DOI:10.14015/j.cnki.1004-8049.2023.01.007
苗争鸣:“网络赋权北约亚太扩张演进路径及其影响”,《太平洋学报》,2023年第1期,第79-91页。
MIAO Zhengming,“The Cyber Empowering NATO's Asia-Pacific Expansion:Evolution,Paths and Influence,” *Pacific Journal*, Vol. 31, No. 1, 2023, pp.79-91.

网络赋权北约亚太扩张演进路径及其影响

苗争鸣[1]

(1.清华大学,北京 100084)

摘要: 北约在物理空间与网络空间都有意增强全球影响力。自1949年成立至今,北约已实施8轮扩员,而在网络空间北约同样呈现扩张特征。传统关于北约影响亚太权力格局观点,主要是从北约霸权扩张、同盟机制以及国际组织官僚能力角度,鲜有基于数字时代网络赋权北约塑造亚洲权力格局的技术能力视角。数字化时代北约在网络空间战略演进可划分为网络安全认知萌芽、网络攻防能力发展和网络地缘重心扩散三阶段,在此过程中北约扩充网络盟国数量,构建网络规则体系与增强网络互操作性实践能力,塑造其亚太影响力。通过分析北约网络合作防御卓越中心等机构的具体行动,梳理其在网络空间亚太扩张态势、特征及对亚太权力格局的影响,能够为学界提供网络技术赋权北约塑造亚太权力格局的补充性解释。

关键词: 北约;亚太扩张;网络赋权;网络合作防御卓越中心

中图分类号: D815 **文献标识码:** A **文章编号:** 1004-8049(2023)01-0079-13

北约作为北大西洋区域性军事安全组织,近年有在安全领域扩大全球影响的趋势。北约于1949年成立,从1952年开始到2020年实施8轮扩员,成员国家已从12个创始国,变成目前的30个。北约源自冷战时期美国领导对抗苏联集团的地区安全军事组织,其活动范围一直在北美与欧洲地区。近年北约自身全球化战略转型进程加快,其在欧洲内部积极扩员的同时,也在不断拓展其全球影响力。特别是在乌克兰危机爆发后,北约抱团对乌克兰实施经济支持、政治声援与军事援助,北约联盟属性再次被“激活”,在美国的推动下,北约有意捆绑中俄,扩大其战略竞争对象,全球阵营化对立态势日益明显。

北约积极与亚太国家发展互动关系。北约与9个全球合作伙伴在政治协商与情报共享领域密切合作,其中包括日本、蒙古、韩国、阿富汗、伊拉克和巴基斯坦等亚洲国家。北约

收稿日期: 2022-08-16;**修订日期:** 2022-11-10。
基金项目: 本文系国家社科基金青年项目“中美网络空间竞争与权力测量研究”(22CGJ005)的阶段性研究成果。
作者简介: 苗争鸣(1990—),男,安徽亳州人,清华大学国际关系学系博士后,清华大学战略与安全研究中心助理研究员,法学博士,主要研究方向:技术与国家安全。
* 感谢《太平洋学报》编辑部和匿名审稿专家提出的建设性修改意见,文中错漏均由笔者负责。

与四个亚太伙伴国——日本、澳大利亚、新西兰与韩国接触密切,定期举行政治与军事安全态势感知会议,并特别强调加强不受地理约束的网络空间合作。2020年12月,北约与日本、澳大利亚、新西兰与韩国四国首次举行外长会晤,商讨如何平衡所谓的"中国力量崛起"。2022年6月,上述四国领导人首次受邀参加北约马德里峰会。特别是日本有意与带有"暴力多边主义"性质的北约加强合作,①如日本外务大臣林芳正称,日本欢迎北约发展与亚太国家的伙伴关系,日本愿为实现"自由开放的印太"(Free and Open Indo-Pacific, FOIP)而努力,也有意愿推动北约进一步参与亚太区域事务。②

此外,北约加强涉华事务的参与力度。一方面,北约不断在涉华议题上,跟随美国"印太战略"节奏,污蔑中国"威胁国际制度"。如北约发布"北约2030议程",明确提出加强联盟集体防御韧性及技术合作力度,特别在网络空间强调合作,应对所谓的"中国威胁"。③ 另一方面,北约加大与中国周边国家如日韩等国合作制衡中国。从历史上看,北约与中国交集较少,北约首次引起中国关注是在1999年,其轰炸中国南斯拉夫大使馆引发民众声讨,而后在2003年建立半官方半民间关系。④ 近年北约参与涉华事务频次增多,如2019年北约70周年峰会上,其认为中国崛起将带给北约"机遇和挑战",因而要应对中国崛起影响,但尚未将中国定位为"威胁",2021年北约布鲁塞尔峰会上,其首次称中国为国际秩序和北约安全的"系统性挑战"(systemic challenges)。

综上可知,北约近年逐步扩大在全球、亚太以及与中国相关议题和事务上的影响力,开始在亚太特别是中国周边参与地区权力格局塑造,威胁亚太及中国周边安全。上述现象构成本研究问题:北约如何从一个北大西洋区域性国际军事组织,逐步在亚太地区产生巨大影响力?北约"跨地缘"在亚太实现势力扩展和影响力塑造的动能来自哪里?

一、既有研究及其不足

学界关于北约获取亚太影响力的研究,鲜有网络盟国亚太扩张的视角和成果,大多是基于传统国际关系理论视角,具体来看可归纳为三种观点。(1)北约追求全球化的霸权扩张视角。该视角强调北约国家具有欧洲霸权国基因和历史积淀,其全球扩张经验丰富;(2)北约关联美国盟友体系的同盟理论视角。该视角涉及三个维度,一是北约维度:北约跟随美国"印太战略",以此获得战略利益。二是美国维度:美国主动拉拢北约作为美国扩大全球影响力,增强霸权投射能力的工具。三是亚太维度:亚太成为全球战略核心,日韩等国积极拉拢北约入局,部分亚太国家倾向"脱亚向西",加强与北约国家互动;(3)北约组织与领导人维度的国际官僚组织视角。该视角强调北约作为国际官僚组织,其最大限度追求组织自我生存利益,确保组织存活并推动组织扩张。⑤ 具体表现为,一方面北约作为国际组织,需要拓展生存空间,其不断加入地缘政治热点区域,以获得"存在感"和"需要感"。⑥ 另一方面北约秘书长依靠丰富的外交经验,能够协调成员国间的利益诉求,将内部矛盾转移到外部,并运筹北约组织跟随美国找到所谓"共识性竞争对手"。

---

① 刘江永:"战后日本国家战略演进及岸田内阁战略走向",《东北亚论坛》,2022年第1期,第31页。

② Minister of Foreign Affairs of Japan, "Foreign Minister Hayashi Attends the Meeting of NATO Ministers of Foreign Affairs," April 7, 2022, https://www.mofa.go.jp/erp/ep/page4e_001226.html, 访问时间:2022年7月15日。

③ NATO, "Leaders Agree NATO 2030 Agenda to Strengthen the Alliance," June 15, 2021, https://www.nato.int/cps/en/natohq/news_184998.htm? selectedLocale=en, 访问时间:2022年7月1日。

④ 许海云:"北约对华政策调整走势及其影响",《太平洋学报》,2022年第1期,第25页。

⑤ 吴文成:"组织文化与国际官僚组织的规范倡导",《世界经济与政治》,2013年第11期,第107页。

⑥ 吴昕泽、王义桅:"北约再转型悖论及中国与北约关系",《太平洋学报》,2020年第10期,第27页。

1.1　全球扩张视角

该视角强调北约具有全球霸权扩张的基因。欧洲天然霸权文化赋予北约通过全球化来体现组织价值,[①]其有意愿成为世界警察,维护全球安全和自由秩序。[②] 北约强调全球的威胁不能依赖区域性组织解决,北约需要向非欧洲国家如日本、韩国等开放,以实现民主国家的集团自卫目的。[③] 且北约内部存在强大的自由主义改革派追求基于民主价值观念的多边合作,推动北约全球化进程。[④] 此外,随着北约参与全球事务的增多,北约的世界话语权与议程设置能力逐步增强。但北约追求全球化过程中,出现一种观点认为北约面临的威胁将超越地理界限,特别是中国崛起将威胁美欧主导的国际秩序和价值观,造成北约主动将中国作为攻击与竞争对象,[⑤]而乌克兰危机爆发后,北约将中俄捆绑,更关注涉及中国安全领域的问题。欧洲作为威斯特伐利亚体系的发源地,曾是全球地缘政治中心。特别是北约成员国英国,作为曾经的“日不落帝国”,其有强大意愿推动北约参与全球安全事务,如英国前首相利兹·特拉斯(Liz Truss)曾指出,冷战后的世界秩序不再有效,需要构建“全球北约”,以增强北约在全球地缘政治中的作用。随着亚太在大国竞争战略中地位的上升,其对关注全球安全的国际组织具有天然吸引力。

1.2　同盟理论视角

该视角强调北约依赖美国盟友体系发挥影响力。联盟作为美国战略的核心,是其保持优势的重要因素,增强美国全球影响力的投射空间。2022 年美国《国家安全战略报告》称支持北约适应包括网络空间防御在内的现代安全挑战。北约依附美国的全球霸权战略与“印太战略”,在逐步融入亚太过程中赋予其区域影响力。美国全球战略转移到亚太地区,北约作为美国全球联盟体系的关键节点,也跟随美国战略将中国视为其关键对象。北约与美国及其盟友互动关系历史悠久,特别是在“9·11”之后,美国将北约作为打击全球恐怖主义的桥梁,确保美国全球反恐战略的实现,[⑥]而北约也将美国作为通往全球的重要地缘政治纽带。随着全球政治和经济重心正从北大西洋转向亚太,北约有意通过美国的全球战略,在亚太实现北约自身利益诉求。[⑦]

最后,是亚太亲北约国家的拉拢和推动作用。以东北亚地区日韩为代表,其积极参与北约的全球战略,意图将北约拉入亚洲地区,参与北约国家构建的准联盟体系,推动北约将中国作为战略目标,[⑧]以此实现“脱亚向西”的目的。特别是日韩近期向美欧靠拢,明确自身属于西方民主阵营的身份认同:韩国认为其政治体制、意识形态与美国相似,其内在认同通过外在具象化的表现为“反华亲美”。日本受到欧盟等西方势力拉拢,积极参与北约活动,如加入北约网络防御计划,对抗所谓中国“威胁感知”。北约称日本为可信赖的“天然伙伴”,彼此拥有共同的自由、民主、人权、法治价值观和战略利益,同时面临崛起中国的挑战。此外,鉴于日韩在中国周边的特殊的地缘战略位置,在美国“重返亚太”与“印太战略”中的作用愈发凸显,加上北约拉拢日韩合作,增加其“全球联盟”的政治、经济和军事实力,特别是增加亚太影响力,亚太版“小北约”有加速形成趋势。

---

① Andrew Cottey, “NATO: Globalization or redundancy?” *Contemporary Security Policy*, Vol.25, No.3, 2004, pp.391-408.

② Karl-Heinz Kamp, “A global role for NATO?” *The washington quarterly*, Vol.22, No.1, 1999, pp.5-11.

③ Ivo Daalder and James Goldgeier, “Global Nato,” *Foreign Affairs*, Vol.85, No.9, 2006, pp.105-113.

④ Tobias Bunde and Timo Noetzel, “Unavoidable Tensions: the Liberal Path to Global NATO,” *Contemporary Security Policy*, Vol.31, No.2, 2010, pp.295-318.

⑤ Liselotte Odgaard, “NATO's China Role: Defending Cyber and Outer Space,” *The Washington Quarterly*, Vol.45, No.1, 2022, pp.167-183.

⑥ Umair Pervez Khan and Kashaf Sohail, “Globalization and the Changing Concept of NATO,” *AUSTRAL: Brazilian Journal of Strategy & International Relations*, Vol.10, No.20, 2021, p.194.

⑦ Zbigniew Brzezinski, “An Agenda for NATO: Toward a Global Security Web,” *Foreign Affairs*, Vol.88, No.5, 2009, pp.2-20.

⑧ 刘江永:“世界大变局与中美日三国战略选择”,《东北亚论坛》,2020 年第 3 期,第 12 页。

1.3 国际官僚视角

该视角强调北约组织与领导人的官僚能力突出。国际组织作为自主性独立行为体,发挥重要领导作用,[①]其领导人能在受限的组织与环境中开展工作,而且做出助于组织发展的政治选择。[②] 北约领导人自身领导能力出色,能够公开接受对本组织危害最小的要求,同时巧妙地抵制破坏组织完整性的要求。北约秘书长斯托尔滕贝格(Jens Stoltenberg)根据美国总统的特质,灵活运用程序权力,调整2018年北约峰会公共议程设置,并战略性回应特朗普的言论。北约作为一个具有适应能力的安全组织,其现有权力比成员国赋予的权力更大。[③] 而对于法国总统马克龙(Emmanuel Macron)的北约"脑死亡"言论,斯托尔滕贝格则回应北约具有自我调适能力,是"最成功的联盟体系",并强调北约能"克服分歧,围绕核心任务"团结起来。[④]

北约秘书长的领导力和组织内关键决策者,塑造北约发展行动议程。[⑤] 北约联盟"国际化"的特征之一是后冷战时代秘书长政治地位的提高,北约选择一位前国家元首担任北约发言人并组织北约峰会,表明北约提升秘书长在组织内部及全球政治中的话语权,特别是在战争决策中,北约秘书长影响和塑造集体决策。例如北约曾对波斯尼亚发动军事打击,时任北约秘书长威利·克拉斯(Willy Claes)发挥关键作用。[⑥] 此外,北约依靠官僚组织能力扩大北约机构的资源,北约将自身视为全球关键行为体,其组织内部及员工有意愿维持北约运行,并强调北约实体存在的必要性。[⑦] 北约在布鲁塞尔有1 000名文职工作人员,[⑧]其庞大的组织架构造就北约需迎合成员国家的意图和诉求来赢得自身生存。

既有三种研究视角,阐释北约全球特别是亚太影响力形成动因,在学理和实践上都具有借鉴意义,能够为本研究奠定基础。但既有研究未能从数字能力视角,特别是在数字时代北约借助网络技术合作,集合盟国网络权力的能力构建维度,回答北约为何有能力塑造亚洲影响力,本研究基于既有研究成果,对北约亚太扩张提出一个补充性的解释角度——网络赋权的能力维度解释。即数字化时代,网络权力与物理权力转变过程中,北约在网络空间拓展联盟体系构建、制度规则塑造及协同能力,为北约在亚太扩展影响力提供可能性。具体来说,本研究从技术赋权特别是网络赋权视角,分析北约为何能够越来越多地参与物理距离遥远的亚太事务,并影响亚太安全走势。本研究给出解释是北约追求全球影响力的方式和手段,已有所突破,即北约在网络空间有能力去做过去想做而不能做的事情。研究从技术赋权视角,归纳北约在网络空间通过设置仪程、拉拢盟国以及开展集体行动等方式获取权力,解释数字时代网络技术如何赋权北约影响亚太安全局势。

二、网络赋权与北约网络战略演进

2.1 网络权力与赋权功能

网络空间赋权北约超越传统物理空间界限。在网络空间,信息通信技术无处不在,其不仅超越国家管辖范围,还影响几乎社会生活的

① Robert W. Cox, "the Executive Head: an Essay on Leadership in International Organization," *International Organization*, Vol.23, No.2, 1969, pp.205-230.

② Nina Hall and Ngaire Woods, "Theorizing the Role of Executive Heads in International Organizations," *European Journal of International Relations*, Vol.24, No.4, 2018, pp.865-886.

③ Leonard Schuette, "Why NATO Survived Trump: the Neglected Role of Secretary-General Stoltenberg," *International Affairs*, Vol.97, No.6, 2021, pp.1863-1881.

④ NATO, "Doorstep Statement," December 14, 2019, https://www.nato.int/cps/en/natohq/opinions_171552.htm, 访问时间:2022年6月9日。

⑤ Ryan Hendrickson, "Leadership at NATO: Secretary General Manfred Woerner and the Crisis in Bosnia," *Journal of Strategic Studies*, Vol.27, No.3, 2004, pp.508-527.

⑥ Ryan Hendrickson, "NATO's Secretary General and the Use of Force: Willy Claes and the Air Strikes in Bosnia," *Armed Forces & Society*, Vol.31, No.1, 2004, pp.95-117.

⑦ Robert B. McCalla, "NATO's Persistence after the Cold War," *International organization*, Vol.50, No.3, 1996, pp.445-475.

⑧ Ramses A, Wessel, "International Organizations and Military Affairs, Written by Hylke Dijkstra," *International organizations law review*, Vol.14, No.1, 2017, pp.215-219.

所有领域。[①] 随着人类活动与社会资源逐步迁移至网络空间,各国及其他行为体也对该领域愈发重视,这促使大国权力竞争从传统地缘政治扩展至网络空间。网络权力竞争涉及网络基础设施、技术规范以及网络空间发展理念等方面,其特殊扁平化、分布式和脆弱性的技术属性,导致传统权力与资源的流散,多行为体均可参与网络权力的再分配。此外,网络空间的攻击主体难以被追踪溯源,其攻击手段不易察觉,且网络战的时间边界模糊,其攻防转换的灰色空间巨大,这些特点增加各国追求获取网络权力的意愿。而北约声称获得网络权力既降低成员国的网络安全风险,又形成网络防御合力以应对威胁,同时也可发展集体网络攻击能力。

网络权力来源于权力,但与传统权力结构模式有区别。作为权力的延伸,网络权力当前尚未有统一的定义,但借鉴权力定义,可将网络权力定义为行为体(多指国家行为体)在网络空间内可支配的资源和能力。有学者认为,网络权力是一国对其他国家使用网络威慑,实现政治、经济或军事目的能力。[②] 网络权力包含物理层面(以外交、信息、军事和经济为代表)和抽象认知成分,网络权力是实现国家权力的一种方式,而非仅是权力的属性。[③] 约瑟夫·奈认为网络空间存在软实力和硬实力,其体现在关系性权力的三个层面:第一层是促使其他行为体违背最初偏好或战略行事的能力;第二层是议程设置与建构——某行为体可将其他行为体排除在议程之外,使其选择难以实现;第三层是某行为体塑造另一行为体的最初偏好,如最初代码的选择。约瑟夫·奈将"网络权力"定义为一种新权力,"包括基础设施、网络、软件以及人自身的技能,是借助网域空间互相连通的信息资源,获取偏好结果"的一种能力。[④] 总结来看,"网络权力"是行为体利用网络基础设施、网络软件系统以及技术人才,依靠信息资源交流,实现意图的一种能力。

网络空间权力能够赋能行为体,即网络赋权。数字化时代,网络空间映射是非同构映射,物理空间映射到网络空间的内容愈发多样,物理世界与网络世界通过融合和塑造、改变和共同演进。[⑤] 当前在国际关系领域,数据型权力已崛起成为新的权力形式,各国对数据权力的竞争,成为国家网络权力竞争中的重要领域。[⑥] 信息技术赋能行为体参与全球政治,影响文化传播与政治议程塑造。[⑦] 有学者将"网络权力"的基础概括为四部分:一是经济或科技基础,具有支撑网络空间运行的基础,若无技术基础,那至少需有足够市场;二是具有军事或情报实力,能够在网络空间实施行动;三是需要拥有网络空间议程设置的叙事能力,即如何使用和管控网络,以及被他国接受的能力;四是要拥有网络科技公司捍卫本国利益。[⑧] 北约作为全球军事组织,在网络空间构建的网络盟国,集成各成员国的网络权力,具有超国家的网络博弈能力,在科技、经济、市场、军事情报及议程设置领域已初具规模和全球影响力。

2.2　北约网络战略演进

北约不仅是一个由共同威胁感知维系在一起的政治联盟,它还是一个以紧密机构组织、相互依存关系与共同价值观为支撑的军事安全机

---

① Karen Lund Petersen, "Public-Private Partnerships on Cyber Security: a Practice of Loyalty," *International Affairs*, Vol.93, No.6, 2017, pp.1435-1452.

② Munish Sharma, "China's Emergence as a Cyber Power," *Journal of Defence Studies*, Vol.10, No.1, 2016, pp.43-68.

③ Joey Jansen van Vuuren and Louise Leenen, "A Model for Measuring Perceived Cyberpower," *ICCWS* 2018 13*th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited*, 2018, pp.329-320.

④ [美]约瑟夫·奈著,王吉美译:《论权力》,中信出版社,2015 版,第 143-153 页。

⑤ 周宏仁:"网络空间的崛起与战略稳定",《国际展望》,2019 年第 11 期,第 23 页。

⑥ 董青岭、王海媚:"21 世纪以来中国的大数据国际关系研究——董青岭教授访谈",《国际政治研究》,2019 年第 4 期,第 157 页。

⑦ Joseph Nye, "The Information Revolution and American Soft Power," *Asia-Pacific Review*, Vol.9, No.1, 2002, pp.60-76.

⑧ Andrew Ivers, "Adam Segal: Life in the Hacked World Order," *Bulletin of the Atomic Scientists*, Vol.72, No.5, 2016, pp.267-272.

构。[①] 对于安全的关注促使网络成为北约近些年活动的重点领域。当前北约在物理空间已扩员8轮,将边界东推1 000多公里的同时,也部署威胁地区稳定的武器。[②] 北约加大防御性网络能力建设就是表现之一,从近几次北约峰会看,1999年北约在战争中使用网络攻防技术,2002年北约首次将“网络防御”设置为联盟政治议程。此后,北约峰会还陆续推出拓展其网络盟国的政策路线,逐步提升北约在全球网络权力竞争中的地位。总体来说,北约网络理念和实践的演变可划分萌芽、发展到扩散三阶段,特别是在第三阶段,北约提升亚太在其全球网络战略中的地位。

(1)萌芽阶段:网络攻防认知觉醒提升(1999—2007)

北约重视网络攻防能力建设源于战时的网络攻击,该阶段北约开始感知到网络攻防的重要性,但未将亚太地区及与亚太国家网络合作当成其工作重点。以美国为首的北约在1999年参加科索沃战争期间,其电子系统及网站服务器遭受“拒绝式服务”等网络攻击,导致北约公共事务网站瘫痪数天。[③] 而在2002年北约布拉格峰会上首次强调要“加强防御网络攻击能力”,此次峰会北约还提出建立计算机事件响应能力系统(NATO Computer Incident Response Capability, NCIRC),其目的是增强北约网络快速反应和防御能力,将网络防御整合到空中指挥控制系统、地面监视和导弹防御系统中,后续该中心与欧盟的计算机应急响应小组合作。[④] 自此之后,“网络防御”成为北约防长讨论的重要议题。2006年里加峰会,北约不仅提出要“加强保护关键信息系统,使其免受网络攻击”,还提出在联盟行动中发展“可靠、安全、无延迟地共享信息、数据与情报”能力。[⑤] 2007年网络化程度高度发达的成员国爱沙尼亚,成为史上首个关键基础设施遭受网络攻击的国家,[⑥]受此事件影响,北约重新审视自身网络安全与网络防御的问题。可以说,在此阶段北约逐步意识到网络安全的重要性,并且强化网络集体防御能力的认知。

(2)发展阶段:集团防御与攻击能力增强(2008—2015)

该阶段北约加大网络空间集团防御和攻击能力建设,开始在亚太地区战争中使用网络攻击。爱沙尼亚遭到网络攻击后,北约意识到解决成员国脆弱性网络系统问题的重要性,而北约在亚洲参加阿富汗战争期间,其加强成员国网络协同攻击能力建设。2008年1月,北约颁布首个网络防御政策,同年4月,北约布加勒斯特峰会签署通过该条约并强调加强北约与成员国间的网络联系。[⑦] 2008年5月,北约网络合作防御卓越中心(The Cooperative Cyber Defense Center of Excellence, CCDCOE)在塔林成立,爱沙尼亚、德国、意大利、拉脱维亚、立陶宛、斯洛伐克共和国和西班牙为初始成员国,该机构建立目的是研究网络攻防、开发应对网络攻击方法、分享网络安全法律与培训网络人员等事宜,北约还授予该防御中心国际军事组织地位。[⑧] 同一时期,北约在布鲁塞尔成立网络防御管理局(The Cyber Defence Management Authority, CDMA),该机构作为一个快速网络反应中心,主要负责网络防御,检测并管理安全风险以打击

① DAVID S. YOST, “NATO's Evolving Purposes and the Next Strategic Concept,” *International Affairs*, Vol.86, No.2, 2010, pp.489-522.

② 钟声:“美国对危机负有不可推卸的责任”,《人民日报》,2022年3月29日,第3版。

③ Jason Healey and Leendert van Bochoven, “NATO'S Cyber Capabilities: Yesterday, Today, and Tomorrow,” February 27, 2012, https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022712_ACUS_NATOSmarter_IBM.pdf, 访问时间:2022年6月9日。

④ Sorin Ducaru, “Is Cyber Defense Possible?” *Journal of International Affairs*, Vol.70, No.1, 2016, pp.182-189.

⑤ NATO, “Riga Summit Declaratio,” November 29, 2006, https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en, 访问时间:2022年5月6日。

⑥ Stephen Herzog, “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,” *Journal of Strategic Security*, Vol.4, No.2, 2011, pp.49-60.

⑦ NATO, “Bucharest Summit Declaration,” April, 2008, https://www.nato.int/cps/en/natolive/official_texts_8443.htm?msclkid=de008436b0f511ecbd77b2120e73612c, 访问时间:2022年5月6日。

⑧ CCDCOE, “About us,” April 3, 2022, https://ccdcoe.org/about-us/, 访问时间:2022年4月3日。

针对北约成员国关键基础设施的网络攻击行为。①

2010 年北约里斯本峰会首次提出网络攻击可能威胁欧洲的繁荣、安全和稳定,需加强成员国的网络合作。北约提出要提升北约计算机事件响应能力(NCIRC)系统的全面作战能力(Full Operational Capability, FOC),它将预防、检测与响应网络攻击事件,并保障所有北约机构网络运行,同时协助个别网络水平欠缺的盟国,提升其技术互操作性与信息共享能力。如北约构建的数据标准和数据共享协议,在 2010 年阿富汗战争期间为构建联合网络作战奠定基础:北约构建阿富汗任务网络(The Afghan Mission Network, AMN),将多国数据信息网络整合到一个联合作战网络中,实现盟国间的数据情报共享,将信息共享模式从“需要知道”(need-to-know)转变为“需要共享”(need-to-share),该措施增加了北约信息系统支持作战的经验。②

2011 年北约出台第二份网络防御政策,该政策提出面对快速发展的技术威胁,提升联盟网络集体防御和危机管控能力至关重要。③ 在此诉求背景下,北约于 2012 年全面部署快速反应小组(Rapid Reaction Teams, RRTs),帮助北约成员国快速恢复系统,提升预防网络攻击风险和增强网络攻击瘫痪后的复原能力。此外,2012 年北约多个机构合并形成北约通信和信息局(NATO Communications and Information Agency, NCI Agency),合并后的机构为北约通信和信息组织(NATO Communication and Information Organisation, NCIO)的执行机构,④其参与指挥计算机通信、卫星监视和侦察技术以及网络技术培训等工作。2014 年北约威尔士峰会宣言称,网络攻击与常规攻击的危害相同,并认为国际法适用于网络空间,盟国将网络防御作为集体防御的核心部分。北约宣布网络攻击可能导致触发《北大西洋公约》的第五条,即攻击任意缔约国将被视为攻击所有缔约国,这被认为是北约网络政策的重要调整。⑤ 2014 年 9 月,北约发起一项倡议,以加强与私营部门合作应对网络威胁和挑战。北约工业网络伙伴关系(NATO Industry Cyber Partnership, NICP)将聚集众多行业领导者和政策制定者,共同讨论如何促进北约网络协作。北约借助工业界力量,帮助其实现网络防御目标,通过网络威胁信息的及时共享,增强其威胁态势感知能力。

(3)外溢阶段:网络攻防重心的地缘扩散(2016—至今)

该阶段北约将网络视作军事行动领域,并强调要与其物理空间战略协同一致,增强其亚太网络影响力。2016 年北约华沙峰会宣称网络空间等同陆海空一样的“军事领域”,即承认网络空间与传统空间同等重要,并承诺将加强北约双边与多边的网络防御合作,把提升网络基础设施防御性能作为其优先事项。⑥ 2017 年 11 月,北约成立“网络行动中心”,其强调“防护北约成员国及其盟友的网络”,而非进攻性的“网络战”,在此阶段北约与欧盟的网络合作规模和程度都在增加。⑦ 2018 年北约布鲁塞尔峰会,北约领导人称网络安全威胁正变得越来越频繁和复杂,且具有破坏性。北约有必要将主权国家网络能力融合进入北约行动中,网络攻击归因溯源应是主权国家应有的权利,并强调国际法

① NATO, “Nato Sets Up Cyber Defence Management Authority in Brussels,” April 4, 2008, https://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels, 访问时间:2022 年 5 月 3 日。

② RAND, “Lessons Learned from the Afghan Mission Network Developing a Coalition Contingency Network,” December 31, 2014, https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR302/RAND_RR302.pdf, 访问时间:2022 年 5 月 5 日。

③ NATO, “Defending the Networks the NATO Policy on Cyber Defence,” August 19, 2011, https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf, 访问时间:2022 年 7 月 5 日。

④ NCI, “About us,” May 9, 2022, https://www.ncia.nato.int/about-us.html, 访问时间:2022 年 5 月 9 日。

⑤ Khatuna Burkadze, “A Shift in NATO's Article 5 in the Cyber Era,” *The Fletcher Forum of World Affairs*, Vol.42, No.2, 2018, p.215.

⑥ NATO, “Warsaw Summit Communiqué,” July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, 访问时间:2022 年 7 月 1 日。

⑦ Jeppe T Jacobsen, “Cyber Offense in NATO: Challenges and Opportunities,” *International Affairs*, Vol.97, No.3, 2021, pp.703-720.

在网络空间的适用性问题,[①]此外,北约还提出通过实施《网络防御承诺》来提供网络防御保障,拓展与北约盟国在网络学术与实践领域关系。[②] 2018年8月,北约成立网络空间运营中心(The Cyberspace Operations Centre, CyOC),并将"进攻性网络"概念整合到网络运营中,以提升初始作战能力(Initial Operational Capability, IOC)。作为北约网络战的重要组成部分,北约网络空间运营中心负责感知联盟网络态势,集中规划网络联盟行动和任务以及协同网络空间运营等问题。

2019年北约伦敦峰会强调北约正面临网络攻击等混合威胁,要加强应对网络攻击的能力建设。其强调要与美国合作,确保拥有弹性与安全的关键基础设施系统来应对中国崛起。2021年北约布鲁塞尔峰会在总结既有网络空间安全经验的基础上,指出网络威胁具有复杂性、破坏性和频繁性特点。北约批准网络防御政策,提出面对政治、军事和技术层面的网络安全问题,应主动构架防御体系应对网络威胁,将网络战纳入北约的混合战中。2021年9月,北约任命首任首席信息官(CIO),以整合北约军事和民用领域信息通信技术,该机构由信息技术和网络专家组成,直接向北约秘书长报告。[③] 这一阶段北约网络战略是从欧洲外溢扩展到亚太,目的是针对日益崛起的中国,北约提出"中国威胁"言论,污蔑中国使用"网络战和虚假信息",以及要求中国在"太空、网络等领域负责任"。[④] 上述言论体现北约在为网络空间转向亚太寻求所谓合法性的借口。

总结来看,北约网络空间政策的演化经历了萌芽、发展到扩散三个阶段,主要有以下特点。一是网络安全已逐步成为北约重要安全事项以及维系联盟的核心战略之一。北约网络安全战略是从全球视角出发,伴随其亚太化战略逐步转向中国周边地区。二是北约在网络空间强调预防前置、防御能力以及冗余弹性机制愈发明显,网络能力建设是其关注重点:北约构建的强大网络防御保护联盟、协调机制日渐完善,且参与行为体日益多元,除北约国家也有非北约国家,以及高科技企业、学术界等行为体。三是北约网络空间战略已凸显地缘战略属性,开始转向亚太。北约将网络作为参与亚太区域博弈重要抓手,并积极拉拢亚太国家构筑网络空间的"北约合作机制",以实现孤立中国意图,而与此同时,诸多亚太国家已表达加入北约网络空间联盟体系的意愿。

三、北约网络空间亚太扩张路径

网络权力赋权北约跨越传统物理空间的限制。受到地缘政治和历史因素影响,北约在物理空间活动受限;而在网络空间,北约则可将影响的对象扩大化,将活动范围扩展至中亚甚至中国周边,以期实现网络情报共享、理论培训及战术训练的意图,威胁中国网络空间安全。目前来看,北约已在网络规则塑造、国际话语权建构及盟国合作等方面,呈现领导性的地位,影响亚洲乃至全球的网络格局,可以说网络技术赋权北约影响全球格局的能力,其通过网络信息战以所谓安全威胁为幌子扰动亚太舆论局势。为其战略重心转向亚太的"合法性"背书。最具代表性的是以北约成员国为基础建立的北约网络合作防御卓越中心,其在亚太网络空间实施扩张行动。该中心是北约的密切支持单位和亲密伙伴,虽不是官方性质的隶属关系,但从其参与成员、研究成果以及交流实践的表现,该中心的作用甚至胜过北约官方组织,且该中心众多研究成果,已是北约官方机构实施网络攻防活

① Steven Hill, "Cyber Defense Norms and NATO," *Proceedings of the ASIL Annual Meeting*. Cambridge University Press, Vol.111, 2017, pp.145-146.

② NATO, "Brussels Summit Declaration," July 11, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20, 访问时间:2022年6月3日。

③ NATO, "Manfred Boudreaux-Dehmer," November 15, 2021, https://www.nato.int/cps/en/natohq/who_is_who_188597.htm, 2021-09-15. 访问时间:2022年6月7日。

④ Steven Erlanger, Michael D. Shear. Shifting Focus, "NATO Views China as a Global Security Challenge," June 14, 2021, https://www.nytimes.com/2021/06/14/world/europe/biden-nato-china-russia.html, 访问时间:2022年7月2日。

动的重要参考。北约网络合作防御卓越中心一方面接纳北约国家,将其作为拥有投票权的“资助国”(Sponsoring Nations),另一方面则吸收非北约国如韩国,将其作为“贡献国”(Contributing Participants)。2022 年 4 月,乌克兰正式成为该组织的“贡献国”,更体现北约参与全球热点地区事务的内在基因。北约网络合作防御卓越中心作为多国参与的平台,其背后服务对象及运行掌控者就是北约,该组织与北约通信和信息局等机构合作,共同扩大北约在亚太网络空间的影响力。

网络赋权北约将其参与亚太事务的意愿转化为能力。北约在亚太的网络扩张主要通过吸纳盟国,塑造规则与集体行动这三种路径,具体体现如下:在国家主体层面,北约积极与亚太国家合作,吸纳其加入北约构筑的网络组织团体;在网络规则理念层面,北约意图将其塑造的网络规则迁移至亚太网络空间;在网络实践操作层面,北约强化与亚太国家在网络空间的集体行动与互操作协同能力建设。可以说,获得网络赋权的北约逐步在亚太网络空间扩张,这对亚太稳定以及中国周边安全造成极大挑战。

3.1　盟国吸纳:网络技术增加北约与亚太国家互动

北约积极在亚太地区扩充网络盟友。北约网络合作防御卓越中心成员由最初的“北约成员”扩展到“非北约盟国”加入。由此成员国呈现“北约—非北约”国家融合趋势。自北约网络合作防御卓越中心成立后,北约国家数量不断扩增。2014 年奥地利以首个非北约国家身份加入,此后成员国覆盖区域已由北大西洋区域,逐步扩展至亚太的日本和韩国。2018 年日本首相表示希望加入北约网络合作防御卓越中心,而北约则称“欢迎技术和网络安全大国日本作为参与方加入”,2022 年 11 月,日本宣布正式加入该中心。2020 年北约秘书长在“北约 2030 倡议”中强调北约要加强与日本、韩国、澳大利亚在网络等领域的合作。2021 年北约协助蒙古国新建网络安全中心,并得到了北约通信和信息局的技术支持。① 2022 年 9 月,北约接受韩国政府请求,批准韩国开设代表处,标志着北约在亚太的四个伙伴国全部拥有了各自的代表处。这符合北约最新战略理念,即在颠覆性技术研发合作及网络安全等国际竞争新领域加大投入并增加与亚太国家的助力。②

亚太国家以北约亚太网络纽带为基础,构建区域网络合作联盟。日韩澳加等国以北约网络合作防御卓越中心为桥梁,强化区域网络关系纽带,形成内部组织协同,在中国周边构筑网络情报围墙。经过 14 年发展,北约网络合作防御卓越中心已由最初 7 个北约创始国增至 38 个,③体现该中心的全球地位和亚太影响力在逐步上升,近期新加入或有意加入该组织的国家,均位于中国周边区域。此外,北约网络盟国与其他包括亚太国家的区域组织交织融合。该中心基本将美日印澳四边安全对话机制(Quad)、美英澳安全联盟(AUKUS)、美英澳加新五眼联盟(Five Eyes Alliance)与七国集团(G7)的成员国,纳入其网络合作中心,实现区域组织间的多重融合交错,共同在网络空间构建模块化联盟以实现北约网络权力的增长。北约依靠亚太网络盟国对中国实施模块化联盟竞争,实现在网络空间对中国的技术围堵,增强北约在亚太数字空间的影响力,进而反作用于现实物理空间。

3.2　议程设置:网络赋权北约塑造亚太网络规则

北约拓展全球核心区域的网络话语权、叙事能力与规则建构能力。当前亚太在全球政治经济秩序中权重上升,体现国际力量格局“东升西降”演变态势。北约正打造一个以自身为中心,全球特别是亚太国家参与的排他性网络集团,操纵和塑造亚太网络规则。一方面,北约网络合作防御卓越中心发布的《塔林手册》,构建包含和平时期与战争时期的网络空间国际法规

① NATO, “NATO Helps to Strengthen Mongolia's Cyber Defence Capacity,” January 18, 2021, https://www.nato.int/cps/en/natohq/news_180697.htm, 访问时间:2022 年 5 月 7 日。

② 郭籽实、洪邮生:“北约新一轮变革趋势与影响:‘北约 2030’改革报告评析”,《太平洋学报》,2021 年第 11 期,第 97 页。

③ 目前官网显示为 29 个“资助国”和 9 个“贡献国”。

则体系,增强北约及其伙伴国家在网络国际法、网络战略等领域的话语权削减网络空间技术社群推崇的去中心化的网络规范的国际影响力。北约借助网络赋权机制,吸纳盟国参与网络规范建构,将北约内部已成型的网络制度规范体系迁移全球,具体做法是北约在全球展开网络技能培训,积极在网络公域内“圈地”,提供涵盖网络技术、法律、战略与网络操作的广泛课程。例如在2022年,北约网络合作防御卓越中心课程培训点达32个,涵盖韩国、美国和加拿大等国。①

另一方面,亚太网络空间尚未形成完备的共识性规则体系。网络空间作为新领域,各国尚未达成彼此认同规则体系,而北约网络合作防御卓越中心网络议程设置能力强,随着加入国家的持续增加,包括中国在内的国际社会,可能被迫对其产生依赖性,这将成为未来其制裁中国的手段。如北约在与网络数字技术紧密相关的人工智能等颠覆性技术领域,谋求技术规则的制定权,其还通过构建跨学科的技术态势感知平台系统,在智能时代打造攻防兼备的智能武器,并在军事演习中使用多种类型的智能武器。② 此外,北约将恶意网络攻击等入侵责任无端归咎中国。日本等国政府也跟随北约污蔑中国“实施网络攻击”,指责中国发动所谓“高级持续性威胁”。③ 其真实目的是在网络空间挤压中国参与建构全球网络规则,实现由美国主导的北约在新型网络空间具有更多话语和规则塑造权。

3.3 协同行动:网络强化北约与亚太国家集体行动

北约依靠网络技术增强与亚太国家集体协同行动。北约在亚太地区强调网络预防前置、冗余和具有弹性,多主体参与的网络协同合作能力建设是其关注重点。特别是北约提出的伙伴关系互操作倡议(The Partnership Interoperability Initiative, PII),指出要加强北约和伙伴国家间兼容性的协作能力,增强机会伙伴机制(Enhanced Opportunities Partners, EOP),加强与澳大利亚等六国的合作关系,为应对网络空间的情报共享、教育培训以及混合战争等事宜做准备。④ 北约在物理空间对亚太影响有限,虽然历经几次东扩,但对亚太难以形成实质威胁,所以北约加大与亚太国家“网络联系”,弥补与亚太国家的“物理距离”。其主要做法是强化其网络空间集体协同的作战能力,⑤乌克兰危机中北约展现出的集体网络援助迅速与信息共享便捷特点,可以推测该组织未来在涉及亚太网络冲突时,将强化网络集团协同能力的建设。

北约增强亚太网络集体能力还体现在从强调“演练防御”转为强调“实战博弈”。北约网络合作防御卓越中心初期专注网络防御演练,逐步转化为强调增强进攻能力建设。如该中心举办的年度机制性“锁定盾牌”(Locked Shields)演习,是世界上规模最大的内部网络防御演习,便于其盟国分享网络攻防技术和经验。以2022年的演习为例,全球近33个国家的2 000多名专家,线上线下联动参与北约网络演习,同时在演习中检验北约防御网络快速反应小组的综合能力,⑥日韩等亚太国家也积极参与其中。此外,北约连续14年举办网络冲突国际会议(International Conference on Cyber Conflict, CyCon),包含亚太国家在内的近50国的政府、军队、学术界和工业界的600多名决策者、法律学者与技术专家,为北约提供专业的建议,其目

① CCCDCOE, “Training,” May 1, 2022, https://ccdcoe.org/training/, 访问时间:2022年5月7日。

② 高望来:“北约人工智能反恐新态势及其困局”,《欧洲研究》,2021年第2期,第147页。

③ Minister of Foreign Affairs of Japan, “Cases of Cyberattacks Including Those by a Group Known as APT40 Which the Chinese Government is behind,” July 19, 2021, .https://www.mofa.go.jp/press/danwa/press6e_000312.html, 访问时间:2022年5月7日。

④ CSIC, “Battle Networks and the Future Force,” March 4, 2022, https://www.csis.org/analysis/battle-networks-and-future-force-1, 访问时间:2022年4月7日。

⑤ Duncan McCrory, “Russian Electronic Warfare, Cyber and Information Operations in Ukraine Implications for NATO and Security in the Baltic States,” *The RUSI Journal*, Vol.165, No.7, 2020, pp.34-44.

⑥ NATO, “EXERCISE LOCKED SHIELDS 2022 CONCLUDES,” April 23, 2022, https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes, 访问时间:2022年5月8日。

的之一是增加北约与网络合作伙伴国的网络互操作与协同能力。由于网络防御与攻击能力共生,以守转攻能力便捷。如前所述,北约网络合作防御卓越中心虽然标榜防御意图,但攻防可以转换,网络防御能力越强,越易转换成攻击武器。且北约在网络空间联合亚太国家,更加强调演习的实战性、进攻性和侵略性,挤压亚太国家网络安全边界。

四、北约网络空间亚太扩张影响

4.1　威胁中国网络及主权安全

北约网络空间亚太扩张直接干扰中国网络安全。北约通过散布所谓“中国数字技术威胁论”,为其强化亚太网络影响力寻求借口。2021 年 6 月,北约布鲁塞尔峰会公报中首次将中国称为“系统性挑战”,公报第 55 条污蔑中国“使用虚假信息”。① 2022 年 3 月,欧洲议会全会通过《外国干涉欧盟民主进程及传播虚假信息报告》,污蔑中国利用信息操纵等策略干涉欧洲民主进程,提出要发挥北约在网络领域的作用。同时北约网络合作防御卓越中心发布的《2030 年网络空间战略展望》,首次用一个章节内容描述中国为“网络霸权”,提出要联合北约盟友力量对抗和打击中国。② 此外,北约还污蔑中国为网络攻击的施行主体,称中国在网络空间“不负责任”,③其通过抹黑中国形象服务其对华遏制打压目的,将直接影响中国与亚太国家的网络合作。

北约亚太网络扩张将强化北约亚太涉华情报收集能力。一方面有助于美国完善亚太网络情报体系。美国作为北约网络合作防御卓越中心的“资助国”,对该组织提供技术支持、文化塑造与经济资助。北约网络战略重心的东移在一定程度上是为配合美国重返亚洲战略,协助其构筑网络空间情报联盟体系。另一方面科技公司选边站队将影响中国技术情报安全。多国政府部门、科技公司和科研机构参与北约网络合作防御卓越中心的演习,以微软、思科、西门子和爱立信等掌握网络基础资源的科技巨头为代表,为该中心提供大量技术支持。鉴于乌克兰危机中,被网络赋权的科技公司自主或被迫选边站队并实施制裁的教训,这些公司在未来亚太地区潜在的网络冲突中,可能跟随北约参与搜集涉华网络情报的行动,威胁中国数字主权安全。

4.2　加速亚太网络阵营化态势

当前,世界之变、时代之变、历史之变正以前所未有的方式展开,网络空间也不断受到地缘政治的影响,北约亚太网络扩张加剧了区域竞争态势。首先,日本在网络空间加入西方阵营的态度明显,其配合美欧对华网络污蔑,意图稳固护持“日美同盟”,并继续推动构建“四边安全对话机制”。与此同时,拜登(Joe Biden)政府则推出“印太经济繁荣框架”,拉拢亚太国家在数据跨境流动和数据本地化等领域开展合作。其次,韩国加入北约网络合作防御卓越中心后,其在网络空间作为北约网络行动的支持参与者,将搅动东北亚地区的网络安全局势。特别是伴随韩国民众对华好感度的下降,民意将会进一步扰动韩国政治力量、舆论思潮,重塑其认同偏好,加快韩国在网络空间等领域转向西方阵营,可见未来亚太地区将出现更复杂的网络攻防局势。最后,由于朝核问题日益紧张,朝鲜在网络空间拥有一定的攻防能力,这增加中美战略互疑,削弱中韩战略互信,亚太地区呈现阵营化趋势。

此外,北约还明确提出构筑基于“价值观认同”的网络团体,构建排挤中国的“网络联盟”,亚太网络空间对立紧张局势凸显。北约网络合作防御卓越中心从成立之初,就将网络规则与

① NATO, “Brussels Summit Communiqué,” June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm#32, 访问时间:2022 年 7 月 5 日。

② CCDCOE, “Cyberspace Strategic Outlook 2030,” March 15, 2022, https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_vol2_15032022.pdf, 访问时间:2022 年 5 月 7 日。.

③ Kristen Eichensehr, “United States Joins with Allies, Including NATO, to Attribute Malicious Cyber Activities to China,” *American Journal of International Law*, Vol.115, No.4, 2021, pp.715-721.

现行国际法融合,意图占据网络空间国际话语权、舆论主导权、规则制定权的高地。它以网络攻防技术培训、网络演练支持以及网络法律规则塑造闻名,并深度影响网络学术界和工业界。北约在亚太地区与澳大利亚、日本、韩国等所谓“民主”国家合作,并“确保其盟国网络防御能力提升”,而实际意图是在亚太对冲所谓的“中国网络威胁”。北约将物理空间构筑针对中国的小多边机制,迁移到网络空间,这种趋势必然导致网络空间冲突对抗事件频发。北约在网络空间的承诺是对每一个盟国安全都予以保护,这就导致北约在网络空间容易将双边小规模对抗,上升为区域性、高烈度的集体性对抗行为,加速亚太网络阵营化趋势。

4.3 阻碍全球网络分工与合作

北约亚太扩张破坏全球网络空间互信与合作基础。当前北约成员国家与亚太国家,掌握着全球绝大部分的数字资源和网络权力,在美国主导下的北约亚太网络扩张,意图在网络空间构筑美国式的“自由网络规则体系”,并加大部署网络监控技术获取情报,实施大规模数据收集和监控。北约及其盟国的行为造成全球网络空间“碎片化”趋势愈发明显,引发网络空间“巴尔干化”反应,导致各国加大对网络信息、技术及关键基础设施的管控,在网络空间出现排他性制衡措施,网络空间出现技术流通性减弱现象,[①]严重破坏全球网络合作互信基础。

北约网络亚太扩张冲击全球既有网络空间秩序与分工。亚太网络空间市场主体是以中国等新兴经济体为代表,其在全球网络空间供应链中发挥重要作用。北约亚太网络扩张,以“区域安全受威胁”为借口,无节制地泛化安全议题,污蔑中国网络技术获取模式,意图维护北约盟国主导的技术霸权和已有制度的“控制权”,同时削减亚太新兴经济体在全球网络市场及供应链体系中的影响力。北约网络空间亚太扩张也造成全球网络规则体系、市场秩序与供应链结构混乱,对全球网络技术分工合作、经贸交流与数字资源分配产生消极影响,导致全球的数字鸿沟问题持续恶化,让全球发展中国家获取网络技术与发展数字经济步履维艰,不利于全球网络空间健康和有序发展。

五、结 语

网络技术赋权北约获取塑造亚太权力格局能力。网络赋权作为补充性解释路径,与传统研究北约塑造全球和亚太影响力的成果——北约霸权扩张、同盟机制以及国际组织官僚能力的视角融合,提出数字化时代网络赋权北约具备“跨越地缘”塑造亚太权力格局的能力。历届北约峰会公报涉及网络安全部分内容,能体现北约网络空间政策的演变过程,北约网络理念与行动的演变可划分网络安全认知萌芽、网络攻防能力发展和网络地缘重心扩散亚太三个阶段。技术赋权后的北约的网络实践意图与手段发生变化,其亚太活动日趋频繁。北约在网络空间的规则塑造能力强大,成员国规模扩展迅速,活动烈度呈现持续增加趋势,特别是近年来随着美国战略中心转移到亚太,并实施“印太战略”。部分亚太国家“脱亚向欧”倾向明显,且与北约互动频繁,以美国为首的北约意图在亚太物理空间构建“小北约机制”的同时,在网络空间也有意构建模块化的反华联盟体系。

数字化时代面对北约亚太网络扩张影响国际秩序、亚太稳定以及中国周边安全,中国树立长期的网络权力竞争理念,跟踪北约网络空间盟国在亚太的组织、成员及网络活动动向。首先,中国应主动参与网络空间规则博弈。虽然《塔林手册》对网络规则建构影响不容小觑,但目前构筑新的网络规范体系仍为时不晚,中国可依靠网络人口与市场优势,依托世界互联网大会,增强网络话语的国际影响力,构筑符合本国利益的网络规则。中国参与构建国际网络规则体系的同时,应总结北约网络盟国亚太扩张的特点,在更好了解其运行模式与实践经验的

① 苗争鸣:“碎片化”的网络空间趋势——基于俄罗斯‘断网’的研究”,《信息安全与通信保密》,2020年第9期,第72页。

基础上,为自身参与国际网络空间规则建构,提供经验指导。其次,中国要跟踪北约组织、成员在亚太网络活动的动向。中国应关注周边国家加入该组织后的活动情况,警惕其构筑“网络民主联盟”动作,并持续跟踪北约网络盟国在亚太及中国周边发展态势,以及其战略演练内容与课程培训体系变化。最后,中国要树立长期全面的网络权力竞争理念。中国应重视北约网络盟国亚太扩张及其组织情报化与实战化的趋势。相关部门要从网络空间全球发展趋势着手,全面评估北约获取亚太乃至全球网络话语权对中国的影响。

编辑　邵雯婧

The Cyber Empowering NATO's Asia-Pacific Expansion: Evolution, Paths and Influence

MIAO Zhengming[1]

(1. *Tsinghua university*, *Beijing* 100084, *China*)

Abstract: The NATO intends to increase its global influence in both physical space and cyberspace. Since its establishment in 1949, the NATO has increased its membership for eight times, and it has reflected its expansion in the field of cyberspace. The existing studies on the NATO shaping power structure in the Asia-Pacific region focus on NATO's hegemonic expansion, alliance mechanism and bureaucratic capabilities of international organizations. There are very few perspectives on the technological capabilities of the NATO to shape the power structure in the region in the context of the cyber empowerment in the digital age. The evolution of NATO's strategy in cyberspace in the digital age can be divided into three stages: the germination of cybersecurity cognition, the development of offensive and defensive capabilities of cybersecurity, and the proliferation of cyber geo-centricity. With the purpose of shaping its Asia-Pacific influence, the NATO increases the number of cyber allies, constructs a system of cyber law, and enhances cyber practices of interoperability. By analyzing the specific actions of the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) and its reflection, characteristics and influence in the cyberspace of NATO's Asia-Pacific expansion, this research can provide an academic explanation for having cyber technology to empower the NATO to shape the Asia-Pacific strategy.

Key words: NATO; Asia-Pacific expansion; cyber empowerment; CCDCOE