人工智能时代的恐怖主义：挑战与应对[1]

谢　磊

【内容提要】人类社会已经进入到人工智能时代。恐怖分子利用人工智能带来的“红利”，通过使用无人机进行袭击、搜集情报、实施网络攻击和网络宣传等，对国际社会造成了严重威胁。人工智能的使用，增强了恐怖分子与国家政府进行不对称冲突的能力，加之恐怖分子伦理标准低，因此造成的伤害更大、活动的范围更广。国家政府需要在人工智能领域建立绝对优势，加强国际合作以及与重要人工智能商业公司和研究机构的合作关系，防止高等级人工智能被恐怖分子利用，从而有效避免恐怖分子利用这种新兴技术手段获得最大收益的可能性。

【关键词】人工智能　恐怖主义　无人机　技术革命

【作者简介】谢磊，国际关系学院《国际安全研究》编辑部编辑、助理研究员、法学博士。

【中图分类号】D815

【文献标识码】A

【文章编号】1006-6241(2021)02-0115-19

[1] 本文受国际关系学院2020年度中央高校基本科研业务费（项目编号：3262020T29）资助。

人类社会已经进入到人工智能时代。“人工智能”是指研究和创造信息系统，使之具备类似通过人力解决问题的能力。其主要采用计算机算法从事需要人类智商进行的工作，比如语音识别、视觉感知和决策制定等。[1] 简单来说，人工智能是一门科学，这门科学让机器做需要人类智能才能完成的事，涉及领域包括博弈、专家系统、神经计算、进化计算、自然语言处理、生物信息学等。[2]

人工智能正从各个方面改变着我们的日常生活，也对国际关系和国家安全产生了重大且深远的影响。一方面，作为人类文明发展的最新前沿科技成果，人工智能推动形成新的军事能力和战略博弈模式，维护经济、环境、网络、能源等领域安全，打击恐怖主义和跨境犯罪等方面都发挥了重要作用。[3] 但另一方面，人工智能的发展不可避免地会使其成为“双刃剑”，即在为人类社会带来便捷生活的同时，也会导致一些负面影响。例如，2018 年 2 月，生命未来研究所（Future of Humanity Institute）、牛津大学、剑桥大学、新美国安全中心（Center for a New American Security）等 7 家机构共同发布报告指出，人工智能的发展将会导致数字层面、物理层面和政治层面的安全问题。[4] 如人工智能的发展可能会造成个体隐私和个人信息的严重泄露；由于以往需要大量人力从事的工作改由人工智能承担，可

[1] Daniel Wagner, “Artificial Intelligence and Virtual Terrorism,” *Huffpost,* Aug. 17, 2017, https://www.huffpost.com/entry/artificial-intelligence-and-virtual-terrorism_b_5995c144e4b00dd984e37d08.

[2] [美] 史蒂夫·卢奇、[美] 丹尼·科佩克：《人工智能（第 2 版）》，林赐译，北京：中国工信出版集团、人民邮电出版社 2018 年版，第 5 页、第 29—36 页。

[3] 阙天舒、张纪腾：《人工智能时代背景下的国家安全治理：应用范式、风险识别与路径选择》，载《国际安全研究》2020 年第 1 期，第 4—38 页。

[4] Miles Brundage, et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,* Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI, Feb. 2018.

能会导致一些行业出现严重的失业问题；此外，一些犯罪分子可能会利用人工智能进行洗钱、银行诈骗和其他犯罪活动，对国家稳定和社会治安造成负面影响。最为悲观的预言是，随着人工智能技术的日趋成熟，其意识将会最终“觉醒”，从而成为人类自我制造的“潘多拉魔盒”，使得人类彻底沦为人工智能的奴隶。

在人工智能时代，反恐形势也面临着同样困境：一方面，利用人工智能打击恐怖主义具有得天独厚的优势，可以比其他手段花费更小的成本。例如，建立各种可疑信息、身份、面容、声音等的识别系统，辅助控制恐怖组织在社交媒体上的信息传播；通过开发新的芯片和深度算法，促进反恐情报的开发和利用；推动自主武器的研发，并将其运用到反恐实战中；基于大数据、机器学习和人工智能技术，对恐怖组织的行为进行预测，从而避免恐怖袭击发生。[1]

另一方面，随着人工智能在社会各领域的普遍运用，恐怖分子也认识到了其在组织活动中的优势，并将其作为一种行动工具运用到与国家政府对抗的实践之中。当前有一种值得担忧的趋势是，人工智能领域的军备竞赛将导致“流氓国家和非国家行为体，例如恐怖组织”通过黑市获得这些武器。[2] 恐怖组织利用人工智能带来的“红利”从事恐怖活动并非耸人听闻的宣传，而是一个客观存在的事实。相较于以往的传统方式，使用人工智能进行的恐怖活动有其自身鲜明的特点，即扩大了活动范围，减少了伤亡状况，同时也对国际局势产生了更为深远的影响。然而，相较于当前对人

[1] 董青岭：《机器学习与冲突预测——国际关系研究的一个跨学科视角》，载《世界经济与政治》2017 年第 7 期，第 100—117 页；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；肖军：《人工智能背景下公安反恐多技术融合模型的构建与运用》，载《中国刑警学院学报》2019 年第 4 期，第 12—17 页。

[2] Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence,* New York: Alfred A. Knopf, 2017, p.141.

工智能在反恐行动中优势的研究[1]，学术界对恐怖分子利用人工智能手段进行恐怖袭击的研究普遍关注不够。本文将对恐怖组织此类恐怖活动的主要表现及特点进行分析，并提出应对人工智能时代恐怖袭击的政策思考。

一、恐怖组织使用人工智能的主要方式

传统的恐怖袭击主要是通过放置爆炸物、使用枪械射击、驾驶或劫持交通工具撞击，甚至使用管制刀具行凶等方式，针对目标进行物理层面的攻击，以造成民众的恐慌情绪，要挟国家政府作出政治妥协或重大让步。然而，随着时代的进步，特别是新科学技术的发展与成熟，极大地改变了恐怖分子实施恐怖袭击的方式，他们开始利用诸如网络之类的虚拟空间从事恐怖主义活动。尤其是以“伊斯兰国”（IS）为代表的国际恐怖组织，熟谙各种网络技术手段和西方式舆论宣传工具，组建了专门的行动部门，并将网络宣传的功效最大化。在实践中，“伊斯兰国”通过使用脸书（Facebook）、推特（Twitter）、优兔（YouTube）、照片墙（Instagram）等热门社交平台，以及开发应用程序等方式，宣传本组织的恐怖主义主张，灌输恐怖主义思想，

[1] 例如，Kathleen McKendrick, “Artificial Intelligence Prediction and Counterterrorism,” Research Paper, Chatham House, Aug. 2019; Boaz Ganor, “Artificial or Human: A New Era of Counterterrorism Intelligence?” *Studies in Conflict & Terrorism,* 2019, https://www.tandfonline.com/doi/full/10.1080/1057610X.2019.1568815; “Artificial Intelligence and Counterterrorism: Possibilities and Limitations,” Prepared Written Testimony and Statement for the Record of Alexander Stamos, Director, Stanford Internet Observatory before The U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence and Counterterrorism, June. 25, 2019; Julian Sanchez, “Artificial Intelligence and Counterterrorism: Possibilities and Limitations,” Cato Institute, June. 25, 2019, https://www.cato.org/publications/testimony/artificial-intelligence-counterterrorism-possibilities-limitations; 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；马方、王文娟：《构筑“人工智能+情报反恐”生态系统》，载《山东警察学院学报》2018年第4期，第105—112页；李龙、支庭荣：《“算法反恐”：恐怖主义媒介化与人工智能应对》，载《现代传播》2018年第9期，第13—18页，等等。

进行组织成员招募，并通过网络攻击等形式不断扩大组织的影响力。

近期随着人工智能不断成熟且日益深入普通人的日常生活，恐怖组织开始使用人工智能手段从事恐怖袭击活动。具体方式主要有以下几种：

（一）使用无人机发动恐怖袭击

与恐怖组织以往惯用的行动方式相比，人工智能开发门槛较高，恐怖组织没有足够的人才、资金和时间进行深度研发，因此，主要采用“模仿”而非“创新”的手段，在一种较低的水平上使用这种最新的科学技术。当前，恐怖组织主要是通过操控小型无人机对目标物发动袭击，这是最低程度的人工智能攻击手段。早在 2012 年，就有报道称黎巴嫩真主党尝试使用商业无人机运载爆炸物攻击以色列目标。[1] “伊斯兰国”兴起之后，就多次使用装有爆炸物的小型商业无人机进行恐怖袭击活动。[2] 此外，“伊斯兰国”还经常使用无人机发动自杀式袭击，即接近并撞击敌对目标，并通过捆绑爆炸物以增加威力。2016 年 10 月 2 日，“伊斯兰国”使用一架无人机攻击了位于伊拉克北部的一个库尔德人和法国的军营，造成“库尔德人敢死队”（Peshmerga）2 名队员死亡、法国特种部队 2 名士兵受伤。[3] 在 2016—2017 年的摩苏尔战役中，“伊斯兰国”使用了装备爆炸物的小型便捷式商用无人机，通过自杀式攻击对抗伊拉克的正规军事力量。[4]

---

[1] Gili Cohen, “IDF Shoots Down Drone That Penetrated Israeli Airspace,” *Haaretz,* Oct. 6, 2012, https://www.haaretz.com/watch-idf-shoots-down-drone-1.5177128.

[2] David Hambling, “ISIS Is Reportedly Packing Drones with Explosives Now,” Popular Mechanics, Dec. 16, 2015, https://www.popularmechanics.com/military/weapons/a18577/isis-packing-drones-with-explosives.

[3] Michael Horton, “Inside the Chilling World of Artificially Intelligent Drones,” The American Conservative, Feb. 12, 2018, https://www.theamericanconservative.com/articles/inside-the-chilling-proliferation-of-artificially-intelligent-drones/.

[4] Ben Watson, “The Drones of ISIS,” Jan. 12, 2017, https://www.defenseone.com/technology/2017/01/drones-isis/134542; Ben Solomon, “Witnessing an ISIS Drone Attack,” *The New York Times,* Apr. 14, 2017, https://www.nytimes.com/video/world/middleeast/100000005040770/isis-drone-attack-mosul.html.

尽管恐怖组织与先进国家在人工智能领域存在着代际差距，恐怖分子尚处于以人工方式对无人机进行远程遥控为主的初级阶段，而且难以通过有竞争力的条件招募到愿意为之效力的人工智能专家，但是恐怖组织并未放弃将人工智能作为组织行动重要方式的努力。2016年，就有相关领域的科学家和工程师应恐怖组织邀请到访伊拉克和叙利亚，为其开发无人机武器系统。[1] 由于目前已有一些从事无人机开发及相关领域工作的工程师和科学家加入“伊斯兰国”，2017年该组织成立了一个“圣战无人航空器”（Unmanned Aircraft of the Mujahideen）分部，任务是发展和使用无人机技术，这是恐怖组织将无人机技术武器化的重要一步。[2]

这种情况已得到相关国家政府的高度关注。2018年，美国联邦调查局重要事件响应小组副助理斯科特·布伦纳（Scott Brunner）在参议院国土安全与政府事务委员会作证时指出，联邦调查局“关心犯罪分子和恐怖分子将利用无人机系统（UAS）对美国人民的安全造成严重威胁”。无人机系统的方式包括多种形式，如非法监控及使用化学、生物或放射性材料发动袭击，对露天场馆（如演唱会、典礼或体育赛事）的传统攻击，或者是袭击政府机构和军事设施及人员。[3] 需要高度警惕的是，当前恐怖分子实施的无人机袭击主要采取投掷爆炸物的方式，而如果恐怖分子使用无人机空运化学、

[1] Joby Warrick, “Use of Weaponized Drones by ISIS Spurs Terrorism Fears,” *The Washington Post,* Feb. 22, 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html; Serkan Balkan, *DAESH's Drone Strategy: Technology and the Rise of Innovative Terrorism,* Istanbul: SETA, 2017, p.10.

[2] Joby Warrick, “Use of Weaponized Drones by ISIS Spurs Terrorism Fears,” *The Washington Post,* Feb. 22, 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.

[3] Brian Blodgett, “Drones Becoming Frightening Weapon of Choice for Terrorists,” May 6, 2019, https://inhomelandsecurity.com/drones-frightening-weapon-terrorists.

生物或者放射性材料攻击目标，将会导致更为严重的人员伤亡并产生更长时间的社会和经济影响。[1]

（二）利用人工智能搜集情报

与国家政府类似的是，恐怖组织也非常重视情报的搜集工作，一般较大型的恐怖组织都有自己专门的情报部门。过去恐怖组织主要采取人工方式并辅以技术手段搜集情报。而在社交网络与人工智能兴起之后，恐怖组织充分意识到上述方式在减少情报人员压力、情报搜集时间、资金消耗及提高情报可信度等方面具有优势，并将其运用到情报工作之中。自 2014 年起“伊斯兰国”已经开始使用无人机搜集战场情报。[2] 特别是在叙利亚和伊拉克的军事行动中，使用无人机侦查已经成为“伊斯兰国”的重要“标配”，极大地提高了其获取情报的便捷性和情报的可信度。无人机一般配置有高清摄像头，通过摄像头拍摄的视频，使恐怖组织能够以鸟瞰的方式，更为直观地了解敌方防御体系中的薄弱之处，以及整个区域的实时交通状况。此外，安装了红外摄像头的无人机可以在夜晚进行工作，它因目标较小且更为隐蔽，不容易被防御力量发现。事实上，“伊斯兰国”最早使用无人机就是对伊拉克安全部队和“库尔德人敢死队”驻扎区域进行调查和搜集情报。[3]

另外，“伊斯兰国”还利用人工智能进行社会网络关系的绘制工作，以确认哪些目标更有攻击价值，并以更小的代价获得更大的组织收益。“伊斯兰国”在多个城市使用监测系统识别重要人物，以更有效地锁定和攻击特

---

[1] “New Technologies, Artificial Intelligence Aid fight against Global Terrorism,” UN News, Sept. 4, 2019, https://news.un.org/en/story/2019/09/1045562.

[2] Joby Warrick, “Use of Weaponized Drones by ISIS Spurs Terrorism Fears,” *The Washington Post,* Feb. 22, 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.

[3] Serkan Balkan, *DAESH's Drone Strategy: Technology and the Rise of Innovative Terrorism,* Istanbul: SETA, 2017, p.24.

定目标。[1] 例如，2016 年 3 月，“伊斯兰国”在北非的分支机构袭击了突尼斯边境城镇本加尔丹（Ben Gardane），并暗杀了当地的重要安全官员。有证据表明，此前“伊斯兰国”就是通过利用人工智能绘制“人文地形系统”（human terrain system）[2] 的方式，掌握了当地重要人物的分布状况。[3]

（三）利用人工智能进行网络攻击和宣传

恐怖组织利用网络空间进行恐怖袭击已经有较长一段历史。恐怖分子主要是通过对计算机系统、程序、数据和信息等进行有预谋和有政治动机的系统攻击，以制造社会恐慌，从而影响国家政府实现特定的政治、宗教和意识形态目标。当前，随着“人工智能 + 网络空间”逐渐融为一体，网络空间处于恐怖组织与国家政府争夺跟随者的关键位置，并得到了恐怖组织的更多关注。

传统的网络攻击主要是利用计算机代码存在的各种漏洞展开，恐怖分子主要通过“网络钓鱼”或是在计算机系统和软件安装“后门”的方式对网络空间进行攻击；而当前的人工智能主要是通过算法，即类似于人类学习的方式，从数据集（dataset）中提炼有用信息进行机器学习。[4] 因此，恐怖分子使用人工智能进行的网络攻击行为，主要是利用人工智能算法存在的内在缺陷，而目前对这些缺陷尚不能如传统的代码漏洞那样，通过给计

---

[1] Richard Blech, “How Artificial Intelligence Advancements Have Impacted Cybersecurity,” Nov. 21, 2018, https://www.cpomagazine.com/cyber-security/how-artificial-intelligence-advancements-have-impacted-cybersecurity.

[2] 人文地形系统，源于美军针对非常规作战对文化情报的特殊需求，通过收集地区部落关系、种族渊源、宗教、政治、经济、语言等文化情报资源，绘制“人文地形图”，向作战指挥官制定战术行动计划提供必要的咨询和建议。参见庞超伟、马晓雷、侯豫、王泳利：《论美军在非常规作战中的文化情报工作》，载《情报杂志》2015 年第 3 期，第 5—9 页。

[3] Daveed Gartenstein-Ross, “Terrorists Are Going to Use Artificial Intelligence,” *Defense One,* May 3, 2018, https://valensglobal.com/2018/06/03/terrorists-going-use-artificial-intelligence.

[4] Marcus Comiter, “Attacking Artificial Intelligence: AI’s Security Vulnerability and What Policymakers Can Do about It,” Belfer Center Paper, Kennedy School at Harvard University, Aug. 2019, p.12.

算机系统“打补丁”的方式迅速加以修复。[1] 具体来说，恐怖组织在进行网络攻击的时候，通过使用人工智能执行自动化任务，以使袭击的潜在规模和影响更大，而且相对于其他网络攻击手段，这种方式的隐蔽性更强。

恐怖分子使用人工智能进行网络攻击，也涉及到数字安全问题。恐怖分子未来很可能采用语音合成、自动黑客攻击、在深度学习时插入恶意样本、污染数据等方式，发动新型的网络攻击。[2] 恐怖分子还有可能通过破解生物特征数据或者在人工智能系统中安装后门程序等方式，发动更大规模的网络袭击。[3]

此外，恐怖组织还经常利用无人机将恐怖袭击拍摄成视频，并上传到网络空间，尤其是各类社交媒体进行宣传。“伊斯兰国”等恐怖组织还充分利用青少年的活动特点，将视频编辑成类似于电脑游戏的形式，以吸引更多受众。视频的主要内容包括：袭击之前的画面、被袭击后的人员伤亡、被袭击军事目标的混乱情况，以及为恐吓目的而通过无人机拍摄的各种高清图像，如对人质进行斩首等。这些视频的文字和图片版本也会在 Al-Naba 和 Rumiyah 等“伊斯兰国”的官方刊物发表，以增强宣传效果。[4]

从现实看，目前恐怖组织使用人工智能还处于层次较低的阶段，但是从发展趋势看，不排除其利用人工智能进一步扩大自身影响、发动更大规

[1] Marcus Comiter, “Attacking Artificial Intelligence: Al’s Security Vulnerability and What Policymakers Can Do about It,” Belfer Center Paper, Kennedy School at Harvard University, Aug. 2019, p.28.

[2] Miles Brundage, et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,* Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI, Feb. 2018, p.6; Renske van der Veer, “Terrorism in the Age of Technology,” Clingendael Institute, Netherlands Institute of International Relations, https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology.

[3] Marcus Comiter, “Attacking Artificial Intelligence: Al’s Security Vulnerability and What Policymakers Can Do about It,” Belfer Center Paper, Kennedy School at Harvard University, Aug. 2019, p.28.

[4] Serkan Balkan, *DAESH’s Drone Strategy: Technology and the Rise of Innovative Terrorism,* Istanbul: SETA, 2017, pp.38-39.

模恐怖袭击的可能性，国际社会需对此保持高度警惕。

二、恐怖组织使用人工智能的主要特点

作为一种全新的恐怖袭击策略，人工智能的应用对恐怖组织的行动方式、组织生态、未来发展都将产生重大影响。恐怖组织很可能进一步利用人工智能的技术特点，扩大行动范围，甚至创新恐怖主义的形态。具体来说，当前恐怖组织使用人工智能具有以下几个特点：

（一）增强了恐怖组织在不对称冲突中的实力

从某种意义上说，人工智能迅速填平了恐怖组织与国家政府在技术层面的鸿沟，使处于劣势地位的恐怖分子也可享受到前沿技术的红利，并将其运用到与国家政府的对抗之中。一般而言，无论是战斗人员规模，还是资金和物资保障、科学技术水平等方面，恐怖组织均与国家政府存在较大差距。因此，能否使用代价最小的行动方式获得最大的收益，是恐怖组织发动袭击时所考虑的最重要的衡量标准之一。

按照美国著名学者戴维·拉波波特（David Rapoport）的观点，20世纪80年代以来的“第四波恐怖主义”以自杀式袭击为主[1]，特别是“9·11”事件造成包括19名恐怖分子在内的2996人死亡，给美国经济造成严重损失，也对整个国际体系尤其是国家间关系带来了深远影响，标志着国际恐怖主义进入自杀式袭击的高潮期。尽管自杀式恐怖袭击的影响较大，但这种方式需要通过数量稀缺的恐怖分子的死亡来赢得成功，是恐怖组织在不得已情况下选择的一种“终极”手段。从不对称冲突的角度讲，人工智能为恐怖袭击带来的优势是，恐怖分子可以通过远程遥控的方式实施恐怖袭击活动，以零伤亡的代价造成所针对目标物的巨大损失，而国家政府却很难追踪到恐怖袭击实施者的情况，这对恐怖分子来说堪称“完美”。

[1] David Rapoport, “The Fourth Wave: September 11 in the History of Terrorism,” *Current History*, Vol.100, No.650, 2001, pp.419–424.

此外，引入人工智能技术可减少人力资源在恐怖活动中的使用，恐怖主义的组织形态将由“劳动密集型”向“知识密集型”转变。一些规模较小的恐怖组织或是“独狼”式恐怖分子，可以利用技术上的优势，获得与大型国际恐怖组织同样的能量。在人工智能时代，组织规模不再是衡量恐怖组织获得权力大小的首要指标，而是否掌握先进的人工智能技术、尤其是自主性致命武器系统，将是决定恐怖组织影响力的关键。因此，在人工智能时代，恐怖组织的规模可能出现小型化趋势。随着技术的发展，恐怖组织有可能只需使用售价几千美元的武装无人机“蜂群”，就可对国家政府拥有的价值上亿乃至几十亿美元尖端装备的军事力量造成威胁。这使得在新科技革命条件下，恐怖组织与国家政府不对称冲突的能力进一步增强。

（二）在使用人工智能方面，恐怖分子采取无差别进攻方式实施恐怖袭击的可能性大

国家作为国际社会中最为重要的行为体，有着相对较高的伦理道德标准。同时，一系列的国际公约和国际人道主义法，例如《联合国宪章》《海牙公约》《日内瓦议定书》《日内瓦公约》《特定常规武器公约》《公民权利与政治权利公约》等，都对国家使用武力的行为进行约束，并规定了国家在保障人权和不得随意剥夺任何人生命方面的义务。如果国家违反这些国际公约和国际人道主义法，将会遭到国际社会道义层面的谴责。比如，美国多次使用无人机对恐怖分子实施“定点清除”，这在战争伦理和国际法角度都存在很大争议。[1] 联合国 2013 年的 A/68/382 号文件指出，尽管无人机

[1] 例如，对于无人机伦理和法理的主要中文文献包括但不限于：黄云松、蔡瑞艳：《无人攻击机面临的国际法挑战——以美国在巴基斯坦的无人机攻击为例》，载《南亚研究季刊》2012 年第 1 期，第 21—25 页；钱铖、石斌：《“雄蜂”的阴影——美国无人机作战对当代战争伦理的挑战》，载《世界经济与政治》2013 年第 8 期，第 86—99 页；梁亚滨：《武装无人机的应用：挑战与影响》，载《外交评论》2014 年第 1 期，第 143—156 页；袁靖：《无人机袭击造成的国际法挑战——以美国实践为视角》，厦门大学硕士学位论文，2014 年；张蛟龙：《无人机作战对国家武力使用规范的影响——以美国为例》，天津师范大学硕士学位论文，2016 年；刘树才：《武装无人机与战争变迁：以社会－技术系统为视角》，载《国际安全研究》2018 年第 2 期，第 72—90 页，等等。

不是非法武器，但是它的使用对普遍民众的生命权造成了严重损害。[1] 因此，考虑到国际社会的压力，国家在使用人工智能应对恐怖分子时会持相对谨慎的态度。同时，各国的国内法也对利用人工智能等技术手段打击恐怖主义加以限制，一些国家还制定相关法律法规，禁止武装使用无人机以及使用私人无人机侦查他人。[2]

在使用人工智能方面与国家政府存在着较多道德和国际公约的制约不同，恐怖组织则没有太多顾忌，他们认为，自己进行的暴力活动实际上是反抗那些压迫人民以及进行宗教迫害的邪恶政府的正义行为。恐怖组织考虑最多的只是如何以最小成本获得最大收益，而显然以无人机作为主要袭击手段符合这一要求。恐怖组织甚至认为，采取人工智能方式是遵循“真主的旨意”，“伊斯兰国”因而将自己的无人机行动小组命名为“圣战无人航空器”分部。

此外，致命性自主武器的发展也引发了法律、道德和军控等方面的一系列问题。[3] 尽管当前一些国际非政府组织以及众多的科学家和知名人士，包括联合国人权理事会“法外处决、即审即决或任意处决问题”特别报告员，“禁止杀手机器人运动”国际化组织，生命未来研究所等，都要求对致命性自主武器加以限制，但是以美国和俄罗斯为代表的一些国家反对任何禁止自主性武器的国际条约。因为国际社会无法达成普遍共识，如果致命性自主武器得不到有效控制，那么终有一天它将会被恐怖组织获取，并被用于进行恐怖袭击。即便国际社会通过相应的国际条约，其对恐怖组织的行动也没有约束力，恐怖组织只考虑如何使用先进科技手段获得更大利益，并不在意使用这种手段是否符合人类社会的普遍伦理准则。

---

[1] United Nations, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions,* Sept. 13, 2013, A/68/382, p.2.

[2] Michael Froomkin and Zak Colangelo, “Self-Defense against Robot and Drones,” *Connecticut Law Review,* Vol.48, No.1, 2015, pp.3-69.

[3] Chase Winter, “‘Killer Robots’: Autonomous Weapons Pose Moral Dilemma,” *Deutsche Welle,* Nov.14, 2017, https://www.dw.com/en/killer-robots-autonomous-weapons-pose-moral-dilemma/a-41342616.

（三）使用人工智能简单廉价并扩大了恐怖组织的袭击范围，使得国家政府难以跟踪和及时获得恐怖分子的信息来源

当前，无人机技术存在扩散容易、技术简单及缺乏有效国际监控等问题。[1] 尽管恐怖组织没有足够的资金和人才进行高端人工智能的研发工作，但是随着技术的进步，使用人工智能的成本会越来越廉价，低端人工智能的制造也相对比较简单。此外，很多人工智能具有军民两用特征，这进一步加大了国家政府对相关技术的监控难度。[2] 比如，一些专门的商业技术网站对自制无人机进行全程介绍，而且普通人都可以通过网站购买制造无人机的各种材料和获得软件支持。“伊斯兰国”甚至已经建立了多个制造无人机的专门作坊。[3] 2018 年 1 月，一个叙利亚反政府团体就自制了 13 架简易无人机，用以攻击位于叙利亚境内的两处俄罗斯军事基地。[4] 据估计，一台小型人工智能杀人无人机的价格相当、甚至低于一台智能手机的价格，恐怖分子花费大约 1100 英镑就可以在商店购买到一台最新式的无人机。[5]

此外，人工智能的使用也扩大了恐怖组织的活动范围。当前成熟且价格低廉的无人机技术，使得恐怖组织可以利用航空器进行抵近侦察和实施恐怖袭击，其活动范围已扩展到高空并且机动性更强。一架装载了炸药物

---

[1] Paul Schulte, “Future War: AI, Drones, Terrorism and Counterterror,” in David Martin Jones, Paul Schulte, Carl Ungerer and M. L. R. Smith, eds., *Handbook of Terrorism and Counter Terrorism Post 9/11,* Northampton, MA: Edward Elgar Pub, 2019, pp.416–433.

[2] 刘杨钺：《全球安全治理视域下的自主武器军备控制》，载《国际安全研究》2018 年第 2 期，第 65 页。

[3] “Islamic States’ Weaponised Drones,” Conflict Armament Research Ltd., 2016, pp.1–2, http://www.conflicttarm.com.

[4] Jacob Ware, “Terrorist Groups, Artificial Intelligence, and Killer Drones,” War on the Rocks, Sept. 24, 2019, http://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones.

[5] Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence,* New York: Alfred A. Knopf, 2017, p.141; Harvey Gavin, “Terrorists Could Use Bomb Drones to Attack Streets of the West, Security Experts Warn,” Express, Feb. 3, 2018, https://www.express.co.uk/news/world/913155/terrorist-weaponise-drone-threat-attack-bomb-acid-warning-2018.

的小型无人机可以在大约 122 米的高度以 48—64 公里的时速飞行，不加注意很难及时发现。[1] 即便能够发现，因这种小型无人机目标太小且移动速度较快，也很难被击落。如果恐怖分子想要暗杀一名政客，他只需将目标的照片和地址上传至“杀人无人机”，无人机便会飞到指定地点确认和清除目标，并在完成任务后自毁，以确保暗杀行动的实施者不被发现。[2] 无人机具有匿名性质，从而进一步增大了打击这种恐怖袭击方式的难度。

人工智能武器的另一个特点是能够在极端和恶劣气候条件下进行物理层面的打击，让袭击目标防不胜防。恐怖组织在恶劣气候和复杂地形条件下利用人工智能，使用无人机“蜂群”攻击敌对国家的重要地标性建筑物甚至是重要的军事设施，都是极有可能的。

从恐怖分子的角度来看，利用人工智能进行组织活动具有其他技术手段无法比拟的巨大优势。恐怖组织的组织理念和运作方式，使之在行动时极少考虑是否滥杀无辜，是否违背人类道德和伦理等非技术因素，而仅仅希望通过杀伤力和影响力最大的方式达到组织利益最大化。因此，在恐怖组织使用人工智能的情况下，国际社会需采取及时、有效和有针对性的措施加以应对。

三、应对人工智能恐怖主义的具体措施

随着人工智能的日趋成熟和普及，恐怖组织使用先进技术手段进行恐怖袭击的可能性会进一步增大。除传统的无人机恐怖袭击外，恐怖分子还可能利用无人机自带或是安装的摄像头，通过网络传输将恐怖袭击的实时场景上传到社交媒体，从而造成民众恐慌。此外，随着 5G 技术的普遍运用及其在人工智能和物联网运用中的优势日益显现，恐怖分子也可能通过“智能手机 + 人工智能”方式，针对特定用户的智能手机或智能操作系统，实施一起本方零伤亡却能造成极大社会恐慌的恐怖袭击事件。比如，在一辆无

[1] Tung Yin, “Game of Drones: Defending against Drone Terrorism,” *Texas A & M Law Review,* Vol.2, No.4, 2015, p.650.

[2] Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence,* New York: Alfred A. Knopf, 2017, p.141.

人驾驶的汽车里安装恶意软件，造成车上的重要政治人物因为严重车祸身亡，或是远程操控无人驾驶汽车撞向无辜行人或是建筑物等。3D 打印技术的普及可使恐怖分子获得武器的方式更加简单。据称，只需要一个周末的时间以及 50 美元的花费就能 3D 打印出一支枪只。[1] 利用 3D 打印技术，恐怖分子甚至可以制造更加复杂的袭击工具，从而对国际社会造成更大威胁。人工智能时代，国家打击恐怖主义面临着新问题，亟需通过有效方式加以应对。

（一）国家应充分利用技术优势，占领人工智能应用领域的高地

相对于恐怖分子，国家政府在人工智能方面应进一步加大研发力度，始终在该领域占据优势地位，这是一个关键。美国已充分意识到人工智能和机器学习在未来战争中的作用，成立了“算法战跨职能小组”（AWCFT）、国家人工智能安全委员会、联合人工智能中心（JAIC）等机构，以整合资源进行技术开发，寻求在人工智能反恐等领域的优势地位。例如，美国国防部联合人工智能中心工作的 5 个重点领域是：提供能够完成关键任务的人工智能能力；通过一个共同的基础，扩大人工智能对国防部的影响，促成分散开发和实验；培养一流的人工智能人才队伍；与商业界、学术界及国际盟友和合作伙伴开展合作；在军事道德和人工智能安全领域发挥领导作用。[2] 以色列也注重通过大数据以及机器学习等方式应对恐怖主义威胁。由于在打击恐怖主义的过程中广泛使用了人工智能技术，以色列境内的恐怖袭击数量出现了降低趋势。[3]

值得注意的是，恐怖组织使用人工智能的方式目前尚以低端无人机攻

[1] Lizzie Dearden, “Use of 3D Printed Guns in German Synagogue Shooting Must Act as Warning to Security Services, Experts Say,” *Independent,* Oct. 11, 2019, https://www.independent.co.uk/news/world/europe/3d-gun-print-germany-synagogue-shooting-stephan-balliet-neo-nazi-a9152746.html.

[2]《美国国防部联合人工智能中心及其发展规划》，载《中国航天报》2019 年 4 月 9 日，第 A06 版。

[3] Boaz Ganor, “Artificial or Human: A New Era of Counterterrorism Intelligence?” *Studies in Conflict & Terrorism,* 2019, pp.12-16, https://www.tandfonline.com/doi/full/10.1080/1057610X.2019.1568815.

击为主。虽然各国都通过立法对无人机使用的范围、条件、规模等进行了限制，但这些立法对恐怖组织而言没有任何约束力。因此，从技术而非法律层面对恐怖组织在制造、获取和使用民用无人机等方面加以限制，才是国家在应对人工智能恐怖主义的重点领域。

（二）重视人工智能高新技术企业和科研机构在反恐方面的优势

人工智能的特点，决定了开发和研制新型技术离不开商业公司和一线科研机构的支持，在人才、资金、技术等领域更是如此。因此，国家与企业、高校、研究机构建立合作关系，利用其在人工智能领域的优势地位开展反恐工作是十分必要的。

特别是对于“独狼”恐怖分子，由于其目标小且行动机动性强，很难用传统的人工情报和通讯情报对其可能发动的恐怖袭击事先监控，但是“独狼”恐怖分子很有可能会在袭击前利用社交媒体发布其采取行动的原因，因此通过人工智能手段对社交媒体进行监控的方式开展反恐是极有必要的。[1] 当前一个被反复提及的重要案例是“脸书”公司利用人工智能技术寻找和移除该平台上的恐怖主义内容。其主要方式是“脸书”公司在后台通过图像匹配技术，识别和防止那些知名恐怖分子的照片和视频出现在个人账户上。此外，“脸书”公司还利用机器学习算法寻找恐怖分子开展宣传的惯用模式，以便快速移除这些账号的信息流（newsfeeds）。[2] 再比如，美国空军与一家以色列公司签订了一份价值1560万美元的协议，以开发反无人机袭击技术。[3] 高校以及企业还可通过开发机器翻译、数据挖掘、语音

[1] Boaz Ganor, “Artificial or Human: A New Era of Counterterrorism Intelligence?” *Studies in Conflict & Terrorism,* 2019, pp.6–7, https://www.tandfonline.com/doi/full/10.1080/1057610X.2019.1568815.

[2] “Facebook Using Artificial Intelligence to Fight Terrorism,” CBS News, Jun. 15, 2017, https://www.cbsnews.com/news/facebook-using-a-i-artificial-intelligence-against-terrorism/.

[3] Oriana Pawlyk, “Air Force Works to Track ISIS Drones to the Source,” Military.com, Mar. 6, 2017, https://www.military.com/daily-news/2017/03/06/air-force-works-to-track-isis-drones-to-the-source.html.

识别、文本分析等技术，加强对恐怖分子行动的预测，配合做好应对恐怖袭击的预警工作。[1]

未来，国家与商业公司和研究机构在反恐领域的合作需进一步增强。例如，商业公司可通过人工智能手段更好更快地锁定恐怖分子的行踪，而不是像现在一样仅仅对疑似恐怖分子的账号进行销号。商业公司还可利用开发软件以及为公共部门提供数据集等方式介入反恐行动。[2] 通过更多地引入非国家行为体的力量，将人工智能技术更好地运用于反恐行动，将是打击人工智能恐怖主义的一个重要依托。

（三）加强人工智能反恐领域的国际合作

加强在人工智能反恐领域的国际合作，是打击恐怖主义的一个重要途径。2019 年 9 月 3—4 日，白俄罗斯政府与联合国反恐办公室共同主办的“通过创新方法和使用新兴技术应对恐怖主义”高级别国际会议在明斯克举行，会议主要聚焦全球、区域和国家层面恐怖分子使用新技术和人工智能问题，以及对这些恐怖分子采取措施的方法和战略。[3] 各国共享恐怖分子人脸、语音、指纹等方面的数据库，利用大数据技术对恐怖分子进行甄别、监控和打击，共同将人工智能领域的前沿成果运用到反恐工作中，将有利于从国际层面使用人工智能手段对恐怖分子进行精准打击。

当前，利用人工智能技术方面的国际合作尚处于初级阶段，相关国家需要进一步就利用人工智能反恐的优势和必要性达成共识，尽快成立政府间的人工智能反恐合作机制，举行定期或不定期的高层官员会谈，并利用国家政府在人工智能领域的技术优势，分享有关恐怖主义活动的相关情报，同时各国利用人工智能技术打击恐怖主义的经验，特别是使用生物特征识

[1] Sheryl Prentice, “How Technology Could Help Predict Terrorist Attacks,” https://www.iflscience.com/technology/how-technology-could-help-predict-terrorist-attacks/all/.

[2] Kathleen McKendrick, “Artificial Intelligence Prediction and Counterterrorism,” Research Paper, Chatham House, Aug. 2019, p.8.

[3] “New Technologies, Artificial Intelligence Aid fight against Global Terrorism,” UN News, Sept. 4, 2019, https://news.un.org/en/story/2019/09/1045562.

别技术搜集汇总恐怖分子和高危犯罪分子相关信息，建设各国都可以正常接入的数据库，以便更好地对恐怖组织的活动进行监测。国际社会尤其需将涉及致命性自主武器的高级人工智能的研发、交易、部署和使用全过程置于有效监管之下，并确保其研发和部署符合人道主义原则。[1]

（四）避免高级人工智能技术落入恐怖分子手中

随着一些恐怖组织实力的增强，他们有可能会招募到专门从事人工智能研发的高级科技人才或者一些拥有高学历、高智商的“独狼”式恐怖袭击者，从而可能使用技术更为高端的袭击方式，并造成更为严重的袭击后果。在此背景下，提高重要实验室的安保级别，确保关键性的人工智能技术掌握在国家政府手里，避免其落入恐怖分子手中，这非常重要。

当前，恐怖分子利用人工智能实施袭击已经不是一个假设，而是一个迫在眉睫的现实问题。面对恐怖分子利用人工智能日益增多的情形，国家政府需要充分利用自身的技术优势地位，阻断恐怖组织发展人工智能技术手段的路径，否则，一旦恐怖分子掌握的人工智能技术日趋成熟，将会对国际社会造成无法想象的灾难。

结 论

人工智能运用领域的不断扩展，在给人们带来方便的同时，也存在着一定的负面影响，这是先进技术发展所带来的不可避免的“双刃剑”效应。恐怖分子利用技术革命的有利契机，开始使用各种人工智能手段进行恐怖活动，对国际社会造成严重危害，需引起各国高度重视。

国际社会与恐怖活动将在很长一段时间内处于共存状态。恐怖分子并不排斥人类最先进的科学技术，而是“以子之矛，攻子之盾”，充分利用这些技

[1] 董青岭：《新战争伦理：规范和约束致命性自主武器系统》，载《国际观察》2018年第4期，第62—65页。

术手段对国家和社会发动恐怖袭击。此外，尽管恐怖分子使用人工智能尚处于较低水平，但我们绝不能忽视他们利用人工智能手段扩大组织影响，以及实施更具威胁的恐怖袭击的可能性，尤其是那些拥有较高学历和较高智商的“独狼”恐怖分子，更有可能使用人工智能方式进行恐怖袭击。在这种情况下，国家政府应采取各种手段对其加以遏制，使之不会成为影响国际社会发展的一个重要负面因素，这在当前是一个非常紧迫的现实问题。国家需要在人工智能领域建立相对恐怖分子的绝对优势，加强国际合作以及与重要人工智能商业公司和研究机构的合作关系，避免高等级的人工智能被恐怖分子利用，有效防止恐怖分子利用这种新兴的技术手段获得最大收益。

人类社会对先进技术的追求是无止境的。人工智能的发展作为人类社会又一场具有跨时代意义的“技术革命”，正在改变着我们的日常生活，也对国际秩序产生了深远影响，甚至将会彻底改变国际体系的权力分配状况。因此，我们应当对人工智能技术持开放态度。但是，我们也需要警惕和遏制这种技术被国际恐怖分子滥用，从而更好地实现人类社会整体的安全、发展与进步。

【收稿日期：2020–10–20】
【修回日期：2021–01–10】
（责任编辑：李万胜）