·专题报道——公共卫生信息化建设与人工智能·

人工智能与生物技术融合的风险分析与治理启示

祖勉，李丽娟，陈婷

军事科学院军事医学研究院，北京 100850
通信作者：陈婷，E-mail：chentingjky@163.com

【摘　要】以机器学习、深度学习和基础模型为代表的人工智能技术不断与生物技术融合，为人类健康带来诸多益处，也不可避免地衍生出一系列风险，受到政府、企业、智库、研究机构等高度关注。本文基于知识获取、毒物设计、病原体改造等分析了人工智能与生物技术融合的潜在风险，从国际框架、国家立法、行业准则和科学家行动四个方面综述了全球生物技术领域人工智能治理现状，并针对降低我国相关风险提出开发风险评估方法手段、加强立法和参与全球治理系列建议，以期为构建负责任的中国特色治理框架提供参考。
【关键词】人工智能；生物技术；融合；风险分析；治理

Risk analysis and governance implications of integrating artificial intelligence and biotechnology

ZU Mian, LI Lijuan, CHEN Ting (*Academy of Military Medical Sciences*, *Academy of Military Sciences*, *Beijing* 100850, *China*)
Corresponding author: CHEN Ting, E-mail: chentingjky@163.com

【**Abstract**】 The continuous integration of artificial intelligence (AI) technologies, represented by machine learning, deep learning, and foundation models, with biotechnology has brought numerous benefits to human health, but it has also inevitably given rise to a series of risks that have attracted significant attention from governments, businesses, think tanks, and research institutions. This paper analyzes the potential risks of integrating AI and biotechnology, focusing on knowledge acquisition, toxin design, and pathogen modification. We review the current status of AI governance in the global biotechnology field from four perspectives: international frameworks, national legislation, industry guidelines, and scientist initiatives. To mitigate relevant risks in China, we propose a series of recommendations, including developing risk assessment methods and tools, strengthening legislation, and actively participating in global governance, aiming to contribute to the construction of a responsible governance framework with Chinese characteristics.
【**Keywords**】 artificial intelligence; biotechnology; integrate; risk analysis; governance

近年来，随着人工智能技术的迭代更新，大语言模型、深度学习、自然语言处理、图像识别等在各个领域的应用不断拓展，尤其与生物技术交织融合日益紧密，有力推动了 DNA 序列发现、蛋白质结构设计和生物制造等方向迅猛发展，并在智慧诊疗、新药设计和临床决策等开展了广泛应用，同时也带来了两用技术滥用等潜在风险，已引发多国政府和专家的重视。新美国安全中心认为[1]，参照克利福德奥利弗提出的事件“量级连续体”理论，根据事件影响范围和治理复杂性，将人工智能衍生的危机分为“紧急事件”“灾害”“重大危机”和“毁灭性危机”等，其中人工智能与生物技术融合衍生的危机定为“重大危机”，如利用人工智能技术设计开发兼具毒力和传染性的病原体，造成公共卫生、经济的毁灭性损失，甚至威胁国家的长期健康、安全和稳定，且造成的严重后果无法被任何指挥控制系统管控。多个智库机构评估了人工智能与生物技术融合的风险，均得出类似结论。本文综合认为人工智能和生物技术融合或将带来严重风险。从上述问题出发，本文结合当前人工智能和生物技术融合相关技术进展，系统分析其潜在风险，并探讨未来可行的治理措施，以期为国家提前防范相关风险提供参考借鉴。

1　人工智能与生物技术融合的潜在风险

当前，两类代表性人工智能技术在生物技术领域广泛应用：大语言模型（large language models，LLMs）和生物设计工具（biological design tools，BDTs）。LLMs 是一种采用大量自然语言语料进行训练的人工智能模型，旨在理解和生成自然语言文本，广泛用于文本生成、机器翻译、问答系统和解决数学问题，随着大模型量级和复杂度不断

开放获取：CC BY-NC-ND 4.0 DOI：10.11847/zgggws1145911
第一作者：祖勉（1987—），助理研究员，博士，研究方向：国防生物科技情报。
收稿日期：2024-09-10　修回日期：2024-10-14　录用日期：2024-11-22
利益冲突：不存在　伦理审查：不需要　出版授权：全体作者已与编辑部签署作者贡献声明及版权转让协议

增加，其可表现出“涌现能力”；生物设计工具是一类由机器学习、深度学习等人工智能算法驱动的工具，训练包含 DNA 或蛋白序列等生物数据集，用于设计蛋白质、病毒载体和其他生物剂[2]。上述技术存在如下潜在风险：

1.1　大语言模型显著降低生物学知识获取门槛　近年来，自然语言处理（natural language processing，NLP）和机器学习模型功能发展迅速，大语言模型已经基本具备识别、分析生物医学专业知识，并回答专业问题的能力。研究表明，大语言模型能快速且较为全面地回答烈性病原体的选择、生产和使用，大幅降低非专业人士的专业知识获取难度。2023 年 6 月，麻省理工学院研究人员进行了一项测试，该学院大学生利用 ChatGPT 在 1 h 内，即可获得高危病毒的候选名单，以及能够合成上述病毒基因并组装病毒片段的公司名单[3]。2023 年 8 月，美国兰德公司发布大语言模型初步测试结果，发现大语言模型可向非专业人士提供大规模生物袭击的生物剂类别、获取和分发鼠疫耶尔森菌感染样本过程中面临的实际问题和预计死亡人数等专业信息；以及肉毒毒素气溶胶传播的投放方式、风险、专业知识要求及其合法获取途径等信息[4]。

大语言模型可为非专业人士提供专业知识，降低了对生物技术专业知识的获取壁垒，提供了有害生物剂的多源获取途径，随着大语言模型技术不断成熟，以及与其他技术的联用，特别是与知识图谱技术联用，大语言模型有望解决现有存在幻觉问题、可解释性差等诸多短板[5]，不断提升答案的准确性和专业性，相应潜在风险也随之增加。

1.2　生物设计工具或可用于毒物设计　BDTs 在药物设计和毒性预测领域显示出强大能力，人们可利用大量公开数据作为预训练集，基于机器学习算法建立有毒物质预测模型，随后设计合成毒性分子[6]。美国合作制药公司（Collaborations Pharmaceutics, Inc.）研究人员设计实验验证了机器学习模型在药物分子设计和毒性预测领域的滥用潜能[7]，基于小分子对乙酰胆碱酯酶的抑制活性数据建立一个大型数据集，利用公司特有 MegaSyn 生成方法训练机器学习模型，学习药物相似性、疏水性等药物特征信息，使之识别对分子毒性贡献相对大和相对小的官能团、母核等，结果在 6 h 内设计出 4 万种毒性小分子，其中部分小分子远高于已有经典神经毒剂 VX。目前生成式药物结构设计工具已经能够开发潜在的毒物分子，包括《禁止化学武器公约》附录之外的毒性分子[8]。

药物和毒物本无明确界限，医疗用毒性药品的治疗剂量和中毒剂量相近，如 A 型肉毒毒素可有效治疗肌张力障碍，也可导致呼吸和吞咽困难，甚至危及生命，具备两用性，人工智能可加速人们对已有毒性分子特征的识别和掌握，进而设计出毒性更强的分子；另一方面，药物公司在研发保护性药物分子的同时，也具备反向设计能力，可研发新型毒物分子，如新精神活性物质、失能性毒剂等，上述功能与设计治疗性分子并无二致，人工智能技术有助于设计合成母核结构新颖、不易被现有手段检测、活性更强的毒物分子。

1.3　生物设计工具增强病原体定向改造　合成生物学、基因组编辑技术的发展，病原体逆向合成和改造已成为现实，人工智能技术的引入则显著增强了病原体定向改造设计能力，可预测提高病原体致死率和传播力的改造方法，缩短试验流程[9]。英国牛津大学学者分析了生物设计工具风险，认为病毒载体优化相关生物设计工具，用于开发免疫调节相关通用遗传学元件、设计具备大流行潜能的病毒衣壳用于免疫逃逸、开发计算方法用于衣壳工程，可大大提升对病原体的设计能力，使之突破自然进化中病原体“传播性”“毒力”的相互制约法则，可能创造出兼具以上两种属性的“优化”病原体[10]。

生物设计工具，特别是 AlphaFold、RoseTTAFold 等人工智能驱动的结构预测类工具，对病原体毒力因子识别、毒力预测、病毒宿主相互作用预测具有优势，有助于设计出致病性更强、宿主范围更广、传播途径改变、耐药性突变和免疫逃逸等的微生物病原体，且随着高效算法出现和数据量不断累积，人工智能的辅助设计能力将不断提升[11]，可能产生人工改造的“X 病原体”。

1.4　人工智能加速生物武器研发技术迭代　新型生物武器研发需要一个过程，英国非盈利组织长期复原力中心对此提出了“产生意图–设计制造–武器化释放”的生物武器研发链条。该机构在 2023 年 10 月发布“人工智能助力生物武器开发”报告[12]，认为人工智能工具可通过“自学习自迭代”模式对风险链多个环节实现赋能提速，大语言模型、生物设计工具以及其他人工智能工具（如自动化实验平台）联用可推动“设计–构建–测试–学习”（DBTL）周期实现自动化，如大语言模型可用于确定候选生物剂，解释迭代循环的实验结果；而生物设计工具有助于优化感染剂量并保证递送载体在环境中存活；其他人工智能工具可实现实验流程自动化，进而迭代优化生物武器设计开发过程。目前受技术限制，大语言模型等人工智能技术尚无法独立学习或掌握生物武器制造相关新技能，随着模型不断增大，其有可能获

得包括推理和规划等高级能力，其滥用风险将大大提高。未来，若恶意行为者若将足够成熟的人工智能算法模型用于生物武器研发，可简化武器效能验证流程，缩短周期，降低成本，扩大规模，造成不可预知的后果。

2 全球生物技术领域人工智能治理现状

人工智能与生物技术融合可能会带来潜在巨大风险，制定精准治理框架，既避免无效治理，又防止过度治理导致正常的生物医药科技发展受到制约。全球已掀起讨论制定生物技术领域人工智能治理框架的高潮，但相关原则、法律法规、具体措施等尚处于起步阶段。

2.1 国际治理框架已见雏形 生物技术领域人工智能治理是一项需全球参与、多方贡献智慧的长线工程，目前尚没有形成相关全球治理框架，但已初见框架讨论的雏形。2023 年 11 月，英国主办了首届全球人工智能安全峰会[13]，欧盟及中、美、韩等 28 个国家共同签署了《布莱切利人工智能安全宣言》，该宣言是全球首份针对人工智能作为新兴技术的国际声明，体现了国际社会对未来强大人工智能模型构成人类生存威胁和当前人工智能增强有害信息生成的高度关注。该宣言重申了“以人为中心、可信任的和负责任的”人工智能发展模式；倡导在“已有的国际平台和相关倡议”框架下，实现前沿人工智能技术跨国家和跨部门合作，帮助加强人工智能在发展中国家的发展；欢迎以“发展为导向”加强人工智能能力建设，倡导“有利于创新”和“适当”监管；呼吁前沿人工智能开发者开展安全测试、多重评估，保持透明和建立问责制；在国际层面设立共同原则和行为准则，支持建立一个具有国际包容性的前沿人工智能安全科学研究网络。该宣言特别关注生物技术领域的人工智能风险，认为人工智能的有意或无意使用，可能在该领域导致严重或灾难性后果，应通过国际合作加深对潜在风险的认识，并制定风险应对策略，为后续制定生物技术领域人工智能治理框架提供总体参考。

2.2 风险监管法案尚未成形 生物技术领域人工智能监管法案是国家实施宏观调控的重要抓手，有利于保护人工智能技术和产业良性发展，降低其潜在风险。目前生物技术领域人工智能风险监管法案仍有待完善，仅有人工智能通用领域的相关法案。世界首部人工智能风险监管法案已于 2024 年 5 月 21 日获得欧盟理事会签署[14]。欧盟《人工智能法案》（AI Act）将人工智能风险等级按照功能和用途分为不可接受、高风险、限制性风险和最低风险 4 个等级，并对逾越红线行为明确了处罚细则，旨在监管其他国家和地区在欧盟开展人工智能业务实体机构。该法案根据人工智能业务实体机构在产业链角色（人工智能技术的“提供者”“用户”和“最终用户”）区分监管等级，其中“提供者”作为技术或产品开发方，受到法案重点监管。此外，英国政府在 2023 年 3 月发布《促进创新的人工智能监管方法》白皮书[15]，提出建立中央风险职能部门，识别、评估和监测包括生物安全风险在内的人工智能交叉风险。

美国对生物技术领域人工智能监管法案建设进行了探索，相关举措包括议员提案、签署总统行政令和发布智库报告等。美国国会议员于 2023 年 7 月 19 日向国会提交两项议案，一项为《人工智能与生物安全风险评估法案》（Artificial Intelligence and Biosecurity Risk Assessment Act）[16]，要求卫生与公众服务部（HHS）战略准备和应对管理局（ASPR）开展开源人工智能和大型语言模型用于合成新型病原体、开发生物武器的风险评估；另一项为《公共卫生准备和应对人工智能威胁战略法案》（Strategy for Public Health Preparedness and Response to Artificial Intelligence Threats）[17]，要求 HHS 制定相应战略，以应对人工智能驱动的生物威胁引发的公共卫生紧急事件。美国拜登总统于 2023 年 10 月 30 日签署《安全、可靠地开发和使用人工智能》行政令，明确要求能源部开发人工智能模型相关风险评估工具和测试平台，评估包括人工智能模型增强化生放核威胁、人工智能与合成生物学交叉风险等[18]，并要求人工智能系统开发商开发任何对国家公共健康和安全构成严重风险的人工智能模型时，需在发布成果前向政府报告并要求其共享所有红队安全测试结果，有助于监管对美国国家安全、经济、公共卫生或安全构成威胁的人工智能系统开发活动。美国诺兰智库呼吁美国商务部修订现有法规《出口管制条例》，将具备病原体设计和改造潜能的人工智能技术（包括大语言模型和生物设计工具）增列出口管制清单，以减轻其带来的风险[19]。

2.3 行业内部自发制定风险监管准则 面对国际社会对人工智能潜在风险的质疑声不断加大，亚马逊、谷歌 DeepMind、Meta、OpenAI 等 7 家全球领先的人工智能公司提出行业准则，包括负责任的能力扩展、保护模型权重、漏洞报告结构（使外部人员可识别人工智能系统的安全问题）、预防和监控模型误用等行业监管对策，以期引领人工智能产业良性发展，回击外界的“人工智能威胁论”。以谷歌为例，2024 年 5 月 17 日，谷歌 DeepMind 推出了人工智能前沿安全框架（Frontier Safety Framework Version 1.0）[20]，包括早期识别危害阈

值、定期评估检测和应用缓解措施三大组成部分。该框架认为生物安全是未来基础模型可能产生严重风险的高风险领域之一，评估了恶意行为者使用基础模型实施破坏活动并造成严重后果的程度，当风险超过危害阈值时，可行的缓解措施包括防止模型权重泄露和设置对关键能力的访问权限等。

2.4 *科学家对风险治理发挥专业智囊作用* 人工智能和其他颠覆性技术赋能潜在大流行病原体的研究，对公共卫生构成了巨大威胁，科学家作为研究一线人员，是发现问题、评估风险和制定缓解措施的最佳人选，科学家对生物安全治理的专业智囊作用正越来越显著。2024 年 6 月 12 日，天津大学学者在《原子能科学家公报》发文[21]，认为在人工智能与生物技术融合的风险监管领域，由于科学研究本身具有不确定性，监管机构的工作节奏相对于科学发展明显具有滞后性，使得存在潜在“溢出风险”的病原体功能获得性研究难以被及时有效监管，而科学家处于评价研究风险的最佳位置，呼吁加强对科学家的支持，让科学家参与到生物安全风险相关规范、工具和机制的制定中，发挥专业作用，主动评估和减轻科研工作中的潜在风险。

3 对策建议

人工智能技术迅猛发展引起的潜在生物安全风险已受到多方关注，全球掀起人工智能安全治理热潮，我国应注重整合优势资源，建立早期风险识别和监测预警机制，定期开展风险评估，制定可行的风险缓解策略，完善法律法规框架，积极融入国际人工智能与生物技术融合治理格局。

3.1 *探索开发科学严谨的风险评估工具* 随着人工智能应用在生物领域不断拓展，以事件报告、情报收集等作为支持性数据，识别和评估公共和社会风险、潜在危害类型和程度，有助于监管机构根据评估结果划分优先级，采取人工智能治理行动[22]，因此风险评估对于治理工作开展至关重要，开发严谨可靠的人工智能模型风险评估工具和测试平台可发挥关键支撑作用，使得人工智能与生物技术融合“精准”监管框架的制定有“法”可依。建议采用多种模型方法开展人工智能与生物技术融合风险分级评估，如“红队”模拟评估法[23]，通过设定特定生物事件发生场景，由研究人员扮演“红队”，利用人工智能技术制定生物事件策划方案，在此基础上，组织第三方专家团队对方案可行性打分，早期识别潜在风险点和制定缓解措施；也可从头开发生物领域的人工智能风险评估结构化工具[24]，理解人工智能在生物技术领域的具体应用场景，识别潜在风险点，评估人工智能技术的弱点和威胁，基于人工智能系统的成熟度和自动化程度评估后果和风险等级，为制定并实施风险缓解策略提供理论基础。

3.2 *在立法层面为风险治理提供法律保障* 当前，全球人工智能立法已进入快车道新阶段，欧盟、英、美等国家推进人工智能立法的特点和趋势带给我国诸多启示和思考方向。一是明确权利执行实体。欧洲《人工智能法案》提出在欧委会内部设立人工智能办公室、咨询论坛和独立专家科学小组，负责欧盟层面人工智能监管。我国已发布《生成式人工智能服务管理暂行办法》[25]，规定“网信、发展改革、教育、科技、工业和信息化、公安、广播电视、新闻出版等部门，依据各自职责依法加强对生成式人工智能服务的管理”，我国可以此为基础，将生物技术领域纳入监管范围，整合卫生健康委、中国疾病预防与控制中心、食品药品监督管理部门等力量，共同参与讨论制定包含生物技术领域在内的人工智能监管政策，同时更新《生物安全法》管理范畴，酝酿出台相关生物技术领域人工智能管理下位法，提前布局防范相关风险。二是坚持安全和发展并重。明确生物技术领域人工智能立法的边界，制定 DNA 和蛋白序列设计、病原体–宿主相互作用预测等领域涉及的人工智能技术工具清单，制定生物数据集预训练和优化训练规则，对数据来源、规模、类型、标注规则、算法机制等进行重点监督检查，对高风险人工智能模型设置访问权限，制定违背红线的处罚规则；鼓励人工智能算法、芯片等基础技术的自主创新，推动生物领域公共训练数据资源平台建设。

3.3 *积极参与全球生物技术领域人工智能治理* 目前，在全球经济一体化的大环境下，全球病原体基因序列数据资源共享，人工智能聊天机器人开源使用，基因合成公司全球分布，一个国家想独立解决人工智能对生物安全的影响不具备可行性。世界各国需要开展广泛合作，研讨潜在风险，制定可行的治理框架。

我国重视在人工智能安全全球治理中发挥大国作用，于 2023 年 10 月 20 日发布了《全球人工智能治理倡议》，倡导各国加强信息交流和技术合作，形成广泛共识的人工智能治理框架，不断提升技术安全性、可靠性、可控性和公平性，为讨论制定国际人工智能与生物技术融合治理框架提供了蓝本；2024 年 7 月 1 日，我国提出的“加强人工智能能力建设国际合作”也经第 78 届联合国大会以协商一致方式通过，上述倡议可为践行生物领域的人工智能治理提供引导。

我国是生物产业和人工智能科技发展大国，在当前国际社会团结协作聚力发展的良性环境中，我国应抓住发展机遇，顺势为之，借助国际合作大力开展我国基础设施和平台建设，提升硬实力；基于《全球人工智能治理倡议》“以人为本”理念和“智能向善”宗旨，在构建人类健康命运共同体的大框架下，擘画生物技术领域人工智能治理蓝图，积极为全球治理贡献自身智慧，提升我国国际形象和话语权，实现我国生物领域人工智能技术的健康可持续发展。

参考文献

[1] CNAS. Catalyzing crisis: a primer on artificial intelligence, catastrophes, and national security[EB/OL]. (2024-06-11)[2024-09-09]. https://www.cnas.org/publications/reports/catalyzing-crisis.

[2] Sandbrink J B. Artificial intelligence and biological misuse: differentiating risks of language models and biological design tools[EB/OL]. arXiv: 2306.13952. (2023-12-23)[2024-09-09]. https://arxiv.org/abs/2306.13952.

[3] AI’s bioterrorism potential should not be ruled out [EB/OL]. (2024-02-07)[2024-09-09]. https://www.ft.com/content/e2a28b73-9831-4e7e-be7c-a599d2498f24.

[4] Mouton C A, Lucas C, Guest E. The operational risks of AI in large-scale biological attacks: a red-team approach[EB/OL]. (2023-10-16)[2024-09-09]. https://www.rand.org/pubs/research_reports/RRA2977-1.html.

[5] Pan S R, Luo L H, Wang Y F, et al. Unifying large language models and knowledge graphs: a roadmap[J]. IEEE Transactions on Knowledge and Data Engineering, 2024, 36(7): 3580-3599.

[6] Blay V, Li X Y, Gerlach J, et al. Combining DELs and machine learning for toxicology prediction[J]. Drug Discovery Today, 2022, 27(11): 103351.

[7] Urbina F, Lentzos F, Invernizzi C, et al. Dual use of artificial-intelligence-powered drug discovery[J]. Nature Machine Intelligence, 2022, 4(3): 189-191.

[8] Urbina F, Lentzos F, Invernizzi C, et al. AI in drug discovery: a wake-up call[J]. Drug Discovery Today, 2023, 28(1): 103410.

[9] de Lima R C, Sinclair L, Megger R, et al. Artificial intelligence challenges in the face of biological threats: emerging catastrophic risks for public health[J]. Frontiers in Artificial Intelligence, 2024, 7: 1382356.

[10] Sandbrink J B, Alley E C, Watson M C, et al. Esvelt KM. Insidious Insights: Implications of viral vector engineering for pathogen enhancement[J]. Gene Therapy. 2023, 30(5): 407-410.

[11] Krin A, Jeremias G. Artificial intelligence: possible risks and benefits for BWC and CWC[EB/OL]. (2023-07-05)[2024-09-09]. https://cbwnet.org/media/pages/publications/working-paper/artificial-intelligence-possible-risks-and-benefits-for-bwc-and-cwc/ff95cdf423-1702984262/wp-5-website-version.pdf.

[12] Nelson C, Rose S. Understanding risks at the intersection of AI and bio [EB/OL]. (2023-10-18)[2024-09-09]. https://www.longtermresilience.org/post/report-launch-examining-risks-at-the-intersection-of-ai-and-bio.

[13] AI Safety Summit programme [EB/OL]. (2023-10-16) [2024-09-09]. https://www.gov.uk/government/publications/ai-safety-summit-programme.

[14] European Parliament . EU AI Act: first regulation on artificial intelligence[EB/OL]. (2024-06-18)[2024-09-09]. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[15] Department for Science, Innovation and Technology and Office for Artificial Intelligence. AI regulation: a pro-innovation approach [EB/OL]. (2023-08-03)[2024-09-09]. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach.

[16] S. 2399 - Artificial intelligence and biosecurity risk assessment act[EB/OL]. (2023-07-19)[2024-09-09]. https://www.congress.gov/bill/118th-congress/senate-bill/2399/text.

[17] S. 2346 - Strategy for public health preparedness and response to artificial intelligence threats[EB/OL]. (2023-07-18)[2024-09-09]. https://www.congress.gov/bill/118th-congress/senate-bill/2346.

[18] The White House. Executive order on the safe, secure, and trustworthy development and use of artificial intelligence[EB/OL]. (2023-10-30)[2024-09-09]. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[19] Jacob M. Advances in AI and increased biological risks[EB/OL]. (2024-07-12)[2024-09-09]. https://councilonstrategicrisks.org/2024/07/12/advances-in-ai-and-increased-biological-risks/.

[20] Dragan A, King H and Dafoe A. Introducing the frontier safety framework[EB/OL]. (2024-05-17)[2024-09-09]. https://deepmind.google/discover/blog/introducing-the-frontier-safety-framework/.

[21] Zhang W W, Wang L F. Scientists are the best judge of research risks, but they need support[EB/OL]. (2024-06-12)[2024-09-09]. https://thebulletin.org/2024/06/scientists-are-the-best-judge-of-research-risks-but-they-need-support/#post-heading.

[22] Daniels O, Murdick D. Enabling principles for AI governance[EB/OL]. (2024-07)[2024-09-09]. https://cset.georgetown.edu/publication/enabling-principles-for-ai-governance/.

[23] Mouton C A, Lucas C, Guest E. The operational risks of AI in large-scale biological attacks: results of a red-team study[EB/OL]. (2024-01-25)[2024-09-09].https://www.rand.org/pubs/research_reports/RRA2977-2.html.

[24] De Haro L P. Biosecurity risk assessment for the use of artificial intelligence in synthetic biology[J]. Applied Biosafety, 2024, 29(2): 96-107.

[25] 国家互联网信息办公室, 中华人民共和国国家发展和改革委员会, 中华人民共和国教育部, 等. 国家互联网信息办公室 中华人民共和国国家发展和改革委员会 中华人民共和国教育部 中华人民共和国科学技术部 中华人民共和国工业和信息化部 中华人民共和国公安部 国家广播电视总局令 第 15 号 [EB/OL]. (2023-07-10)[2024-09-09]. https://www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm.