阿拉伯，阿拉伯文）。

④ 《国家网络安全战略 2019》（阿拉伯文），阿联酋电子通信和数字政府监管局，2019 年 6 月，https://tdra.gov.ae/ar/national-cybersecurity-strategy，上网时间：2022 年 9 月 15 日。

⑤ 《国家网络安全战略》（卡塔尔，阿拉伯文）。

⑥ 《巴林国家网络安全战略》（阿拉伯文）。

⑦ “CAIT Chief Briefs HH the Amir on National Cybersecurity Strategy — Vision to Protect Kuwait's National Interest,” *Arab Times*, July 31, 2017, https://www.arabtimesonline.com/news/cait-chief-briefs-hh-amir-national-cybersecurity-strategy-vision-protect-kuwaits-national-interest/, 上网时间：2022 年 9 月 16 日。

⑧ 《国家网络安全战略》（卡塔尔，阿拉伯文）。

⑨ United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime: Draft*, February 2013, p. 53, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, 上网时间：2022 年 9 月 16 日。

法为政府提供了一个动态工具来平衡社会对安全、隐私和言论自由的需求。① 同时鉴于技术的发展速度,网络犯罪立法往往要保留一定的灵活性和解释空间来应对新技术带来的后果。

2006 年至 2021 年间,海湾阿拉伯国家陆续制定并不断更新了本国国内的网络犯罪法律,而大部分国家的网络犯罪法是在 2010 年阿盟《阿拉伯公约》这一网络犯罪的区域协议以及 2012 年"阿拉伯之春"的背景下出现并完善的。《阿拉伯公约》签署于 2010 年 12 月,除沙特阿拉伯以外的所有海湾合作委员会国家都批准了该公约。《阿拉伯公约》是在《布达佩斯网络犯罪公约》的文本基础上参照建立的,但不同于后者,《阿拉伯公约》包含了许多有政治和社会争议内容的条款。② 而阿拉伯国家网络安全法律的模糊性正体现在,尽管实际上存在有争议以及同西方国家所提倡的网络规范不相符的内容,但这些国家的法律并没有将以《布达佩斯网络犯罪公约》为代表的国际规范作为反面进行抵制或回避,而是对《布达佩斯网络犯罪公约》中的一些概念加以扩展或模糊化。例如,《阿拉伯公约》第 12 条扩大了"网络犯罪"的概念范围,将不雅内容的传播包含在内,但条约并没有给出"不雅内容"的标准和定义;第 14 条提到了"隐私"问题,但没有提及要采取任何严格的措施;第 21 条还允许各国对在线行动和言论实行更严厉的惩罚。③

此外,海湾阿拉伯国家的网络犯罪法广受西方学者诟病的原因在于,它们被认为与《阿拉伯公约》一样,将网络犯罪的概念扩大到涵盖网络政治言论。有学者指出,除巴林外,所有海湾阿拉伯国家的网络犯罪法律都有"其他法律文书所没有预见到的额外罪行",如造谣罪和污蔑罪、未经许可组织游行罪以及散布损害国家声誉的虚假新闻罪等,且"大多数海湾合作委员会的网络犯罪法律都受到人权组织的严厉批评,因为它们限制言论自由,并对公民和活动人士实施自我审查"。④ 还有学者认为,这些法律对"公共道德"和"国家团结"给出了相当广泛的定义,这意味着许多社交媒体评论、包括任何政治反对派,都可能被视为网

① United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime: Draft*, February 2013, p. 53.

② 《阿拉伯公约》第 12 条、第 13 条、第 14 条和第 15 条条款中对"与计算机有关的违反公共秩序、道德或安全的罪行"的相关规定,以及第 21 条中关于"通过计算机系统实施的加重传统犯罪的情节"的相关规定是《布达佩斯网络犯罪公约》所没有的。

③ League of Arab States General Secretariat, *Arab Convention on Combating Information Technology Offences*, 2010, https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf, 上网时间:2022 年 9 月 15 日。

④ Joyce Hakmeh, *Cybercrime Legislation in the GCC Countries: Fit for Purpose?*, London: Chatham House, July 2018, p. 9.

络犯罪。① 许多法律专家和人权活动家认为，这些网络犯罪法过度使用破坏“社会公德”条款来对社会活动者、博客异见者以及有着政治或宗教诉求的民众进行罚款、逮捕和提起诉讼，而并未真正用在处罚网络犯罪行为和保护数据资产上。② 更有甚者认为，这些国家的网络犯罪法纯粹是为了借网络犯罪的名义来对付其国内的政治反对派。③

有学者认为，这种模糊性反映了海湾阿拉伯国家在对国内网络安全、国际法和全球网络安全规范表达态度的同时，也在有意识地选择保持灰色地带的广阔空间。④ 通过这种方式，海湾阿拉伯国家在网络安全治理问题上的对外活动空间和战略回旋余地大大增加，能够在国际网络安全治理平台表达自身政治诉求的同时，通过一些双边关系和非正式渠道参与一些网络安全领域的国际对话和战略伙伴关系。从另一个角度来说，这也反映了海湾阿拉伯国家在网络安全治理问题上的战略自主性不断增强：海湾阿拉伯国家从自身的安全与发展利益出发，自主制定网络安全战略，强调走符合本国国情和文化的发展道路。在涉及网络安全与发展的问题上，海湾阿拉伯国家不是对西方惟命是从，在关系自身利益的网络安全治理问题上，在自身利益同西方不一致时，地区国家选择走自己的治理模式和道路。

第三，在区域层面，非正式和次国家层面的合作模式成为海湾阿拉伯国家区域网络安全合作的主要形式。

尽管都面临严重的网络安全威胁问题，但阿拉伯地区在网络安全领域的区域性合作机制建设方面乏善可陈。在区域层面，2010 年生效的《阿拉伯公约》是阿盟内部的一项国际法律框架，旨在促进阿拉伯国家之间在“抗击危害其国家安全、利益和联盟安全的信息技术犯罪”方面进行合作，以及使各签约国“在打击信息技术犯罪、保护阿拉伯社会安全上采取共同的刑事政策”。⑤ 目前除沙特阿拉伯以外，包括阿联酋、阿曼、巴林、卡塔尔和科威特在内的《阿拉伯公约》的 18 个

① Matt Duffy, “Arab Media Regulations: Identifying Restraints on Freedom of the Press in the Laws of Six Arabian Peninsula Countries,” *Berkeley Journal of Middle Eastern & Islamic Law*, Vol. 6, No. 1, 2014, p. 1.

② “UAE: Sweeping Legal ‘Reforms’ Deepen Repression,” *Human Rights Watch*, June 5, 2022, https://www.hrw.org/news/2022/06/05/uae-sweeping-legal-reforms-deepen-repression; Ahmed Shaheed and Benjamin Greenacre, “Binary Threat: How Governments’ Cyber Laws and Practice Undermine Human Rights in the MENA Region,” in *Digital Activism and Authoritarian Adaptation in the Middle East*, POMEPS Studies, No. 43, April 2021, https://pomeps.org/wp-content/uploads/2021/08/POMEPS_Studies_43_Draft3-1.pdf, 上网时间：2022 年 9 月 16 日。

③ James Shires, “Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf,” p. 220.

④ Ibid.

⑤ League of Arab States General Secretariat, *Arab Convention on Combating Information Technology Offences*.

签约国均正式批准了该公约。但由于该公约的条款未参照任何阿拉伯国家的网络犯罪法规,且该公约在网络犯罪的定义和相关条款上十分模糊,因此尽管已经被广泛接受,但该公约仍未正式生效。尽管公约的第五章第一条规定了“缔约国主管当局应采取必要的国内程序来实施本公约”①,但缔约国的任何国内网络犯罪法律都没有提及该公约的相关规定,公约中有关 18 个签约国之间进行协调工作的要求也毫无法律效力。但这一区域法律框架的建立仍是阿拉伯国家在构建其自身的网络安全治理体系时的重要背景。

除了阿拉伯国家联盟框架下的《阿拉伯公约》外,海湾阿拉伯国家还通过海合会、伊斯兰合作组织计算机应急响应小组(Organisation of the Islamic Cooperation-Computer Emergency Response Teams, OIC-CERT)、国际电联阿拉伯区域网络安全中心(ITU Arab Regional Cyber Security Center , ITU-ARCC)等组织建立了一些增进网络安全领域的互信与信息共享的平台,但受到阿拉伯地区主要国家之间复杂的地缘政治和宗教历史等因素影响,其网络安全合作存在较多不稳定因素,这些官方层面的国际合作机制成效十分有限。例如,海合会在网络安全合作领域仅有的参与是曾于 2006 年成立的海合会计算机应急响应联合小组,尽管受到来自主要安全盟友的外部激励,但海合会国家之间开展的官方网络安全合作仍然十分匮乏。正式的海合会级别的网络安全合作通常只是象征性的姿态:海湾合作委员会“网络安全常设委员会”的第一次会议于 2017 年 2 月在阿布扎比举行,由海湾合作委员会警察局主持。但是,与会者只是口头上表示要在海合会之间交流专业知识和经验。这与五年前广为宣传的海合会安全协议中所作的声明遥相呼应,该协议也承诺通过数字手段共享信息。该会议四个月后,卡塔尔被巴林、沙特阿拉伯和阿联酋等国完全排斥。目前,海合会作为一个组织,在网络安全方面仍处于完全的休眠状态。就目前情况而言,海湾阿拉伯国家内部打击网络犯罪的合作主要依赖于双边关系和非正式渠道,如国家间公安部门或网络安全培训机构的合作。然而,阿拉伯地区网络犯罪的频率和跨国的性质使得这些双边和非正式渠道在应对网络犯罪时的效率十分有限。

在网络安全治理的实践中,海湾阿拉伯国家逐渐探索出了一些非正式的进行区域网络安全合作的形式。例如,沙特阿拉伯同以色列在面对共同威胁时在网络安全方面开展过非正式合作,海湾阿拉伯国家内部通过区域内的学术共同体等形式也建立了非正式的合作关系。以色列与沙特等阿拉伯国家向来不和,但面对日益扩张的伊朗,双方却可以开展网络安全方面的合作。以色列国防部在 2019 年放宽了对部分恶意软件的出口管制规则,使得一些能够使用户从其他用户的硬盘驱动器中秘密获取信息的间谍软件和其他形式的恶意软件只能由沙特阿拉伯和阿联酋购买。2016 年,以色列网络情报公司 NSO Group 将以色列“飞马”

① League of Arab States General Secretariat, *Arab Convention on Combating Information Technology Offences*.

(Pegasus)间谍软件出售给了阿联酋等海湾阿拉伯国家,帮助后者政府利用这套软件入侵其国内异见人士和活动家的手机。几个月后,阿联酋活动家艾哈迈德·曼苏尔(Ahmad al-Mansur)被指控犯有破坏国家统一的罪行,并被判处有期徒刑 10 年。① 在以色列前情报人员的帮助下,阿联酋的间谍系统还可以监控土耳其和卡塔尔等其他国家的高级官员。② 2018 年曾有媒体爆出,沙特阿拉伯国内的一些反对派的电话被“飞马”间谍软件所监控,而这一间谍软件正是由以色列网络情报公司 NSO Group 所开发。③ 有学者认为,以色列公司向沙特政府销售恶意软件的这一做法加速了两国之间的和解,并为改善中东地区的稳定提供了机遇。④

尽管区域组织层面在网络安全方面的合作有所欠缺,但海湾阿拉伯国家仍通过第二轨道和第三轨道的对话协调机制在网络安全治理领域存在一定的合作关系。有学者统计出在 2007 年至 2016 年期间,海湾阿拉伯国家之间举行的网络安全会议的数量大幅增加。⑤ 其中,一些会议主要由网络安全供应商主办,一些由专业网络安全活动公司组织,还有一些得到了政府或国际组织的支持。这些非官方层面的对话协调机制从网络安全实践的角度促进了海湾阿拉伯国家在网络安全领域的信息共享,为建立国家间合作关系提供了新的途径。

四、海湾阿拉伯国家采取混合立场的动因

互联网最初是在一个高度自由和不干预的环境中出现的,但随着时间的推移,国家对威胁认知的不断变化以及网络空间给国家安全带来了一系列挑战,使得全球互联网治理中所谓的“规范回归”(norm regression)、“主权回归”的现象

① Bill Marczak and John Scott-Railton, “The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender,” *The Citizen Lab*, August 24, 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, 上网时间:2022 年 10 月 2 日。

② Wadih Awawdah, “Israeli Sources: ‘Tel Aviv Uses UAE to Spy on Qatar, Iran and Hezbollah’,” *Middle East Monitor*, October 19, 2019, https://www.middleeastmonitor.com/2019-1019-israeli-sources-tel-aviv-uses-uae-to-spy-on-qatar-iran-and-hezbollah/, 上网时间:2022 年 9 月 16 日。

③ Bill Marczak *et al.*, “The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil,” *The Citizen Lab*, October 1, 2018, https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/, 上网时间:2022 年 11 月 23 日。

④ Simon Handler, “The Zero-Day War? How Cyber Is Reshaping the Future of the Most Combustible Conflicts,” *Atlantic Council*, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-zero-day-war-how-cyber-is-reshaping-the-future-of-the-most-combustible-conflicts/, 上网时间:2022 年 9 月 16 日。

⑤ James Shires, *Moral Manoeuvres: Cybersecurity in Egypt and the Gulf States*, p. 50.

不断发生。[①] 国家控制作为网络空间一种日益增强的趋势,引发了网络空间规范的结构性变化。海湾阿拉伯国家在网络安全治理领域的行为规范的形成,同样与其对威胁认知的不断变化和网络安全带来的挑战密不可分。由于复杂的种族、宗教、教派以及域外大国等因素的影响,中东地区历来是矛盾冲突和政治动荡的多发点,而随着阿拉伯国家网络的普及和数字化的发展,这些矛盾和冲突也延伸到了网络领域,成为左右海湾阿拉伯国家在网络安全治理议题上的立场的重要因素。

(一)"阿拉伯之春"对海湾政治、文化和社会安全的影响

自 2006 年以来,针对阿拉伯国家的关键基础设施的袭击显著增加,而这些基础设施在其国家和社会的运行中发挥着重要作用。这些网络袭击采取不同的形式,目的是窃取或破坏高度保密的信息,以及通过引入恶意软件扰乱文计算机系统的活动。自此,部分阿拉伯国家开始制订有关网络安全的相关政策和法律,但网络安全问题真正引起阿拉伯国家的重视还是在 2010 年前后,网络对海湾阿拉伯国家政治、文化和社会安全的巨大冲击使得阿拉伯国家纷纷意识到网络安全的重要性,纷纷着手建立自己的网络安全治理体系。

肇始于 2010 年底的"阿拉伯之春"是一场以民主和经济为议题、旨在改变所在国社会、政治模式的社会运动,互联网在这场运动中发挥了不可替代的重要作用。"阿拉伯之春"的起因是 2010 年 12 月 17 日突尼斯一名大学生为抗议警方阻止他贩卖水果蔬菜谋生而自焚身亡,这一事件激发了突尼斯国内对于失业率高涨、物价飞涨以及政府腐败等不满情绪,短时间内蔓延成全国性的骚乱和暴力冲突,不仅导致突尼斯政权更迭,还外溢至埃及、阿尔及利亚、利比亚、阿曼等国,最终引发了阿拉伯世界一场来势猛、烈度强、持续久、影响巨大的政治和社会危机。在这场运动的发生及其产生的连锁效应中,随处都有网络的影子。大量运动参与者通过社交媒体发布信息、相互联络并进行社会动员,而网络新媒体传播速度快、辐射面广、更新速度快以及成本低等特点使得这场社会运动如多米诺骨牌一般,对阿拉伯世界的政治走向产生了深远影响,也让阿拉伯国家深刻认识到网络对于国家政治安全的巨大影响。在这场社会运动中,互联网显现了其对国家安全的巨大影响力,在运动的前期酝酿、中期谋划与实施以及后期影响扩散的整个过程中,网络都扮演了关键角色。

在"阿拉伯之春"爆发前,网络空间已经积累了民众的大量反抗情绪。在互联网新的应用形式不断出现并在海湾阿拉伯国家普及的态势下,一方面,网络成为西方国家评议、揭露众多政治现实的手段,大量有关政府腐败、暴力、无能和分裂的问题暴露在民众视野里,使其对国家政权产生了失望和不满情绪,这种情绪因网络而触发,也在网络中传播和累积;另一方面,海湾阿拉伯国家内部的一些

① Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance: A Review of Multilateralism and International Organizations*, Vol. 18, No. 3, 2012, pp. 339-361.

反政府力量意识到网络的巨大威力，并使其成为本国不满政府统治力量进行动员和抗议的平台，网络成为“阿拉伯之春”中舆论动员、民众串联的主要工具。①

这场社会运动发生之后，网络再次在其中起到了推波助澜的作用。首先，网络新媒体成功地放大了反对派大的力量与声音，使得反抗运动的人数迅速成为关键多数，这挑战并动摇了一些国家政府的根基；其次，反对力量通过脸书、推特等社交媒体完成了抗议示威的前期策划和动员任务；最后，在示威抗议运动的过程中，社交媒体放大了参与者对自身力量的预期，成为参与者用来鼓舞士气和汇集抗议力量的重要工具。“阿拉伯之春”之所以在阿拉伯世界产生“多米诺骨牌”一般的效应，与网络发挥的扩散功能也牢不可分。突尼斯小贩自焚事件的出现及其效应通过新媒体迅速在其他阿拉伯国家引发关注，这些国家的民众从突尼斯事件中得到启示，开始推动本国的社会运动和“革命”，民众将这些倡议和观点发布到网络空间并使其经网络广泛传播，进一步推动了人气的聚集。而相较于传统媒体时代，网络时代的政府在新闻传播中的直接控制力也相对减弱。网络社交媒体去中心化的模式使得屏蔽网络的效果甚微，也使得政府对网络空间信息传播的把关能力被严重削弱。在突尼斯发生政变之前，尽管该国政府对当地新闻媒体已经严格管制，却无法阻止游行示威的画面和信息在网络上传播。同时，网络也为西方国家在这场运动前期进行意识形态渗透和情绪煽动提供了机会，助推了这场危机的持续深化。

“阿拉伯之春”运动发生后，海湾阿拉伯国家对网络安全，尤其是网络空间的内容管理和信息安全给予了更高程度的重视，这反映在其网络安全战略的目标描述中。这些战略中的网络安全目标被描述为网络、数字、信息或电子安全。②有学者认为，国家战略中的语言差异反映了国家在治理方式上的不同，如在社会层面，这些国家的网络安全战略使用的更多是中国和俄罗斯所使用的“信息安全”的概念而非“网络安全”的概念。③ 这种重视更直观地反映在“阿拉伯之春”后海湾阿拉伯国家更新的网络犯罪相关法律规定上，如 2011 年更新的阿曼法律有一节明确题为“内容犯罪”，涵盖任何使用信息通信技术“制作、出版、分发、购买或拥有任何可能损害公共秩序或宗教价值的东西”。④ 阿联酋政府在 2012 年更新的网络犯罪法中更是直接禁止了任何形式的网络政治辩论。

---

① 蔡翠红：《网络时代的政治发展研究》，北京：时事出版社 2015 年版，第 141-145 页。

② James Shires, “Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf,” p. 220.

③ Keir Giles and William Hagestad II., “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English,” in Karlis Podins, Jan Stinissen and M. Maybaum, eds., *2013 5th International Conference on Cyber Conflict*, Tallinn: NATO CCDCOE, 2013, p. 2.

④ “Royal Decree No 12/2011 Issuing the Cyber Crime Law,” *Government of Oman*, 2011, https://www.qcert.org/sites/default/files/public/documents/om-ecrime-issuing_the_cyber_crime_law-eng-2011.pdf, 上网时间：2022 年 9 月 16 日。

除政权方面的国家安全考量外,对文化和社会安全的特别关切也是理解海湾阿拉伯经济体在实践网络安全规范时的重点。有学者认为,阿拉伯国家往往具有“整体社会”(holistic society)的特征,即存在一种文化意识形态(大多以宗教的形式存在)主张在所有行动和思想领域的有效性。在一个整体社会中,一个行动的合法性是基于“上级施加的具有普遍约束力的道德规定”,而非经济逻辑、政治逻辑或法律逻辑。① 这意味着,文化和社会因素对这些国家的网络安全实践具有重要影响。例如,2010 年 8 月,沙特阿拉伯扬善惩恶委员会宣布将成立打击网络犯罪的单位,并将打击网络犯罪的重点放在了涉及网络勒索妇女的一系列案件中,这与妇女在阿拉伯社会中的独特地位和作用以及女性网络犯罪受害者的污名化程度有关。这也是海湾阿拉伯国家对网络安全,尤其是网络空间的内容管理和信息安全给予了更高程度重视的原因。

第一,网络空间对抗已成为中东地区竞争和冲突的新形式。

地区竞争是促使海湾阿拉伯国家加强网络安全治理的另一项重要动力,而中东地区成为世界上网络攻防战最为频繁的地区之一,是中东地区的霸权斗争、领土争端以及低强度冲突的自然结果。② 中东地区历来矛盾错综复杂、相互交织,这些矛盾不仅体现在连绵不断的武力战争中,也逐渐延伸至网络空间。在如今网络战争频发的时代,网络领域可以为埃及、伊朗和沙特阿拉伯等中等大国提供非同寻常的不对称权力使用机会,使它们在地区政治的权力竞赛中获得更有利的地位。③ 同时,地区大国还可以利用网络新技术来扩大自己在区域层面的影响力,或是借此削弱区域内的竞争对手。这些地区大国也会根据任务聘用黑客或网络战士来代表政府进行网络活动。海湾阿拉伯国家之所以同欧美私人网络安全公司之间形成密切的合作关系,不仅是出于应对层出不穷的网络攻击的需要,也有提高进攻性网络安全能力以参与地区竞争的考量。

在石油、天然气等能源行业,中东地区能源出口国之间存在激烈竞争,这些竞争同国家间矛盾紧密交织在一起,使得石油天然气开采系统中涉及的工业控制系统以及外连互联网设备均成为这场能源战中网络攻击的目标。从 2010 年起,以沙特阿拉伯为代表的海湾阿拉伯国家连续遭受了一系列重大网络攻击事件。2012 年 8 月,占沙特政府收入 80%的国有石油企业、同时也是全球能源市场

① Nir Kshetri, *Cybercrime and Cybersecurity in the Global South*, Houndmills: Palgrave Macmillan, 2013, pp. 119-134.

② James Shires, “Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf,” p. 205.

③ Halil Kürşad Aslan and İkra Ercanlı, *Controversial Issues in Global Internet Governance and Their Reflection in Middle Eastern States and Societies*, The Center for Middle Eastern Studies (ORSAM), December 2020, https://www.orsam.org.tr/d_hbanaliz/controversial-issues-in-global-internet-governance-and-their-reflection-in-middle-eastern-states-and-societies-1_1.pdf, 上网时间:2022 年 9 月 16 日。

最大的石油生产公司和世界第六大石油炼制商——沙特阿美石油公司(Saudi Aramco)内部通信网络遭到了沙蒙(Shamoon)病毒的入侵。该病毒导致沙特阿美公司的3万多台电脑受损,磁盘上的所有数据都被删除并被一张燃烧的美国国旗图片所取代,造成袭击的恶意软件一度试图从业务系统入侵该公司的油气生产和分销网络,使得这家供应全球10%原油的公司完全暴露于网络威胁之中。为阻止病毒进一步扩散,沙特阿美公司被迫停止运作并封锁了所有员工的电子邮件和互联网接入,这使得公司的生产经营活动停止了数周,使沙特蒙受巨大经济损失。2016年11月和2017年1月,同样的软件沙蒙2.0再次对沙特阿美公司实施了攻击。同时,网络攻击并不是单向的,有进攻也有反击。网络领域的安全困境一直在发挥作用。2016年5月,伊朗和沙特之间网络紧张局势升级,沙特黑客破坏了伊朗统计中心的网页。作为回应,“伊朗安全小组”损坏了阿卜杜勒·阿齐兹国王大学和沙特国家统计总局的网站。在接下来的一段时期内,沙特与伊朗相互之间网络攻击频发,包括伊朗司法部、外交部、警察和网络警察部队以及沙特商务部在内的多个网站遭到破坏,伊朗和沙特的黑客展开了一场激烈网络战争。

与国家间紧张关系相对应,近年来,阿拉伯世界陆续出现了多个高级持续性威胁(Advanced Persistent Threat, APT)组织,针对海湾阿拉伯国家的金融、石油和天然气行业,以及公用事业和交通基础设施的APT攻击更是层出不穷。① 相对于普通的黑客攻击,APT攻击的针对性、持续性强,攻击的复杂程度更高,且隐蔽性更强。APT组织则是主要以获取政治、经济利益为目的,或是窃取目标的核心资料,或是对关键基础设施进行破坏的黑客组织。相比于普通的黑客组织,APT组织一方面组织更为严密,技术能力更强,一方面往往具有国家背景,以国家利益为主导发起攻击。APT组织的攻击十分隐蔽,攻击目标和对象常常难以明确,其国家背景往往也十分模糊。鉴于中东地区复杂的地区局势,现实世界国家间的冲突也常常延伸到网络空间,每当中东地区局势紧张、地缘政治和军事冲突升级,网络空间的APT攻击活动也会更加猛烈。这使得海湾阿拉伯国家所面临的网络安全环境比世界上的其他地区更加复杂。这一系列事件提升了海湾阿拉伯国家对网络威胁的认识,令其对未来网络袭击的恢复能力重视了起来,一些阿拉伯国家纷纷投入大量资源提升自身网络安全能力,并推进国内和国际措施来解决其网络安全问题。

地区竞争与冲突除了带来客观的安全威胁以外,也为海湾阿拉伯国家的网络能力建设和网络安全实践提供了空间和合法性来源。有研究认为,海湾阿拉伯国家的政府和网络安全公司在将伊朗描绘成“不可预测的”和“破坏性的”国家

① 近年来出现的以海湾阿拉伯国家为攻击目标的APT组织有Leafminer、OilRig、DarkHydrus、MuddyWate、Equation Group、MoonLight、Lyceum等,攻击的行业包括能源、政府、军事、金融、通信、科技公司、教育机构等,沙特阿拉伯、阿联酋、科威特和卡塔尔等海湾阿拉伯国家都曾成为APT组织的攻击对象。

方面存在算计。对于海湾阿拉伯国家而言,伊朗在该地区的活动为其围绕网络活动的安全化行为以及其在解释网络安全国际规范方面提供了灵活的空间。网络安全公司也通过提出关于伊朗网络安全威胁的报告以期进入海湾地区有利可图的网络安全市场。① 因此,政府和企业都在积极强化和重新诠释网络安全作为国家安全的一个维度。这也能够解释为什么海湾阿拉伯国家在私营部门方面同西方国家存在的密切的网络安全联系。

也有学者认为,网络空间的作战并不会加剧中东地区的紧张局势,反而可以缓解区域紧张局势,为国家间冲突的进一步升级提供可替代的缓和方案。② 这类观点认为,网络攻击作为一种等级较低的国家风险形式,可以成为一国向敌对方释放不使用武力的信号的手段,甚至有可能缓解紧张或是挑衅性的局面。同时,网络战还具有成本低、风险低、影响大的优势。

第二,经济和数字化转型催生安全漏洞和对网络安全的巨大需求。

提高网络安全防御能力以及扩大其网络空间能力是海湾阿拉伯国家进行国内经济发展的重要一环,新冠肺炎疫情大流行与国际油价大幅下跌使得这一需求更加紧迫。2016 年,沙特政府提出《沙特 2030 愿景》(*Saudi Vision 2030*),强调本国经济发展要减少对能源的依赖,努力实现经济多元化并大力发展卫生、教育、基础设施、娱乐和旅游业,这一计划的核心正是关注技术、数字转型和数字基础设施的建设。与此类似,其他海湾阿拉伯国家也制定了国家转型计划,都声称要将经济重心从能源转向科技和创新,注重发展智能城市、电子政府等新兴领域以及卫生、金融等技术娴熟的部门,强调减少公共部门在生活所有领域的作用,通过更好的教育和更高的国民待遇吸引在外侨民回国。虽然这些转型计划本身没有涉及网络空间治理的问题,但它们为海湾阿拉伯国家开展网络安全治理提出了更高要求和变革方向。

海湾阿拉伯国家在追求经济和社会发展的过程中日益强调并依赖数字化,但这也扩大了其遭受网络攻击的可能漏洞。随着其经济数字化程度的提高,该地区在数字技术方面的落后使得大量网络安全漏洞得以暴露。阿联酋网络安全公司暗物质(DarkMatter)2019 年发布的报告指出,中东四分之三的油气公司都存在某种形式的网络安全漏洞,大多数网络入侵都利用了过时的软件或弱密码,83%的公司使用的是未经验证的软件,91%的公司使用的旧软件缺乏关键的网络安全补丁,90%的公司使用不安全的网络协议负责管理系统之间的通信。③

2020 年新冠肺炎疫情暴发之初,阿拉伯地区主要国家遭受的恶意软件攻击

① James Shires, *The Politics of Cybersecurity in the Middle East*, New York: Oxford University Press, 2021, p. 56.

② Simon Handler, "The Zero-Day War? How Cyber Is Reshaping the Future of the Most Combustible Conflicts".

③ DarkMatter, *Cyber Security Report*.

增加了22%，垃圾邮件攻击增加了36%。① 海湾地区国家丰富的能源资源及其战略地位，使得这些国家的公共和私营部门的信息与通信技术（ICT）基础设施持续受到网络安全威胁，这些网络攻击在金融、运营和战略层面对经济产生巨大的影响，可能会削弱公民对政府服务和管理的信任进而影响该国的政治稳定，也可能导致网络犯罪分子的进一步攻击。同时，疫情还加速了这些国家的数字化转型，远程办公、网上购物以及线上教育的推广对整个地区的网络安全维护提出了更高要求。疫情期间各种形式的通信被传输到互联网，重要数据存储于数据云，网络安全的维护水平已成为衡量企业业绩和数字化转型的重要指标之一。企业和政府管理部门不仅需要通过投资新技术和实施抵御网络攻击的安全措施以提高网络空间的安全水平，还需要提升工作人员维护网络安全的意识和能力，这意味着这一地区在网络安全防护方面的支出还将不断增加。据数据分析公司的估计，自2022年至2029年，海合会国家网络安全市场规模将以至少7.6%的年增长率持续增长。②

第三，联盟关系及其变化是影响海湾阿拉伯国家网络安全治理立场的重要因素。

美国是海湾阿拉伯国家的长期盟友，也是为海湾阿拉伯国家提供安全保护最重要的域外大国。美国与海湾阿拉伯国家的安全合作涵盖军售、军事人员培训、反恐、推动中东和平进程等多个领域。军事领域的联盟关系为海湾阿拉伯国家同美国等西方国家在网络安全领域的合作关系奠定了基础。随着美国维持中东地区秩序能力和意愿的下降，海湾阿拉伯国家进一步认识到独立维护国家安全的重要性，由此在维护自身网络安全方面的自主性进一步凸显。奥巴马政府时期，美国国内对美国在中东地区的军事干预和推行“大中东民主计划”的反对声日益高涨。美国政府将战略资源转移到亚太地区，在中东实行战略收缩，以配合“亚太再平衡”战略的实施。美国在中东地区的战略收缩使海湾阿拉伯国家逐渐意识到，美国不愿像过去那样通过军事等手段维护中东地区既有的安全秩序。“阿拉伯之春”发生后，美国不仅放弃了盟友穆巴拉克政权，还通过网络外交在中东的政局动荡中推波助澜，利用网络平台传播美式自由民主价值观，通过美国信息技术公司提供技术支持，确保阿拉伯国家反对派的网站处于运营状态，为其普及现代网络通讯工具的使用，强化组织联系沟通与信息交换，提高政治组织的运行效率和政治影响。这使得阿联酋等美国的地区盟友进一步意识到独立维护自

① Aleksander Olech and Karolina Siekierka, “Cybersecurity in Saudi Arabia,” *Instytut Nowej Europy*, October, 11, 2021, https://ine.org.pl/wp-content/uploads/2021/08/Cybersecurity-in-Saudi-Arabia.pdf, 上网时间：2022年9月16日。

② “GCC Cyber Security Market-Industry Trends and Forecast to 2029,” *Data Bridge Market Rearch*, August 2022, https://www.databridgemarketresearch.com/reports/gcc-cyber-security-market, 上网时间：2023年4月15日。

身安全和政策自主性的重要性,在“阿拉伯之春”后的网络安全战略制订和网络安全法律实施过程中,海湾阿拉伯国家更加明确地从自身安全与发展利益出发,自主制定网络安全战略和法律,并强调走符合本国国情和文化的发展道路。

区域内国家间的关系变化同样对海湾阿拉伯国家的网络安全治理产生重要影响。地区国家间的紧张关系向来是海湾阿拉伯国家开展区域安全合作的重要障碍。历史上,阿联酋曾一度将沙特视为国家安全的第二大威胁,但本国的脆弱性使得阿联酋无力左右地区局势而被迫加入沙特倡导成立的海合会,以避免受到地区动荡带来的负面影响。“阿拉伯之春”发生后,地区国家无法独自承担维护地区秩序的现实,迫使其结成战术性联盟,以共同应对冲击地区安全与稳定的威胁,其中就包括网络安全威胁。这些战术层面的合作旨在最大限度避免“阿拉伯之春”对海湾阿拉伯国家政权的冲击,以及应对伊朗地区扩张、政治伊斯兰力量兴起和宗教极端主义抬头对地区秩序和国家安全造成的冲击。出于同样的目的,部分阿拉伯国家选择缓和同以色列之间的紧张关系,2020 年阿联酋和巴林相继与以色列实现了关系正常化,根据新协议,预计以色列与这些国家将进一步加强在网络安全领域的交流与合作,①沙特同以色列的关系同样因网络安全领域的合作而有所改善。这是海湾阿拉伯国家得以通过第二轨道和第三轨道的对话协调机制在网络安全治理领域推进区域安全合作的重要原因。

五、结论

受复杂的种族、宗教以及地缘政治等因素影响,中东地区向来是网络安全问题的重灾区,网络战场逐渐成为地区冲突的新区域。本文研究了海湾阿拉伯国家在网络安全治理议题中的混合性立场及其成因。不同于既有研究将处于中间地带的海湾阿拉伯国家作为“规范扩散”的接受者,或以“规范挪用”的视角将其置于大国战略竞争的框架下解释其混合性立场,本文从海湾阿拉伯国家在国际、国内和区域层面的网络安全治理实践等角度,考察了这些国家在国际网络安全规范领域的真实立场。在国际治理平台,海湾阿拉伯国家在网络安全规范之争中的定位十分谨慎,在网络大国之间巧妙地采取混合性立场:在围绕网络犯罪国际协定等问题的多边论坛,海湾阿拉伯国家同中国、俄罗斯等国家的立场相近,但在私营部门的网络安全合作、政府间的情报关系以及进攻性网络活动领域,这些国家同欧美国家之间也存在密切联系。在国内层面,海湾阿拉伯国家国内的政策和法律框架为其国家权力的行使保留了较大的灵活性和解释的空间。在区域层面,非正式的合作模式和次国家层面的对话协调机制是海湾阿拉伯国家进

① [巴林]优素福·哈姆丹:《以色列批准与阿联酋的航空和科学合作协议》(阿拉伯文),《日子报》(Alayam)网站,2020 年 11 月 30 日,https://www.alayam.com/alayam/world/882260/News.html,上网时间:2022 年 9 月 16 日。

行区域网络安全合作的主要形式。面对域外大国竞争时，作为中间地带的海湾阿拉伯国家并非只是在被动接受外部网络安全规范，或是简单地通过“两面下注”实现“对冲”，其无论是在立场取向还是在治理措施上都选择了更符合自身利益的网络安全治理道路。

海湾阿拉伯国家在网络安全治理领域所形成的规范是复杂因素作用的结果。首先，对国内政治、文化和社会安全的考量是海湾阿拉伯国家将网络活动安全化的直接原因。“阿拉伯之春”之后，网络传播的巨大影响力及其对政治安全的威胁逐渐引起阿拉伯国家领导人的重视，为他们制定网络安全战略与加强网络安全立法提供了重要契机。对文化和社会安全的特别关切也是海湾阿拉伯国家对网络安全，尤其是网络空间的内容管理和信息安全给予更高程度重视的原因。其次，随着网络空间的对抗成为中东地区竞争和冲突的新形式，加强网络安全能力以参与地区竞争成为海湾阿拉伯国家网络安全治理的另一项重要动力。在这一过程中，海湾阿拉伯国家的政府和网络安全公司在将网络安全提升至国家安全的重要维度方面，不同程度地发挥了作用。再次，海湾阿拉伯国家在追求其经济和社会发展的过程中日益强调并依赖数字化，但这事实上扩大了其网络攻击面，催生了对网络安全产品和网络安全治理的巨大需求。最后，联盟关系及其变化是影响海湾阿拉伯国家对网络安全治理，尤其是跨国网络安全合作态度的重要因素，这也为其在区域安全合作领域实践网络安全规范奠定了基础。

海湾阿拉伯国家数字经济发展的潜力巨大，中国同海湾阿拉伯国家在数字领域的合作前景广阔。自中国国家主席习近平在 2017 年第一届“一带一路”国际高峰论坛上提出建设“数字丝绸之路”以来，海湾阿拉伯国家纷纷积极响应。2017 年 12 月，中国同沙特阿拉伯、埃及、阿联酋等七国共同发起了《“一带一路”数字经济国际合作倡议》，致力于构建实现互联互通的“数字丝绸之路”。在同海湾阿拉伯国家共建“数字丝绸之路”的过程中，如何确保数据安全、提升网络安全水平、应对地区复杂网络安全威胁的挑战，是中阿双方需要共同解决的命题。因此了解海湾阿拉伯国家的网络安全治理现状、其在网络安全治理议题中的立场、态度及其影响因素，对于中国同海湾阿拉伯国家开展数字领域合作、在国际网络安全治理平台共同捍卫发展中国家权益、推动尊重网络主权等安全规范的国际化，具有重要现实意义。同时，伴随海湾阿拉伯国家数字化进程不断加快，其对网络安全产品的需求也在不断增加，中国应努力在对海湾阿拉伯国家的网络安全和发展战略及现状加深了解的基础上，通过与海湾阿拉伯国家的战略对接和政策沟通实现需求对接，帮助海湾阿拉伯国家加强数字基础设施建设，进而推动中阿合作不断深化。

（责任编辑：包澄章　责任校对：章　远）

Abstracts

3 Cross-border E-Commerce Cooperation Between China and Arab Countries: Current Situation, Challenges and Countermeasures

Abstract Arab countries are important partners of China's "Digital Silk Road", and the cooperation of cross-border e-commerce between China and Arab countries has become a new choice for deepening digital economic cooperation between China and Arab countries and achieving mutual benefit and win-win results. The penetration rate of e-commerce in the Arab countries is generally low, while the market potential is huge. The Covid-19 accelerates the further release of online purchasing power in the Arab region, and promotes Arabic e-commerce to enter the stage of rapid development, and also brings opportunities to strengthening cooperation in the field of e-commerce between China and Arab countries. Based on the docking of the government levels of the two sides, cross-border e-commerce cooperation between China and Arab countries covers e-commerce platforms, logistics services, electronic payment and other key areas and achieved significant progress. At the same time, there are many constraints in payment cooperation and the supply of e-commerce talents, and constraint the further deepening cooperation between the two sides. Chinese cross-border enterprises should take positive measures for key issues and key difficulties, and promote the high-quality development of cross-border e-commerce cooperation between China and Arab countries through compliance management, brand strategy, overseas warehouse construction, localized cooperation, and strengthening the training of e-commerce talents.

Key Words China-Arab Cooperation; E-Commerce; Cross-border E-commerce; Digital Economy

Authors LIU Bin, Ph. D., Associate Professor, Zhejiang International Studies University; Adham Sayed, Ph. D., Associate Professor, Zhejiang Gongshang University.

21 Complex Intermediate Zone: The Positions and Motivations of the Gulf Arab States in the Cybersecurity Norm Debate

Abstract With the intensification of strategic competition among major powers and the development of global political multipolarity, the position of the Gulf Arab states in the global cybersecurity governance cannot be ignored. By examining the position of six Gulf Arab states, Saudi Arabia, Kuwait, Qatar, the UAE, Oman and Bahrain in the international cybersecurity norm debate, and their cybersecurity governance practices, this paper finds that the Gulf Arab states have chosen a path of cybersecurity governance that is in line with the interests of the intermediate zone. On the international cybersecurity governance platform, the Gulf Arab states occupy a mixed position between the two camps. At the domestic level, the Gulf Arab states' domestic policies and legal frameworks allow for greater flexibility in the exercise of state power. At the regional level, informal cooperation and sub-national dialogue and coordination mechanisms are becoming the main forms of regional cybersecurity cooperation among Gulf Arab states. Considerations of political security and cultural and social security, the emergence of new forms of regional competition and conflict, the security vulnerabilities and huge demand for cybersecurity generated by economic and digital transformation, as well as the alliance relations at the international level are important factors influencing the position of these Arab countries in the international cybersecurity norm debate.

Key Words Gulf Arab States; Cybersecurity; International Norms

Authors CAI Cuihong, Ph. D., Professor, Center for American Studies, Fudan University; ZHANG Ruoyang, Ph. D. candidate, School of International Relations and Public Affairs, Fudan University.

44 On the NGOs' Activities and Roles in the Jordanian Livelihood Fields

Abstract The Jordanian NGOs have launched numerous activities in the livelihood