

北京信息科技大学研究生导师简介

导师姓名	李军	性 别	男	出生年月	1983.11	
政治面貌	中共党员	专业技术职务	教授	现任职务	科技处副处长 兼先进技术研究院副院长	
所属学院	计算机学院	人才称号	某国家级创新人才项目入选者	个人邮箱	lijun@bistu.edu.cn	
任硕导时间	2020 年 12 月	任博导时间	2025 年 12 月	最后学历/学位	博士研究生/工学博士	
所属学科	网络空间安全、计算机科学与技术			主要研究方向	人工智能安全	
					网络智能安全	
加入学术团体		中国网络空间安全人才教育联盟、北京市多维空间安全专委会、中国CAAI智能信息网络专委会、NISIA工业互联网安全专委会、工信部区块链重点实验室电力应用工作委员会等				
个人简历 (主要经历)	自何年月	至何年月	就学或工作单位（填至专业或系部）			
	李军，博士，教授，博士生导师，入选中央部委某国家级创新人才项目；博士毕业于北京邮电大学计算机科学与技术专业，现任北京信息科技大学科技处副处长兼先进技术发展研究院副院长，方班全国培养基地分基地兼鹏城靶场分靶场负责人、中国商业联合会大模型智能应用与安全计算重点实验室常务副主任、北京信息科技大学计算机学院人工智能安全研究所所长。					
承担部分科研课题（横纵向课题 5 项）	长期致力于人工智能安全、智能化网络攻防、大模型智能信息处理等方向研究工作。近年来主持国家自然科学基金、GFKGJ基础科研课题、GFKGJ配套科研课题、装发HY课题合计10余项。部分代表性前沿课题： [1] 基于集成模型的网络行为数据流敏感目标跟踪和检测技术，国家自然科学基金联合基金，纵向，2020-2023，主持； [2] *****反智能技术研究，国防军工基础科研，2023-2025，主持； [3] *****情报挖掘技术研究，军工HY课题预研，2023-2025，主持； [4] *****智能化研制，国防军工配套科研，2025-2027，主持； [5] 基于大模型的网络威胁发现及主动防御技术研究，国家电网横向，2026-2028，主持； [6] 基于属性图的多模态电子证据融合表征方法，国家电网横向，2023-2025，已结题 [7] 基于人机物的安全可信体系技术研究，国家电网横向，2021-2023，已结题 [8] 能源电力区块链安全支撑，国家电网横向，2022-2024，已结题					
近五年主要成果及培养方向 (限填 5 项，包括代表性的论文、专著、专利、科技奖励等)	(1) 成果概况：在IEEE Internet of Things Journal、ACM SIGKDD Conference on Knowledge Discovery and Data Mining、ICDM（IEEE International Conference on Data Mining）、CIKM（ACM International Conference on Information and Knowledge Management）、《计算机研究与发展》、《计算机学报》、《网络空间安全》等国内外期刊发表A类、B类及C类以上期刊论文10余篇，担任多个国际国内学术期刊编委、项目评审专家，软件著作权8项，专利10余项；部分最新论文和专利： 1) Li J, Jiang W, Shen L, et al. Optimized Frequency Collaborative Strategy Drives AI Image Detection[J]. IEEE Internet of Things Journal, 2025. 2) Li J, Jiang W, Zhang J, Shao Y, Zhu W. Fake User Detection Based on Multi-Model Joint Representation. Information 2024, 15, 266. 3) Li J, Shan C, Shen L. PNAP-YOLO: An Improved Prompts-Based Naturalistic Adversarial Patch Model for Object Detectors. Ann. Data. Sci. 12, 1055 - 1072. 更多2025年10月之前论文可查阅google学术页面。					
	(2) 学生获奖：2023 年指导优秀研究生获“兆易创新杯”第 18 届中国研究生电子设计竞赛全国赛区三等、华北赛区一等奖；2025 年指导优秀研究生获全军人工智能大赛全国总决赛					

	赛赛道第三名的历史性成绩。 （3）科研思路：在工程实践中，我们常会遇到具体的技术难题。将这些问题凝练成科学问题并开展研究，在形成论文和课题成果的同时，也能进一步推动工程应用的创新。作为应用科学，科研的根本目的在于解决实际问题；论文发表只是在解决问题过程中，伴随新发现、新想法而产生的自然成果。因此，我个人并不主张任何脱离实践、“从论文到论文”的研究方式。 实验室具有稳定的 AI 实验环境和尽最大能力的课题开展条件，已支持多名毕业生到 985/211 高校优势学科继续深造，招收致力于在人工智能安全、智能化网络攻防、大模型智能信息处理等领域具有研究兴趣和技术创新意愿的研究生。希望你有扎实的数学和编程基础、踏实肯干的精神和乐观积极的心态。
--	--