

浅析人工智能在网络安全中的应用与挑战

许文明

陕西能源职业技术学院 712000

DOI:10.32629/ems.v8i3.18770

[摘要] 在数字化时代快速发展的背景下，网络技术的普及已渗透到社会生产生活各领域，网络攻击手段呈现智能化、多样化、隐蔽化趋势，传统网络安全防护技术难以应对复杂威胁，网络安全形势愈发严峻。人工智能作为新兴综合性技术，凭借自主学习、智能分析、精准识别的核心优势，广泛应用于网络安全防护领域，有效提升了防护效率与精准度，为网络安全保障提供了新路径。本文结合人工智能技术特点与网络安全实际需求，浅析其在网络安全中的具体应用场景，剖析应用过程中面临的技术、管理、伦理等挑战，提出针对性应对策略，为推动人工智能与网络安全深度融合、提升防护水平、保障数字空间安全提供参考，助力数字化社会高质量发展。

[关键词] 人工智能；网络安全；应用场景；安全挑战；应对策略；数字安全

引言

随着大数据、云计算、物联网等数字技术快速迭代，人类社会进入数字化转型阶段，网络空间作为第五大主权空间，其安全稳定关乎国家主权、社会稳定及公众权益。与此同时，网络安全威胁激增，攻击手段向人工智能驱动的自动化、定向化、隐蔽化升级，精准度与破坏力大幅提升，给防护工作带来巨大压力。

传统网络安全防护以被动防御为主，依赖人工操作，存在响应慢、识别准确度低、难以应对未知威胁等局限，无法适配复杂网络环境。而人工智能凭借自主学习、海量数据处理及智能分析能力，打破传统防护瓶颈，实现从“被动防御”向“主动预警、智能防控”的转型，成为提升网络安全防护水平的核心支撑。

一、人工智能技术的核心特点及其在网络安全中的应用优势

（一）人工智能技术的核心特点

人工智能是模拟、延伸和扩展人类智能的综合性技术，核心特点体现在三方面：一是自主学习能力，可通过算法模型分析海量数据、自主总结规律、优化模型，无需人工干预即可提升性能，快速适应复杂网络环境；二是海量数据处理能力，能高效处理网络流量、日志、行为等各类数据，快速筛选有价值信息，为安全决策提供支撑；三是智能分析与决策能力，可基于学习到的规律，精准分析网络行为与威胁，识别潜在隐患并自动采取防控措施，实现智能化防护。

（二）人工智能在网络安全中的应用优势

相较于传统防护技术，人工智能的应用优势显著：一是提升威胁识别精度，通过深度学习精准识别已知威胁，同时发现传统技术难以察觉的未知、隐蔽威胁，降低漏报与误报

率；二是加快响应速度，实现威胁的实时监测、快速识别与自动响应，将响应时间从小时级、分钟级缩短至秒级，最大限度降低攻击损失；三是降低人工成本，替代传统人工排查与防御工作，减少对专业安全人员的依赖，提升防护效率；四是适应复杂网络环境，可快速适配多样化网络设备、终端与协议，实现全面防护，提升防护的综合性与有效性。

二、人工智能在网络安全中的具体应用场景

随着人工智能技术的成熟，其在网络安全领域的应用场景不断拓展，渗透到防护各环节，全方位提升防护水平，成为网络安全保障体系的核心组成部分。

（一）网络威胁检测与预警

网络威胁检测与预警是防护第一道防线，也是人工智能应用最广泛、最成熟的场景。传统检测技术依赖人工规则，仅能识别已知威胁，对未知、变异威胁识别能力薄弱。人工智能通过构建深度学习、机器学习模型，实时监测并智能分析海量网络数据，可精准识别病毒攻击、黑客入侵、DDoS攻击等各类恶意行为。

人工智能驱动的检测系统可通过自主学习更新威胁特征库，实现对未知、变异威胁的精准识别与提前预警，同时分析攻击来源、路径与目的，为防护决策提供依据。通过异常检测算法识别网络流量波动、异常连接，及时发现DDoS攻击迹象；通过行为分析算法识别用户异常登录、操作行为，防范账号被盗与恶意操作，实现威胁早发现、早预警、早处置。

（二）入侵防御与攻击阻断

入侵防御与攻击阻断是网络安全防护的核心，目标是阻止攻击实施、保护网络设备、终端与数据安全。传统入侵防御依赖规则匹配，仅能防御已知入侵行为，对新型、自动化入侵应对不足。人工智能技术的应用，实现了防护从“被动”

向“主动”的转型。

人工智能驱动的入侵防御系统，可通过自主学习掌握各类入侵行为的特征与规律，实时监测网络入侵迹象，自动采取阻断攻击连接、封禁攻击IP、清理恶意程序等措施，及时阻断攻击、降低损失。同时，可预测攻击发展趋势，提前优化防御策略，提升对智能化、自动化攻击的应对能力。

（三）恶意代码与恶意软件识别

恶意代码与恶意软件是主要网络威胁，种类繁多、变异速度快，传统特征码匹配技术难以应对，漏报与误报率较高。人工智能凭借强大的自主学习与智能分析能力，有效解决了这一局限，实现了精准识别与防控。

人工智能驱动的身份认证系统，通过深度学习海量恶意代码样本，提取行为与结构特征、构建识别模型，既能识别已知恶意代码与软件，也能识别未知、变异及新型恶意程序。同时，可实时监测恶意软件传播行为，发现传播路径并自动采取隔离、清理措施，阻止其扩散，保护网络终端与数据安全。

（四）身份认证与访问控制

身份认证与访问控制是网络安全的重要基础，核心是确认用户身份合法性、限制访问权限，防范未经授权访问与数据窃取。传统单一认证方式（密码、验证码）安全性低、易被破解，难以满足当前安全需求。人工智能推动认证与访问控制技术升级，实现多维度、智能化防护。

人工智能驱动的身份认证系统，结合生物特征识别（人脸识别、指纹识别等）与行为特征识别（操作习惯、登录信息等），构建多维度认证模型，精准识别用户身份，防范身份伪造、密码破解等问题。同时，可根据用户身份、权限与行为特征，智能调整访问控制策略，实现网络资源精细化管控，保护资源与数据安全。

（五）数据安全防护

数字化时代，数据成为重要生产要素，数据安全关系个人隐私、企业利益与国家安全。随着数据量激增，数据泄露、篡改、滥用等问题日益突出，给防护工作带来巨大挑战。人工智能凭借强大的数据处理与分析能力，在数据安全防护领域发挥重要作用，有效提升防护水平。

其应用主要体现在三方面：一是数据加密与解密，通过智能算法优化加密方案，提升安全性与效率，同时实现智能解密，保障合法用户便捷访问；二是数据泄露检测与预警，实时监测数据传输、存储、使用全过程，识别泄露迹象并及时预警、采取防控措施；三是数据脱敏，通过智能算法隐藏敏感信息，保护个人隐私与企业商业秘密，不影响数据正常使用。

三、人工智能在网络安全应用中面临的主要挑战

尽管人工智能显著提升了网络防护水平，但受技术局限、网络环境复杂及管理不完善等影响，其应用仍面临诸多挑战，制约二者深度融合发展。

（一）技术自身局限性带来的安全风险

人工智能技术自身局限可能引发新安全风险。一是模型安全性不足，训练数据若有漏洞、被篡改或算法存在缺陷，易导致模型被攻击、操控，出现误判漏判，还可能遭遇对抗性攻击、模型投毒攻击等，其中对抗性攻击隐蔽性强、危害极大。二是“黑箱”问题突出，多数人工智能模型决策过程不可解释，出错后难以排查优化，限制其在高安全要求领域的应用。三是模型泛化能力有限，难以快速适配升级后的网络环境与攻击手段，防护效果下降。

（二）数据安全与隐私保护面临严峻挑战

人工智能应用需海量含敏感信息与隐私的数据支撑，但数据全流程安全防护难度大。采集环节存在过度采集、未授权采集等问题；存储与处理环节因设备、加密技术不足，易发生数据泄露篡改；数据滥用现象突出，部分主体非法利用数据侵犯权益。此外，数据跨境流动频繁，不同地区法规差异进一步加剧防护难度。

（三）网络安全人才短缺问题突出

二者深度融合需大量懂人工智能与网络安全的复合型人才，当前我国此类人才缺口巨大。该类人才需扎实的多领域知识，培养周期长、成本高；人才培养体系与市场需求脱节，高校培养的人才难以适配实际工作；同时行业人才流动性大，优秀人才流向高薪领域，加剧短缺困境。

（四）相关管理制度与法律法规不完善

缺乏完善的制度法规保障人工智能在网络安全领域的规范应用。管理制度上，无统一应用规范与标准，企业应用缺乏指导，管理不到位；法律法规上，针对新型网络安全问题的法规存在空白，违法行为界定模糊、处罚不足，且跨部门监管职责不清，监管效率低下，难以防范风险。

（五）伦理道德风险日益凸显

人工智能应用引发诸多伦理道德风险。一是替代传统安全岗位，调整就业结构，带来就业压力；二是训练数据偏差、算法缺陷可能导致模型决策偏见，出现歧视性判断；三是技术可能被用于非法攻击，造成重大损失；四是少数企业垄断市场，限制行业健康发展，影响社会公平。

四、应对人工智能在网络安全应用中挑战的策略

针对上述挑战，需结合人工智能技术发展趋势与网络安全实际需求，采取针对性措施，完善技术体系、管理制度与法律法规，推动二者深度融合、健康发展。

（一）强化技术研发，破解技术自身局限性

加大人工智能安全技术研发投入,重点研发对抗性攻击防御、模型安全检测、模型可解释性等技术,提升模型安全性与可靠性,通过对抗性训练增强模型抵御攻击的能力,借助可解释性算法破解“黑箱”问题,提升决策透明度。加强人工智能与网络安全技术深度融合,优化模型泛化与适应能力,推动模型迭代升级,适配复杂网络环境与新型攻击手段。

建立模型安全评估体系,全面评估模型安全性、可靠性与准确性,及时排查漏洞、优化完善;加强国际技术交流合作,引进先进技术与经验,结合我国实际消化创新,提升整体技术水平。

(二) 完善数据安全保障体系,强化隐私保护

规范数据采集行为,明确采集范围、权限与流程,要求采集用户数据必须获得明确授权,杜绝过度、非法采集,保护用户隐私。加强数据存储与处理环节防护,完善存储设备,采用先进加密、备份技术,防止数据泄露、篡改,保障数据安全完整。

建立健全数据安全管理制度,明确各环节责任,加强监督管理,严厉处罚数据滥用、泄露等违法行为;完善隐私保护法律法规,明确隐私界定与保护范围,加大处罚力度;建立数据跨境流动安全评估机制,规范跨境流动行为,防范跨境安全风险。

(三) 加强人才培养,弥补复合型人才缺口

完善人才培养体系,优化高校、职业院校培养方案,结合市场需求增设相关专业课程,强化计算机、数学、算法及网络安全知识教学,注重实践教学,提升学生综合素养与实操能力,培养适配市场需求的复合型人才。加强校企合作,建立人才培养基地,开展订单式培养、顶岗实习,实现人才培养与市场需求无缝对接。

加强在职人员培训,定期开展人工智能与网络安全技术培训,提升从业人员专业技能;制定优惠政策,加大复合型人才引进力度,弥补人才缺口,为二者深度融合提供人才支撑。

(四) 完善管理制度与法律法规,强化监管力度

建立健全人工智能在网络安全领域应用的管理制度,制定统一应用规范与标准,明确各方责任义务,规范应用行为,提升防护规范化水平。建立跨部门协同监管机制,明确监管职责,加强沟通协作,避免监管重叠与空白,提升监管效率。

加快完善相关法律法规,明确新型网络安全违法行为的界定与处罚标准,加大处罚力度,形成有效震慑;加强法规宣传普及,提升企业、机构与公众法律意识,引导依法应用、

依法维权;加强国际合作,参与全球网络安全治理,推动建立统一的国际规则与标准,应对跨境威胁。

(五) 防范伦理道德风险,推动健康发展

建立人工智能伦理道德规范,明确应用伦理准则,禁止利用人工智能从事非法活动,杜绝模型偏见与歧视,保障社会公平正义与公众权益。加强伦理道德教育,提升从业人员伦理素养,引导规范从业。关注就业结构调整影响,制定就业扶持政策,帮助被替代从业人员转岗再就业,缓解就业压力。

加强技术监管,防范技术垄断,鼓励中小企业参与研发与应用,促进市场公平竞争;建立公众监督机制,鼓励公众监督违法行为与伦理问题,形成全社会共同防范的良好氛围。

五、结论

数字化时代网络安全形势严峻,传统防护技术难以适应复杂威胁,人工智能凭借自身优势广泛应用于网络安全领域,实现防护模式转型、提升防护水平,成为网络安全保障体系的核心,为数字空间安全提供有力支撑。

同时,人工智能在网络安全应用中仍面临技术局限、数据安全、人才短缺等多重挑战,制约二者深度融合。对此,需通过强化技术研发、完善数据保障、加强人才培养等针对性措施,积极应对挑战、发挥技术优势。

未来,随着人工智能技术成熟与相关制度完善,二者深度融合将成为必然趋势。我们应顺应趋势、破解难题,持续提升网络安全防护水平,保障数字空间安全、助力数字化社会高质量发展,同时参与全球网络安全治理,推动构建网络空间命运共同体。

[参考文献]

[1] 邹雨琛, 郑志慧. 人工智能在网络安全中的应用与挑战[J]. 信息记录材料, 2024, 25(6): 173-175.

[2] 曹淼, 程泉. 人工智能在网络安全中的应用与挑战[J]. 通信世界, 2025(13): 23-26.

[3] 黄秋实. 人工智能在网络安全威胁检测中的应用与挑战[J]. 科技视界, 2025, 15(27): 82-85.

[4] 何龙. 人工智能在网络安全防护中的应用与挑战[J]. 中国安防, 2025(8): 91-94.

[5] 许艳云, 魏言兵. 人工智能技术在网络安全中的应用与挑战[J]. 中国新通信, 2023, 25(18): 113-115.

作者简介: 许文明, 男, 汉族, 山东德州, 出生年月: 1979年10月, 学位: 学士, 职称: 工程师, 研究方向: 计算机科学与大数据。