附件 5

“网络空间安全治理”重点专项
2021 年度项目申报指南

为落实“十四五”期间国家科技创新有关部署安排，国家重点研发计划启动实施“网络空间安全治理”重点专项。根据本重点专项实施方案的部署，现发布 2021 年度项目申报指南。

本重点专项总体目标是：围绕全球网络公害、涉及民生的数据资产和“新基建”基础设施等领域的安全挑战，开展互联网基础设施、数据、网络公害、新技术新应用领域安全治理的战略性、基础性、前沿性研究，到 2025 年力争打造自立自强的网络空间安全治理技术体系，形成中国特色的网络空间安全治理方案，支撑“共建、共治、共享”的网络空间命运共同体建设。

2021 年度指南部署坚持需求牵引、问题导向、强化基础、引领前沿的原则，围绕互联网基础设施治理、网络空间数据安全治理、网络公害与内容治理及新技术新应用安全治理等 4 个技术方向，按照基础前沿技术、共性关键技术，拟启动 15 个项目，拟安排国拨经费 2.55 亿元。其中，拟部署 5 个青年科学家项目方向，每个方向支持 2 个项目，拟安排国拨经费 3000 万元，每个项目 300 万元。

项目统一按指南二级标题（如 1.1）的研究方向申报。每个项

目拟支持数为 1~2 项，实施周期不超过 3 年。申报项目的研究内容必须涵盖二级标题下指南所列的全部研究内容和考核指标。基础前沿技术类项目下设课题数不超过 4 个，项目参与单位总数不超过 6 家，共性关键技术类和示范应用类项目下设课题数不超过 5 个，项目参与单位总数不超过 10 家。项目设 1 名负责人，每个课题设 1 名负责人。

青年科学家项目（项目名称后有标注）不再下设课题，项目参与单位总数不超过 3 家。项目设 1 名项目负责人，青年科学家项目负责人年龄要求，男性应为 1983 年 1 月 1 日以后出生，女性应为 1981 年 1 月 1 日以后出生。原则上团队其他参与人员年龄要求同上。

指南中“拟支持数为 1~2 项”是指：在同一研究方向下，当出现申报项目评审结果前两位评价相近、技术路线明显不同的情况时，可同时支持这 2 个项目。2 个项目将采取分两个阶段支持的方式。第一阶段完成后将对 2 个项目执行情况进行评估，根据评估结果确定后续支持方式。

1. 基础前沿技术

1.1 抗量子计算的加密体系及安全机理研究（青年科学家项目）

研究内容：针对量子计算对传统密码体系的威胁，研究公钥密码算法经典数学困难问题的传统计算和量子计算算法；研究抗量子计算公钥加密、密钥封装、密钥交换、数字签名算法的设计理论与分析技术；研究抗量子计算密码算法的安全性；揭示对称

密码算法组件抗量子计算攻击的安全机理，刻画抗量子计算对称密码算法的安全强度。

考核指标：密码算法在电子计算和量子计算下的安全强度不低于128比特，给出具体参数选取下密码算法的电子计算和量子计算下的安全强度；设计抗量子密码算法≥10个，开发提供抗量子计算公钥加密、密钥封装、密钥交换、数字签名等功能齐备的开源库；申请国家发明专利≥20件，其中国际专利≥3件，获批密码行业标准或国家标准≥3项。

有关说明：青年科学家项目，支持2项。

1.2 隐私计算及安全保障基础理论研究（青年科学家项目）

研究内容：围绕建立体系化的隐私计算及安全保障理论，形成数据处理全流程的隐私保护能力，研究面向隐私信息采集、发布、共享等阶段的隐私计算及安全保障模型；研究多维度隐私信息形式化描述方法、隐私信息的智能感知技术；研究保护效果与数据可用性平衡的高效数据采集隐私保护技术；研究跨系统数据统计、查询、发布的隐私保护技术；研究隐私信息延伸控制、销毁与取证溯源监管机制；研究场景适应的隐私动态度量与隐私保护效果评估技术。

考核指标：提出不少于5类数据采集本地差分隐私保护机制和信息率失真隐私保护机制；提出不少于5类跨系统数据发布和查询统计的扰动、脱敏混淆等机制；提出跨系统转发行为的延伸控制和隐私侵犯行为的审计监管机制；开发隐私动态度量与保护效果评估工具集，支持不少于5类的隐私保护算法保护效果评估。

有关说明：青年科学家项目，支持2项。

1.3 面向去中心化网络的信任模型与密码算法研究（青年科学家项目）

研究内容：针对去中心化网络中身份互认困难、共识性能要求高、核心密码算法缺乏设计与分析的问题，研究去中心化内生信任建立与跨域管理技术；研究去中心化网络共识机制设计与分析方法；研制去中心化网络节点身份管理系统；研究面向去中心化网络应用的加密算法和数字签名算法；研究去中化网络安全评估模型与主动动态防御方法；研究去中心化网络节点的身份可信认证与授权技术。

考核指标：设计满足大规模去中心化节点信任管理的轻量级信任模型1个；提出至少1种新型节点共识算法，共识节点数超过200个，事务处理时延小于800ms；设计至少1种适用于去中心化网络的新型加密算法和数字签名算法，单核验签处理速度大于40000次/秒；构建一套去中心化网络安全评估模型，提出一种去中心化网络主动动态防御方法；研制一套软硬件自主可控去中心化网络节点的身份管理系统，支持每秒签发可信凭证大于100000个，支持亿级可信凭证管理。

有关说明：青年科学家项目，支持2项。

1.4 面向网络公害治理的知识图谱构建理论研究（青年科学家项目）

研究内容：针对新型匿名化网络公害源头发现难、取证难、

溯源难等问题，研究网络公害的多模态信息抽取技术；研究基于公害威胁数据时态特征的知识图谱构建方法；研究适合网络公害治理的知识图谱存储方法；研究基于图挖掘的公害源关联分析方法；研究匿名网络公害行为主体画像及个体影响力分析模型；研究主体行为预测、特定群体公害行为预测的技术；研究面向特定公害行为群体的画像追踪技术。

考核指标：实现 1 套数据规模在 TB 级别的公害威胁知识图谱系统，支持 10 种以上的异构数据输入，支持亿级以上的图数据查询和机器学习处理，支持近实时的数据更新；设计实现公害源关联分析模型和策略不少于 3 项；可发现网络公害行为的匿名化手段不少于 2000 种，匿名网络公害行为主体刻画准确度达到 95%，匿名化网络公害主体源头定位精确到城市级别，主体行为预测准确度达到 90%；支持不少于 10 种特定群体公害行为类型，且每种群体公害行为预测成功率达到 80%。

有关说明：青年科学家项目，支持 2 项。

1.5 人工智能安全防御及评估技术（青年科学家项目）

研究内容：研究偏见等定向、非定向风险，突破人工智能模型脆弱性分析理论基础，设计面向数据和模型的检测、防御方法；突破鲁棒性人工智能核心理论，设计对抗训练、网络蒸馏等人工智能模型防御方法；研究面向神经网络模型的复制、破坏、非法分发等行为的防御手段；研究面向人工智能模型的安全性评估体系，突破人工智能可解释性难点，研发模型的可信性、公平性、

鲁棒性与可解释性评测工具。

考核指标：提出人工智能模型脆弱性分析、鲁棒性分析与可解释性评测核心理论体系；提出不少于5种针对分类器威胁的检测和防御方法、不少于3种面向数据和模型的去偏方法、不少于5种鲁棒性人工智能算法、不少于3种人工智能模型安全完整性认证和盗版溯源方法、不少于5种人工智能模型安全性评测方法；支持不少于3种常用开发框架、上亿级神经网络参数的规模化安全防御与评估。

有关说明：青年科学家项目，支持2项。

2. 共性关键技术

2.1 纳米级芯片/硬件综合安全评估技术

研究内容：围绕纳米级处理器集成电路、微体系结构和芯片三个层面的硬件安全需求，研究微体系结构逆向工程技术和底层固件代码读取技术；研究处理器硬件脆弱性检测技术；研究具备验证权限正确性、数据完整性、信息私密性等的漏洞测评方法；研究能够与功能性电子设计自动化流程有效融合的安全验证方法及量化评估体系；研究面向白盒测试的芯片设计代码加速仿真与设计结构安全检测。

考核指标：支持不少于5类主流芯片厂商的处理器芯片的安全测试，支持对处理器微体系结构设计的批量形式化安全检测，可覆盖已发现的主要硬件安全漏洞；支持Verilog和VHDL两类设计语言的白盒测试加速仿真与设计结构安全检测，具备基于形

式化模型实现设计中时间、能量和电磁侧信道检测的能力；芯片层反向码点提取技术支持纳米级空间分辨率，底层固件代码读取技术支持微米级空间电磁能力和亚微秒级时间分辨率。

2.2 互联网源地址验证表的分布式生成协议及设备研发

研究内容：针对当前互联网体系结构缺乏源地址验证体系的问题，研究自治域内部的源地址验证表分布式生成协议；研究自治域之间的源地址验证表分布式生成协议；研发高性能路由器，实现基于源地址验证表的源地址验证功能，实现源地址验证表的分布式生成协议。

考核指标：支持源地址验证表的分布式动态生成；支持路由不对称和多路径路由场景下的源地址准确验证；自治域内部的源地址验证表生成协议支持路由环路检测；自治域之间的源地址验证表生成协议的通信开销不高于边界网关协议（BGP，Border Gateway Protocol）；提交 IETF 标准草案 3 项以上；路由器单槽位交换容量不低于 1.8T，单机端口交换容量不低于 36T。

2.3 高性能可扩展的资源公钥基础设施关键技术研究

研究内容：针对当前资源公钥基础设施（RPKI）存在的同步开销大、难以设置最长前缀长度、难以保障路径通告正确性等问题，研究 RPKI 的高性能数据同步方法，提高 RPKI 的可扩展性；研究 RPKI 最长前缀设置方法；研究 RPKI 根证书和授权单边撤销、删除、重写和增加的应急响应与主动防御技术；研究 RPKI 的路径验证技术；研究 RPKI 的路由策略验证技术。

考核指标：RPKI 资料库支持依赖方在分钟级别增量同步所有资料库，并保证依赖方对 RPKI 资料库视图的一致性；最长前缀设置既能支持灵活的流量工程优化，又能防范子前缀劫持；提出降低 RPKI 对 5 个信任锚依赖程度的新技术，有效降低 RPKI 根证书和授权单边撤销、删除、重写和增加的风险；通过同时支持源验证、路径验证以及路由策略验证，RPKI 对 BGP 路由劫持和路由泄露的有效防范率达到 95%以上；提交 IETF 标准草案 2 项以上；在真实网络开展试验验证。

2.4 开放环境下大数据安全利用研究

研究内容：针对当前开放环境中数据泄漏、恶意篡改、删除等问题,研究海量数据存储服务中的轻量级加密和安全存储理论，以及相应的安全高效存储、数据备份、高效数据同步技术；研究加密数据的高效安全检索技术，实现数据不解密情况下常用的数据检索操作；研究加密数据的高效计算技术，支持常用的数据运算操作；研究对平台数据、检索结果和计算结果的高效完整性验证技术；研究对开放平台的数据滥用监管技术，实现针对开放平台数据滥用的有效监管。

考核指标：实现至少对 1PB 数据的高效存储、备份和同步；设计至少三种常用的加密数据计算方法，并在标准安全模型下证明其安全性；支持亿级数据量的存储、检索和计算，检索时间在秒级以下，并能对计算结果进行有效验证；实现存储、检索和计算的全日志功能，开展示范应用，供第三方进行监管。

2.5 智能终端场景中移动应用的隐私检测和分析研究

研究内容：针对智能终端场景中移动应用隐私保护与监管面临的底层安全支撑能力薄弱和运行时检测缺失难题，研究移动应用的数据敏感性量化及隐私保护效果评估方法；研究恶意应用和应用恶意收集数据行为的有效检测和准确溯源；研究从单一恶意应用检测到恶意应用家族检测以及恶意应用开发者、发布者和传播渠道的整体生态的安全性；研究应用运行时的恶意收集和威胁发现技术；研发大规模移动应用隐私保护和检测平台。

考核指标：研制一套大规模移动应用隐私保护和检测平台，支持日活亿级的移动设备运行时检测；研制一套恶意应用家族检测系统和恶意应用开发者、发布渠道生态感知系统，支持不少于100 种恶意应用家族，覆盖恶意代码数量超 1000 万；研发一个大规模移动应用隐私保护和合规检测平台，支持定制检测、众包检测等检测方式；研发一套代码审计工具，能发现隐私和安全威胁不少于 10 种，数量不少于 20 个；在不少于三个现实业务场景开展应用示范。

2.6 隐私数据的个人权益保障研究

研究内容：针对个人数据被非法获取、交易和滥用等问题，研究个人敏感信息识别以及分类技术；研究公民个人采集信息的分散存储脱敏技术；研究针对个人敏感信息的监管技术；研究基于属性的个人信息保护和访问控制方法和理论，实现对个人信息扩散范围和使用期限的控制；研究数据删除技术，支撑公民对个

人信息的删除权。

考核指标：提出个人敏感信息安全分类标准，支持 10 类以上不同安全级别个人敏感信息分类和识别，实现至少对 100 万个个体敏感信息按照敏感级别进行分类，个人敏感信息识别准确率 90%以上；支持至少对 100 万人的个人信息进行拆分脱敏存储和信息重构，实现毫秒级内对单条个人敏感信息进行拆分和重构；研制一个个人敏感信息存储、管理和使用的综合性平台，提供对个人敏感信息监管服务，以及公民对个人信息的删除权和个人信息被使用的知情权等服务。

2.7 加密流量中网络公害检测与行为识别、处置研究

研究内容：针对加密流量中网络公害监管与分析难、行为主体溯源难等问题，研究网络公害行为在加密流量各粒度层次下的形式表征方法；研究新型加密协议的流量的检测、工具识别；研究加密流量分类与网络公害行为识别方法；研究加密流量中公害网页、图片和视频的识别方法；研究网络公害行为与主体的关联分析方法；研究针对性网络公害行为流量阻断技术。

考核指标：可支持单点网络流量带宽峰值不少于 100Gbps，TLS 1.3 协议全加密流量承载的移动 APP 应用识别种类不低于 300 种，误报率小于 5%，漏报率小于 5%；支持不少于 300 种常见加密应用分类，不少于 5 类网络公害行为分类与识别，时间不超过 2 秒，误报率小于 10%，漏报率小于 5%；实现网络公害行为与主体间的映射，主体数据库规模达千万级；加密视频识别需包含使用

多路复用技术传输的自适应流媒体视频，视频精准识别所需视频数据的播放时间不超过30秒，支持常见加密视频平台不少于10种，能精准识别40万个以上的视频，达到准确性不低于98%，误识率不高于1%，图片公害类型不少于5类，黑名单网页数量不低于十万个，同时访问加密网页的终端类型不少于5类。

2.8 智能驾驶汽车内部异构网络轻量化安全防护

研究内容：针对智能驾驶汽车内部异构网络安全防护严重缺失，传统安全方案受计算、带宽等资源限制难以有效实施的问题，研究面向嵌入式ECU的轻量化身份认证、消息加解密及密钥协商安全算法，研究安全系统资源占用轻量化技术；突破安全数据载荷的轻量化技术，减少由安全数据引发的报文帧增多及报文数据位占用；研究车载网络不同功能区域的安全等级划分、分域隔离及车载网络专用防火墙技术。

考核指标：车内时间敏感关键功能区域，数据加密处理与传输新增时延不超过5ms；安全防护相关应用占用运行内存不超过10%、占用存储空间不超过5%；安全数据载荷新增报文帧不超过10%、占用数据段不超过10%；车载网络支持多层级安全域划分，防火墙支持访问行为控制、危险操作阻断、可疑行为审计等；轻量化信息安全防护技术在不少于3款车型上开展应用验证。

2.9 基于国产密码算法的工控编程平台安全防护技术

研究内容：围绕工控系统典型共性安全问题，研究工控安全防护模型，构建基于国产密码技术的工控编程平台安全防护框架；

研究应用层代码、工程文件、操作记录、通信等加密技术；研究适配工业领域嵌入式平台运算能力的轻量级加密算法；研究编程平台应用层细粒度管控、运行态访问许可等认证技术；研究安全通信、静态可信认证、动态度量和身份认证体系。

考核指标：支持 IEC61131-3 规范，支持基于国产密码算法的标准总线协议栈加密，至少 5 种工业协议；可编程逻辑控制器（PLC）控制周期小于 10ms，IO 点数量大于 1000 点；支持不少于 5 种轻量级密码算法，加解密运算性能不低于 20Mbps；分散控制系统支持基于 SM2、SM3、SM4 的算法应用接口，支持通信加密、身份认证等功能，最小控制周期小于 50ms，输入输出点数量大于 10000 点。

2.10 智能网联场景工业控制系统深度防御与安全处置技术

研究内容：针对智能工厂高级持续威胁攻击防护难、溯源难等问题，研究 5G 融合场景下工业控制系统可信启动、动态度量、协同安全认证、商用密码加密通信等一体化安全协同防护关键技术；研究工业网络加密数据流特征提取、异常监测、深度入侵检测及工业通讯协议监测技术；研究智能网联工业控制系统功能安全与信息安全融合设计技术，构建智能工厂工业控制系统安全监测、预警与响应处置技术体系；研究石化、化工、电力等典型行业工业控制系统安全预警和应急响应机制，实现基于数据分析的安全处置。

考核指标：研发 1 套安全可信工业控制系统，支持 5G 网络

可信接入，支持输入输出信号点 10000 点，控制周期 20ms，达到信息安全等级 SL2 深度防御能力；支持至少 3 种工业控制系统网络检测，支持 35 种以上工业通讯协议监测，支持至少 8 类典型攻击异常监测报警，入侵检测的准确率到达 95%；支持至少 3 个行业的安全预警和应急响应方案；针对不少于 2 种重点行业 5G 应用场景中开展应用验证。