

# 教育部工程研究中心年度报告

(2023年1月——2023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 21 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。

2023年中心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2.35亿元，年到款总金额1.28亿元。在IEEE Transactions on Computers, IEEE Trans. Dependable Secur. Comput., IEEE Transactions on Mobile Computing等顶级期刊，IEEE SmartNet、DSC、ICC以及IEEE WCNC等知名国际会议发表论文70余篇，新增高被引论文1篇。出具技术和咨询报告294份，参与编写重要技术标准1项，申请国外专利1项，获得国内授权专利30余项，登记软著2项。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(有限公司)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. 全球全网舆情监测预警重大工程平台

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，先后多次获得党和国家各级领导人的重要批示。

## 2. 军民融合发展信息内容分析与空间对抗技术

深入研究军民融合发展信息内容分析与空间对抗技术，支撑网络安全/国防安全保卫。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、指纹库和社工库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。

## 3. 加密传输与数字认证信息分析检测防护关键技术

长期致力于加密传输与数字认证信息分析检测防护关键技术研究，有力支撑国家重要信息系统数据安全保障。研制国内首套商用密码产品安全检测工具平台：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，全年承担全市近40%的党政机关重要信息系统密码应用评测工作。建设覆盖全市的电子政务内容失泄密集中监管平台：重点突破了大带宽高速传输信息内容分析技术，形成了网上内容失泄密智能化监管整体解决方案与系列工具产品。

## 4. 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

推进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，支撑国家关基系统安全保障。牵头推进特大型城市网络安全态势感知与监测预警平台顶层设计、规范制定与总体建设。本年度工程研究中心支撑网络管理部门通报预警949条网络安全隐患信息、应急处置17起中高危网络安全事件，顺利完成全国两会、进博会等40余次重要活动的网络安保任务。

## 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，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防谍技术能力体系，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。

工程研究中心还在国内率先建成国家级智能网联汽车信息安全研发与公共服务平台，全面支撑汽车软件定义风险评估、未知威胁感知等基础科学问题攻关，持续推动车联网信息安全测试工具与技术标准体系自主科研成果转化，成功通过汽车领域信息安全测试CMA认证，助力智能网联产业健康发展。中心参与国内智能网联汽车综合测试国家示范区的建设，填补国内空白。

## **（二）工程化案例**

### **（一）全球全网舆情监测预警重大工程平台**

该成果先后获评2023年世界互联网大会领先科技奖，CCF 科技成果奖技术发明一等奖，引领互联网内容安全综合管理产业发展。形成云网融合、内容驱动、协同共享体化解决方案，研制的九大类云网内容分发与主动防御工具装备，实现了高可靠内容分发、高可用网络安全和高可管内容安全。

### **（二）军民融合发展信息内容分析与空间对抗技术**

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。本年度工程研究中心与国家AQ部正式启动合作建设部级网络安全高级研究中心，选址校张江科学园3号楼，全面建设国家网络安全威胁情报重大工程平台；突出业务需求引领和实战实效导向

，共同开展威胁感知、网络对抗等领域技术攻关，进一步强化产学研用一体化建设，支撑上海交大建设“国家安全学”一级学科。

### （三）加密传输与数字认证信息分析检测防护关键技术

工程中心长期支撑国家发改委高新司、国家数据局开展网络及数据安全重大问题联合研究协作。“二十大”以来尤其是国家数据局成立后，国家发改委进一步强化网络及数据安全重大问题联合研究协作机制，加大对网络空间安全领域工程研究中心的管理力度。2023年工程研究中心向国家发改委高新司先后报送数据安全“苗倾潜”三性报告、态势分析报告及信息摘编报告各四份，并积极参与国家数据局数据安全保障技术能力对接及服务模式研讨工作。

（四）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，全年新增合同超3000万、进校经费超2800万。

## （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。

2023年度中心对外开展网络安全风险测评服务合同总金额2700万元左右，其中等保项目约2100万元，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600万元左右，测评系统96个。业绩相对比去年提升23%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2023年CNAS检验机构资质现场审查和公安部2023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2023“磐石行动”优秀裁判单位奖。

## （二）对外技术培训情况

中心本年度面向上海市制造业、金融、交通、医疗、建筑工程、环保、互联网等重点行业，开展了人工智能、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）2023年外滩大会“数据安全与隐私保护趋势及产业融合实践论坛”分论坛，论坛聚焦数据安全行业关键技术和产业动态，技术创新对隐私保护的挑战和动力，基于数据安全与隐私保护的现状等，与产学研等各界行业权威专家共同探讨数据安全与隐私保护的挑战和未来发展趋势。



（2）CSIG图象图形中国行活动，会议得到了高校师生和企业界工程师们的广泛关注，线上参会171人，线下参会40人。

（3）中国密码学会大数据与人工智能安全专委会成立大会暨2023年大数据与人工智能安全专题研讨会（CryptoAI 2023），本次活动受到社会各界广泛关注，到场参会人数超过160人，为来自学术界、工业界和政府机构的专家学者、行业精英、工程技术人员和在校研究生搭建了良好的交流平台，为共同探讨大数据与人工智能安全技术应用中的主要理论和现实问题，促进大数据与人工智能安全的产、学、研、用协同创新提供了便捷的交流机会。

（4）2023“中华武数杯”全国网络攻防精英赛，聚焦数字时代网络安全技术创新与人才培养需求，通过高水平安全竞赛带动高层次网络安全人才挖掘与引进，助力网络安全产业生态圈建设。

（5）2023年网络安全创新发展研讨会，聚焦“数智赋能新未来，应对安全新挑战”主题，深入探讨数字化与智能化时代下的网络安全挑战与应对策略。

（6）北外滩网络安全高峰论坛，聚焦“高位筑牢关基数网安全底座，高标保障高质量发展新格局”主题，持续打造“北外滩网络安全高峰论坛”品牌，邬江兴、陈纯、王小云、黄殿中等院士作主旨报告，网络安全领域专家、行业领军人物共200多人参会。

（7）网络安全学科基础知识导论-上海交大青少年网络空间安全实践工作站，为120余名高中生提供网络安全科普教育。

（8）CCF & ATEC首届全国大学生区块链安全隐私技术与创新应用竞赛，竞赛旨在促进区块链人才培养和区块链安全生态建设，提升大学生积极参与区块链技术应用与创新的兴趣，深化大学生对区块

链安全与隐私的认识。

### 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，直接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，例如美国专项投入在普渡大学进行的网络空间安全专业人才培养和在密歇根大学、卡耐基梅隆大学等大学进行的网络空间安全核心技术研究等。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、计算机科学与应用、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潘理教授和郑聪惠老师指导的研究生杨宇佳、张宇恬、姜来在IKCEST第五届“一带一路”国际大数据竞赛中表现出色，荣获国际三等奖。参赛队“Universe Future”创新提出了基于文本特征提取模块与图像特征提取模块提取多通道的领域知识，通过多通道知识融合实现虚假信息检测的方案。该方案能够有效地甄别互联网上的多模态虚假信息，具有较强实际应用价值。由孟魁老师指导，李坤玲、王婉钰和夏心雨三位同学斩获2023“太湖印记”全国大学生网络安全辩论赛全国冠军，荣获一等奖。由薛质教授、王轶骏老师、陈力波老师牵头组织的NSSL-SJTU战队，主力成员包括赵天成、李玉林等学生，在上海市通信管理局组织的“磐石行动”中获“优秀红方单位”和“最佳红方战果”两项殊荣。由

严晓峰、王相哲、董赫、王兆崴四位同学组成的战队荣获CCF & ATEC首届全国大学生区块链安全隐私技术与创新应用竞赛三等奖。由谷大武教授指导，张宁岳、陆稼琦、武飞三位本科生组成的队伍研发的“基于RISC-V的国际新标准典型算法优化”的团队作品，在第八届全国密码技术竞赛决赛答辩中斩获全国一等奖。由徐燕虹老师指导，刘弘庆、张嘉宁、黄峥三位同学以“多方协同PQC公钥密码算法实现”为题，以后量子签名Dilithium为基础，设计的两方参与的协同密钥生成与签名协议获第七届全国密码技术竞赛一等奖；李兆乐、周子 、陈锦涛同学和周恒成、张建超、张佳函同学分获二等奖和三等奖。陈博航、詹云帆和电子工程系朱烨等三位同学斩获国内首届“熵密杯”密码应用安全竞赛特等奖。由詹云帆、赵天成、陈司琪、庄轶哲4人组成的战队闯入由公安部指导的第三届“网鼎杯”网络安全大赛决赛，取得了决赛总分排名第二的好成绩，获得了银鼎杯、最佳防御奖、最佳突破奖等多项荣誉。

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。在亚密会论文接收目录中，共有7项研究成果被录用，此外1项研究成果被美密会录取，2项研究成果被欧密会录取，2项研究成果被四大安全会议之一ACM CCS录取。1项研究成果被IEEE S&P 2023录用，IEEE S&P 全称 IEEE Symposium on Security and Privacy是网络与信息安全领域四大安全会议之一，被认为是计算机安全领域的最高级别会议。

### **（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，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。

在自身核心成员培养与扶持方面，2023年度技术研发骨干孔令和教授荣获长江学者奖励计划，卢策吾教授获长江学者奖励计划和第五届“科学探索奖”，朱浩瑾教授获国家杰出青年科学基金项目支持，徐寒松助理研究员入选东方英才计划青年项目。中心主任李建华教授获评2023全球前2%顶尖科学家。此外，本年度中心引进助理研究员张晓涵等优秀青年人才，中级测评师、高级测评师等近十名工程技术人员。

## **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，91名拥有硕士以上学位的中青年专业科研人员，以及200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。2023年上海交通大学划拨科技创新专项资金100万，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，认真学习宣传贯彻习近平新时代中国特色社会主义思想，深入学习贯彻习近平总书记关于党的建设的重要思想，学习习近平总书记关于严肃党内政治生活的重要论述，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。

2023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2024年3月召开，技术委员会委员、工程研究中心管理团队、科研骨干列席了会议。技术委员会专家听取了工程中心2023年工作总结汇报和2024年工作展望，对工程中心在科研成果、标准研究、产业服务等方面的工作予以肯定。同时技术委员会专家就基于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、智能网联协同安全等具有国际影响力的信息内容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，为中心新一轮发展创造条件。

#### **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。

在成果转化方面：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技术能力攻关与重大工程平台建设工作。

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：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、北京邮电大学、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:



2025 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)

2025 年 3 月 28 日

## 八、年度运行情况统计表

研究方向	研究方向1	网络与信息系统检测与评估		学术带头人		薛质
	研究方向2	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	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5	密码算法设计与安全检测		学术带头人		谷大武
	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 <sup>2</sup>			当年新增面积		0.0 m <sup>2</sup>
固定人员	91 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	1项	二等奖	0项	
当年项目到账总经费	13068.0万元	纵向经费	8075.0万元	横向经费	4993.0万元	
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	30项	其他知识产权	2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	1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	200.0万元	其中专利转让	200万元	
		当年到账金额	200.0万元	其中专利转让	200.0万元	

		以许可方式转化科技成果		合同项数		1项		其中专利许可		2项	
				合同金额		0.6万元		其中专利许可		0.6万元	
				当年到账金额		0.6万元		其中专利许可		0.6万元	
		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		256项		技术开发、咨询、服务项目合同金额		4315.0万元	
当年服务情况		技术咨询		294次				培训服务		3000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	计算机科学技术	
	研究生培养		在读博士		106人		在读硕士			220人	
			当年毕业博士		4人		当年毕业硕士			79人	
	学科建设 (当年情况)		承担本科课程	2180学时		承担研究生课程		1312学时		大专院校教材	3部
研究队伍建设	科技人才		教授	34人		副教授	33人		讲师	12人	
	访问学者		国内			0人	国外		0人		
	博士后		本年度进站博士后			0人	本年度出站博士后			1人	