北约人工智能反恐新态势及其困局*

高望来

内容提要:在21世纪,北约面临的反恐形势日趋复杂多变,人工智能反恐是北约全球安全布局中的重点领域。从2001年至2010年,北约注重为人工智能反恐研究积累原始数据,推进陆上和海上的智能反恐实践。从2011年到2020年,北约全面推进了跨学科的人工智能反恐研发,构建较为完善的智能反恐技术平台,并将智能武器应用于反恐实战中。北约人工智能反恐面临的困局包括反恐政策调整滞后于恐怖主义形势演变、对于网络极端化的管控存在漏洞、智能反恐面临的诸多技术挑战以及成员国之间协调的问题。

关键词:北约　人工智能　反恐　治理

作为引领新一轮科技革命的核心技术之一,人工智能技术的发展促使国际安全和战略研究发生了深刻变化。随着人工智能算法、大数据分析等技术的广泛应用,智能反恐研究在态势感知、威胁评估、数据库建设、恐怖主义防控等领域均取得显著进展。① 北约把恐怖主义作为重要安全威胁,将重金投入到人工智能研发领域,人工智

* 本文系国家社会科学基金一般项目"人工智能时代中美国际安全危机管控研究"(项目批准号:20BGJ063)的阶段性成果。感谢《欧洲研究》审稿专家对本文提出的修改建议。

① 关于恐怖主义数据库建设,参见 National Consortium for the Study of Terrorism and Response to Terrorism, "Global Terrorism Database," https://start.umd.edu/data-tools/global-terrorism-database-gtd; Xianzhi Cao, "Global Terrorism Analysis: An Interactive Tool for Visual Analysis of Global Terrorism," February 24, 2017, https://ict4sd.github.io/Terrorism_Analysis/; RAND National Security Research Division, "RAND Database of Worldwide Terrorism Incidents (RDWTI)," https://www.rand.org/nsrd/projects/terrorism-incidents/download.html; RSIS, "Global Pathfinder Database," https://www.rsis.edu.sg/research/icpvtr/research-programmes/global-pathfinder-database/#.XhVB9_nDrAQ。关于智能反恐领域的主要研究成果,参见傅瑜、陈定定:《人工智能在反恐活动中的应用、影响及风险》,载《国际展望》,2018年第4期,第119-137页;柳思思:《"欧洲反恐怖主义中心"的智能反恐系统构建》,载《社会科学》,2019年第5期,第3-11页;Joel Brynielsson et al., "Harvesting and Analysis of Weak Signals for Detecting Lone Wolf Terrorists," *Security Informatics*, Vol.2, No.11, 2013, pp.197-204; Weisi Guo, Kristian Gleditsch and Alan Wilson, "Retool AI to Forecast and Limit Wars," *Nature*, Vol.562, 2018, pp.331-333; Kathleen McKendrick, "Artificial Intelligence, Prediction and Counter-Terrorism," Chatham House, August 2019, pp.1-35。

能反恐成为北约全球安全布局中的重点领域。2019 年发布的北大西洋议会报告勾勒出人工智能技术广阔的应用前景,即人工智能可以赋能信息和决策体系,提升感知网络袭击的速度,缩短防御系统反应时间,并提升决策质量。① 人工智能技术是一柄双刃剑,它一方面为辨识恐怖分子、清除网络极端信息、军事打击恐怖主义提供了多元化选择,另一方面也可能使恐怖团体如虎添翼,制造反恐中新的难题。北约智能反恐实践是人工智能技术应用于反恐领域的重要个案。相关研究不仅可以反映人工智能反恐在实践中的应用价值及其面临的瓶颈,还可以揭示北约在新的安全环境下的战略诉求及合作动力。

一 研究问题及文献综述

北约在 21 世纪面临的反恐形势日趋复杂多变,恐怖组织与犯罪团伙等非国家行为体相互勾结,恐怖活动的融资渠道也更加多元化。从实体空间的恐怖袭击到网络恐怖主义,从恐怖团体策划的恐怖活动到“独狼式”恐怖袭击,从外来的恐怖分子到源于本土的恐怖分子的演变,使得反恐成为北约安全议程上的重要议题。正如前北约负责反恐问题的官员朱丽叶·伯德(Juliette Bird)所说:“反恐对于北约而言并不是新兴议题,而是主流话题。”②北约积极运筹信息空间,在人工智能反恐领域取得显著进展。本文追溯了 21 世纪以来北约智能反恐的发展历程,提出的研究问题是:为什么北约能够突破重重阻力,在人工智能反恐领域取得进展?其面临的困局又是什么?

国内外学术界与北约反恐相关的文献主要分为三类。

一是梳理在新的安全环境下,北约面临的不同类型的恐怖主义威胁。北约与施普林格出版社(Springer)合作出版了《运用科学保障安全》(NATO Security through Sciences)丛书,全面评估北约面临的国际安全风险。各国学者探析了恐怖分子使用高新技术的新型恐怖袭击以及自杀式恐怖袭击等传统威胁。塞缪尔·阿皮基安(Samuel Apikyan)和大卫·戴蒙德(David Diamond)分析了核恐怖主义和放射性恐怖主义,特

① NATO Parliamentary Assembly Science and Technology Committee Sub-Committee on Technology Trends and Security, “Artificial Intelligence: Implications for NATO's Armed Forces,” *NATO Parliamentary Assembly*, October 13, 2019, p. 3, https://www.nato-pa.int/view-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf.

② Juliette Bird, “Working with Partners to Counter Terrorism,” *NATO Review*, May 16, 2019, https://www.nato.int/docu/review/articles/2019/05/16/working-with-partners-to-counter-terrorism/index.html.

别是恐怖分子破坏核电站、运用放射性材料制造“脏弹”的风险。① 丹尼斯·莫里森(Dennis Morrison)等考察了恐怖分子在恐怖袭击中使用生物毒剂的安全挑战。② 伊夫蒂米亚(Ion A. Iftimie)和拉多萨尔耶维奇(Vlan Radosavljevic)主要关注北约面临的生物安全威胁以及生物恐怖主义的防控。③ 北约反恐卓越中心研究了自杀式恐怖主义和网络恐怖主义威胁及其应对方略。④ 弗里德里希·斯坦豪斯(Friedrich Steinhäusler)和弗朗西斯·爱德华兹(Frances Edwards)综合评估了多种类型的“灾难性”恐怖主义(Catastrophic Terrorism),包括使用常规武器、放射性武器、核武器以及生化武器的恐怖袭击。⑤ 杰奎琳·佩奇(Jacqueline Page)和托马斯·皮克(Thomas Pick)等探讨了北约面临的来自本土极端化的恐怖主义威胁。⑥

二是探析北约反恐战略的演变。美国兰德公司曾于 1997 年发表报告指出,恐怖主义是欧洲国家和美国面临的共同安全威胁之一,美欧可以围绕这些共同威胁构建新的战略伙伴关系。⑦ 多位学者均将“9·11”事件视为北约安全战略转型中的重要分水岭。波尔特和方长平认为,在“9·11”事件后,打击恐怖主义已成为北约议事日程中最紧迫的议题,反恐在北约安全战略中的地位正在不断提升。⑧ 埃伦·哈勒姆(Ellen Hallams)和刘芝平等强调,“9·11”事件推动了北约对于安全威胁的重新定义和战略转型。⑨ 詹姆斯·彼得森指出,北约反恐转型的三种基本动力是恐怖主义的发展、北约任务的转型和北约联盟体系的扩张。⑩

三是梳理北约在反恐中采用的举措。其一是通过与欧盟或其他国际组织合作来

---

① Samuel Apikyan and David Diamond, *Countering Nuclear and Radiological Terrorism*, Springer, 2006, pp.ix-x.

② Dennis Morrison et al., eds., *Defense against Bioterror*, Springer, 2005, pp.9-11.

③ Ion A. Iftimie, “The Implications of *COVID-19* for NATO's Counter-bioterrorism,” in Thierry Tardy, ed., *COVID-19: NATO in the Age of Pandemics*, NATO Defense College, 2020, pp.51-59; Vladan Radosavljevic et al., eds., *Defence against Bioterrorism: Methods for Prevention and Control*, Springer, 2018.

④ Center of Excellence Defence against Terrorism, *Suicide as a Weapon*, IOS Press, 2007; Centre of Excellence Defence against Terrorism, *Response to Cyber Terrorism*, IOS Press, 2008, pp.i-xv.

⑤ Friedrich Steinhäusler and Frances Edwards, *NATO and Terrorism Catastrophic Terrorism and First Responders: Threats and Migration*, Springer, 2007, pp.1-10.

⑥ Jacqueline Page, “The ‘Home Game’ Countering Violent Extremism within NATO,” NATO Research Division, Research Paper, No.104, September 2014; Thomas M. Pick et al., eds., *Home-grown Terrorism: Understanding and Addressing the Root Causes of Radicalization among Groups with an Immigrant Heritage in Europe*, IOS Press, 2009.

⑦ David C. Gompert and F. Stephen Larrabee, eds., *America and Europe*, Cambridge University Press, 1998.

⑧ 波尔特、方长平:《北约反恐战略的演变》,载《国际观察》,2016 年第 5 期,第 122-136 页。

⑨ Ellen Hallams et al., eds., *NATO beyond 9/11: The Transformation of the Atlantic Alliance*, Palgrave Macmillan, 2013, pp.6-9;刘芝平:《国际恐怖主义对北约的冲击》,载《新疆大学学报(社会科学版)》,2003 年第 4 期,第 53-56 页。

⑩ James W. Peterson, *NATO and Terrorism: Organizational Expansion and Mission Transformation*, Continuum, 2011, p.xi.

反恐。考恩特(Christian Kaunert)和韦特曼(Ori Wertman)梳理了北约和欧盟在反恐合作方面取得的进展。① 其二是通过完善基础设施等硬件建设来提升反恐能力。康斯坦丁·弗洛洛夫(Konstantin Frolov)和格雷戈里·贝克尔(Gregory Baecher)提出应在反恐中加强对关键民事基础设施的保护。② 雅罗斯拉夫·波勒特(Jaroslav Pollert)提出应致力于保障供水系统的安全。③ 塔米索格鲁(Mete Tahmisoğlu)和奥赞(Çinar Özen)关注加强反恐领域的交通安全。④ 其三是通过动员民众来反恐。西蒙·韦斯莱(Simon Wessley)和瓦莱里·克拉斯诺夫(Valery N. Krasnov)探析北约如何通过降低恐怖活动对民众的心理冲击以对抗恐怖主义。⑤ 阿波斯托尔(Ion Apostol)等关注调动民众的积极性参与到恐怖主义预防和应对进程中。⑥ 其四是运用新兴技术来反恐。安德鲁·詹姆斯(Andrew D. James)指出,科学技术对于反恐具有重要价值。⑦ 舒伯特(Hiltmar Schubert)和库兹涅佐夫(Andrey Kuznetsov)提出应加强技术革新,提升对爆炸物和可燃物的侦测能力。⑧ 史蒂芬·希尔(Steven Hill)探析了北约运用人工智能技术推动多边军事合作,以应对恐怖主义威胁的经验。⑨

综上所述,国内外学术界有关北约反恐的研究探讨了恐怖主义威胁的性质、北约反恐战略及其反恐举措,很多文献均关注在高科技条件下恐怖主义形态的演变以及北约如何运用新兴科技打击恐怖主义,然而集中论述北约如何在反恐中运用人工智能技术的文献较为有限。就此而言,北约智能反恐研究具有重要的学术价值和现实意义。相关研究既可以揭示北约成员国如何在这一敏感领域凝聚共识,也有助于探析北约如何将智能反恐研发与反恐实践相结合,丰富智能反恐的实证研究。

---

① Christian Kaunert and Ori Wertman, "Counter-terrorism Cooperation," in Gustav Lindstrom and Thierry Tardy, eds., *NATO and the EU: The Essential Partners*, NATO Defense College, 2019, pp.79-89.

② Konstantin V. Frolov and Gregory B. Baecher, *Protection of Civilian Infrastructure from Acts of Terrorism*, Springer, 2006.

③ Jaroslav Pollert and Bozidar Dedus, *Security of Water Supply Systems: From Source to Tap*, Springer, 2006, p.vii.

④ Mete Tahmisoğlu and Çinar Özen, eds., *Transportation Security against Terrorism*, IOS Press, 2009, pp.1-4.

⑤ Simon Wessely and Valery N. Krasnov, *Psychological Responses to the New Terrorism: A NATO-Russian Dialogue*, IOS Press, 2005.

⑥ Ion Apostol et al., eds., *Engaging the Public to Fight the Consequences of Terrorism and Disasters*, IOS Press, 2015.

⑦ Andrew D. James, "Science and Technology Policies for the Anti-Terrorism Era," in Andrew D. James, ed., *Science and Technology Policies for the Anti-Terrorism Era*, IOS Press, 2006, p.3.

⑧ Hiltmar Schubert and Andrey Kuznetsov, eds., *Detection of Liquid Explosives and Flammable Agents in Connection with Terrorism*, Springer, 2008, pp.v-vi.

⑨ Steven Hill, "AI's Impact on Multilateral Military Cooperation: Experience from NATO," *AJIL Unbound*, Vol. 114, 2020, pp.147-151.

二 北约智能反恐的建设进程与战略布局

2019 年 12 月北约伦敦峰会声明指出:“为了安全,我们必须共同展望未来。我们正致力于拓宽新技术的广度和深度,以保持技术优势,同时维系我们的价值观和规范。”①北约《2020-2040 年科技趋势》报告将人工智能(Artificial Intelligence)界定为“通过数字化或自主系统的智能软件赋予机器能力,使之完成原本需要人类智能才能完成的任务,例如模式识别、从经验中学习、得出结论、进行预测或采取行动。”②《北约防御恐怖主义军事概念》将反恐(Counter-terrorism)界定为“通过预防性、防御性和进攻性举措降低军队、个人和财产相对于恐怖威胁或恐怖行动的脆弱性,并对恐怖活动做出回应。”③北约将认知(Awareness)、能力(Capabilities)和参与(Engagement)作为反恐的三大关键领域。④ 北约智能反恐可分为:在认知层次上,构建智能反恐态势感知、情报分析、预警及监控系统;在能力层次上,提升智能决策、技术研发和军事行动等能力;在参与层次上,深化与伙伴国和国际组织在智能反恐领域的合作。北约积极推进反恐能力建设,并将智能反恐纳入北约全球安全战略之中。

(一)北约智能反恐能力的建设进程

21 世纪北约智能反恐能力建设进程可分为三个阶段。

第一阶段从 2001 年到 2006 年,是北约智能反恐能力的初步建设阶段。2001 年“9·11”事件后,北约迅速援引《北大西洋公约》关于集体防御的第五条款,这是其历史上首次为应对恐怖袭击而启动第五条款。⑤ 北约于 2002 年开始着力推进与智能反恐相关的研发工作。2002 年,北约在美国马里兰州亨特谷举办研讨会,探讨如何通过技术创新来防御恐怖分子使用大规模杀伤性武器。会上讨论了如何建立“危险事件自动化决策支持系统”(Automated Decision Aid System for Hazardous Incidents)。该项目得到美国国防部资助,旨在开发可有效应对化学、生物、放射性物质、核、爆炸物等恐

① NATO, “London Declaration,” *NATO.int*, December 4, 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

② NATO Science & Technology Organization, *Science & Technology Trends 2020-2040*, Brussels, March 2020, p.50.

③ NATO International Military Staff, “NATO's Military Concept for Defence against Terrorism,” *NATO.int*, August 19, 2016, https://www.nato.int/cps/en/natohq/topics_69482.htm.

④ NATO, “NATO's Policy Guidelines on Counter-terrorism: Aware, Capable and Engaged for a Safer Future,” *NATO.int*, May 21, 2012, https://www.nato.int/cps/en/natohq/official_texts_87905.htm.

⑤ “Invocation of Article 5 Confirmed,” *NATO Update*, October 2, 2001, https://www.nato.int/docu/update/2001/1001/e1002a.htm.

怖事件的计算机一体化决策支持系统。① 负责新兴安全挑战事务的北约助理秘书长索林·杜卡鲁(Sorin Ducaru)指出,北约在 2002 年布拉格峰会上决定建立计算机事件响应能力技术中心(NCIRC),斥资提升该中心的全面行动能力,并在北约东部扩建多个新总部。② 北约于 2003 年在布鲁塞尔总部成立"恐怖主义威胁情报小组"(Terrorist Threat Intelligence Unit),以促进成员国反恐情报合作。2004 年 6 月,北约伊斯坦布尔峰会将北约特别委员会改组为民事情报委员会,由各成员国政府安全部门代表组成。北约情报理事会改组为军事情报委员会,由各国军方情报机构代表组成。③

第二阶段从 2007 年到 2013 年,是北约智能反恐能力的发展阶段。2007 年 10 月,北大西洋议会通过《保护关键基础设施》特别报告,强调爱沙尼亚于同年遭遇的网络袭击是一场针对政府资产、公共和私营服务的大规模协同网络袭击,各国应增强早期预警能力以迅速对网络威胁做出回应。④ 2008 年,北约在爱沙尼亚首都塔林组建协作网络空间防御卓越中心(CCDCOE)。2010 年,北约国际参谋部设立新兴安全挑战部(Emerging Security Challenges Division),以应对恐怖主义和网络攻击等非传统安全威胁,注重提升运用公开资料、外交报告等素材开展战略情报评估的"战略分析能力"。在 2010-2011 年,北约总部推进情报机制改革,建立"情报小组"(Intelligence Unit)取代"恐怖主义威胁情报小组",以促进北约民事和军事情报机构之间的合作。⑤ 2012 年,北约斥资 5800 万欧元启动网络防御项目,在比利时蒙斯设立技术中心,为北约网络系统提供技术支持。⑥ 北约反恐卓越中心副主任安德鲁·伯纳德(Andrew T. Bernard)指出,北约从 2013 年开始关注网络恐怖主义问题,特别是恐怖分子对于社交媒体的渗透。⑦ 2013 年 3 月 14 日,"多国网络防御能力发展项目"在比利时布鲁塞尔正式启动。该项目由加拿大、丹麦、荷兰、挪威和罗马尼亚五个北约国家投资创建,得到

---

① James A. Genovese and Arthur Stuempfle, "Automated Decision Aid System for Hazardous Incidents (ADASHI)," in Peter J. Stopa and Zvonko Orahovec, eds., *Technology for Combating WMD Terrorism*, Proceedings of the NATO Advanced Research Workshop on Technology for Combating WMD Terrorism, Hunt Valley, November 19-22, 2002, p.149.

② Interview with Sorin Ducaru, "Is Cyber Defense Possible?" *Journal of International Affairs*, Vol.70, No.1, 2016, p.185.

③ 王鑫元:《冷战后北约情报工作发展研究》,载《军事历史》,2019 年第 2 期,第 113 页。

④ NATO Parliamentary Assembly, "The Protection of Critical Infrastructures," 162 CDS 07 E rev 1, October 7, 2007, p.14.

⑤ "Tackling New Security Challenges," *NATO Briefing*, January 31, 2012, p.8, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120116_new-security-challenges-e.pdf.

⑥ 韩雪晴:《全球公域战略与北约安全新理念》,载《国际安全研究》,2014 年第 4 期,第 60-61 页。

⑦ Robert K. Ackerman, "NATO Focuses on Terrorist Cyber Exploitation," *Signal Magazine*, March 1, 2014, https://www.afcea.org/content/nato-focuses-terrorist-cyber-exploitation.

北约信息交通局支持。各国将分享信息技术与情报,共同开发网络防御技术,加强基础设施防护,以提升网络防御能力。① 北约于 2013 年通过《塔林手册》,体现了其主导全球网络空间治理,制定网络空间运行规则的战略目标。

第三阶段从 2014 年至今,是北约智能反恐能力的深化阶段。2014 年 9 月,北约成员国决定进一步加强网络防御,启动“防务能力建设倡议”。时任北约秘书长拉斯穆森指出,北约决定将这一倡议拓展到格鲁吉亚、摩尔多瓦和约旦。② 2016 年,北约华沙峰会明确提出网络袭击将导致北约援引第五条集体防御条款,从而正式将网络空间确定为军事行动空间,并将全方位地考虑网络防御。③ 北约于 2016 年做出“网络防御承诺”,决定在突尼斯建立新的情报融合中心,以改善北约处理情报的能力。2017 年 3 月,北约远景研究工作组(Advanced Research Workshop)在贝尔格莱德会议上决定建立应对生物恐怖主义威胁和生物疾病传播的跨学科平台,加强对生物恐怖主义的防范。④ 北约总部于 2017 年建立了新的情报与安全联合部(Joint Intelligence and Security Division)。北约负责情报事务的助理秘书长洛林齐霍芬(Arndt Freytag von Loringhoven)指出,情报与安全联合部是北约第一个民事与军事联合情报机构。两个部门的联合使北约可以卓有成效地应对混合型威胁、网络安全威胁与恐怖主义威胁。⑤ 2018 年 8 月,北约在比利时蒙斯建立网络空间行动中心。2019 年 6 月,北约在斯洛伐克布拉迪斯拉发举办第一次网络危机模拟会议。会议的主题包括运用网络和人工智能技术管控海上难民危机、应对外国投资带来的网络安全挑战以及运用网络能力来打击不实信息。⑥ 北约盟军转型司令部主持了人工智能等颠覆性技术(Disruptive Technologies)的科技创新和研发工作。2019 年 10 月,盟军转型司令部组织各国大使和军事代表举办非正式研讨会,探讨“北约如何运用数据科学、机器学习和其他新技术来改善

① 高华:《北约组织最新动向及面临的挑战》,载李慎明等编:《国际形势黄皮书:全球政治与安全报告(2014)》,社会科学文献出版社 2014 年版,第 194 页。

② “NATO to Strengthen Collective Defense,” *Foreign Policy News*, September 6, 2014, https://foreignpolicynews.org/2014/09/06/nato-strengthen-collective-defense/.

③ NATO Public Diplomacy Division, “The Secretary General's Annual Report 2018,” *NATO.int*, March 15, 2019, p.64, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20190315_sgar2018-en.pdf.

④ “Preface,” in Vladan Radosavljevic et al., eds., *Defence against Bioterrorism: Methods for Prevention and Control*, p.v.

⑤ Arndt Freytag von Loringhoven, “A New Era for NATO Intelligence,” *NATO Review*, October 29, 2019, https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html.

⑥ NATO, “NATO Supports Groundbreaking Cyber Exercise at GLOBSEC 2019 Forum,” *NATO.int*, June 6, 2019, https://www.nato.int/cps/en/natohq/news_166722.htm.

决策进程”。[①] 2019 年 12 月,北约网络联盟军演在爱沙尼亚共和国国防军事学院基地举行。至今为止,北约通信与信息局已主办十余届信息保障研讨会(NATO Information Assurance Symposium)。2019 年 10 月,以“数字化转型”为主题的第 15 届研讨会在比利时蒙斯举行。[②] 北约通信与信息局正在牵头打造新“网络防御社区”,计划于 2019 年底前覆盖各成员国的网络安全机构,并逐步将其融入北约作战指挥链。[③]

(二)北约智能反恐的战略布局

北约在网络空间采取进攻性战略,针对恐怖主义威胁做出了全面的战略布局。北约智能反恐战略包括五项重要内容。

一是将恐怖主义作为北约面临的重要安全威胁。2010 年,北约战略新概念文件《积极接触、现代防务》强调,网络袭击已经处于威胁欧洲—大西洋地区繁荣、安全和稳定的临界点,可能危及政府、商业和经济,对交通、供应网与其他关键基础设施构成潜在威胁。外国军队和情报部门、有组织犯罪团伙、恐怖主义和极端主义分子均可能策划网络袭击。[④] 2014 年,北约威尔士峰会宣言强调恐怖主义对北约国家公民的安全、国际繁荣和稳定构成“直接威胁”。[⑤] 2018 年,北约秘书长年度报告指出:“恐怖主义关系到每个北约盟国,对北约国家的价值观、自由和生活方式构成了长期威胁。”[⑥] 同年 10 月,北约副秘书长露丝·戈特莫勒(Rose Gottemoeller)在香山论坛上指出:“我们不能用今天的工具来对抗明天的威胁。防御不再意味着展开地图思考如何部署军队和装备。我们需要在数字时代保卫自己,在人工智能时代保卫自己。”[⑦]2019 年 12 月,北约峰会《伦敦宣言》强调,一切形式和表现的恐怖主义仍然是我们面临的持续威胁。我们正在增加应对网络威胁的工具,确定应对该威胁的混合式战术。[⑧] 2020 年 6 月,北约负责新兴安全挑战事务的助理秘书长安东尼奥·米西罗利(Antonio Missiroli)

① NATO, “NATO Ambassadors and Military Leaders Meet to Discuss Disruptive Technologies,” *NATO.int*, October 1, 2019, https://www.nato.int/cps/en/natohq/news_169264.htm.

② NCI, “NATO and National Experts to Share Ideas at Cyber Security Symposium,” *NATO.int*, October 2, 2019, https://www.ncia.nato.int/about-us/newsroom/nato-and-national-experts-to-share-ideas-at-cyber-security-symposium-.html.

③ 赵云:《“网络联盟”军演开练,看北约如何锻造坚强“网盾”》,《科技日报》,2019 年 12 月 10 日,第 6 版。

④ NATO, “Active Engagement, Modern Defence,” *NATO.int*, November 19, 2010, https://www.nato.int/cps/en/natolive/official_texts_68580.htm.

⑤ NATO, “Wales Summit Declaration,” *NATO.int*, September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm? selectedLocale=en.

⑥ NATO Public Diplomacy Division, “The Secretary General's Annual Report 2018,” p.64.

⑦ NATO, “NATO Deputy Secretary General Rose Gottemoeller at the Xiangshan Forum in Beijing, China,” *NATO.int*, October 25, 2018, https://www.nato.int/cps/en/natohq/opinions_160121.htm.

⑧ NATO, “London Declaration,” *NATO.int*, December 4, 2019.

在演讲中指出,恐怖主义并未因全球疫情的流行而逐渐消失。恐怖主义削弱了我们的安全感,也削弱了支撑并激励我们社会的价值观。北约将运用一切可能的手段来应对这一威胁。①

二是抢占人工智能领域的战略制高点。北约在人工智能领域将中国作为竞争对手和防范对象。北约秘书长斯托尔滕贝格于 2018 年强调,北约不能再想当然地认为其拥有技术优势。中国将在人工智能领域投入 1500 亿美元,有望在 2030 年成为人工智能领域的全球领袖。② 2019 年 11 月,斯托尔滕贝格在演讲中指出,北约面临的最新及最先进的技术挑战来自北约之外。中国是世界第二大经济体,也是第二大防务支出国,更是从人脸识别到量子计算等技术研发方面的全球领袖。③ 为了在人工智能领域占据全球领先地位,北约已在该领域投入重金。北约科学事务署(NATO Scientific Affairs Division)主持了“为了和平和安全的科学计划”,反恐是该项目的五大优先事项之一,已经建立包括 22 位诺贝尔奖获得者在内的科学家协作网络。④ 2018 年 10 月,北大西洋议会科学技术委员会在考察美国圣地亚哥和硅谷后得出结论:人工智能将是民事和军事领域内多数未来前沿科技的核心内容。⑤ 北约盟军转型司令部在 2018 年启动了“新兴及颠覆性技术路线图计划”,谋求在人工智能技术等高科技领域的优势地位。⑥ 斯托尔滕贝格宣布,北约计划将预算开支的 20%投入研究开发和新设备领域,加大对人工智能、机器学习和自主系统等新兴颠覆性技术的支出。北约各国将争取在 2024 年达到防务预算占国民收入 2%的门槛。⑦

三是奉行进攻性的网络安全战略。2017 年 11 月,斯托尔滕贝格在北约防长峰会后表示,在网络空间的防御必须要像在陆地、海洋和空中一样有效,必须实时了解我们

---

① NATO, “NATO Launches Counter-Terrorism Reference Curriculum,” *NATO.int*, June 12, 2020, https://www.nato.int/cps/en/natohq/news_176304.htm.

② Transformation Network Branch SACT NATO, *2018 Chiefs of Transformation Conference Analysis Report*, February 2019, p.8, https://www.act.nato.int/images/stories/events/2018/cotc/2018-cotc-report.pdf.

③ NATO, “Keynote Address by NATO Secretary General Jens Stoltenberg at the NATO Industry Forum,” *NATO.int*, November 14, 2019, https://www.nato.int/cps/en/natohq/opinions_170786.htm.

④ NATO Public Diplomacy Division, “The Secretary General's Annual Report 2018,” p.86.

⑤ “Artificial Intelligence Central to All Future Defence Capabilities,” *NATO Parliamentary Assembly*, October 23, 2018, https://www.nato-pa.int/news/artificial-intelligence-central-all-future-defence-capabilities.

⑥ “Extracts from the Emerging and Disruptive Technologies Roadmap,” *NATO.int*, June 11, 2018, p.6, https://extranet.nshq.nato.int/sites/innovation/NATO%20Guidance%20on%20Innovation/Extracts%20from%20the%20Emerging%20and%20Disruptive%20Technologies%20Roadmap%20Selective%20Lines%20of%20Effort%20for%20Rapid%20Development.pdf.

⑦ NATO, “Keynote Address by NATO Secretary General Jens Stoltenberg at the NATO Industry Forum,” *NATO.int*, November 14, 2019, https://www.nato.int/cps/en/natohq/opinions_170786.htm.

面临的威胁,有能力在我们选择的时间内、以我们想要的方式做出回应。① 2018 年 7 月,北约布鲁塞尔峰会宣言将网络防务确定为北约集体防务的核心内容。② 美国国防部联合人工智能中心主任约翰·沙拉汉(John Shanahan)指出,人工智能技术应用前景广阔,可以强化北约同盟。我们将迅速应用人工智能技术,让军队赶上数字现代化的潮流,保持在承担重大、复杂使命时的灵活机动性。③ 北约战略沟通卓越中心明确表示,恶意行为体操纵社交媒体,侵害了北约的利益。我们应更有成效地分析、预防、早期侦测问题,增强我们的防御能力。倘若敌手有能力操纵信息空间,将削弱北约在危机或冲突时刻有效传递信息的能力。北约必须改善在信息环境中的沟通战略,同时增强辨别真假信息的能力。④

四是通过制度建设和成员国自愿贡献资源的方式来提升反恐能力。北约在人工智能反恐方面建立了多个机构,在职权划分上更为细化。位于安卡拉的反恐卓越中心提供了防御恐怖主义的专业知识和训练,主要关注恐怖主义威胁的战略和行动层面。⑤ 位于塔林的协作网络空间防御卓越中心侧重于网络防务。⑥ 位于蒙斯的网络空间行动中心向成员国提供网络威胁的实时情报。⑦ 新升级的联合情报和安全部(Joint Intelligence and Security Division)与各成员国首都建立了保密通信渠道,可以分享机密的恐怖主义威胁情报。⑧ 驻那不勒斯盟军联合司令部负责评估联盟南部的危机态势并做出回应。⑨ 北约注重通过核心成员参与来提升网络行动能力。反恐卓越中心由

---

① NATO, "Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Defence Ministers," *NATO.int*, November 8, 2017, https://www.nato.int/cps/en/natohq/opinions_148417.htm? selectedLocale=en.

② NATO, "Brussels Summit Declaration," *NATO.int*, July 11, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

③ Yasmin Tadjdeh, "DoD Seeks AI Alliance to Counter China, Russia," *National Defense Magazine*, March 3, 2020, https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia.

④ NATO Strategic Communications Centre of Excellence, "How Social Media Companies Are Failing to Combat Inauthentic Behaviour Online," November 2019, p.30.

⑤ Anita Hawser, "NATO to Use Cyber Effects in Defensive Operations," *Defense Procurement International*, November 11, 2017, https://www.defenceprocurementinternational.com/features/maritime/nato-and-cyber-weapons.

⑥ "About Us," https://ccdcoe.org/about-us/.

⑦ Robert K. Ackerman, "NATO Focuses on Terrorist Cyber Exploitation," *Signal Magazine*, March 1, 2014.

⑧ Julian Lindley-French, "Adapting NATO to an Unpredictable and Fast-changing World," *NATO.int*, February 19, 2018, https://www.nato.int/docu/review/articles/2018/02/19/adapting-nato-to-an-unpredictable-and-fast-changing-world/index.html.

⑨ NATO, "Countering Terrorism," *NATO.int*, December 10, 2019, https://www.nato.int/cps/en/natohq/topics_77646.htm.

土耳其、保加利亚、德国、匈牙利、荷兰、罗马尼亚、英国和美国八国共同参与。① 北约成员国网络安全合作采取自愿参与的原则。北约秘书长斯托尔滕贝格指出,各国国防部长达成协议,在完成北约使命和行动时使用本国网络进攻能力。各国仍然拥有这些能力,正如其在北约行动中仍然拥有坦克、舰船和飞机一样。②蒙斯网络空间行动中心副主任尼尔·杜瓦(Neale Dewar)在采访中表示,北约本身并没有进攻性网络进攻能力,因此进攻性网络行为的发起者是几个北约国家,或者由某个北约国家在与北约达成共识后贡献其网络进攻能力。③已有 9 个北约成员国表示愿意向网络空间行动中心提供网络进攻能力,包括美国、英国、荷兰、爱沙尼亚、挪威、德国、法国、丹麦和立陶宛。④

五是深化与欧盟及私营部门之间的合作。2016 年 2 月,北约计算机事件响应能力协调中心和欧盟计算机应急响应团队(CERT)签署技术合作协议。⑤ 斯托尔滕贝格指出,北约和欧盟可以分享信息、联合开展培训和教育、共同举办军事演习,以保障我们拥有最强大的工具来应对日益增长的网络威胁。欧盟曾多次参加北约的网络联盟军事演习。北约和欧盟可以深化反恐合作,共同推动立法和警务安全改革、制定国内紧急情况规划、处理放射性弹药和小武器等问题。⑥ 在与私营部门合作方面,北约工业咨询团体侧重于探究机器学习、大数据分析等技术对北约的影响。北约联盟转型司令部与一些公司开展人工智能领域的合作,制定防务决策的改革方案,并研发应对新形势的技术工具。⑦ 北约工业网络伙伴关系(NATO Industry Cyber Partnership)旨在加强与工业界和学术部门之间的关系。斯托尔滕贝格指出,深化和工业界合作可以赶上技术进步的潮流,运用科技创新成果,提升我们的网络防御能力。随着我们转型到“物联网”,智能系统将与我们的生活息息相关,我们将频繁使用人工智能、机器学习和量子计算,因此,与工业界的关系显得尤为重要。⑧

---

① NATO, “NATO's Defence against Terrorism Program,” *NATO.int*, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_10/20151029_141007-dat-prog.pdf.

② NATO, “Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Defence Ministers,” *NATO.int*, November 8, 2017.

③ Shannon Vavra, “NATO Cyber-operations Center Will Be Leaning on Its Members for Offensive Hacks,” *Cyber Scoop*, August 30, 2019, https://www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/.

④ Ibid.

⑤ Interview with Sorin Ducaru, “Is Cyber Defense Possible?” p.186.

⑥ NATO Public Diplomacy Division, “The Secretary General's Annual Report 2018,” pp.65-66.

⑦ Ibid., p.43.

⑧ Jens Stoltenberg, “NATO Will Defend Itself,” *Prospect's Cyber Resilience Supplement*, October 2019, p.4.

三 北约在智能反恐应用方面的进展

21 世纪,北约在智能反恐领域取得稳步进展。从 2001 年至 2010 年,北约在反恐十年间注重为智能反恐积累原始数据,推进陆上和海上的智能反恐实践。从 2011 年至 2020 年,北约全面推进了跨学科的智能反恐研发,构建较为完善的智能反恐技术平台,并将多种智能武器应用于反恐实战中。

(一)21 世纪第一个十年的主要进展(2001-2010 年)

从 2001 年至 2010 年,北约在智能反恐领域取得的进展主要包括三方面。

一是在反恐行动中广泛使用无人机积累原始数据。在“9·11”事件后,北约在反恐战争中频繁使用无人作战系统。无人机成为索马里等地反恐行动使用的主要武器系统。① 2004 年 4 月,北约批准了“联合地面监视系统”(Alliance Ground Surveillance)项目,将无人机作为该系统的机载平台,主要部署于伊拉克和阿富汗等地区。② 该项目由十几个北约国家共同出资,可用于清除位于阿富汗的简易爆炸装置或打击索马里海盗。截至 2010 年,丹麦退出该项目以前,其预算已高达 17 亿美元。③ 北约在伊拉克和阿富汗的反恐行动中,无人机的数量与日俱增,成为搜集情报的重要工具。其拍摄的照片和视频均被搜集分类并存档,作为后续分析的重要资料。④

二是致力于推进陆上智能反恐中的清除爆炸物研究与实践。在 21 世纪初,炸弹袭击是造成北约国家人员伤亡最多的恐怖袭击形式。为了应对简易爆炸装置,北约调研了恐怖分子研制武器的过程及其爆炸效应,探究如何运用高科技使炸弹发生故障,并确定其产地和隐藏之处。北约炸弹专家探究如何利用机器人等智能技术来加强北约部队的装备力量,提升其应对爆炸物的能力。北约充分运用大数据分析研究恐怖活动,北约科学家构建了爆炸物数据库,记录在关键行动领域发现的各类未爆炸物,帮助

① Can Kasapoğlu and Barış Kırdemir, “Wars of None: Artificial Intelligence and the Future of Conflict,” Centre for Economics and Foreign Policy Studies, May 2019, p.16.

② 柯边:《北约启动联合地面监视系统计划》,载《航天电子对抗》,2004 年第 5 期,第 4 页。

③ Reuters, “Danish Pullout Hits NATO Drone Project,” *Defence Web*, June 24, 2010, https://www.defenceweb.co.za/aerospace/aerospace-aerospace/danish-pullout-hits-nato-drone-project/.

④ Jason Ditz, “Military Struggles to Make Sense of Drone Video Archive,” *anti-war.com*, January 10, 2010, https://news.antiwar.com/2010/01/10/military-struggles-to-make-sense-of-drone-video-archive/.

炸弹技术人员提升清除炸弹技能。①

三是推动海上智能反恐的研究。北约在 2001 年 10 月启动“积极努力”(Active Endeavour)海上行动,致力于在地中海打击恐怖主义。位于意大利的北约水下研究中心建立了部署于海平面上下的感应器网络,用于锁定恐怖分子并使其丧失行动能力,并尝试构建自动化的水下排雷装置,将人力解放出来。② 北约那不勒斯海事指挥中心(Headquarters Maritime Command Naples)构建了海上态势感知网络及进程。海事指挥中心可处理部署于陆海空各处的感应器传递的海量信息。15 个位于地中海和黑海的北约成员国组建了不断扩大的感应器网络,可实时传递数据,在监视能力方面实现了质的飞跃。③ 这一态势感知网络可以迅速侦测海上舰船的异常行为,例如不明原因的游荡行为及航道的异常变化。此外,北约还举办了一系列海上反恐演习,如 2003 年 11 月在土耳其多安贝伊军事基地举行海陆空联合反恐军事演习,2007 年 5 月在波罗的海展开以扫雷和反恐为主要内容的军事演习。

(二)21 世纪第二个十年的主要进展(2011-2020 年)

在 21 世纪第二个十年间,北约人工智能反恐实战能力显著提升。北约构建了以人工智能技术为核心的态势感知系统,积极打造攻防兼备的无人机作战平台,并在军事演习中频繁使用智能武器。

一是构建以人工智能技术为核心的跨学科态势感知系统。人工智能技术可从全局高度把握恐怖主义发展态势,并感知恐怖主义的发展动向。北约总部特种作战指导小组官员德韦克(De Wijk)指出,人工智能系统可以优化决策进程,在实战场景中,灵活的防御概念将会缩短“观察—适应—决策—行动”的周期。随着智能武器、超音速与超高音速武器以及蜂群战术(Swarm Tactics)的发展,这一周期将变得更为自动化。在这类超级战争(Hyper War)中,人工智能和机器学习算法将优化决策进程,并有可能将人类从决策周期中解放出来。④ 史蒂芬·希尔(Steven Hill)指出,北约运用人工

① Marshall Billingslea, “Military Matters: Combating Terrorism through Technology,” *NATO Review*, Issue 3, 2004, https://www.nato.int/docu/review/2004/issue3/english/military.html#:~:text=As%20a%20result%2C%20NATO%20launched%20a%20Countering%20Improvised,sufficient%20speed%20and%20accuracy%20to%20return%20fire%20effectively.

② Ibid.

③ Commander Brian Finman, “Keeping the Med Safe: How It's Done,” *NATO Review*, May 4, 2010, https://www.nato.int/docu/review/articles/2010/05/04/keeping-the-med-safe-how-it-s-done/index.html.

④ Andrew White, “How NATO's Special Operations Can Take Advantage of the Tech Boom,” *C4ISR.net*, July 26, 2019, https://www.c4isrnet.com/artificial-intelligence/2019/07/26/how-natos-special-operations-can-take-advantage-of-ai/.

智能系统来筛选北约和成员国搜集的信息,以增强态势感知能力以及行动中的决策能力。① 北约“联合地面监视系统”包括远程控制的飞行器、地面和支持系统,已具备在各种气象条件下对各类地域的全天候监控能力。② 北约依托“恶意软件信息共享平台”(The Malware Information Sharing Platform)监控各类网络威胁事件,在成员国之间共享有关恶意软件的技术信息。③ 针对潜在对手运用信息技术来散布不实信息的做法,北约运用人工智能技术处理网络信息可以迅速辨别并打击因特网上的虚假新闻。④

二是打造攻防兼备的无人机作战平台,削弱恐怖分子运用无人机制造恐怖活动的能力。无人机空袭在北约反恐军事行动中所占比例已经从 2011 年的 5%提升到 2015 年的 56%,再到 2016 年第一季度的 61%。⑤ 据军事专家预测,到 21 世纪 30-40 年代,人工智能技术将为北约军事行动提供决策支持,无人机系统的自主性将进一步提升。⑥ 2019 年 2 月 14 日,北约国防部长批准了旨在打击无人机系统的行动计划,并确定了深化民事与军事合作,以应对核生化与放射性恐怖事件的指导原则。⑦ 同年 11 月,北约从诺格公司订购的首架“全球鹰”无人侦察机进驻意大利锡戈内拉空军基地,标志着北约“联合地面监视系统”进入实战部署阶段。“全球鹰”无人机可以完成长航程、长时间、全区域动态监视任务。⑧ 同年 12 月,北约与福特姆科技公司(Fortem Technologies)签署反无人机协议,共同构建打击恐怖主义的网络防御平台。该系统可以运用人工智能技术自动拦截无人机,削弱恐怖分子使用无人机发动袭击的能力。⑨

三是在军事演习中频繁试验各类人工智能武器。北约科学家正加强跨学科研究,将生物信息学、机器学习、以 DNA 为基础的生物计算等前沿技术应用于反恐领域。北

---

① Steven Hill, “AI's Impact on Multilateral Military Cooperation: Experience from NATO,” *AJIL Unbound*, Vol. 114, 2020, p.150.

② Arndt Freytag von Loringhoven, “A New Era for NATO Intelligence,” *NATO Review*, October 29, 2019, https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html.

③ NATO, “Sharing Malware Information to Defeat Cyber Attacks,” *NATO.int*, November 29, 2013, https://www.nato.int/cps/en/natolive/news_105485.htm.

④ Michael Rühle and Clare Roberts, “NATO's Response to Hybrid Threats,” in Marc Ozawa, ed., *The Alliance Five Years after Crimea: Implementing the Wales Summit Pledges*, NATO Defense College, 2019, p.66.

⑤ Can Kasapoğlu and Barış Kırdemir, “Wars of None: Artificial Intelligence and the Future of Conflict,” p.16.

⑥ Ibid.

⑦ NATO, “Countering Terrorism,” *NATO.int*, December 10, 2019.

⑧ 胡小刀:《北约实战部署“联合地面监视系统”》,《中国国防报》,2019 年 12 月 2 日,第 4 版。

⑨ “Fortem Technologies Selected by NATO For Defence Against Terrorism Program To Premiere Counter-UAV Solutions,” *fortemtech.com*, Press Release, December 9, 2019, https://fortemtech.com/blog/selected-by-nato-defense-against-terrorism/.

约战略司令部计划在生物识别领域全面提高能力,以保护实战中的部队,帮助部队确认已知或潜在的暴乱人员。① 生物感应器既可以探测出恐怖分子使用的爆炸物和化学毒剂,又具备独立决策能力和行动能力。② 2018 年 10 月 18 日,北约成功试验了三种可用于反恐的军事设备,包括可以探测并排除地雷和简易爆炸装置的半自动机器人、轻型地雷探测器以及手持脏弹探测系统。③ 同年 10 月,北约"三叉戟接口"联合军演试验了微型无人机和 3D 打印等新技术。④ 人工智能机器人可用于排除恐怖分子部署的爆炸物,保护人员安全,并向在恐怖活动中受伤的人员提供医疗服务。北约盟军转型司令部最高司令德尼·梅西耶(Denis Mercier)透露,我们在联合军演中首次运用人工智能来衡量士兵的压力水平,我们在士兵身上安置感应器,可感知他们是否受伤,并运用人工智能技术向其提供医疗援助。⑤ 梅西耶指出,这次演习表明人工智能可以将人类从非致命性决策中解放出来。北约还在演习中试验了如何运用人工智能来辨认袭击后勤基地的人员,同时测验的技术还包括机器人、人机合作与信息战。⑥ 2020 年 9 月 21 日,北约在军事演习中通过无人机群追踪地面形势演变,使用无人机向地面部队精准补给弹药物资。北约官员迪特尔·科尔(Dieter Kohl)指出,盟军转型司令部致力于推动新兴科技在军事应用方面的创新,本次演习展示了新兴科技在军事领域的应用前景。⑦

四 北约智能反恐面临的困局

在信息战场上制胜对手是智能反恐成功的关键。北约在信息分析、信息运筹和制信息权领域,均拥有相对于恐怖分子的绝对优势。然而从北约智能反恐的成效看,北

① NATO, "Defence against Terrorism Programme of Work (DAT POW), " *NATO.int*, July 3, 2018, https://www.nato.int/cps/en/natohq/topics_50313.htm.

② NATO Science & Technology Organization, *Science & Technology Trends 2020-2040*, p.96.

③ NATO, "New NATO Scientific Projects to Help with the Fight against Terrorism," *NATO.int*, October 17-18, 2018, https://www.nato.int/cps/en/natohq/news_160271.htm.

④ NATO, "Keynote Address by NATO Secretary General Jens Stoltenberg at the NATO Industry Forum," *NATO.int*, November 14, 2019, https://www.nato.int/cps/en/natohq/opinions_170786.htm.

⑤ Patrick Tucker, "How NATO's Transformation Chief Is Pushing the Alliance to Keep up in AI," *Defense One*, May 18, 2018, https://www.defenseone.com/technology/2018/05/how-natos-transformation-chief-pushing-alliance-keep-ai/148301/.

⑥ Patrick Tucker, "How NATO's Transformation Chief Is Pushing the Alliance to Keep up in AI," *Defense One*, May 18, 2018.

⑦ "DroneUp Delivers on NATO Allied Command Transformation Experiment," *Suas News*, September 29, 2020, https://www.suasnews.com/2020/09/droneup-delivers-on-nato-allied-command-transformation-experiment/.

约在全面掌控信息、预测恐怖袭击发展态势、预防和应对恐怖袭击等领域,均面临重重困难。正如北约副秘书长罗斯·高特莫勒(Rose Gottemoeller)指出,当网络危机发生时,北约并没有办法迅速化解一切问题。① 北约智能反恐面临的困局主要表现在四个方面。

其一,北约智能反恐政策的调整明显滞后于瞬息万变的恐怖活动发展态势。丹尼尔·菲奥特(Daniel Fiott)和古斯塔夫·林德斯特罗姆(Gustav Lindstrom)指出,人工智能引导的训练平台可以基于恐怖分子过去的行为,更精确地对恐怖团体的行动、原则和战略做出预判。然而恐怖活动具有不可预测性。人工智能技术无法模拟恐怖分子的偷袭以及恐怖袭击中的意外因素。② 面对有关恐怖活动的海量无序信息,北约还不能迅速完成对数据的整理分类工作,探究恐怖分子的行为模式,并预测恐怖活动的未来走向。一位英国军官曾经这样诟病北约国家在数据分析方面的短板,各国军队恰似漂泊于探测设备之间,淹没于海量数据中,严重缺乏洞察力。③

其二,北约对于网络极端化的管控存在漏洞。北约科学技术委员会于 2018 年发表的《黑暗勾当:恐怖分子如何运用加密通信、暗网和密码货币》报告指出,恐怖分子正在运用信息加密技术来躲避政府的监控,他们在信息通信、指挥控制、融资和非法交易方面均在使用该技术。④ 北约网络专家指出,网络空间的社交媒体交易黑市规模庞大,不法分子可以通过搜索引擎来购买社交媒体操纵软件、制造虚假账号、获得手机代理服务。⑤ 为了检验社交媒体公司监测并删除虚假信息的能力,北约专家曾购买了 16 家社交媒体操纵机构的服务。其中 11 个机构位于俄罗斯,5 个机构位于欧洲国家。他们仅用 300 欧元就在脸书(Facebook)、照片墙(Instagram)、推特(Twitter)和优兔(YouTube)上的 105 个站点,买到了 3530 个评论、25750 个点赞、20000 次阅读量以及 5100 个粉丝。在购买四周后,五分之四的虚假信息仍然挂在网上。北约专家主动向社交媒体平台举报了虚假账号,然而三周后被举报的 95%的账号仍活跃在网上。⑥ 虚

① 陈雅东:《北约加强网络防御的"门道"》,《解放军报》,2019 年 3 月 21 日,第 11 版。

② Daniel Fiott and Gustav Lindstrom, "Artificial Intelligence: What implications for EU Security and Defence?" European Institute for Security Studies, November 2018, p.5.

③ NATO Parliamentary Assemby Science and Technology Committee Sub-Committee on Technology Trends and Security, "Artificial Intelligence: Implications for NATO's Armed Forces," pp.3-4.

④ Matej Tonin, "Dark Dealings: How Terrorists Use Encrypted Messaging, the Dark Web and Cryptocurrencies," p.1.

⑤ NATO Strategic Communications Centre of Excellence, "How Social Media Companies Are Failing to Combat Inauthentic Behaviour Online," p.6.

⑥ Ibid., p.3.

拟空间的丰富资源拓宽了恐怖分子活动的空间,也加大了北约管控网络极端化的难度。

其三,北约智能反恐面临诸多技术挑战。一是智能反恐决策体系尚不完善。北约首席科学家托马斯·基利昂(Thomas Killion)透露,北约尝试通过人工智能技术加速军事决策进程,人工智能将参与决策中的"观察—适应—决策—行动"周期。① 人工智能系统缺乏人类的基本常识,很多深度学习模型采用黑箱运作模式,人类无法理解其决策的逻辑。将人类的生杀予夺大权交给人工智能系统,存在诸多安全隐患。二是需要突破智能反恐军事行动中的技术瓶颈。德尼·梅西耶(Denis Mercier)司令指出,北约在军事行动中的互操作能力(Interoperability)亟待加强,我们的军队应该能共同协作,并在分享信息方面无缝衔接。② 在反恐行动中,北约现阶段仍需同时使用传统武器系统和智能武器系统,不同系统之间的鸿沟可能削弱北约的实战能力。③ 三是智能武器技术向非国家行为体扩散的风险日益扩大。自 2015 年 7 月开始,全球已有 3 万多位科学家联名签署公开信,呼吁禁止研发人工智能武器。他们指出,人工智能武器研发将不可避免地导致全球军备竞赛。人工智能武器不需要造价高昂或者难以获得的原材料就可以大规模投入生产,这些武器不久后就会进入黑市,落入恐怖分子之手,沦为新的屠杀工具。④ 北约强调人工智能将改变战争面貌,积极研发人工智能武器。⑤然而此举不仅无助于消弭恐怖威胁,还带来了更棘手的安全挑战。

其四,北约仍然面临着成员国之间的协调问题。北约各成员国的技术水平参差不齐,如爱沙尼亚信息技术水平较为落后,仍需付出较大努力才能赶上北约强国。马格努斯·彼得森(Magnus Petersson)指出,北约内部围绕什么是最重要的安全威胁存在分歧,美国关注反恐和中东局势,同时欧洲北部、东部和地中海地区的国家对于重点安全威胁的认知也各不相同。⑥ 朱丽叶·伯德(Juliette Bird)表示,北约各国对于恐怖主义的讨论并不在同一个水平线上。波罗的海国家关注乌克兰、俄罗斯等邻国的形势,

① Jessica Bayley, "Transforming ISR capabilities through AI, Machine Learning and Big Data," *Defence IQ*, July 30, 2018, https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data.

② Denis Mercier, "How Will Artificial Intelligence and Disruptive Technologies Transform Military Operations and Organizations?" *NATO.int*, May 31, 2018, p.9, https://www.act.nato.int/images/stories/media/speeches/180531_sto.pdf.

③ NATO Science & Technology Organization, *Science & Technology Trends 2020-2040*, p.26.

④ "Autonomous Weapons: An Open Letter from AI and Robotics Researchers," *FutureTimeline.net*, July 28, 2015, https://www.futuretimeline.net/blog/2015/07/28.htm.

⑤ NATO Science & Technology Organization, *Science & Technology Trends 2020-2040*, p.9.

⑥ Magnus Petersson, *NATO and the Crisis in the International Order*, Routledge, 2019, pp.49-60.

而土耳其关注来自南方的安全威胁。北约各国要摒弃分歧采取大规模行动仍然举步维艰。① 数据是人工智能分析的关键要素,然而一些北约成员国并不愿意和其他国家分享情报和数据。波兰学者格鲁兹扎克(Artur Gruszczak)指出,尽管北约所拥有的总体情报资源相对庞大,这些资源却仍然属于各成员国的情报界。美国几乎完全独占着卫星感应器等情报资源,因此北约情报能力的提升取决于美国是否愿意与其他成员国共享资源。② 北约盟军转型司令部最高司令梅西耶曾经呼吁各成员国在目睹人工智能的效能后,主动分享敏感信息或机密信息。③ 为了更有效地提升智能反恐能力,北约成员国需要尽快达到防务开支占国内生产总值 2%的标准,并更有效地分配资源。北约助理秘书长索林·杜卡鲁指出,在网络防务开支方面,将同样的资金投入不同领域,其结果将截然不同。若将大部分预算用于发展高精尖的网络防御技术,用于人力资源的资金就会极其有限。若将全部资源用于训练和演习,却仍然固守于上一代的技术,那么技术专家就像把一只手反绑在背后那样进退维谷。④

五 结论

2020 年 9 月 28 日,北约副秘书长米尔卡·吉奥纳(Mircea Geoană)在人工智能网上论坛发表演讲指出,在过去的 70 年间,北约的创新能力使其保持了军事优势地位和科技领先地位。北约将继续保持对现代科技的投入,以应对未来的威胁。⑤ 在新的安全形势下,北约在智能反恐方面拓展思路,采用新举措来应对恐怖主义威胁。北约在智能反恐领域主要取得四项新进展。一是增强对新型恐怖威胁的态势感知能力。北约密切追踪恐怖主义的发展态势,关注并积极防范生化恐怖主义、海上恐怖主义、网络恐怖主义等新型恐怖主义。二是通过科技攻关抢占人工智能领域的战略制高点。北约努力构建人工智能研发领域的科学家网络,注重在研发中深化与私营部门的合作,加快新兴技术应用于反恐的速度,取得显著成效。三是推进智能反恐制度建设。北约在实践中不断完善自身的制度架构,已构建起颇具规模的反恐制度网络,增强态势感

① Juliette Bird, "NATO's Role in Counter-Terrorism," *Perspectives on Terrorism*, Vol.9, Issue 2, 2015, p.66.

② Artur Gruszczak, "NATO's Intelligence Adaptation Challenge," *GLOBSEC*, p.7, https://www.globsec.org/wp-content/uploads/2018/03/NATO%E2%80%99s-intelligence-adaptation-challenge.pdf.

③ Patrick Tucker, "How NATO's Transformation Chief Is Pushing the Alliance to Keep up in AI," May 18, 2018.

④ Interview with Sorin Ducaru, "Is Cyber Defense Possible?" p.189.

⑤ NATO, "Deputy Secretary General at HumanAIze Forum: We Cannot Fight Tomorrow's Threats with Yesterday's Tools," *NATO.int*, September 28, 2020, https://www.nato.int/cps/en/natohq/news_178374.htm.

知能力、情报分析能力、大数据处理能力和预防恐怖主义的能力。四是通过降低合作门槛深化在敏感技术领域的合作。北约在反恐中积极利用成员国的资源,形成几个国家先行,其他国家自愿参与的模式,克服在敏感领域面临的内部阻力。

同时北约的智能反恐实践,也暴露出智能反恐在应用中面临的三种潜在风险。

其一,人工智能技术可能扰乱正常的决策过程。人工智能系统缺乏人类的判断力和经验,可能曲解对方意图,夸大其敌意,致使外交危机升级为军事对抗,冲突愈演愈烈。① 北约科学家纳撒尼尔·博伦斯坦(Nathaniel S. Borenstein)曾于 1987 年参加了北约人工智能军事行动研发小组。他颇具洞察力地指出,应用人工智能技术潜伏着巨大的风险。倘若有朝一日人工智能掌控了整个指挥控制系统,它必然经常愚蠢地提出糟糕的建议,而人类可能因时间紧迫而不假思索地采纳其建议,最终将人类推向灾难边缘。② 汤姆·瓦莱舍克(Tomáš Valášek)指出,智能系统在实践中具有自主学习和改变行为的能力,它们可能在军事行动中以出乎设计者预料的方式自动改变程序。而在北约跨国军事行动中,多个智能自动系统联合行动意味着机器出错的风险会更大,甚至没有机会通过干预手段来避免局势升级。③

其二,北约使用智能武器降低了恐怖分子获得智能武器的门槛。北约将各种智能武器投入反恐实战中,尽管削弱了恐怖分子的有生力量,却也使这些武器流散到动荡地带。恐怖分子可以通过拆装武器、下载软件等方式掌握人工智能前沿技术,使之可能策划并实施新型恐怖袭击。卡萨波卢(Can Kasapoğlu)和克尔德米尔(Barış Kırdemir)指出,人工智能技术的发展,意味着国家和非国家行为体均可以获得智能化程度更高的自主武器系统。暴力团体可能将人工智能技术用于侦察、强制行为以及收集敌对情报行动中。预防恐怖团体获取致命自主武器系统将很快成为首要国际议程。④

其三,需要警惕北约在人工智能反恐领域谋求规则制定权。北约在精心储备智能反恐领域的原始数据,动员多位法律专家从事智能反恐规则制定方面的研究,以抢占战略先机。北约战略分析能力小组成员丁达尔(Gjert Lage Dyndal)指出,自主军事系

① Andrea Gilli, "Preparing for 'NATO-mation': The Atlantic Alliance toward the Age of Artificial Intelligence," *NDC Policy Brief*, No.4, February 2019, p.3.

② Nathaniel S. Borenstein, "My Life as a NATO Collaborator," *Bulletin of the Atomic Scientists*, Vol.45, Issue 3, April 1989, p.18.

③ Tomáš Valášek, "NATO at 70: Enter the Technological Age," *NDC Policy Brief*, No.10, NATO Defense College, April 2019, p.3.

④ Can Kasapoğlu and Barış Kırdemir, "Wars of None: Artificial Intelligence and the Future of Conflict," p.16.

统带来了责任的空白,必须通过完善技术方案和法律规范来解决责任追究问题。北约正致力于推进与致命自主武器(LAWS)相关的法律和伦理研究。① 北约法律专家提出“法律互操作性”(Legal Interoperability)的概念,并将其界定为“两个或者更多的国家有效的协同训练、演习和行动的能力,以执行使命和任务”。北约在 2016 年华沙峰会宣言和 2018 年布鲁塞尔峰会宣言中均使用了“法律互操作性”这一术语。② 发展中国家应加强合作,避免北约在智能反恐领域抢占规则制定的主动权。

人工智能时代,高新技术给国际反恐行动带来更多选择,也使恐怖袭击的模式发生深刻变化。恐怖团体具备迅速适应新形势和应用新技术的能力,他们可能会积极寻找人工智能算法公式中的漏洞,甚至操纵并破坏智能决策系统。人工智能技术的发展意味着未来的恐怖袭击可能具备多元化和混合型的特质,甚至可能使用具备自主决策能力的大规模杀伤性武器。要消除恐怖主义风险,世界各国应深化合作,从全局感知恐怖主义发展态势,针对不同类型的恐怖活动构建不同的智能反恐模型,确立全面的人工智能反恐战略。与此同时,各国应深化在信息动态感知、智能反恐预警、数据精准分析、深度学习平台开发等领域的合作,共同探究如何应对新技术条件下的恐怖安全威胁。

(**作者简介**:高望来,外交学院国际关系研究所副教授;**责任编辑**:蔡雅洁)

① Col G. Lage Dyndal et al., “Autonomous Military Drones: No Longer Science Fiction,” *NATO Review*, July 28, 2017, https://www.nato.int/docu/review/articles/2017/07/28/autonomous-military-drones-no-longer-science-fiction/index.html.

② Nadia Marsan and Steven Hill, “International Law and Military Applications of Artificial Intelligence,” in Andrea Gilli, ed., *The Brain and the Processor: Unpacking the Challenge of Human-Machine Interaction*, NATO Defense College, 2019, p.57.