

# 人工智能在反恐活动中的应用、影响及风险\*

傅瑜 陈定定

**【内容摘要】** 随着反恐形势的日益严峻与人工智能技术的日趋成熟，人工智能在反恐领域已经部分应用到反恐活动中。具体而言，人工智能辅助控制了恐怖组织信息的传播，促进了反恐信息的开发和利用，提升了对恐怖活动的预测能力，也促进了智能武器的开发。此外，人工智能技术已经成为国家反恐战略的重要组成部分，在反恐资源融合、反恐活动主体及反恐合作方式方面革新了传统反恐领域的基本规则，也从法律、道德和心理角度影响了人类反恐活动的展开。但与此同时，反恐视野下人工智能手段的开发和利用在准确性、公平性和伦理道德方面仍面临风险。未来人工智能技术在计算机视觉、自然语言处理等方面可能迎来速度和质量上的飞跃，人工智能武器的开发也将继续，人工智能领域很可能成为未来反恐力量与恐怖组织的角逐场。

**【关键词】** 人工智能 深度学习 反恐 系统性影响 潜在风险

**【作者简介】** 傅瑜，暨南大学 21 世纪丝绸之路研究院研究助理；海国图智研究院助理研究员（广州 邮编：510000）；陈定定，暨南大学国际关系学院教授（广州 邮编：510000）

**【中图分类号】** D815.5 TP18 **【文献标识码】** A

**【文章编号】** 1006-1568-(2018)04-0119-19

**【DOI 编号】** 10.13851/j.cnki.gjzw.201804007

---

\* 本文是国家社会科学基金重点项目“海外中国公民利益保护机制研究”（16AZZ016）的阶段性成果。

自1956年达特茅斯会议首次提出人工智能的概念以来,学术界对此尚未有统一和明确的定义。<sup>①</sup>总的来说,目前对人工智能的定义主要从“像人一样思考和行动”和“合理地思考和行动”两个维度进行分析。<sup>②</sup>鉴于人工智能与智慧及计算机的密切关系,本文中人工智能指利用计算机算法和其他前沿科技研究、创建和模仿人类解决问题的方式的技术手段,比如语音识别、视觉感知和决策等。“9·11”恐怖袭击事件发生以来,恐怖主义活动对国家和公民安全造成日益严重的威胁。恐怖袭击遍布美国、法国、英国、中国、印度、澳大利亚等许多国家。以卡车和自制炸弹等为手段的自杀式爆炸袭击屡屡发生。目前的反恐投入大、消耗多,但效果有限。<sup>③</sup>如何运用科技高效反恐成为各国反恐的核心需求。

人工智能在反恐中的应用可以划入人工智能与国际关系的范畴,广义上则属于对科技与安全关系的讨论。现代对人工智能的研究最早可以追溯到图灵(A. M. Turing)发表的《计算机与智能》一文。<sup>④</sup>对人工智能的研究随后主要停留在技术及概念的探讨上。直到20世纪80年代,西方学者开始围绕计算机与武器控制、人工智能与国土安全等话题进行讨论。<sup>⑤</sup>进入21世纪,随着大数据、云计算和认知技术等出现,人工智能在学界引发广泛关注,产生了更多关于人工智能研究模型、机器学习、人工智能带来的社会

---

<sup>①</sup> “Preparing for the Future of Artificial Intelligence,” Executive Office of the President National Science and Technology Council Committee on Technology, October 2016, p. 6; John McCarthy et al. “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence,” August 31, 1955, <https://www.aaai.org/ojs/index.php/aimagazine/article/view/1904/1802>; John McCarthy, “What is Artificial Intelligence?,” November 12, 2007 <http://www-formal.stanford.edu/jmc/whatisai/whatisai.html>; Frank Chen, “AI, Deep Learning, and Machine Learning: A Primer,” Andreessen Horowitz, June 10, 2016; and Pedro Domingos, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*, New York: Basic Books, 2015, pp. 57-203.

<sup>②</sup> [美]罗素、诺维格著:《人工智能:一种现代的方法》,殷建平、祝恩、刘越等译,清华大学出版社2013年版,第3页。

<sup>③</sup> “The War in Afghanistan: By The Numbers,” NBC News, August 22, 2017, <https://www.nbcnews.com/politics/politics-news/war-afghanistan-numbers-n794626>.

<sup>④</sup> A. M. Turing, “Computing Machinery and Intelligence,” *Mind*, October 1950, Vol. 59, No. 236, p. 433.

<sup>⑤</sup> Stephen J. Cimbala, ed., *Artificial Intelligence and National Security*, MA: Lexington Books, 1987; and Allan M. Din ed., *Arms and Artificial Intelligence: Weapon and Arms Control Applications of Advanced Computing*, Oxford: Oxford University Press, 1988.

变化及问题与挑战等主题的研究。<sup>①</sup>就中国而言,人文领域早期鲜有对人工智能的直接研究,更多是探讨科技对国际关系的影响,这一研究话题曾在20世纪末的中国引发一股研究热潮,代表人物是王逸舟和张骥。<sup>②</sup>进入21世纪以后,人工智能对国际关系产生影响的话题引起国内学者的极大关注。董青岭等学者在相关文章中深入探讨了科技对国家安全的影响。<sup>③</sup>

探寻人工智能在反恐活动中的应用、影响和风险,不仅有利于反恐工作的提升,也是对科技与安全这一重大问题的探索,是当前和未来全球安全维护的重点方向之一。囿于研究材料和信息保密性等问题,本研究存在缺陷和不足,希望能够抛砖引玉,推动学界对此话题做更为深入的研究。

## 一、人工智能参与反恐活动的技术基础

进入21世纪,大数据、高性能芯片与深度算法推动了人工智能走向跨越式发展,人工智能在自然语言处理、计算机视觉、智能决策等方面的发展为人工智能的反恐应用奠定了技术基础。

(一) 大数据和计算芯片的发展提升了人工智能的数据处理能力

21世纪以来,亚马逊(Amazon)、谷歌(Google)、雅虎(Yahoo)、推特(Twitter)、脸书(Facebook)等积累了大量的用户信息。到2020年,数据总量将达到40万亿G,较2011年提升21倍。<sup>④</sup>通过挖掘数据背后的

---

<sup>①</sup> George F. Luger, *Artificial Intelligence, Structures and Strategies for Complex Problem Solving*, Boston: Addison-Wesley, 2005; Erik Brynjolfsson and Andrew Mcfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, New York: Norton, 2014; Martin Ford, *Rise of the Robots: Technology and the Threat of a Jobless Future*, New York: Basic Books, 2015; and Jerry Kaplan, *Humans Need Not Apply: A Guide to Wealth and Work in the Age of Artificial Intelligence*, New Haven: Yale University Press, 2015.

<sup>②</sup> 王逸舟:《试论科技进步对当代国际关系的影响》,《欧洲》1994年1期,第7页;张骥:《新科技革命与当代国际关系的转型》,《现代国际关系》1996年第11期,第40-46页。

<sup>③</sup> 参见武贤明:《科技发展对国际关系的影响》,《当代世界》2008年1期,第51页;石海明:《科学、冷战与国家安全:美国外空政策变革背后的政治(1957-1961)》,解放军出版社2015年版,第I-II页;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》,《世界经济与政治》2017年第7期,第117页。

<sup>④</sup> John Gantz and David Reinsel, "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East," IDC, 2012, <https://www.emc.com/>

规律，大数据为人工智能和智能决策提供了数据基础，也为机器学习提供了训练数据库。围绕神经网络开发的新型高性能计算芯片及架构不断涌现。随着英特尔处理器由 CPU 为主转变为 GPU 为主 CPU 为辅的结构，计算机运行速度提升了近 70 倍。<sup>①</sup> Google 的机器学习定制芯片 TPU、Altera 公司和 IBM 使用的芯片 FPGA，分别在分析、预判效率和灵活性上有突出优势。<sup>②</sup> 这些新型高性能计算芯片及架构为人工智能处理和分析恐怖主义相关信息奠定了技术基础。

## （二）深度算法提升了人工智能对恐怖分子的语音和图像处理能力

深度学习可以识别非结构化数据，模拟人脑神经元多层深度传递的过程，通过多隐层的神经网络模型的构建和海量数据的训练，极大提升数据的表征学习能力。通过在并行计算平台的训练，“谷歌大脑”（Google Brain）语音识别准确度从 2012 年的 84% 上升到 2014 年的 98%。<sup>③</sup> 在深度神经网络技术的基础上，Facebook 的研究小组创建的深度学习面部识别系统“深度辨脸”<sup>④</sup>（Deep Face）以用户上传的 400 万张图片为基础进行了训练，将面部识别算法精度提升到 97%。<sup>⑤</sup> 基于卷积神经网络（Convolutional Neural Network, CNN），汤晓鸥开发的“深度识别”（Deep ID）深度学习模型识别率达到了 99.15%。<sup>⑥</sup> 2016 年 9 月，谷歌旗下的“深度思维”（Deep Mind）利用深度神经网络对原始音频波形建立模型，研发能够自动辨别语言和语音的“波网”（Wave Net），促发了图像和语音识别的又一次飞跃。<sup>⑦</sup>

---

collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf.

<sup>①</sup> Rajat Raina, An and Madhavan, and Andrew Y. Ng, “Large-scale Deep Unsupervised Learning using Graphics Processors,” Proceeding ICML '09 Proceedings of the 26th Annual International Conference on Machine Learning, June 2009, p. 873.

<sup>②</sup> “Altera and IBM Unveil FPGA-Accelerated POWER Systems,” HPC Wire, November 17, 2014, <https://www.hpcwire.com/off-the-wire/altera-ibm-unveil-fpga-accelerated-power-systems/>.

<sup>③</sup> 尹丽波主编：《工业和信息化蓝皮书：人工智能发展报告（2016-2017）》，社会科学文献出版社 2017 年版，第 11-13 页。

<sup>④</sup> 本文涉及的部分技术名词没有统一译名，本人翻译不当之处请相关人员和读者见谅。

<sup>⑤</sup> Dino Grandoni, “Facebook’s New ‘DeepFace’ Program Is Just As Creepy As It Sounds,” The Huffington Post, March 3, 2014, [https://www.huffingtonpost.com/2014/03/18/facebook-deepface-facial-recognition\\_n\\_4985925.html](https://www.huffingtonpost.com/2014/03/18/facebook-deepface-facial-recognition_n_4985925.html).

<sup>⑥</sup> 《港中大教授揭秘人脸识别技术：“你喜欢的美颜相机也涉及刷脸”》，《南方都市报》，2017 年 5 月 2 日，[https://ipaper.oeeee.com/ipaper/H/html/2017-05/02/content\\_26565.htm](https://ipaper.oeeee.com/ipaper/H/html/2017-05/02/content_26565.htm)。

<sup>⑦</sup> 尹丽波主编：《工业和信息化蓝皮书：人工智能发展报告（2016-2017）》，第 88 页。

### （三）人工智能在武器中的应用促进了自主武器的研发

武器自主化是自主将环境中的数据转化为有目的的计划和行动的过程。从技术角度而言，自主武器（autonomous weapons）的研发依赖于图像和语音识别、反射控制系统（reactive control systems）、传统控制系统（deliberative control systems）以及行动指令等。<sup>①</sup> 而反射控制系统又包括简单的反射控制系统和基于模型的反射控制系统。自然语言处理和计算机视觉的发展从速度和准确度上提升了自主武器获取外界信息的能力。大数据基础上的算法训练推动了智能决策的研究。蒙特卡洛决策树与深度神经网络的结合使得阿尔法狗（AlphaGo）在棋类游戏中所向披靡。自主武器需要明确运作程序、规则和目的，这一过程需要在大量模型基础上进行训练。在每一个训练模型都需要人类设定时，会出现因操作环境复杂以至于人类无法建立模型的情况，制约了自主武器的发展。<sup>②</sup> 计算机性能和深度学习的发展使得机器可以在训练数据的基础上自主学习，通过经验来提高知识，而不依赖于人类定义的有限模型。

总而言之，人工智能在数据处理、自然语言处理、计算机视觉和深度学习等方面正逐步走向更加高效的发展阶段，将为今后人工智能的反恐应用提供更为有效的技术支持。

## 二、人工智能技术在反恐活动中的初步应用

人工智能在计算机视觉、自然语言处理和智能决策等方面的迅速发展为人工智能在反恐活动中的实际应用提供了基础条件。总的来说，充分利用持续进步的人工智能技术，可以在控制恐怖组织信息传播、解读反恐情报、预防恐怖事件方面发挥更大的作用。

### （一）通过人工智能技术辅助控制恐怖组织信息的传播

---

<sup>①</sup> Vincent Boulanin and Maaïke Verbruggen, “Mapping the Development of Autonomy in Weapon Systems,” Stockholm International Peace Research Institute (SIPRI), November 2017, pp. 5-12.

<sup>②</sup> Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, Harlow: Pearson Education, 2014, p. 56.

利用推特、脸书、优兔网（YouTube）、图享（Instagram）等社交媒体招募潜在恐怖行为支持者，已经成为“伊斯兰国”（ISIS）等极端恐怖组织影响力扩张的重要途径。仅在2014年9月至12月期间，“伊斯兰国”的支持者就使用了约46 000个推特帐号。<sup>①</sup>恐怖组织利用推特宣扬“圣战”，对个人账户、机构账户及整个社交网络都进行充分的内容控制。<sup>②</sup>恐怖主义的支持者们关注并转发此类信息，使得极端意识形态从有关机构账户流向更广泛的传播网络。此外，恐怖组织发布的内容以视频形式为主，相较于文字更难控制。

随着深度学习算法的不断完善，人工智能技术在视频、语音和图像识别方面的能力不断增强。目前，科技手段已经能够有效参与到反恐行动中：YouTube的“变革创造者”（Creators for Change）以及Facebook的“点对点”（Person-to-person, P2P）和“线上公民勇气倡议”（Online Civil Courage Initiative, OCCI）正加入到“反击演讲”（counter speech）的操作中。<sup>③</sup>人工智能手段在反恐活动的作用也开始引发更广泛的关注。

人工智能可以通过图像匹配技术控制之前被标记为恐怖主义的宣传图像或视频的上传。<sup>④</sup>系统可以将用户上传的照片或视频与已知恐怖信息数据库比对，以此来决定上传行为是否被拒绝。<sup>⑤</sup>Facebook、微软、Twitter和YouTube已经着手共建欧盟互联网论坛和共享行业数据库，改进现有的联合工作技术，利用机器学习，开发和实施新的内容检测和分类技术，交流实践经验，并确定恐怖主义相关内容的删除标准。<sup>⑥</sup>事实上，YouTube的“重定

---

<sup>①</sup> “The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter,” Brookings Institution, March 5, 2015, <https://www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/>.

<sup>②</sup> Jytte Klausen, “Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq,” *Studies in Conflict & Terrorism*, Vol. 38, No. 1, 2015, pp. 1-22.

<sup>③</sup> David Cohen, “4 Internet Giants Formed the Global Internet Forum to Counter Terrorism,” ADWEEK, June 26, 2017, <http://www.adweek.com/digital/four-internet-giants-formed-the-global-internet-forum-to-counter-terrorism/>.

<sup>④</sup> Ubaid Ahmed, “Artificial Intelligence: Transpiring Journey To Counter Terrorism – OpEd,” *Eurasia Review*, August 30, 2017, <https://www.eurasiareview.com/30082017-artificial-intelligence-transpiring-journey-to-counter-terrorism-oped/>.

<sup>⑤</sup> Luke Chambers, “How Artificial Intelligence may be the Answer to the Terror Problem,” Rude Baguette, September 12, 2017, <http://www.rudebaguette.com/2017/09/12/artificial-intelligence-addresses-terror-problem/>.

<sup>⑥</sup> David Cohen, “4 Internet Giants Formed the Global Internet Forum to Counter Terrorism.”

向方法”（redirect method）已经部分实现了定位和消除社交媒体网络极端主义宣传的智能化。“重定向方法”会在检测到“伊斯兰国”相关搜索、材料、广告和“相关内容”后破坏这些宣传信息；在 YouTube 上搜索与“伊斯兰国”相关的内容时，该平台也将搜索到与这一极端恐怖组织有关的视频，并加以“攻击”。<sup>①</sup> 利用人工智能控制恐怖组织的信息传播目前已经取得了良好效果。通过利用人工智能算法工具，仅 2017 年上半年，推特就减少了近 30 万个恐怖分子的账户，清除效率提升了约 20%。<sup>②</sup> 人工智能也辅助 Facebook 删除了 99% 的基地组织和“伊斯兰国”的材料。<sup>③</sup> 随着人工智能继续向前发展，社交媒体对恐怖主义信息的控制能力还将进一步增强。

## （二）依靠人工智能技术促进反恐情报的开发和利用

人工智能在机器翻译和图像、语音识别等方面的发展使得高效开发和利用现有的反恐情报成为可能。现代技术的进步带动了反恐情报数量的急剧增长。无人机平台及其全运动视频传感器收集了海量反恐情报。<sup>④</sup> 受制于有限的人力资源，这些传感器平台和监控设备收获的大量视频数据过去并没有得到及时解析。<sup>⑤</sup>

随着计算机芯片的不断进化，人工智能对数据的高速处理能力可以实现低层次计算活动的完全自动化，进一步发展和有效利用现有数据的价值。例如，人工智能在语言识别上的技术优势能够节省培养新语言学家所需要的时间，大大提升了语言处理速度和准确度。通过深度算法，人工智能还可以抓取恐怖组织成员及其支持者的文字和图片。早在 2013 年，为探查潜在的自杀式爆炸袭击者等恐怖分子，美国国土安全部已经把深度学习技术应用于

<sup>①</sup> Tyler Cote, “Tech Giants’ Role in Countering Violent Extremism,” Atlantic Council, August 24, 2017, <http://www.atlanticcouncil.org/blogs/futuresource/tech-giants-role-in-countering-violent-extremis>.

<sup>②</sup> “Twitter Takes Down 300,000 Terror Accounts as AI Tools Improve,” *Financial Times*, September 20, 2017, <https://www.ft.com/content/198b5258-9d3e-11e7-8cd4-932067fbf946>.

<sup>③</sup> “Facebook’s AI Wipes Terrorism-related Posts,” BBC News, November 29, 2017, <http://www.bbc.com/news/technology-42158045>.

<sup>④</sup> Gregory C. Allen, “Project Maven Brings AI to the Fight Against ISIS,” *Bulletin of the Atomic Scientists*, December 21, 2017, <https://thebulletin.org/project-maven-brings-ai-fight-against-isis11374>.

<sup>⑤</sup> Gregory C. Allen, “The Pentagon is Using AI to Fight ISIS but It’s not quite the ‘Terminator,’” CNN, December 30, 2017, <https://edition.cnn.com/2017/12/29/opinions/pentagon-is-using-artificial-intelligence-not-quite-the-terminator-opinion-allen/index.html>.

“生物特征识别视觉监控系统”（Biometric Optical Surveillance System, BOSS），通过链接计算机与摄像头，在扫描人群后根据面孔自动识别和定位目标。<sup>①</sup> 2017 年 4 月，为将国防部的大量数据快速转换为具有实际价值的情报，美国国防部启动了“算法战跨职能小组”（Algorithmic Warfare Cross-Functional Team, AWCFT）。<sup>②</sup> 目前该小组正在利用人工智能解析 MQ-9 和 MQ-19 无人机平台上的全运动视频传感器数据，首批 4 套智能算法已经进入测试阶段。<sup>③</sup>

### （三）利用人工智能技术预测以防范恐怖活动的发生

人工智能系统可以根据现有恐怖活动案例数据库和各类政府数据库及社交媒体数据库，利用人工智能预测恐怖活动嫌疑人和恐怖行为，从而在必要时对嫌疑人进行防范和监督，在可能发生恐怖袭击的地点做好防范和应急准备工作。目前马里兰大学开发的全球恐怖主义数据库（Global Terrorism Database）涵盖了近 17 万起恐袭案例，随着人工智能技术对人力的解放，以大数据为基础的恐怖行为分析预测将得到显著提升。

目前，已经有利用大数据和人工智能算法来模拟和分析“伊斯兰国”的案例。<sup>④</sup> 2015 年，安德鲁·斯坦顿（Andrew Stanton）等人评估了 2 200 多起涉及“伊斯兰国”的交战案例，通过挖掘这些事件来推导“伊斯兰国”的车载简易爆炸活动与伊拉克的军事行动、联军空袭、“伊斯兰国”简易爆炸活动之间的关系，以及间接打击、自杀式袭击和逮捕行动的发生规律。通过分析“伊斯兰国”的行为，研究人员判断出恐怖组织的优先目标，发现了以前未被认识到的战术之间的相关性。<sup>⑤</sup>

---

<sup>①</sup> Charlie Savage, “Facial Scanning Is Making Gains in Surveillance,” *The New York Times*, August 21, 2013, <http://www.nytimes.com/2013/08/21/us/facial-scanning-is-making-gains-in-surveillance.html>; and David Hafemeister, *Nuclear Proliferation and Terrorism in the Post-9/11 World*, Switzerland: Springer, 2016, p. 281.

<sup>②</sup> “Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven),” Deputy Secretary of Defense of the United States, April 26, 2017, [http://www.govexec.com/media/gbc/docs/pdfs\\_edit/establishment\\_of\\_the\\_awcft\\_project\\_maven.pdf](http://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf).

<sup>③</sup> “DOD Maven AI Project Develops First Algorithms, Starts Testing,” Defense Systems, November 3, 2017, <https://defensesystems.com/articles/2017/11/03/maven-dod.aspx>.

<sup>④</sup> “This Algorithm Could Help Predict ISIS' Future Moves,” Business Insider, September 29, 2015, <https://www.businessinsider.com.au/machine-learning-used-to-predict-and-model-isis-2015-9>.

<sup>⑤</sup> Andrew Stanton et al. “Mining for Causal Relationships: A Data-Driven Study of the

此外，人工智能技术正逐步被应用到对恐怖袭击嫌疑人的预测之中。以色列公司 Faception 以人物性格为分类，利用算法对一个人在分类项中的匹配度打分，预测虽未列入官方数据但有可能发动袭击的人员。截至 2016 年，该公司已经开发了 15 个分类数据库，其首席执行官称，Faception 识别人格特征的准确率已经达到 80%。<sup>①</sup> Faception 的面部分析技术也可以预测潜在的恐怖分子。在 2015 年 11 月巴黎恐怖袭击涉及的 11 名恐怖分子中，只有 3 人有犯罪记录，而 Faception 的面部分析技术在没有档案的情况下可以将其中的 9 人都标记为潜在恐怖分子。<sup>②</sup> 美国国家安全局开发的“天网”（SKYNET）也可以利用机器学习在 555 万人的蜂窝网络元数据基础上评估可能成为恐怖分子的潜在对象。<sup>③</sup>

#### （四）人工智能技术推动了自主武器的研发和运用

自主武器按照人类在其执行任务过程中的角色可以分为遥控阶段、半自主阶段和全自主阶段。目前自主武器智能化水平不高，尚且处于遥控阶段和半自主阶段。

当前，无人机是自主武器研发和使用的典型代表。随着智能化的发展，世界上已有 70 多个国家军队在发展无人化系统平台。截至 2017 年，美军已装备 7 000 多架无人机，在伊拉克、阿富汗战场上投入运用的履带式机器人超过 12 000 个。<sup>④</sup> 俄罗斯也测试了包括“巨蜥-9”（Uran-9）、索拉特尼克（Soratnik）、“平台-M”（Platforma-M）等多种无人地面车辆（Unmanned

Islamic State,” Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015: 2137-2146, <https://arxiv.org/abs/1508.01192>.

<sup>①</sup> Matt McFarland, “Terrorist or Pedophile? This Start-up Says It Can Out Secrets by Analyzing Faces,” *The Washington Post*, May 24, 2016, [https://www.washingtonpost.com/news/innovations/wp/2016/05/24/terrorist-or-pedophile-this-start-up-says-it-can-out-secrets-by-analyzing-faces/?utm\\_term=.1492b3c6fdff](https://www.washingtonpost.com/news/innovations/wp/2016/05/24/terrorist-or-pedophile-this-start-up-says-it-can-out-secrets-by-analyzing-faces/?utm_term=.1492b3c6fdff).

<sup>②</sup> Simon Tomlinson, “Can You Spot a Terrorist just by Looking at Their Face? New Software Can Tell if You are Anything from a Paedophile to an Ace Poker Player by Analysing Your Features,” Mail Online, May 24, 2016, <http://www.dailymail.co.uk/news/article-3606811/Can-spot-terrorist-just-looking-face-Israeli-company-claims-predict-paedophiles-geniuses-ace-poker-players-analysing-features.html>.

<sup>③</sup> Christian Grothoff and Jens Porup. “The NSA’s SKYNET Program may be Killing Thousands of Innocent People. ArsTechnica,” WIRED Media Group, 2016.

<sup>④</sup> 《人工智能叩开智能化战争大门》，新华网，2017 年 1 月 23 日，[http://www.xinhuanet.com/mil/2017-01/23/c\\_129459228.htm](http://www.xinhuanet.com/mil/2017-01/23/c_129459228.htm)。

Ground Vehicle)。<sup>①</sup> 无人机“扫描鹰”（Scan Eagle）、“灰鹰 MQ-1C”（MQ-1C Gray Eagle）和“MQ-9 收割机”（MQ-9 Reaper）在全球抗击“伊斯兰国”的战斗中发挥了重要作用。<sup>②</sup> 俄罗斯联邦安全局在其国内有关地区利用反恐机器人引爆，消灭了 11 名恐怖分子。<sup>③</sup>

人工智能的发展促使各国更加重视自主化武器的研发。美国辛辛那提大学研发的 ALPHA 系统击败前美国空军上校李·吉恩（Gene Lee）的事件促使美国对自主武器、无人机和深度学习投入更多资金。<sup>④</sup> 美国海军陆战队的持枪机器人、以色列的“多戈”（DOGO）自动武装战术作战机器人都部分利用人工智能尝试实现机器人的自主化行动。俄罗斯的“涅列赫塔”（Nerehta）机器人尝试将无人战车与人工智能技术结合，目前在侦察、运输和地面保护等方面表现良好。<sup>⑤</sup> 2018 年 3 月，俄罗斯宣布战斗机器人最早将在年内开始批量生产。<sup>⑥</sup> 全自主化武器的研发需要机器具有独立的知识和专家推理能力，如何攻克这两个难题有赖于人工智能在机器学习和智能决策上的进一步推进。<sup>⑦</sup>

目前，自主武器的研制已经取得一些成果。俄罗斯联合仪表制造公司的 Unikum 机器人能在控制过程中完全排除人工工作。<sup>⑧</sup> 三星公司研发的机器人哨兵 SGR-A1 通过内置的摄像头、热量及运动传感器来检测入侵者，已经实现了自主发射。<sup>⑨</sup>

---

<sup>①</sup> Samuel Bendett, “Is Russia Building an Army of Robots?,” *The National Interest*, March 19, 2018, <http://nationalinterest.org/blog/the-buzz/russia-building-army-robots-24969>.

<sup>②</sup> Gregory C. Allen, “Project Maven Brings AI to the Fight Against ISIS.”

<sup>③</sup> 《俄罗斯：反恐机器人协助剿灭恐怖分子》，央视网，2018 年 5 月 3 日，<http://news.cctv.com/2018/05/03/ARTIzJpkRejBkUrEkgWH8yPy180503.shtml>。

<sup>④</sup> “Artificial Intelligence and the Future of Defense,” The Hague Centre for Strategic Studies, 2017, p.84, <http://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf>.

<sup>⑤</sup> 《钢铁近卫军：俄罗斯最具作战机器人》，俄罗斯卫星通讯社，2017 年 10 月 17 日，<http://sputniknews.cn/military/201710171023832665/>。

<sup>⑥</sup> “Russia to Begin Serial Production of Combat Robots in 2018: Defense Minister,” Xinhua News, March 17, 2018, [http://www.xinhuanet.com/english/2018-03/17/c\\_137044253.htm](http://www.xinhuanet.com/english/2018-03/17/c_137044253.htm).

<sup>⑦</sup> Mary L. Cummings, “Artificial Intelligence and the Future of Warfare,” Chatham House, January 2017, p. 8.

<sup>⑧</sup> 《俄将用机器人守卫核武器并发射弹道导弹》，透视俄罗斯，2016 年 1 月 14 日，<http://tsrus.cn/junshi/lujun/2016/01/14/558959>。

<sup>⑨</sup> “Future Tech? Autonomous Killer Robots Are Already Here,” NBC News, May 15, 2014, <https://www.nbcnews.com/tech/security/future-tech-autonomous-killer-robots-are-already-here-n10>

### 三、人工智能对反恐领域的系统性影响

人工智能不仅在具体应用上提升了反恐能力，也对反恐领域产生了系统性影响。各国普遍提升对人工智能技术的重视程度，甚至将其视为国家反恐战略的重要组成部分。在反恐行动上，人工智能促进了反恐资源的融合、丰富了反恐活动主体，加强了反恐合作，也在法律、道德和心理上影响了人类反恐活动的展开。

#### （一）人工智能技术已经成为各国反恐战略的重要组成部分

随着人工智能在新世纪的迅速发展，技术在安全领域的作用也逐渐显现，人工智能开始参与到反恐活动的方方面面，并逐渐影响到反恐活动的顶层设计，成为各国反恐活动的重要组成部分。中美等国在反恐形势日益严峻的背景下都将利用人工智能反恐纳入国家发展战略。

中国已经将发展人工智能作为一项基本国策，在战略层面多次强调发挥人工智能在反恐中的作用。《新一代人工智能发展规划》《促进新一代人工智能产业发展三年行动计划（2018—2020年）》《人工智能标准化白皮书》都重视利用人工智能提升公共安全保障能力。<sup>①</sup>把现代信息技术与反恐维稳工作有机融合，推进大数据、人工智能等新技术的深度应用，不断提高信息化、智能化水平，已经成为有关地区维稳工作的指导原则。<sup>②</sup>

作为五角大楼“第三次抵消战略”（Third Offset Strategy）的核心逻辑，美国早在2007年就将人工智能作为反恐所需的核心技术之一。<sup>③</sup>2016年发

---

5656.

<sup>①</sup> 《国务院印发〈新一代人工智能发展规划〉》，中国政府网，2017年7月20日，[http://www.gov.cn/xinwen/2017-07/20/content\\_5212064.htm](http://www.gov.cn/xinwen/2017-07/20/content_5212064.htm)；《促进新一代人工智能产业发展三年行动计划（2018-2020年）》，工业和信息化部网站，2017年12月14日，第12页，<http://www.mii.gov.cn/n1146285/n1146352/n3054355/n3057497/n3057498/c5960779/part/5960803.docx>；《人工智能标准化白皮书》，中国电子技术标准化研究院，2018年1月24日，第87页，<http://www.cesi.ac.cn/201801/3545.html>。

<sup>②</sup> 《孟建柱：全力开创社会稳定和长治久安新局面》，新华社，2017年8月28日，<http://cpc.people.com.cn/n1/2017/0828/c64094-29499816.html>。

<sup>③</sup> John Markoff, "Pentagon Turns to Silicon Valley for Edge in Artificial Intelligence," *The New York Times*, May 11, 2016, <http://www.nytimes.com/2016/05/12/technology/artificial-intelligence-as-the-pentagons-latest-weapon.htm>.

布的《为人工智能的未来做好准备》和《国家人工智能研究与发展战略规划》提出，将人工智能技术的研发确定为国家战略中的重点发展对象，建议在国际人道主义基础上推进自动和半自动武器的发展。<sup>①</sup> 美国陆军部则将机器学习、传感器与控制系统、人机交互列为最值得关注的科技发展趋势之一。<sup>②</sup> 目前，美国在国家层面愈加重视人工智能的发展，将加强对自主武器、人工智能、机器学习等的投入视为防范和打击恐袭的战略途径之一。<sup>③</sup>

日本和俄罗斯也不断提升对人工智能的重视程度。日本内阁召开“人工智能技术战略会议”，将发展人工智能纳入了《第 5 期科学技术基本计划》和《科学技术创新综合战略 2016》，强调人工智能关系到国家工业和军事的发展，将人工智能视为提升国家竞争力的手段。<sup>④</sup> 俄罗斯外交和国防政策委员会也认为人工智能是维护主权和保持国防能力的关键。<sup>⑤</sup>

## （二）人工智能技术正在改变传统反恐领域的基本规则

在人工智能纳入国家顶层设计的背景下，传统的反恐领域的很多基本规则——例如反恐资源融合，反恐活动主体、反恐合作方式等也正一一发生微妙的变化。

第一，人工智能的介入促进了国家组织机构的资源融合和共享。美国国防部内部复杂的职位设置和分工一定程度上干扰了反恐行动的策划和有效实施。利用人工智能反恐涉及多个组织部门的协调与合作，在一定程度上促进了国防资源的整合。2017 年 4 月启动的“算法战跨职能小组”（AWCFT）将联合参谋部、国防部顾问办公室（the Office of the DoD General Counsel）、

---

<sup>①</sup> “Preparing for the Future of Artificial Intelligence,” p. 38; “The National Artificial Intelligence Research and Development Strategic Plan,” National Science and Technology Council & Networking and Information Technology Research and Development Subcommittee, October 2016, p. 3.

<sup>②</sup> “Emerging Science and Technology Trends: 2016-2045,” Office of the Deputy Assistant Secretary of the Army (Research & Technology), April 2016, p. 3.

<sup>③</sup> “Summary of the 2018 National Defense Strategy,” U.S. Department of Defense, January 19, 2018, p. 7.

<sup>④</sup> 《日本将人工智能研究作为国家增长战略的优先领域》，中国科学院科技战略咨询研究院，2017 年 7 月 3 日，[http://www.casisd.cn/zkcg/ydkb/kjczyzskb/2016/201612/201707/t20170703\\_4822010.html](http://www.casisd.cn/zkcg/ydkb/kjczyzskb/2016/201612/201707/t20170703_4822010.html)。

<sup>⑤</sup> 《俄罗斯智库：人工智能在军事领域的发展现状及应用前景》，原文来自俄罗斯外交和国防政策委员会网站，搜狐科技，2018 年 3 月 31 日，[http://www.sohu.com/a/226907061\\_297710](http://www.sohu.com/a/226907061_297710)。

国防部分管情报的副部长等国防部成员组合在一起，在组织结构上实现了国防部内部的资源整合。<sup>①</sup>此外，人工智能在反恐领域的介入也促进了国家职能机构间的资源重组，促进专业化机构的产生。2018年3月，美国国会建议成立“国家人工智能安全委员会”，号召组建主管人工智能建设的独立政府部门，探究军事上应用人工智能和机器学习的风险，促进美国人工智能、机器学习和相关技术的发展，全面解决国家安全需要。<sup>②</sup>

第二，人工智能的介入也使得反恐活动组织方式发生了变化。在国家安全部门的领导下，科技公司逐步成为反恐活动的主要参与者，政府与企业的合作成为反恐合作的重要方向。作为反恐行动的主导，美国政府已经在开展“深绿”（Deep Green）计划。<sup>③</sup>人工智能自适应无线电技术和人机协作项目等多个以人工智能为核心的反恐项目也在推进。<sup>④</sup>目前，在美国国防部主导人工智能反恐活动的同时，越来越多的科技企业也融入其中。美国人工智能公司帕兰提尔（Palantir）开发的“帕兰提尔科技”（Palantir Technologies）被用于追捕“基地”组织头目本·拉登（Osama Bin Laden）。<sup>⑤</sup>“算法战跨职能小组”也整合了机器学习、自动化、计算机视觉算法等方面的国防情报企业资源。

第三，人工智能也加强了国家间的反恐合作，智能武器和情报共享可能成为未来反恐国际合作的主流。在人工智能的帮助下，未来国家间情报共享程度有望得到进一步提升，反恐情报可能从人工智能技术发达的国家和地区流向技术落后的国家和地区。与此同时，智能武器可能成为反恐国际合作的

---

<sup>①</sup> “Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven),” Deputy Secretary of Defense of the United States, April 26, 2017.

<sup>②</sup> “H. R. 5356: To Establish the National Security Commission on Artificial Intelligence,” United States Congress, March 20, 2018, <https://www.congress.gov/bill/115th-congress/house-bill/5356/text>.

<sup>③</sup> John R. Surdu and Kevin Kittka, “The Deep Green Concept,” Proceedings of the 2008 Spring Simulation Multiconference, Society for Computer Simulation International, 2008, p. 623.

<sup>④</sup> 王莉：《人工智能在军事领域的渗透与应用思考》，《科技导报》2017年第35期，第15页。

<sup>⑤</sup> “Palantir Technologies Spots Patterns to Solve Crimes and Track Terrorists,” Wired, July 31, 2012, <http://www.wired.co.uk/article/joining-the-dots>; and “Palantir Settles U.S. Lawsuit Charging Bias Against Asians,” Reuters, April 26, 2017, <https://www.reuters.com/article/us-palantir-technologies-labor/palantir-settles-u-s-lawsuit-charging-bias-against-asians-idUSKBN17R2VP?il=0>.

重点。由于“彩虹—4”无人机在执行反恐任务时表现出色，沙特于2017年确定引进中国无人机生产线，服务国内反恐需要。<sup>①</sup> 埃及也从中国引进了翼龙侦察打击一体化无人机，用于提高埃及作战能力。<sup>②</sup> 由于智能武器引进便捷、打击高效、耗资较少等特点，未来可能会有更多传统军事力量薄弱但面临恐怖威胁的国家或地区引进智能武器。

### （三）人工智能对开展反恐活动的法律、道德和心理影响

对于智能武器的应用是否符合现有的国际法，目前存在争议，国际社会就智能武器的使用规范尚未达成共识。1983年生效的《特定常规武器公约》规定禁止或限制使用某些被认为具有过分伤害力或滥杀滥伤作用的常规武器。1977年《日内瓦四公约第一附加议定书》禁止附带使平民生命受损失、平民受伤害、平民物体受损害。在实际应用中，自主武器在行动中容易造成大量平民伤亡。巴基斯坦“基本权利基金会”主席沙赫扎德·阿克巴尔表示，在过去12年中，至少有3000名巴基斯坦平民死于美国无人机空袭，其中至少包括200名儿童。<sup>③</sup> 联合国全球反恐战略提出，确保尊重所有人的人权和法治是打击恐怖主义的根本基础，规定各国必须确保其打击恐怖主义所采取的任何措施符合人权法、难民法和国际人道主义法。<sup>④</sup> 从反恐的角度看，智能武器的滥杀行为一定程度上削弱了反恐的法律和道德基础。

自由意志和道德责任控制着人类对一般武器的使用，而自动武器依据固定程序做出判断，既没有责任主体，也不会对杀戮产生道德反思。<sup>⑤</sup> 所以利用缺乏道德和法律约束的智能武器杀人的行为一定程度上冲击了大众对反恐的心理认识。美籍俄罗斯裔科幻作家艾萨克·阿西莫夫（Isaac Asimov）

---

<sup>①</sup> 《与中国合作制造无人机有利于沙特反恐》，俄罗斯卫星通讯社，2017年3月27日，<http://sputniknews.cn/opinion/201703271022191229/>。

<sup>②</sup> 《埃及引进中国翼龙无人机反恐可侦察地雷及路边炸弹》，新浪军事，2017年11月27日，<http://mil.news.sina.com.cn/world/2017-11-27/doc-ifypceiq4116126.shtml>。

<sup>③</sup> 《杀戮与冷漠——盘旋在巴基斯坦上空的美国无人机》，新华网，2016年7月21日，[http://www.xinhuanet.com/2016-07/21/c\\_1119255706.htm](http://www.xinhuanet.com/2016-07/21/c_1119255706.htm)。

<sup>④</sup> “UN Global Counter-Terrorism Strategy,” United Nations Office of Counter-terrorism Counter-Terrorism Implementation Task Force, <https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy#poa4>。

<sup>⑤</sup> 《杀人机器人“自主”杀人，这个真的可以吗？》，搜狐网，2018年4月12日，[http://www.sohu.com/a/228007732\\_612623](http://www.sohu.com/a/228007732_612623)。

提出机器人伦理问题的三定律，认为机器人不得伤害人类族群，或坐视人类族群受到伤害，以三定律来约束人工智能机器的行为，赋予它们服从和保护人类的强制性道德准则。<sup>①</sup> 但人工智能拥有自主性或自我意识后，将不可能服从机器人定律或任何人类法律的约束，对机器人的道德要求很难实现。

当前人工智能的直接行动方尚未成为法律和伦理主体，无法为其行为负责。目前联合国教科文组织和欧盟等都将人类代理人（如制造商、经营者、所有者或使用人）作为人工智能行为责任的承担者，主张让机器人的行为及决策全程处于监管之下。<sup>②</sup> 但此种倡议也仅适用于弱人工智能阶段。从技术的角度出发，目前有两种规范机器人行为的设想。其一是自上而下，在人工智能机器中预设一套可操作性的伦理准则；其二是自下而上，通过研究人类现实和模拟场景让机器学习人类在实际情况中的行为，使其树立与人类相似的价值观念。<sup>③</sup> 这两种设想在现阶段都还难以实现。

#### 四、人工智能技术参与反恐活动的潜在风险

作为一项正在高速发展进程中的新技术，人工智能技术的发展还远未成熟，这也就意味着人工智能在反恐领域的应用必然伴随着一定的风险。

第一，在反恐领域应用人工智能需要以人工智能技术的稳定性和可操控性为基础，但目前人类尚未实现对人工智能体系及相关设施的完全控制，人工智能的发展存在失控的风险。目前，已经出现了人工智能失控的情况。Facebook 两个昵称为 Alice 和 Bob 的程序使用了研究人员无法解读的交流方式，亚马逊人工智能程序 Alexa 随意发出了“令人毛骨悚然”的笑声。<sup>④</sup> 英

---

<sup>①</sup> 《杀人机器人：危险不科幻》，光明网，2016年5月29日，[http://news.gmw.cn/2016-05/29/content\\_20311065\\_2.htm](http://news.gmw.cn/2016-05/29/content_20311065_2.htm)。

<sup>②</sup> “Draft Report with recommendations to the Commission on Civil Law Rules on Robotics,” Committee on Legal Affairs, European Parliament, May 31, 2016, p. 6; and “Report of COMEST on Robotics Ethics EPORT OF COMEST ON ROBOTICS ETHICS,” United Nations Educational Scientific and Cultural Organization & World Commission on the Ethics of Scientific Knowledge and Technology, September 14, 2017, p. 42.

<sup>③</sup> 苏令银：《能将伦理准则嵌入人工智能机器吗》，《理论探索》2018年第3期，第40-42页。

<sup>④</sup> “Amazon is Aware that Alexa is Scaring People with Seemingly Random Laughter,” CNBC,

国巴斯大学的一个编程团队曾透露，就连设计者仅凭观察来破译他们所研发的机器人的行为也有困难。<sup>①</sup> 这意味着利用人工智能进行反恐活动时很可能失控，可能会错误地删除用户信息，也可能随意将普通民众识别为恐怖分子。在涉及自主武器时，人工智能的失控将导致自主武器失控，造成重大伤亡。

第二，人工智能的预测功能尚无法保证准确性和公平性。伊斯兰堡半岛电视台记者艾哈迈德·穆法克·扎伊丹（Ahmad Muaffaq Zaidan）工作中曾与恐怖组织有多次接触，美国政府“天网”程序根据对扎伊丹社交网络的分析将其列为“基地”组织及穆斯林兄弟会成员。<sup>②</sup> 即便系统做出了准确预测的结果，也不一定是出于正确的原因。在训练计算机系统区分狗和狼的实验中，计算机系统准确率几乎达到 100%。但事实证明，计算机学会的并非是识别狼与狗的图像差异，而是识别照片中的雪，所有的狼的照片都是在雪地里拍的，狗的照片却不是。<sup>③</sup> 所以人工智能在少数案例中的准确性并不能成为其广泛可靠应用的保证。此外，计算机系统很难保障公平性。美国《科学》杂志曾指出，当智能算法通过分析处理人类书写的文本来学习词句的含义时，可能获得类似于人类偏见那样的刻板印象，所以计算机向人类学习时可能会产生偏见。<sup>④</sup> 例如，某些以算法为基础的广告会出现向女性推荐低薪工作及向非裔美国人推荐低档社区的现象。<sup>⑤</sup> 这意味着数据库的性质会影响人工智能的判断，人工智能很可能会将具有某一肤色、种族特征的人识别为恐

---

March 7, 2018, <https://www.cnn.com/2018/03/07/amazon-is-aware-of-alexa-creepy-laughter.html>; and Matthew Field, “Facebook Shuts Down Robots After They Invent Their Own Language,” *The Telegraph*, August 1, 2017, <http://www.telegraph.co.uk/technology/2017/08/01/facebook-shuts-robots-invent-language/>.

<sup>①</sup> 《人工智能的失控风险》，金融时报，2017 年 8 月 14 日，<http://www.ftchinese.com/story/001073808>。

<sup>②</sup> Roy Greenslade, “NSA Labelled Al-Jazeera Journalist as ‘Suspected Terrorist,’” *The Guardian*, May 11, 2015, <https://www.theguardian.com/media/greenslade/2015/may/11/nsa-labelled-al-jazeera-journalist-as-suspected-terrorist>.

<sup>③</sup> Matt McFarland, “Terrorist or Pedophile? This Start-up Says It Can Out Secrets by Analyzing Faces.”

<sup>④</sup> Aylin Caliskan, Joanna J. Bryson, and Arvind Narayanan, “Semantics Derived Automatically from Language Corpora Contain Human-like Biases,” *Science*, Vol. 356, No. 6334, 2017, pp. 183-186, <http://science.sciencemag.org/content/356/6334/183.full>.

<sup>⑤</sup> Laura Sydell, “Can Computers Be Racist? The Human-Like Bias Of Algorithms,” NPR, March 14, 2016, <https://www.npr.org/2016/03/14/470427605/can-computers-be-racist-the-human-like-bias-of-algorithms>.

怖分子。

第三，人工智能在反恐领域的应用可能侵犯民众的隐私。从某种意义上说，以大数据为基础的研究是建立在侵犯用户隐私权基础上的，即使对信息来源进行特殊处理，也难以控制用户信息的泄露。2006年，网络视频公司奈飞公司（Netflix）放出上亿条匿名处理的电影评分数据，有研究人员通过对比匿名数据与公开获取的IMDB数据，将匿名数据与具体的用户对了起来。<sup>①</sup>在反恐视野内，有些国家政府对数据的搜集和使用本身涉及了隐私侵犯问题。美国国家安全局开发的“天网”（SKYNET）项目可以获取巴基斯坦境内5500万个手机用户的信号来源、移动轨迹、通话对象、通话时长等信息。<sup>②</sup>部分政府和组织出台了数据使用的相关条例，如《英国数据保护法》（1998）和《欧盟一般数据保护条例》（2016）规定了政府分析人士使用公民数据的方式，推动保护隐私权，但是在数据开源的网络环境中，个人隐私能否得到切实保护尚难以预料。<sup>③</sup>

## 五、简短展望

鉴于人工智能技术的现有发展水平，结合当前恐怖主义的发展状态和近期人工智能技术的发展趋势，未来人工智能在反恐领域的运用有三个可以预见的发展趋势应当引起重视。

首先，人工智能在计算机视觉和自然语言处理方面将很快迎来速度和质量上的飞跃，带动反恐情报处理和恐怖事件防范的提升。在自然语言处理方面，当前的机器翻译严重依赖于大规模平行语料库（large-scale parallel corpora）。反恐情报涉及的语言多样，训练机器以单语语料库（monolingual

<sup>①</sup> 腾讯研究院，中国信通院互联网法律研究中心等著：《人工智能：国家人工智能战略行动抓手》，中国人民大学出版社2017年版，第232页。

<sup>②</sup> Martin Robbins, “Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan?” *The Guardian*, February 18, 2016, [https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan?CMP=fb\\_a-science\\_b-gdnscience](https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan?CMP=fb_a-science_b-gdnscience).

<sup>③</sup> “2018 Reform of EU Data Protection Rules,” European Commission, [https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en).

corpora) 为基础进行自主学习才可能突破平行语料库的局限。目前 Facebook 团队基于重构损失迭代的新翻译模型和 FAIR 研究自动生成平行语料的实验, 已经表明人类在单语语料库运用方面取得突破。<sup>①</sup> 在计算机视觉方面, 反恐信息提取的准确度和速度未来可能得到显著提升。海康威视团队提出的卷积式共现特征学习框架和杰弗里·欣顿 (Geoffrey Hinton) 提出的胶囊网络 (capsule networks) 有望克服当前卷积神经网络结构的层次少, 图像识别不准确的硬伤。<sup>②</sup> 阿里巴巴团队提出的基于交替方向法的多比特量化方案也克服了循环神经网络 (Recurrent Neural Networks) 的延时缺陷, 提升了人工智能的推断速度。<sup>③</sup>

其次, 未来人工智能很可能成为恐怖组织的发动恐袭的工具, 反恐力量与恐怖组织可能面临在人工智能领域的博弈。主要军事力量的自主武器可能通过非法途径落入激进组织手中。随着数字资源越来越面向全世界开放, 恐怖组织可以进行简单人工智能武器的自主研发, 也可以较为容易地获取和使用微型和小型无人系统。<sup>④</sup> 事实上, 很难阻止恐怖组织将人工智能纳入恐袭计划。“伊斯兰国”也已经开始尝试使用商业无人机投掷爆炸物。<sup>⑤</sup> 此外, 反恐力量很难发现并摧毁恐怖分子的人工智能武器生产点, 恐怖组织可以用看似正常的工业和研究活动来掩盖人工智能武器的开发。<sup>⑥</sup> 由于武器的自主

---

<sup>①</sup> Lample, Guillaume, Ludovic Denoyer, and Marc'Aurelio Ranzato, "Unsupervised Machine Translation Using Monolingual Corpora Only," Conference Paper at ICLR 2018, p.1, <https://arxiv.org/pdf/1711.00043.pdf>; Guillaume Lample et al. "Phrase-Based & Neural Unsupervised Machine Translation," Cornell University Library, arXiv preprint arXiv:1804.07755, 2018, p.1, <https://arxiv.org/pdf/1804.07755.pdf>.

<sup>②</sup> Geoffrey Hinton, "What is Wrong with Convolutional Neural Nets?" Youtube, August 2017, <https://www.youtube.com/watch?v=rTawFwUvnLE>; Wentao Zhu et al., "Co-occurrence Feature Learning from Skeleton Data for Action Recognition and Detection with Hierarchical Aggregation," Cornell University Library, arXiv preprint arXiv:1804.06055, 2018, p. 1, <https://arxiv.org/pdf/1804.06055.pdf>; Sara Sabour, Nicholas Frosst, Geoffrey E. Hinton, "Dynamic Routing Between Capsules," Neural Information Processing Systems (NIPS), 2017, p. 6, <https://papers.nips.cc/paper/6975-dynamic-routing-between-capsules.pdf>.

<sup>③</sup> Chen Xu et al. "Alternating Multi-bit Quantization for Recurrent Neural Networks," arXiv preprint arXiv:1802.00150, 2018, p. 9, <https://arxiv.org/pdf/1802.00150.pdf>.

<sup>④</sup> Vincent Boulanin and Maaik Verbruggen, "Mapping the Development of Autonomy in Weapon System," pp. 79, 111.

<sup>⑤</sup> "Iraqi Army Says It Has Put ISIS Drones out of Service," RUDAW, March 7, 2017, <http://www.rudaw.net/english/middleeast/iraq/070320171>.

<sup>⑥</sup> "The New Dogs of War: The Future of Weaponized Artificial Intelligence," A Threatcasting Report from the Army Cyber Institute at West Point and Arizona State University's

性，恐怖组织利用自主化武器屠杀平民也将不再受到组织内部的反对。<sup>①</sup> 这是对反恐事业的巨大威胁。

最后，虽然遭受广泛质疑，自主性武器的研发还将继续，所以自主武器未来可能会应用到反恐等安全领域。埃隆·马斯克（Elon Musk）和穆斯塔法·苏莱曼（Mustafa Suleyman）等多国专家呼吁禁止自主性武器研发，认为目前正在进行的杀手机器人研发竞赛是“潘多拉的盒子”。<sup>②</sup> 2018年4月，也有多国人工智能研究人员联名抵制韩国科学技术院设立人工智能武器实验室的举动。<sup>③</sup> 但目前美国、英国、俄罗斯、以色列等国已经卷入一场打造杀人机器人军团的竞赛，伦理并不能阻碍自主性武器的研制。<sup>④</sup> 正如美国战略与国际研究中心最新报告所指出的，当前最重要的不是考虑全自主武器带来的伦理问题，对于国防部而言，重要的是不能在机器智能的使用和开发领域滞后于他国。<sup>⑤</sup> 这样一种竞赛，对各国的反恐活动和正常生活，究竟是祸是福，也有待进一步观察。

[收稿日期：2018-03-23]

[修回日期：2018-06-09]

[责任编辑：孙震海]

---

Threatcasting Lab, Arizona State University, 2017, p. 36.

<sup>①</sup> “Brian Wheeler, “Terrorists ‘Certain’ to Get Killer Robots, Says Defence Giant,” BBC News, November 30, 2017, <http://www.bbc.com/news/uk-politics-42153140>.

<sup>②</sup> Samuel Gibbs, “Elon Musk Leads 116 Experts Calling for Outright Ban of Killer Robots,” *The Guardian*, August 20, 2017, <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war>.

<sup>③</sup> 《机器杀手？多国研究员抵制韩人工智能武器实验室》，新华网，2018年4月6日，[http://korea.xinhuanet.com/2018-04/06/c\\_129844738.htm](http://korea.xinhuanet.com/2018-04/06/c_129844738.htm)。

<sup>④</sup> 《专家警告：杀人机器人军备竞赛或导致对平民屠杀》，参考消息，2017年11月21日，<http://www.cankaoxiaoxi.com/mil/20171121/2244159.shtml>。

<sup>⑤</sup> William A. Carter, Emma Kinnucan, and Josh Elliot, “A National Machine Intelligence Strategy for the United States,” Center for Strategic and International Studies, March 1, 2018, p. 22.