

教育部工程研究中心年度报告

(2024年1月——2024年12月)

工程中心名称：网络信息安全管理与服务

所属技术领域：信息与电子工程

工程中心主任：李建华

工程中心联系人/联系电话：夏正敏/13641682020

依托单位名称：上海交通大学

2025 年 3 月 25 日填报

一、技术攻关与创新情况

网络信息安全管理与服务教育部工程研究中心功能定位为以新型网络信息安全管理与风险管控服务为研究重点，致力于突破网络空间中密码、网络、系统和应用等领域的安全共性关键技术，服务国家/地方重大工程，促进高级专业人才培养。目标是成为国内一流、国际先进的网络空间安全领域工程研究中心。围绕中心功能定位和目标，中心设置了六个重点研究方向，在密码基础理论与应用领域，设置了密码算法设计与安全检测方向。在网络安全领域重点在新型网络综合安全管理与优化，网络安全态势智能感知与预警两个方向开展研究。在系统安全领域，重点研究网络与信息系统检测与评估技术。在此基础上，面向服务国家战略和产业需求，重点开展公共安全行业管理与决策服务和互联网信息内容安全监管服务两个方向的研究。

网络信息安全管理与服务教育部工程研究中心在充分理解承担国家网络空间安全管理职责的各类职能部门实际业务需求基础上，总结与凝练共性核心技术需求，全面攻关网络空间安全态势感知、智能化信息内容安全管理、区块链及人工智能安全等核心技术。中心围绕网络空间安全的研究开发和产品创新、技术辐射和成果产业化等方面开展了卓有成效的工作，建设了密码算法设计与安全性检测平台、网络与信息系统检测与攻防技术研究平台、互联网内容安全综合监管平台、电子政务安全应用支撑服务平台、面向新一代信息网络技术的网络空间安全教育与工程实践平台及网络空间安全社会化服务咨询平台等研发平台。

2024年中心继续承担国家重大信息化工程项目研发和建设，其中包括：国家重点研发计划、国家自然科学基金重点和重大研究计划、国家自然科学基金面上基金、国家自然科学基金青年基金、科技创新2030等300余项国家级、省部级科研和产学研合作项目，实现年新增承担项目合同额2.4亿元，年到款总金额1.38亿元，获省部级科研和教学类奖项5项。在IEEE TIFS, IEEE TMC, ACM MM, WWW, AAAI等顶会顶刊发表论文106余篇，在三大密码会议、四大安全会议上发表论文14篇，新增高被引论文2篇。出具技术和咨询报告321份，报送研究报告/专报/文章17篇，其中报告(专报)被采纳3篇，1篇获市委领导批示。新增行业标准（中华人民共和国法院行业标准）3项，地方标准申请1项（第二轮送审），新增团体标准申请2项。获得国内授权专利56项，登记软著16项，编写专著1本，教材2本。中心突破了一系列核心关键技术，形成的网络空间安全管理与服务科研成果支撑核心合作企业实现年销售额过亿，产生良好的经济和社会效益。相关成果在上海格尔软件股份有限公司、智巡密码(上海)检测技术有限公司、新疆数字证书认证中心等企业得到了广泛应用，为国家信息安全、能源、金融等行业的网络安全保障提供有力支撑。本年度代表性成果包括：

1. 内容安全重大工程应用平台

全面支撑多媒体信息智能分析等基础科学问题攻克，提升上海全球科创中心网络社会及特大型城市维稳能力，对接服务网信、公安、军队、安全等部门。持续优化更新全球全网舆情监测预警重大工程平台，突破人工智能认知对抗大模型能力，支撑国家网络空间认知对抗战略需求。服务宣传部门网络认知对抗、网信部门舆情监测预

警、公安部门网络社会维稳与安全部门网络情报分析；支撑中国城市治理研究院、YL学研究院等上海交大一级智库推进资政建言工作：面向国家/地方重要部委年均输出近500份网上情报信息决策支持报告。

2. 军民融合主动安全防御技术

全面支撑APT威胁检测、高隐蔽未知攻击检测、木马病毒检测关键技术研究，构建空天地一体的网络攻击检测与主动防御系统。研制储备网络空间主动防御工具和能力，形成战略级威慑力量：为有效捍卫网络空间国家边疆，工程研究中心常年扎根“隐蔽”战线，建设网络漏洞库（超过20万条）、指纹库（1.6万条）和社工库（近4.3亿条）等基础特征数据库平台，应用各类型操作系统脆弱性分析，以及与合作单位（科来网络）共同实现的75%已知网络及工业控制系统通信协议分析成果，YK超过500个境外关键信息基础设施及高防范联网终端，服务国家ZZ部队、AQ部门核心QB中心持续输出对A、对T国防及政经QB。

3. 关键信息基础设施安全检测评估平台（靶场）建设

服务国家/区域关键信息基础设施网络拟态仿真与虚实重构、网络攻击行为追踪溯源等基础科学问题研究，正在全面融入上海全球科创中心重大科技基础设施集群。重点突破了新型网络和芯片工艺环境下密码攻防技术，打破国外密码安全检测技术垄断。金融科技靶场与区块链安全分平台重点攻关关键信息基础设施网络拟态仿真与快速重构、网络攻击行为追踪溯源等基础科学问题，构建金融网络靶场验证测试环境、关键信息基础设施复杂网络环境仿真重构能力、网络安全靶场攻防演练能力，打造国内首创建设金融科技靶场与

区块链安全分平台，同时提升关键信息基础设施网络安全产品相关检测与验证区域性服务能力建设。

二、成果转化与行业贡献

（一）总体情况

本年度工程研究中心持续推动网络空间安全科研成果转化，面向网信、安全、公安、机要、保密等国家重要部委实现网空安全保障综合服务。长期支撑政治安全、公共安全、国防安全、关基安全和数字中国等战略任务，重点服务于国家及地方网络社会舆情治理、关键基础设施及特大型城市网络安全保障。

工程研究中心创新模式开展与相关XX部委科研基地战略合作，贯彻落实总体国家安全观，与XX重要委办局合作建设部级网络空间安全高级研究中心，全面建设国家网络安全威胁情报重大工程平台，重点开展网上反QM及反JIAN防DIE核心支撑能力攻关，以及与公安、WJ、BM的创新合作。开展网络攻防对抗、未知威胁感知、应用安全检测等领域核心关键技术攻关，支撑形成网上反窃密及反间谍技术能力体系，保障我市乃至全国关键信息基础设施/重点单位网络空间安全；部校共建专业研究机构，突出业务需求引领和实战实效导向，进一步强化研究院产学研用一体化建设，全面支撑“互联网+”“网络强国”等系列国家战略，推动学校建设“国家安全学”一级学科。此外工程研究中心还主动对接主管部门下达的运行数据常态采集、高峰创新论坛主办等日常工作，承担以“数字政府安全运营”为代表的重大战略任务。

工程研究中心与上海公安共建部级“认知安全”科技创新平台，全

面服务特大型城市社会治理。中心对标国际AI独角兽建设网络情报分析与预警平台，全面支撑全球全网大数据主动获取、多媒体信息智能分析等基础科学问题攻克，提升上海全球科创中心网络社会及特大型城市维稳能力。

工程研究中心国内首创建设了行业科技靶场与区块链安全平台，服务国家/区域关键信息基础设施网络拟态仿真与虚实重构、网络攻击行为追踪溯源等基础科学问题研究，目前正在全面融入上海全球科创中心重大科技基础设施集群。此外中心还与上海霄元创新中心合作开展“太空安全检测评估平台”研究，支撑筹建国家实验室。工程研究中心还与国防大学共同开展“认知对抗”方向能力域研发与服务。

（二）工程化案例

（一）内容安全重大工程应用平台

中心科研成果已成功集成到上海市多个大型企事业单位信息中心、数据中心，全面支撑上海市十个区的网络安全态势感知与监测预警重大工程项目集成建设，并已协助我市政府、金融、钢铁等重要保护单位完成等级保护测评及相关整改工作，包括国家能源局华东监管局、上海市闵行区财政局、上海证券交易所、上海自由贸易试验区保税区信息中心、宝山钢铁股份有限公司电厂、陆家嘴国泰人寿保险等单位，有力支撑上海市特大型“智慧平安城市”绿色生态网络环境的建设。

（二）军民融合主动安全防御技术

中心贯彻落实总体国家安全观，在国内率先建立网上反窃密及反间

防谍技术能力体系，持续做大做强工程研究中心网络安全“国家队”品牌。中心常年建设网络漏洞库，累计报送漏洞12万+条。此外经上海教委批复，成立上海教育系统网络安全技术检测研究中心，支持教育部安全工作，建设漏洞报告平台，具体包括：分析学术外联XX，发现绕过国家信息关防系统安全风险，向教育部提供安全情报；建设教育漏洞报告平台相关漏洞信息，整合教育系统网络安全管理工作管理平台；培养网络安全人才队伍；组织开展网络安全培训；关注网络安全前沿动态开展创新研究。基于工程中心在网络安全漏洞共享和协同研究工作的贡献，教育部教育管理信息中心特致感谢信至上海交通大学，肯定了中心在教育系统网络安全监测预警与漏洞方面的优势和贡献。

（三）特大型城市网络安全态势感知与监测预警重大工程示范应用中心长期建设国家CNAS检测机构认可的，面向“云大物移智”及关键信息基础设施的等级保护测评重大工程平台。作为公安部等保测评推荐机构，本年度工程研究中心面向长三角地区能源、教育、民航、金融、政务等数十个行业、四百余家企事业单位提供“咨询-集成-测评-服务”全生命周期网络安全综合保障服务。

（三）行业服务情况

（一）对外技术咨询服务情况

工程研究中心对外咨询服务主要有等级保护测评与安全服务两大块。等级保护测评基于《网络安全法》的要求，对信息系统实施等级保护测评，以确保其符合相应安全保障要求。目前工程研究中心的测评实验室作为公安部授权、上海四家等级保护测评机构之一，对

上海地区企事业单位提供等保备案咨询、等保测评服务等，长期服务于政务、教育、金融、科技、能源、商业贸易、IDC、物流、酒店、民航、检验、汽车、医药等数十个行业。安全服务项目主要为企事业单位提供业务系统上线前的安全测评、渗透测试等安全服务，及时高效地为用户业务系统上线提供合规支持。

2024年度中心面向长三角地区数十个行业、四百余家企事业单位提供“咨询-集成-测评-服务”全生命周期网络安全综合保障服务，服务合同金额近4000万元。其中等保项目约2200万元，为300余个三级系统、100余个左右二级系统提供服务；安服项目1800万元左右，测评系统百余个。业绩相对比去年提升20%左右。中心一直严格按照等级保护测评的各项要求开展业务，人员整体技术水平能力较高，通过2024年CNAS检验机构资质现场审查和公安部2024年网络安全等级测评与检测评估机构服务认证年度监督审查。此外中心还通过上海市公安局多次飞行检查，并作为测评质量优秀单位应邀于在沪测评机构年终总结会上作经验介绍，获上海市通信管理局颁布的2024“磐石行动”优秀裁判单位奖。

2024年，经上海市教育卫生工作委员会批复成立上海教育系统网络安全技术检测研究中心，服务于教育系统网络安全，主要职能为：汇聚教育系统网络安全威胁情报；协助开展教育系统网络安全检查；做好教育系统网络安全监测信息通报等等。2024年5-6月教育部教育管理信息中心开展教育系统网络安全攻防演习，中心的团队成员充分发挥技术专长，深入挖掘安全风险，为提升教育系统网络安全防护水平作出了杰出贡献。

（二）对外技术培训情况

中心本年度继续面向上海市制造业、金融、交通、医疗、建筑工程、环保、互联网等重点行业，开展人工智能、网络空间安全、大数据等方面的专业技术培训，取得了良好的社会反响。

（1）持续打造交大“北外滩网络安全高峰论坛”品牌，在上海交大主办、网络安全技术研究院承办的第三届“北外滩网络安全高峰论坛”中，邬江兴院士、黄殿中院士、吴世忠院士、童小华院士作主旨报告，工程研究中心主任李建华、华为安全产品领域副总裁王峰等网络安全领域专家剖析了技术落地中的机遇挑战，为推动网络安全产业升级提供探索路径和宝贵思路。

（2）举办2024高校网络安全实战特训营，全国31所高校59名师生以及上海市有关部门17人参加，特训营设置了思政讲堂、大师面对面、攻防技战法分享、实战对抗指导、企业参观交流等多个环节，邀请了来自上海市委网信办、上海市公安局、公安部第三研究所等政府部门和科研机构，华为终端奇点实验室、腾讯科恩实验室、Offside Labs、深蓝DARKNAVY、长亭科技等知名企业，以及哈尔滨工业大学、上海交通大学的专家们与营员们展开交流，带领营员们从不同角度感受当前我国网络安全面临的挑战，了解最新的攻防对抗技术发展，提升网络安全实战技能。

（3）2024上海市专业技术人才和项目对接大会，工程研究中心开设“人工智能赋能新型工业化——智领未来 智造创新”论坛，面向国家和上海市专业技术人员开展培训。

（4）由上海市人社局支持，依托上海市专业技术人员继续教育基地（人工智能）开设2024高级研修班，设置《人工智能赋能新型工业化》和《AIGC设计生活》等课程，开展AI新知识、新技术、新方

法培训。目前已完成第一期和第二期建设，面向国家/地方重要行业及大中型国有/民营企业、政府，提供了上万人次的信息安全专业人才社会化培训。

（5）上海市青少年科普教育基地，2024年继续为来自全市50余所中学的近千名高中生提供网络安全科普教育，为国家和区域进行了有价值的网络安全青少年人才教育实践。工作站下辖四个实践点：上海集成电路科技馆实践点、上海交通大学附属中学浦东实验中学实践点、上海光明中学实践点、上海松江青少年活动中心（华实高中）实践点。通过高中学校推荐及学生自荐的方式，每年面向全市在籍高中生招收120名学员加入实践工作站实践学习。

（6）2024年国际青年学者论坛—网络空间安全分论坛，论坛通过在线会议形式，汇聚了来自康奈尔大学、约翰霍普金斯大学、印第安纳大学、新加坡国立大学、香港城市大学、纽卡斯尔大学、阿卜杜拉国王大学、清华大学、北京大学、中国科学院等全球优秀青年学者，共同探讨网络空间安全领域的前沿学科与交叉学科发展。

（7）由交大承办的中国密码学会2024年大数据与人工智能安全青年论坛，来自全国知名高校和研究机构的诸多专家学者，围绕大数据与人工智能安全领域的前沿研究成果与产业应用进展展开深度探讨。此外，论坛特别设置了青年学者职业发展交流环节，为青年研究者提供了宝贵的成长平台。

（8）由交大举办，为上海市全民数字素养与技能提升月进基层系列活动的网络安全科普展，展示了“警惕ChatGPT泄露敏感信息”、“安全使用手势口令”、“安全使用手机钥匙”以及“防范家用摄像头泄露隐私”等系列科普作品，希望网络安全紧密结合公众

生活实际需求与社会热点，进一步推进网络安全知识普及传播，提升全民数字素养、网络安全意识和防护技能。

（9）举办网络信息安全管理与服务教育部工程研究中心开放日&青年科技论坛活动，增强本科、研究生同学对网络空间安全学科主要科研方向和前沿学术动态的深入了解，促进师生交流和网安科技创新工作的开展，弘扬“守望初心、强国为民”的红E精神。

三、学科发展与人才培养

（一）支撑学科发展情况

工程研究中心探索科研基地支撑网络空间安全学科创新人才培养模式，继续开展“未来科学家”、“未来工程师”、“网络安全创新人才训练营”等计划。支持网络空间安全学科的课程体系、培养体系、实践体系建设，编写适用于网络空间安全学科教学新体系的系列教材，开发相应的教学实验平台，培养宽口径的网络空间安全复合人才。在通过“未来科学家计划”、“未来工程师计划”、“网络安全创新人才训练营”等方式培养国际顶尖水平的学术型人才，培育国内外知名的行业高端人才，发掘网络安全领域的各层次人才。

针对新工科背景下的人才培养需求，围绕实践创新、工程实训、演示验证、资源共享协同服务模式，提炼人才培养核心理念和方法，构建了完善的科研实践系统，创建了具有核心竞争力的科研攻关平台。由于网络空间安全涉及国家政治、经济及文化安全，密切关系到信息时代国家综合国力的比拼，西方发达国家已经采取了大量的国家扶持政策，在指定高校与研究机构发展网络空间安全学科。

网络空间安全的发展，在依托前述之相关学科发展的同时，也将为各类传统学科开辟新的研究领域，例如智能化多媒体信息融合识别技术、人工智能安全、车联网安全监测技术、区块链理论及应用、新一代密码研究的理论与应用、网络信息系统智能化态势评估与指数分析等。因此，网络信息安全管理与服务教育部工程研究中心的建设，将对网络空间安全、信息与通信工程、计算机科学与技术、自动控制与系统、应用数学、法学等学科的产生整体的促进，加快我国缩短与发达国家在网络空间安全学科上的差距，并将催生新的综合交叉学科。

2024年工程研究中心产教融合及教育教学持续推进，易平老师的人工智能安全原理获上海交大双一流校企合作课程培育项目，郭捷老师的数据库原理及安全、张爱新老师的编译原理入选MOOC课程，刘功申老师的自然语言处理前沿技术、王士林老师的机器学习等4门课程入选教育部-华为智能基座产教融合协同育人基地合作建设课程。

2024年2月中央网信办、教育部公布了新一期国家一流网络安全学院建设示范项目高校名单。上海交通大学继2019年入选国家一流网络安全学院建设示范项目后，再次入选。上海交通大学信息安全专业位列软科中国大学信息安全专业排名全国第1，密码学CS Rankings近十年来亚洲和中国排名均为第1。

（二）人才培养情况

本年度工程研究中心谷大武教授指导的博士生张云聪博士论文入选获得中国密码学会优秀博士学位论文，其学位论文围绕zkSNARK方

案的优化和设计，提出了新型的zkSNARK设计框架和工具，所提通用zkSNARK及查找论证协议在证明大小和验证效率上均达到了现有最优水平。研究成果包括高效易用的zkSNARK设计框架V0Proof，高效的零知识虚拟机内存验证方案Permex，以及证明大小和验证效率最优的查找论证方案Locq等。

在各类竞赛中学生们继续逐鹿群雄，共获特等奖1项，一等奖5项，二等奖3项，三等奖2项，2个季军，1个杰出方案奖。其中：在第七届强网杯全国网络安全挑战赛中荣获季军（高校排名第一），并荣获特等奖；第十七届全国大学生信息安全竞赛中获全国一等奖3项（作品赛），二等奖2项（技能赛1项、作品赛1项），三等奖2项（作品赛），王士林、邱卫东、李高磊3位老师获评优秀指导教师（作品赛）；第17届中国大学生计算机设计大赛中获一等奖；世界互联网大会乌镇峰会-全球AI大模型攻防挑战赛中LoCCS实验室“可信智能队”（学生：徐菲悦、喻宣然、杭晟、赵禹博，指导老师：王烁、贺超翔、孙士锋）表现优异，荣获大赛季军，并斩获“杰出方案奖”；第九届全国密码技术竞赛中获一等奖1项、二等奖1项；2024世界智能驾驶挑战赛-“天融信杯”信息安全攻防赛中荣获铜奖（指导老师：周志洪）。

研究生在网络攻防、物联网安全、嵌入式系统安全、6G安全等领域发表了多篇高水平论文。在CS Rankings列表国际会议论文14篇，在IEEE TIFS, IEEE TMC, ACM MM, WWW, AAAI等顶会顶刊发表论文106余篇，其中ESI高被引论文2篇。

为加强“一流网安”的建设与发展，培养网络安全领域的创新型人才，工程研究中心还开设了“开源安全奖励计划及学生创新资助计

划”，共设置“原创开源软件”、“开源漏洞挖掘”、“开源软件重写”以及“国内开源社区贡献”四个赛道，鼓励学生勇于探索、大胆实践，深度融合开源精神与创新理念。

（三）研究队伍建设情况

网络信息安全管理与服务教育部工程研究中心拥有一支年富力强的科研队伍，组建了一支具有较高工程化、产业化开发能力的多学科交叉的科研团队。中心主任李建华教授担任中国网络空间安全协会副理事长，教育部信息安全教学指导委员会副主任委员，国家“十五”863计划信息安全主题专家组首席/管理专家，中国网络空间安全协会人才培养教育工作委员会主任委员，上海市信息网络安全管理协会名誉会长，上海市信息化培训协会副理事长，上海市商用密码专委会名誉主任，上海市信息化专家委员会专家等职，在国内网络空间安全领域具有很高的知名度。中心14名学术带头人分别从事中心六大研究方向的研究工作，为相应方向的发展建设起到了突出的学术带头作用。

在人才引进方面，引进王烁、许强、黄林庆等青年教师7名。举办国际青年学者论坛，来自美国、法国、澳大利亚、香港、北京等境内外青年学者参加。袁晨等多名青年教师崭露头角，开始承担重大项目，例如陈力波获国家重点研发计划青年科学家项目，孔令和获国家自然科学基金国际合作，孙士锋获军科委项目等。

在自身核心成员培养与扶持方面，伍军教授入选国家万人计划科技创新领军人才，李建华、伍军、陈黎兴等人入选斯坦福大学全球前2%顶尖科学家，徐寒松入选上海市青年科技启明星计划，林夕、陈

黎兴等教师获职称晋升。谷大武教授获上海市技术发明一等奖，蒋兴浩教授获中国图象图形学学会科技进步一等奖，孔令和教授获中国电子学会科学技术奖青年科学家奖和上海市计算机学会科学技术奖一等奖，孙士峰副教授获中国电子学会科学技术奖自然科学二等奖和中国密码学会“密码创新奖”二等奖。孔令和教授荣获2023-2024年度高校计算机专业优秀教师奖励计划，刘功申教授荣获2024年度教育部-华为“智能基座”优秀教师称号，马进老师获得2024年首届电院课程思政教学设计展示活动优秀课程，吴鹏老师获得电院第八届青年教师教学竞赛一等奖等等。

四、开放与运行管理

（一）主管部门、依托单位支持情况

中心人员主要依托上海交通大学网络安全研究院和网络空间安全学院，凝聚了一支由多名国家级专家领军，111名拥有硕士以上学位的中青年专业科研人员，以及300余名硕士、博士研究生为主体的，国内最大规模的网络空间安全专业研究团队。这些都为网络信息安全管理与服务教育部工程研究中心的正常运行奠定了坚实的基础。

目前中心的运行支撑条件包括：上海交通大学张江科学园3号楼（使用面积近5000平米），中心根据自身功能定位对现有场地进行局部地改造和完善，形成了中心产业化开发基地、工程化服务基地和市场化运作窗口；上海交通大学闵行校区微纳网空综合楼五楼（建筑面积近660平米）、软件学院二楼（建筑面积近680平米），建设中心基础理论研究基地。中心使用面积共计6340平米。

2024年上海交通大学划拨科技创新专项资金60万，支持中心基本运营。

（二）仪器设备开放共享情况

为合理合规使用中心仪器，中心制定了固定资产管理制度，规范科学仪器设备的管理使用和开放共享，参照《国家科技资源共享服务平台管理办法》和《网络信息安全管理与服务教育部工程研究中心固定资产管理制度（试行）》，面向全社会开放共享科学仪器装备/设备。

中心主体建设密码与高性能芯片设计开发平台、网络防护性检测与攻防技术研究平台、全球全网内容安全综合监管平台、电子政务安全应用研发平台、面向新一代信息网络技术的网络空间安全教育与工程实践平台、网络空间安全社会化服务咨询平台等六大核心功能平台。由于承担大量信息系统安全等级测评服务，中心Web应用弱点扫描器、数据库弱点扫描器、远程安全评估系统等重点科学仪器设备年使用率达到88%以上。

中心于2021年重点建设了上海交通大学张江科学园人工智能网络安全创新平台。该平台旨在建设具有国际影响力、国内先进、对标美国NIST ITL和国内之江、鹏城等实验室的人工智能网络安全创新中心，在上海交大“双一流”建设项目的支持下，已初步建成网络情报分析与预警、金融科技靶场与区块链安全，以及智能网联安全检测等三大分平台，并进驻上海交大张江科学园，面向上海全球科创中心实现国际领先、国内先进的人工智能网络安全科研基础支撑环境开放共享。

网络情报分析与预警分平台主要集成全球全网多通道全媒体大数据主动获取设备群、全球领先的大数据仓储管理软件Cloudera Enterprise（美国），大数据融合分析引擎Splunk Enterprise（美国），“一带一路”沿线主要国家小语种智能翻译设备，以及多媒体信息智能分析专用设备群，正在全面支撑上海全球科创中心网络社会及特大型城市维稳能力提升，保障国家安全部门华东区域网上反窃密与反间防谍工作全面推进。

金融科技靶场与区块链安全分平台主要集成国内领先的金融科技安全靶场试制平台、区块链安全靶场试制平台，以及国际先进的互联网及设备性能和安全测试设备IXia PerfectStorm ONE（美国）、移动应用程序漏洞检测试制设备等大型专用设备，国内首创建设关键信息基础设施网络拟态仿真、虚实重构与攻击溯源科研支撑环境，正在全面融入上海全球科创中心重大科技基础设施。

智能网联安全检测分平台主要集成国际先进的汽车芯片安全检测套件Riscure（荷兰）、汽车固件二进制安全评估设备Cybellum V-Ray（以色列），以及V2X车路协同协议一致性与仿真测试系统Spirent（美国）等大型专用设备，率先打造国内领先的智能网联汽车车内零部件（软硬件）软件定义风险评估、未知威胁检测基础实验平台，正在全面支撑国内智能网联汽车综合测试国家示范区建设、填补国内空白。

（三）学风建设情况

中心在强调科研服务的同时，不忘师德师风建设，具体举措如下：

（1）中心所在党支部认真贯彻“三会一课”制度，定期召开支部

党员大会、党支部委员会和党小组会，按时上好党课，以党建为引领，推进师德师风建设，把师德师风作为评价中心团队素质的第一标准。

（2）开设专题党课，深入学习贯彻习近平新时代中国特色社会主义思想、习近平总书记关于全面深化改革的一系列新思想、新观点、新论断和党的二十届三中全会精神，加强党风廉政建设和党纪学习教育，把立德树人的成效作为检验中心一切工作的根本标准，把师德师风作为评价中心团队素质的第一标准，将社会主义核心价值观贯穿师德师风建设全过程。

（3）加大师德模范的宣传力度，大力挖掘并宣传“优秀教师”“师德标兵”等先进典型，宣传高尚师德，弘扬主旋律，增强正能量，在中心形成尊师重教的浓厚氛围，激发中心科研人员职业认同感和幸福感。

（4）组织制度规范。中心依托的上海交通大学出台系列相关政策，制定不端学术行为查处办法等文件，强化教师的岗位责任意识，促使教师教学活动规范化、制度化，形成严谨治学、从严执教的良好风气。

（5）中心成立国际化学术委员会，在进行国际国内学术交流的同时，还积极推进师德师风交流，借鉴国外先进的师德师风建设经验。

（四）技术委员会工作情况

2021年12月，工程研究中心技术委员会进行了换届，换届后技术委员会15人，其中技术委员会主任为何德全院士，其他技术委员为柴

洪峰院士、曾庆凯教授、谭成翔教授、谢方军研究员、陈晓桦研究员、蒋力群研究员、顾健研究员、贺 教授、李翔研究员、何大军总经理、夏晓玲教授、杨珉教授、方志军教授、丁岳伟教授。

2024年度网络信息安全管理与服务教育部工程研究中心技术委员会工作会议于2025年1月召开，技术委员会委员、工程研究中心管理团队、科研骨干列席会议，工程研究中心主任向技术委员会专家汇报了工程中心2024年工作总结和2025年工作展望。技术委员会专家对工程中心各方面的工作予以肯定，同时就基于AI的赛博空间未知威胁自适应安全主动防御、数据安全与隐私保护等具有国际影响力的分析理论及应用研究成果等多方面提出建议，希望中心在新技术发展和布局、关键技术成果转化等方面进一步深化发展。

五、下一年度工作计划

技术研发方面：在网络安全的前沿技术和应用技术等方面持续地展开科研工作。深化中心特色技术方向，聚焦拓展建设网络空间安全基础研究与应用科创新高地，服务国家网络空间安全2030战略。重点开展网络攻防对抗、未知威胁感应用安全检测等领域核心关键技术攻关，保障关键信息基础设施安全。以网络空间安全创新“桥头堡”的崭新面貌全面融入上海全球科创中心。

在成果转化方面：加强与产业的对接，服务政务、司法、金融等领域重大项目和工程。进一步深化国家AQ部网络空间安全高级研究中心合作建设工作，支撑形成网上反窃密及反间谍技术示范应用；持续支撑国家公安部门推进特大型城市网络安全态势感知与监测预警及重要信息系统等级保护测评工作；持续支撑国家JY密码部门

开展关键信息系统密码评测工作，基于市BM科技创新联合实验室，持续实现新时代BM科技能力创新；全面支撑央视和JW网信W/政工B，推进网络空间认知对抗核心关键技术能力攻关与重大工程平台建设

建设工作。

人才培养方面：根据科研基地的学术特色，加强专业导师团队的培训与提升，从培养目标和培养过程方面精细化培养流程，并尝试以项目为纽带的研究生校企联合培养模式，营造研究生培养的创新氛围，“做一流学问，育一流人才”。将进一步强化激励机制，加大高端人才的培养和引进，同时加强培养中心中青年领军人才。

社会化培训方面：加强产学研合作，依托中心开展网络空间安全“卓越工程师”人才培养。依托上海市专业技术人员人工智能继续教育基地，结合研究院和学院的师资、课程等优势资源，进一步建设优质课程、人工智能实践教学环境，继续面向全国和上海市人工智能、网络空间安全、大数据信息管理及技术人员开展院士讲座、全国高校师资培训及实战实训、高级研修班和急需紧缺人才培训班等培训服务。

国际交流合作方面：中心将继续拓展国际合作，并将进一步加强与美国国家标准与技术研究院NIST、加州大学伯克利分校、新加坡南洋理工大学、日本早稻田大学、日本国立室兰工业大学、日本国立产业技术综合研究所等的学术交流和科研协作，继续选派青年骨干科研人员到美国、日本等国做访问学者；并将通过中心已建立的海外留学生实习基地，持续招收海外留学生，扩大国际影响。

国内交流合作方面，将继续加强同复旦大学、国防科技大学、中科院信工所等国内知名院校和科研院所的交流与合作。积极推进网络

媒体内容智能分析与安全管控技术等研究成果的转化、转让和产品化。

团队建设和制度优化方面，将继续完善各项保障机制和制度，为中心团队提供更加专业的人才，实现团队实力和综合素养的全面提升。

六、问题与建议

无

七、审核意见

(工程中心负责人、依托单位、主管单位审核并签章)

工程中心负责人审核意见:

同意。

工程研究中心主任:



2015 年 3 月 28 日

依托单位审核意见:

已审核, 同意提交。



依托单位:

(单位公章)

2015 年 3 月 28 日

八、年度运行情况统计表

研究方向	研究方向1	密码算法设计与安全检测		学术带头人		谷大武
	研究方向2	网络与信息系统检测与评估		学术带头人		薛质
	研究方向3	公共安全行业管理与决策服务		学术带头人		潘理
	研究方向4	互联网信息内容安全监管服务		学术带头人		李建华
	研究方向5	新型网络综合安全管理与优化		学术带头人		过敏意
	研究方向6	网络安全态势智能感知与预警		学术带头人		邱卫东
工程中心面积	6340.0 m ²			当年新增面积		0.0 m ²
固定人员	111 人			流动人员		14 人
获奖情况	国家级科技奖励	一等奖	0项	二等奖	0项	
	省、部级科技奖励	一等奖	5项	二等奖	0项	
当年项目到账总经费	13865.0万元	纵向经费	9718.0万元	横向经费	4146.0万元	
当年知识产权与成果转化	专利等知识产权持有情况	有效专利	56项	其他知识产权	16项	
	参与标准与规范制定情况	国际/国家标准	0项	行业/地方标准	3项	
	以转让方式转化科技成果	合同项数	1项	其中专利转让	2项	
		合同金额	117.0万元	其中专利转让	117万元	
		当年到账金额	0.0万元	其中专利转让	0.0万元	

	以许可方式转化科技成果			合同项数	0项	其中专利许可	0项
				合同金额	0.0万元	其中专利许可	0.0万元
				当年到账金额	0.0万元	其中专利许可	0.0万元
	以作价投资方式转化科技成果			合同项数	0项	其中专利作价	0项
				作价金额	0.0万元	其中专利作价	0.0万元
	产学研合作情况			技术开发、咨询、服务项目合同数	261项	技术开发、咨询、服务项目合同金额	5276.0万元
当年服务情况		技术咨询		321次		培训服务	9206人次
学科发展与人才培养	依托学科(据实增删)	学科1	信息安全技术	学科2	数据安全与计算机安全	学科3	安全测评
	研究生培养	在读博士		138人	在读硕士		201人
		当年毕业博士		9人	当年毕业硕士		67人
	学科建设(当年情况)	承担本科课程	5872学时	承担研究生课程	1532学时	大专院校教材	2部
研究队伍建设	科技人才	教授	39人	副教授	37人	讲师	10人
	访问学者	国内		0人	国外	0人	
	博士后	本年度进站博士后		7人	本年度出站博士后		2人