

# 教育部工程研究中心年度报告

(2022年1月——2022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。

2022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、国家基金重点、国家自然科学基金面上基金、国家自然科学基金青年基金等250余项国家级、省部级科研和产学研合作项目，实现年承担项目合同额1.43亿元，到款总金额6233余万元。在IEEE TMC, IEEE TNNLS, IEEE TPDSD等顶级期刊, ACM CCS、USENIX Security、NDSS、IEEE S&P以及WCSP 2022等知名国际会议发表论文50余篇。出具技术和咨询报告百余份，编写重要技术标准1项，获得授权专利40项，建设基础数据库2项，完成重要工程和产品的设计1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共建企业和合作企业实现年销售额过亿，产生了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、奇安信集团、北京瑞星网安技术股份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. 大规模网络安全态势感知与监测预警

大规模网络安全态势感知与监测预警是提高我国网络空间安全预警、对抗、反制的前提，亟需突破网络空间深度资源探测、高隐蔽未知攻击特征检测、网络安全事件精准溯源追踪、监测预警与应急处置等关键技术。基于该成果，提出了基于多源异构全流量大数据动态图计算的网路高隐蔽未知攻击检测发现方法，建立多空间、多场景下差异化智能防御模型，突破了网络攻击跨域协同防御难题。建立了层次化、多模态网络安全大数据关联分析评估体系，突破了网络空间广域资源探测、安全事件追踪预警处置技术，实现了以关键信息基础设施为代表的超大规模云网融合系统安全态势感知与监测

预警示范应用。

## 2. 网络媒体内容智能分析与安全管理

在大国博弈、俄乌冲突背景下，敌对势力不断向国内进行意识形态领域的渗透、煽动和策反，网络中重大政情、疫情、灾情方面的舆情信息泛滥、危害大、管控难，给国家政治安全、社会稳定、经济发展带来深层次风险，亟需研究网上信息内容精准鉴别、传播控制、监测预警及特定群体线索发现技术。网络媒体内容智能分析与安全管理构建了融合多模式匹配、语境关联、深度对抗学习的轻量级、细粒度多模态内容分析理解模型，基于集群运算架构突破了大尺度广域内容分发环境中的全流程监管与舆情监测难题；提出了面向以广域交互式内容分发为中心的信息传播群体行为分析方法、突破了基于群体聚集机理的风险群体发现技术，解决了网络媒体内容监管面临的风险群体及时发现与有效管控难题。应用推广全球全网多媒体内容安全管理技术，服务网信、公安、安全、科技、教育等国家及地方重要部门。

## 3. 网络攻防协同对抗与系统安全评测

随着人工智能、大数据应用技术的发展，以伊朗震网病毒攻击、乌克兰电网攻击为代表的网络攻击呈现组合式、智能化，潜伏深、强对抗等新特征，大规模网络攻击越来越频繁，关键系统/重要数据安全保障需求迫切，亟需研究网络攻击机理与协同防御，构建新型通信系统安全评测技术体系。网络攻防协同对抗与系统安全评测围绕攻防适配、增强推演与溯源定位等科学难题，融合边缘认知、孪生推演与关联反制，实现低资源场景中高隐蔽要求下的网络攻防协同对抗与主动防御理论技术创新。创新构建了新型通信系统“云-

管-端”安全评测体系，推动我国多场景新型通信系统安全检测装备自主可控，填补国内空白。

## 二、成果转化与行业贡献

### （一）总体情况

本年度工程研究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，顺利完成以党的“二十大”、“两会”和进博会为代表的40余次重要会议/活动网络安全，并已协助我市政府、金融、教育、交通等重要保护单位完成等级保护测评及相关整改工作，包括上海公安局嘉定分局、上海商学院、上海携程商务有限公司、上海市杨浦区大数据中心、上海铁路经济开发有限公司、施罗德交银理财有限公司等单位，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，为国家安全保障、城市数字化转型提供完备的网络安全基座。

工程研究中心定期面向上海市委办公厅、市教委党委直报点、中组部、教育部、科技部、上海市公安局、上海市XX局等部门提供互联网公开舆情/情报信息及暗网信息数据服务，同时支撑中国城市治理研究院、YL学研究院等学校一级智库推进资政建言工作，保障数字内容产业健康有序发展。工程研究中心建设的全球全网舆情监测预警重大工程平台面向全球超过200个国家近万个新闻、财经和社交媒体/APP及暗网空间实现政经国防情报搜索分析，面向国家/地方重要部门年均输出近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。

为推动国家级智能网联汽车安全检测平台建设，确保车联网新基建健康快速发展，工程研究中心依托国家智能网联汽车（上海）试点示范区和上海市制造业创新中心（智能网联汽车）牵头制定首个用于物联网安全监测与管理的国际标准IEEE 1451.1.5，为我国掌握物联网通信与安全规则的主导权和话语权奠定基础；初步建成国家级智能网联汽车信息安全研发与公共服务平台建设，突破车联网通信及数据安全检测难题。

## （二）工程化案例

### （一）上海特大型城域网安全态势感知与监测预警重大工程平台建设

牵头制定了区域网络安全保障技术标准规范，面向超大规模城域网创新构建网络安全事件监测预警、应急响应与快速处置技术体系：实现超过4000G城域网流量的全要素采集与实时监测，日均处理近1500万条网络攻击告警关联归并与网络安全事件识别预警。重点建设上海市及十个区的网络与信息安全信息通报中心，顺利完成以党的“二十大”、“两会”和进博会为代表的40余次重要会议/活动网络安保，实现国际APT组织对于国家重要部门、军工国企、金融科研机构及关键民营单位的攻击与窃密行径溯源取证与抵御反制，多次预警以土耳其“图兰军”为代表的国际黑客组织对于境内目标的攻击企图，为国家安全保障、城市数字化转型提供完备的网络安全基座。

### （二）全球全网多媒体内容安全管理技术

应用推广全球全网多媒体内容安全管理技术，服务国家安全部门情

报搜索分析、网信部门舆情监测预警及公安部门网络社会维稳与社会安全保障。支撑中国城市治理研究院、YL学研究院等学校一级智库推进资政建言工作：面向国家/地方重要部门年均输出近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。服务国家XX部门实现境外政治安全风险源头发现与管控：建设面向全球的开源情报分析和境外高风险人群识别与监测能力，在近年中美经贸博弈、新冠疫情溯源等事件中发挥重要作用。

（三）智能网联汽车网络安全管理体系建设及合规性测试关键技术

针对V2X车联网系统的“云、管、端”模式，从网络通信、业务应用、车载终端、路侧设备等方面分析V2X车联网系统面临的安全风险、对安全脆弱性和安全威胁进行分析与建模，构建形式化安全漏洞威胁知识库，开发面向车联网的主动、被动相结合的定制安全检测工具，研究车联网整体系统的深度风险分析的关键技术；面向云平台 and 典型通信业务应用场景，研究基于国密算法的V2X 车联网IPSecC、TLS等身份认证及密钥管理、机密性和完整性保护、抗重放保护的安全架构与安全机制，搭建示范验证系统平台；研究面向V2X车联网中的IPSecC、TLS等安全协议、PKI/CA证书系统的密码合规性、有效性及实现正确性检测、随机数质量检测等关键技术和工具，支持包括SM2/3/4在内的国密算法。工程研究中心在临港南桥科技城建立了智能网联汽车系统安全测试分析环境；建立了1套智能网联汽车系统安全漏洞库，包括漏洞编号、漏洞类型、漏洞评级、影响范围、漏洞成因、检测代码/方法，参考资料等，涵盖10类以上车载传感器和执行器、3类控制器、3类车载操作系统；研发完善的智能网联汽车系统密码产品监督检查工具集，涵盖10类以上的

智能网联汽车密码产品与含密信息部件与产品；形成测评规范草案1份，包括引用标准、测评项目、测评方法、测评工具、评价准则等；交付相关软件模块3组；并完成申请发明专利和/或软件著作权总数8项。

### **（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。

2022年度中心对外开展网络安全风险测评服务合同总金额1859万元左右，其中等保项目约1500万元，为100余个三级系统、80个左右二级系统提供服务；安服项目300万元左右，测评系统58个。业绩相对比去年提升14%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，并获得2022年度测评机构能力验证优秀单位。本次活动依据网络安全等级保护相关标准选取了安全通信网络、安全区域边界、安全计算环境和安全管理中心等四个方面的内容，采用交互式实操配置检查、证据型场景配置



分析和实战化典型漏洞验证三种方式进行考核。

## （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、大数据等方面的共计约3200人次的专业技术培训，取得了良好的社会反响。

（1）《“智”造未来——AI赋能智能制造》高级研修班，为上海市人工智能、计算机、大数据、网络信息安全等相关行业领域政府机构、企事业单位中具备中高级专业技术职务（或职称）的专业技术人员/管理人员开展培训，112人参加；

（2）《数字经济与城市数字化转型》高级研修班，为上海市人工智能、计算机、大数据、网络信息安全等相关行业领域政府机构、企事业单位中具备中高级专业技术职务（或职称）的专业技术人员/管理人员开展培训，111人参加；

（3）网络空间治理中国论坛-主论坛，从科技、哲学、伦理、法律诸方面聚焦人工智能并提供培训，297人参加；

（4）网络空间治理中国论坛-应征论文网上论坛，从科技、哲学、伦理、法律诸方面聚焦人工智能并提供培训，2261人参加；

（5）安全与可信的人工智能，为关注人工智能与安全、数据驱动安全从业者提供培训，39人参加；

（6）人工智能推动制造业高质量发展，为上海市智能制造、工业智能等相关行业领域的专业技术和管理人员提供培训，470人参加；

（7）北外滩网络安全高峰论坛，网络安全领域专家、行业领军人

物共150多人参会；

（8）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。

（9）2022年国际编码与密码会议，展示和探讨编码与密码学领域的前沿发展和最新成果，140人参加；

（10）CSIG在线学术研讨会，大会共邀请了7位国内数字媒体取证领域专家，面向CSIG全体会员、国内外高校学生以及企业工程师等群体，来自全国的共计300余位学者、学生、企业人员参会。

### **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，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。

## **（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夏雯雯和助理研究员王更博士等在后量子密码基础问题研究取得最新进展，成功破解了80维的LWE问题公开挑战，创造了格密码中新的困难问题求解世界记录。

许可副研究员带领4名学生组成SJTU-ICL战队参赛在开放集合防御赛题（Track II）中获得第2名的好成绩，在全球高校战队中排名第一。第六届“强网杯”全国网络安全挑战赛上海交通大学0ops战队网络空间安全专业的庄轶哲、肖轩淦、朱君敏三位同学摘得强网冠军。第十五届全国大学生信息安全竞赛网络空间安全专业学生获

得了全国一等奖2项，二等奖1项，三等奖3项，谷大武、李高磊两位老师获得了优秀指导教师奖。2022字节安全AI挑战赛黄征老师带领2名学生组成Anya战队参赛并夺得冠军。2022全国大学生网络安全辩论赛中孟魁老师指导的“饮水思源”队荣获大赛一等奖，梅皓琛同学获“最佳辩手”称号。“磐石行动”2022年上海市电信和互联网行业网络安全攻防演练活动中由薛质教授、王轶骏老师、陈力波老师牵头组织的NSSL-SJTU战队，包括赵天成、李玉林等学生，获得唯一的“最佳红方战果”称号。2022数字中国创新大赛网络安全赛道车联网安全场景挑战赛，周志洪老师带领的团队获学科竞赛二等奖。

研究生在网络攻防、物联网安全、数字孪生安全、6G安全等领域发表了多篇高水平论文，代表性的论文有：IEEE Transactions on Industrial Informatics (SCI一区，物联网领域顶刊，ESI高被引)；IEEE Transactions on Dependable and Secure Computing (SCI一区，网络与信息安全顶刊)；IEEE Transactions on Mobile Computing上 (SCI一区，移动计算领域顶刊)；IEEE Transactions on Intelligent Transportation System (SCI一区，智能交通领域顶刊)等。

与美国国立产业技术综合研究所、美国天普大学、加拿大麦克马斯特大学、日本室兰工业大学、英国南安普顿大学等高校和科研机构在边缘计算安全、物联网安全等领域有深入的合作。

与北京瑞星网安技术股份有限公司、格尔软件、华为技术有限公司在比特币监测、能源网络安全、移动安全、软件安全等领域展开了产学研合作。

### **（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，2022年度技术研发带头人郁昱教授荣获第十七届中国青年科技奖，中心主任李建华教授获评2022全球前2%顶尖科学家。此外，本年度中心引进助理研究员徐寒松、郑聪惠等优秀青年人才，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，85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）、徐汇校区机械楼（建筑面积近2300平米），建设中心基础理论研究基地。中心使用面积共计8640平米。2022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，在我校“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，正在筹备进驻我校张江科学园，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，认真学习宣传贯彻党的二十大精神，以习近平新时代中国特色社会主义思想为指导，深入学习贯彻习近平总书记关于教育的重要论述和全国教育大会精神，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。

因疫情影响，2022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2022年12月29日通过腾讯视频会议（ID：426363011）在线召开，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2022年工作总结汇报和2023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以ChatGPT为代表的大模型AIGC人工智能技术的网络空间安全、以俄乌网络空间情报战威胁情报共享等等多方面提出建议，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：系统输出基于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，强化国家/区域网络空间安全保障技术支撑能力；贯彻落实总体国家安全观，与国家XX部共同构建网上反窃密及反间防谍技术能力体系并率先在我市实现示范应用，持续支撑我市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保测评整改工作，支撑我市XX密码部门开展关键信息系统密码评测，支撑国家XX研究中心华东分中心落地上海。

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	公共安全行业管理与决策服务		学术带头人		潘理
	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	密码算法设计与安全检测		学术带头人		谷大武
	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	8640.0 m <sup>2</sup>			当年新增面积		0.0 m <sup>2</sup>
固定人员	85 人			流动人员		20 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	0项	二等奖	0项	
当年项目到账总经费	6233.0万元	纵向经费	2489.0万元	横向经费	3744.0万元	
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	40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	1项	
		合同金额	5.0万元	其中专利转让	5万元	
		当年到账金额	5.0万元	其中专利转让	5.0万元	

		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		235项		技术开发、咨询 、服务项目合同 金额		3544.0万 元	
当年服务情况		技术咨询		222次				培训服务		3200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		130人		在读硕士			290人	
			当年毕业博士		5人		当年毕业硕士			76人	
	学科建设 (当年情况)		承担本 科课程	3248学时		承担研究生 课程		1328学时		大专院校 教材	
研究队 伍建设	科技人才		教授	29人		副教授	32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			0人	本年度出站博士后			1人	