自主设置目录内二级学科论证方案

学位授予单位名称：南华大学

<table>
<tr><td>二级学科名称</td><td>网络与信息安全</td><td>二级学科代码</td><td>085412</td></tr>
<tr><td colspan="4">所属一级学科</td></tr>
<tr><td>代　码</td><td colspan="2">名　称</td><td>学位授权级别</td></tr>
<tr><td>085400</td><td colspan="2">电子信息</td><td>博士　□　硕士　☑</td></tr>
<tr><td>接受质询
联系电话</td><td colspan="3"></td></tr>
<tr><td>接受质询
电子邮箱</td><td colspan="3"></td></tr>
</table>

注：1.请填写相关项目，并在相应的“□”划“√”；

2.本方案将上网公示。

2025 年 10 月 12 日

一、该学科基本概况

（一）学科内涵

网络与信息安全是电子信息学科下的重要二级学科，聚焦于数字时代信息系统的安全防护、风险管控与可信交互，尤其强调在核工业等关键基础设施领域的特殊安全需求。其核心目标是保障网络空间中的数据机密性、完整性与可用性，同时应对日益复杂的网络威胁，在核工业场景中，还需确保核设施控制系统、辐射监测数据、核材料运输信息等关键资产的安全。该学科深度融合理论创新与工程实践，涵盖以下关键领域：

(1)密码学与应用加密技术

密码学是学科理论基础，涉及对称/非对称加密、哈希算法、数字签名等，为数据存储与传输提供核心安全支撑。现代研究更注重轻量级密码、后量子密码等前沿方向，以应对量子计算、核工业高敏感数据（如核反应堆控制指令、核材料库存信息）等新型挑战。

(2)网络安全体系与防御技术

包括网络协议安全、入侵检测系统、防火墙配置、零信任架构等，致力于构建多层次动态防御体系，防范 DDoS 攻击、中间人攻击、特别关注核工业工控系统（ICS）的协议安全等威胁。

(3)系统与软件安全

研究操作系统安全加固、软件漏洞挖掘、恶意代码分析、安全开发生命周期，确保从代码到部署的全流程安全可控；强化核设施操作系统的安全加固，针对核反应堆控制软件、辐射监测系统等关键应用，开展漏洞挖掘与恶意代码分析；建立核工业软件安全开发生命周期（SDLC），要求所有核设施软件通过形式化验证，确保代码无逻辑缺陷。

(4)数据隐私与治理

结合数据安全法与网络安全相关法规，研究匿名化技术、差分隐私、数据脱敏等，平衡数据利用与个人隐私保护，并涉及区

块链等分布式信任技术；研究核工业数据分级分类标准，对涉核数据实施“数据主权”管理，确保跨境数据流动符合国际核安全法规。

(5)云与物联网安全

延伸至云计算环境（如虚拟化安全、容器安全）和物联网终端防护，解决边缘设备脆弱性、云平台多租户隔离等新兴场景安全问题；研究核工业物联网的物理-网络融合安全，例如防止通过辐射传感器网络发起的数据篡改攻击。

(6)安全管理与法规合规

涵盖安全政策制定、风险评估、应急响应流程及网络安全法合规性研究，体现技术与管理结合的交叉特性；制定核工业网络安全政策，结合《核安全法》与《网络安全法》，开展核设施风险评估与应急响应演练；建立核工业网络安全事件通报机制，要求核设施运营单位与国家级网络安全机构实时共享威胁情报。

(7)人工智能安全与对抗样本

探索 AI 模型鲁棒性、对抗攻击防御、深度学习在威胁检测中的应用，应对智能化攻击带来的新风险；研究 AI 在核工业威胁检测中的应用（如通过机器学习识别异常辐射数据），同时防范 AI 模型被攻击者利用生成虚假控制指令以及核工业 AI 模型的鲁棒性测试方法，确保其在高辐射环境下的可靠性。

(8)社会工程与人文伦理

关注网络诈骗、钓鱼攻击等人为因素，并深入讨论数据主权、伦理边界及网络安全的社会影响，强化“技术－社会”协同治理；并关注核工业场景中的社会工程攻击。

该学科以计算机科学、电子信息工程、数学和法学为支撑，强调从硬件安全芯片设计到上层应用防护的全栈研究，旨在培养具备攻防兼备能力、能应对动态威胁环境的高层次人才。其发展直接关系到国家安全、数字经济稳定与公民权益保障，是数字化社会的基石学科之一。

（二）国内外设置该学科的状况和发展情况

（1）国际背景

进入21世纪以来，全球数字化进程加速，云计算、物联网、人工智能、大数据、区块链等新兴技术广泛应用于社会经济各领域。与此同时，网络攻击手段持续演化，勒索软件、供应链攻击、数据窃取、人工智能对抗等新型安全威胁层出不穷，网络空间安全形势日趋严峻。网络安全已成为维护国家安全、经济安全、社会稳定的重要基础，被广泛视为全球战略竞争的核心领域[1-2]。国际网络安全机构（ISC²）发布的《AI时代网络安全产业人才发展报告（2025）》报告显示，全球网络安全从业人员约为550万人，但仍存在约480万人的人才缺口；其中云安全、人工智能安全、零信任架构和关键基础设施防护等方向尤为紧缺[3-5]。全球缺口已扩大至480万人，表明供需矛盾长期存在[6]。这一结构性短缺说明网络安全教育体系的建设速度远落后于威胁演化速度，全球各高校纷纷加快安全学科体系布局。

美国、英国、澳大利亚、加拿大等国家的知名高校均设立了网络安全或信息安全硕士学位项目，建立了完备的课程体系与攻防实验平台。例如，卡内基梅隆大学开设了信息安全政策与管理硕士项目，强调技术与政策结合；英国牛津大学、伦敦大学学院等则建立了网络安全研究中心，以应对新型网络威胁[7-9]。国际经验表明，网络安全高层次教育是国家网络安全体系的重要支撑。

同时，新兴技术带来的安全挑战促使国际研究持续前移。AI安全、隐私保护计算、可信AI、大模型安全、量子密码、区块链安全等方向正成为未来网络安全研究的重点[10-11]。这些新领域的快速发展，要求研究生教育体系具备前瞻性与跨学科整合能力。

因此，从国际维度看，网络安全研究生教育既是国家安全战略的关键支撑，也是高校提升国际竞争力的重要方向。南华大学

计算机学院若能设立“网络与信息安全”硕士学位授权点，不仅可以与国际教育体系接轨，也能为我国参与全球网络安全治理贡献高层次人才。

（2）国内形势

我国高度重视网络空间安全，将其纳入国家总体安全观和数字中国建设战略之中。自2016年《中华人民共和国网络安全法》颁布以来，我国陆续出台《国家网络空间安全战略》《网络强国战略纲要》《数字中国建设整体布局规划》等政策文件，明确提出要加快培养网络安全专业人才，强化产学研用协同创新[12-13]。

工信部《网络安全产业人才发展报告》指出，全国网络安全从业人员短缺约为139万人，人才需求集中于人工智能安全、云安全、工业互联网安全、密码学与数据安全治理等新兴方向[14]。中国信息通信研究院发布的《网络安全产业白皮书》指出，2025年我国网络安全产业规模已超过2500亿元，年均增长率超过15%，但高端技术人才供给严重不足[15]。此外，《2025-2030年中国网络安全行业市场分析及发展前景预测报告》指出，随着数字经济规模扩大与数据要素市场化配置推进，网络安全已成为数字化转型的核心保障，而高级安全人才成为制约产业发展的瓶颈[16]。各省市陆续出台地方网络安全人才培养政策，鼓励高校加快设立研究生层次的安全学位点。

教育部《普通高等学校本科专业目录（2021年版）》已将网络空间安全列入一级学科，并明确鼓励高校根据国家战略需求布局相关学位授权点[17]。目前，国内已批准设立网络空间安全一级学科博士点的高校数量逐年增加，但中部地区硕士层次授权点仍然不足，区域分布明显不均衡。

此外，核工业网络安全面临技术与管理双重挑战：技术层面存在老旧系统、过时工业控制及定制协议风险，传统防护难以应对新型攻击；管理层面存在认知误区和人才短缺问题。政策上，

核动力厂网络安全技术政策等文件要求建立防御体系，2025 年新标准强化实战能力。核工业网络安全面临的实战挑战包括 AI 技术监管缺口、OT/IT 融合风险等，需通过零信任体系、模拟演练应对。与一般网络安全相比，核工业更注重功能安全与实时性，防护重点在工业协议解析，安全损失后果可能更严重。当前急需政策完善、技术创新和人才培养构建防护体系，持续应对技术迭代与威胁演化。

（3）南华大学区域使命

全球网络攻击事件年均增长率超过 30%，关键基础设施安全事件频发。AI 大模型、物联网、区块链等新技术带来新的安全威胁，传统防护体系难以应对。若高校教育体系不能及时更新，将面临“教育滞后于威胁”的严重问题[19]。欧美高校已普遍建立网络安全硕士及博士培养体系，中国部分顶尖高校（清华大学、北京邮电大学、电子科技大学等）也纷纷布局网络空间安全一级学科。南华大学若不及时布局，将在区域和全国层面的学科竞争中失去先发优势。

此外，湖南及周边地区网络安全产业规模正快速增长，但缺乏具备创新能力和工程经验的硕士层次人才。湖南省正处于“数字湖南”“智造强省”战略建设关键阶段，能源、制造、交通、医疗、教育等领域的信息化水平不断提高，对网络安全的依赖程度显著增强。与此同时，地方网络安全技术力量薄弱、人才供给不足的问题尤为突出。据《中国网络安全产业人才发展白皮书》数据，中部地区网络安全岗位需求占全国总量的近 15%，但本地人才供给仅约 8%，存在明显缺口[18]。

南华大学作为湖南省重点建设高校之一，计算机学院长期在计算机科学与技术、人工智能、软件工程等领域具有较好的学科基础与科研积累，已建有信息安全实验室、人工智能与大数据研究中心、智能系统研究所等科研平台，具备开展网络安全方向研究生培养的学科支撑。依托现有科研条件、师资力量与区域产业

基础，设立网络与信息安全硕士点可形成学科集聚效应，进一步提升学院科研竞争力和社会服务能力。

该硕士点的建设将服务于湖南省及中部地区网络安全人才体系建设，特别是在核工业网络、智慧城市、工业互联网、公共安全、金融科技、医疗信息系统等关键领域提供安全保障。同时，还能支撑南华大学在“软件+安全”“人工智能+治理”交叉方向上形成新的学科增长点，推动学校整体学科结构的优化升级。

参考文献

[1] 中华人民共和国全国人民代表大会常务委员会. 《中华人民共和国网络安全法》[S]. 北京: 中国人大网, 2016.

[2] 教育部学位与研究生教育发展中心. 新增博士、硕士学位授权审核申请基本条件[S]. 北京: 教育部, 2020.

[3] Cybersecurity Workforce Study. AI 时代网络安全产业人才发展报告[R], 2025.

[4] Boston Consulting Group. 2024 Cybersecurity Workforce Report[R]. Boston: BCG, 2024.

[5] National Institute of Standards and Technology. SP 800-181r1: NICE Framework Workforce Framework for Cybersecurity[S]. Gaithersburg, MD: NIST, 2020.

[6] Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity[S]. New York: ACM/IEEE, 2017.

[7] ENISA. The status of cyber security education in the European Union[R]. Heraklion: ENISA, 2020.

[8] IBM Security; Ponemon Institute. Cost of a Data Breach Report 2024[R]. Armonk, NY: IBM, 2024.

[9] World Economic Forum. Global Cybersecurity Outlook 2023[R]. Geneva: WEF, 2023.

[10] Ramezan C A. Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field[J]. Journal of Information Systems Education, 2023, 34(1): 94–105.
[11] A Curriculum Model of Cybersecurity Bachelor's Programs[J]. Journal of Information Systems Education, 2024, 35(3): 313–324.
[12] Prümmer J. A systematic review of current cybersecurity training methods[J]. Computers & Security, 2024.
[13] Alnajim A M, et al. Exploring Cybersecurity Education and Training Techniques: A Systematic Literature Review[J]. Symmetry, 2023, 15(12): 2175.
[14] Catal C, et al. Analysis of cyber security knowledge gaps based on online resources and curricula[J]. International Journal of Information Management, 2022.
[15] Vogel R. Closing the cybersecurity skills gap[J]. Salus Journal, 2016, 4(2): 32–46.
[16] 中研普华产业研究院. 2025-2030 年中国网络安全行业市场分析及发展前景预测报告[R]. 北京: 中研普华产业研究院, 2025.
[17] 工业和信息化部教育与考试中心. 网络安全产业人才发展报告[R]. 北京: 工业和信息化部, 2022.
[18] 工业和信息化部教育与考试中心等. AI 时代网络安全产业人才发展报告(2025)[R]. 北京: 工信部及联合编制单位, 2025.
[19] Microsoft. Microsoft launches campaign to fill 250,000 cybersecurity jobs [N]. Axios, 2021-10-28.
[20] Franqueira V N, et al. A systematic literature review on cyber security education and recommended curricula[J]. International Journal of Information Management, 2024.

（三）该学科的主要研究方向及研究内容

网络与信息安全强调“理论创新－技术突破－应用实践”的闭环，培养具备多学科交叉融合能力的高层次网络与信息安全人才。面向国家网络与信息安全战略和数字经济发展需求，聚焦人工智能、大数据、区块链等新一代信息技术与网络安全的深度融合，致力于解决智能时代下信息系统面临的可信性、动态性和协同性安全难题，主要可以划分为以下三个方向。

(1) 基于置信规则库的可信AI多模态决策理论与形式化验证

本方向旨在解决AI决策的“黑箱”问题和不可信难题，聚焦于让AI的决策过程变得可理解、可验证、可信任。

- 可信AI决策建模：深入研究置信规则库（BRB）专家系统，利用其半定量、透明化的特性，构建用于网络安全（如入侵检测、恶意软件分类、异常行为识别）的可解释AI决策模型。
- 多模态信息融合：研究如何将网络流量、系统日志、用户行为等多模态安全数据，有效转换为BRB的输入，通过证据推理（ER）算法进行融合与决策，提升决策的准确性和鲁棒性。
- 形式化验证：将构建的BRB模型转换为形式化模型（如时序逻辑、进程代数），利用模型检测、定理证明等工具，严格验证AI决策系统是否满足预设的安全属性（如“永远不会授予非法用户权限”）。
- 模型优化与自学习：研究BRB模型的参数与结构优化方法，并结合强化学习等技术，使模型具备在动态网络环境中自我演进、自我完善的能力。

(2) 多模态可信感知驱动的全域安全动态评估与智能决策

本方向侧重于宏观安全态势的把握，强调从被动防护转向主动、动态、自适应的安全治理。通过利用多模态可信感知、人工智能和大数据分析技术，构建覆盖核燃料循环全链条的动态安全监测、评估、预警与决策支持平台，为实现核能的高效、安全、

可靠发展提供关键技术支撑。

- 核网络安全与工控系统安全：专门研究核电站工控网络（如DCS、PLC）的协议安全、漏洞挖掘与入侵检测技术。分析针对“震网”类高级持续性威胁（APT）的检测与防御方法，构建面向核设施的数字孪生安全靶场，进行攻防演练和系统韧性测试。
- 核材料与废料管理的安全监控：针对核材料与核废料处理、运输、储存等环节，研究基于视频监控、射频识别（RFID）、无人机巡检与辐射探测数据的多源信息融合技术。利用计算机视觉和目标检测算法，实现对于异常、设备状态、封装体完整性的智能识别。结合区块链技术，确保核材料流转数据的不可篡改和全程可追溯。
- 核应急响应与智能决策支持：这是本方向的顶层集成应用。在发生应急工况时，基于前述研究，实时融合事故序列、辐射监测、气象条件、人口分布等多模态数据，利用动态贝叶斯网络、强化学习或案例推理技术，快速生成应急行动方案（如干预水平划分、撤离路径规划、救援资源调度）。并**利用研究方向一的可信 AI 与形式化验证技术，确保应急决策的合理性、可靠性与可解释性**。
- 多模态可信感知：研究从网络设备、终端、云平台、IoT 设备等全域节点，实时、可靠地采集流量、日志、性能指标、威胁情报等多模态数据，并确保感知数据的真实性与完整性。构建基于图计算、深度学习和知识图谱的动态威胁评估模型。分析攻击路径、关联攻击事件，并对潜在的安全风险进行预测性评估。

(3) 跨域数据安全流通的云链协同可信计算与动态防护

瞄准数据作为核心生产要素在流通中的安全与隐私矛盾，构建“数据可用不可见”的可信流通环境。面向多源异构、跨域共享的医学与生命健康数据，构建云-链协同的可信计算与动态防

护体系。依托南华大学软件工程学科优势、八所直属附属医院科研平台以及“湖南省医疗大数据国际科技创新合作基地”等科研条件，研究**人工智能技术与大数据技术在医学健康、生物学领域复杂问题中的应用与安全保障**。目标是实现医疗与生物数据在可信环境下的安全流通、智能分析与动态防护，为智慧医疗与健康中国战略提供安全支撑。

- 多模态医学数据智能分析与软件验证：依托附属医院科研平台与医疗大数据基地，重点研究医学影像（CT、MRI、病理切片）的智能分析算法，如基于深度学习的病灶检测、分割与分类。同时，关注基因组学、蛋白质组学、微生物组学等海量复杂生物数据的特征提取与关联分析。为确保这些分析软件的可靠性与安全性，将引入严格的软件测试与验证方法，确保智能算法在临床与科研应用中的准确、可靠与稳定。
- 跨医疗机构的数据联邦与协同学习：针对医疗数据隐私要求极高、分散在不同医院形成“**数据孤岛**”的现状，**研究基于联邦学习的跨医疗机构协同建模技术**。在不共享原始患者数据的前提下，联合多家附属医院的数据，共同训练更精准的疾病预测、疗效评估和用药推荐模型，推动医学研究的进步。
- 生物医学数据的安全共享平台构建：利用区块链技术，为临床研究数据、生物样本信息构建可信的安全共享与审计溯源平台。记录数据的使用授权、访问记录和计算任务，确保数据流转过程符合伦理规范且全程可追溯，促进科研数据的合规、高效利用。
- 核医结合领域的特色应用探索：这是体现南华大学独特交叉优势的关键。探索将核技术（如放射影像、辐射生物学）与医学人工智能相结合的特色研究方向。例如，研究基于深度学习的放射治疗计划自动优化、辐射损伤的早期智能监测与预警、放射性药物疗效的影像学生物标志物挖掘等。

可信 AI 提供了核心方法与理论，确保智能体的决策是可信

的。全域安全动态决策是宏观应用与体现，将可信 AI 应用于全域安全治理。跨域数据安全流通数据流通是关键场景与支撑，为前两者提供了安全可靠的数据基础和环境。

（四）该学科的理论基础

在网络化、数字化时代背景下，保障网络空间安全、维护信息安全已成为国家战略和经济社会发展的核心需求。网络与信息安全学科在此背景下应运而生并迅速发展。该学科的理论基础深厚且交叉，主要涵盖以下几个方面：

计算机科学与技术：计算机科学与技术是网络与信息安全的基石。它提供了计算机系统结构、操作系统、软件工程、算法与数据结构、程序设计语言等核心知识，为理解信息系统的运行机制、发现软件漏洞、构建安全可靠的软硬件平台提供了基本方法和计算工具。

密码学：密码学是网络与信息安全的支柱与核心理论。它研究信息在传输和存储过程中的机密性、完整性、认证性和不可否认性，涵盖了对称/非对称加密、哈希函数、数字签名、密钥管理、安全协议等关键领域，为构建可信的网络空间环境提供了数学基础和根本性保障。

网络工程与通信技术：网络与信息安全立足于对网络本身的深刻理解。网络工程与通信技术研究网络体系结构（如 TCP/IP 协议栈）、网络设备原理、数据传输机制、无线通信与移动网络等，为分析网络攻击路径、实施网络监控与防护、构建安全通信体系提供了技术基础。

信息对抗与系统安全：该领域聚焦于网络空间的攻防对抗实践与理论。它研究网络攻击的机理、方法与技术（如漏洞挖掘、恶意代码分析、渗透测试），以及信息系统与网络的防护、检测、响应与恢复技术（如入侵检测系统、访问控制、防火墙、安全审计），体现了学科的对抗性与动态发展特性。

数学与法律/管理科学：数学为密码学和复杂安全协议的设

计提供了严密的逻辑工具与复杂性理论依据。同时，网络与信息安全不仅是技术问题，更涉及法律、法规、标准与治理。法学（特别是网络空间安全法、数据隐私法）与管理科学（如信息安全管理体系、风险评估）为安全治理、合规性审查和安全策略的制定提供了制度与理论支撑。

网络与信息安全的理论基础是一个典型的文理渗透、工管结合的交叉融合体系，需要计算机科学、密码学、网络技术、信息对抗、数学、法学与管理学等多个学科的协同支持与持续贡献。

（五）该学科与其相近学科的关系

网络与信息安全是一级学科电子信息下所设立的二级交叉学科。该交叉学科深度融合了计算机、通信、电子、数学、法律、管理等多个领域的知识，旨在系统性地解决网络空间中的安全威胁与综合治理挑战。

一方面，它以密码学、计算机系统软硬件安全、软件工程和网络安全的最新研究成果作为有力的技术支撑；另一方面，立足于现有的多学科基础，旨在构建跨学科的研究平台，形成面向网络空间安全综合治理的新交叉与融合。该学科与“计算机科学与技术”、“信息与通信工程”和“密码学”等二级学科既有紧密的联系，又有显著的区别。

计算机科学与技术是网络与信息安全最核心的支撑学科，它关注计算系统本身的原理、设计与实现，为信息安全提供了运行的平台和实现的手段。然而，计算机科学更侧重于系统的“功能实现、性能提升与正确性”，而网络与信息安全则更侧重于在复杂对抗环境下，保障系统的“机密性、完整性、可用性、可控性与不可否认性”，其核心视角是“安全属性”。前者研究如何让系统“跑起来、跑得快”，后者研究如何让系统在面临攻击时“不被攻破、数据不丢、服务不中断”。

信息与通信工程为网络与信息安全提供了信息传输层面

的理论基础和技术支持，重点关注信号的编码、传输、交换、处理和网络的构建。网络与信息安全则在此基础上，重点关注信息在传输和交换过程中的安全威胁（如窃听、篡改、业务中断、路由欺骗），并设计相应的防护与检测机制。可以说，信息与通信工程致力于构建高效、可靠的“信息高速公路”，而网络与信息安全则负责建设这条公路上的“安保系统、交通法规和应急响应体系”。

密码学是网络与信息安全学科的核心组成部分和关键技术手段，但它通常作为一个更偏重数学和理论的基础学科方向。密码学主要聚焦于利用数学工具构建安全的密码算法和协议本身。而网络与信息安全学科的范围更广，它不仅应用密码学成果，还涉及如何将密码技术安全、有效地集成到复杂的计算机系统、网络协议和应用软件中，并统筹考虑系统安全、应用安全、安全管理、安全法律等诸多非纯密码学问题，是一个更加注重“系统工程”和“综合应用”的学科。

总之，网络与信息安全是一门以“安全”为核心视角，综合应用计算机、通信、密码学等技术，并融合法律与管理知识，以应对网络空间综合风险的综合性交叉学科。它的目标不仅是理解和构建基础安全组件，更是确保整个信息生态系统在复杂的对抗环境中能够安全、可信、合规地运行。随着数字化程度的不断深化，网络与信息安全的战略地位将愈发关键，成为保障国家安全、经济稳定和社会发展的基石性学科。

二、设置该学科的必要性和可行性

（一）社会对该学科人才的需求情况

网络与信息安全是国家安全体系和数字经济发展的重要支撑领域。随着人工智能、云计算、大数据、物联网和区块链等新一代信息技术的快速发展，网络空间安全形势日益复杂，社会对高层次“网络与信息安全”人才的需求愈发迫切。建设数字中国、网络强国和创新型国家，离不开具备智能安全防护、隐私保护与自主可控能力的专业人才队伍。我校设立网络与信息安全二级学科硕士学位授权点既紧迫又必要。

（1）**智能化应用的普及带来了更高层次的信息安全挑战。**在智能制造、智慧城市、智能医疗、自动驾驶等领域，人工智能系统与网络安全问题深度交织。社会迫切需要掌握智能算法与安全防护技术的高层次人才，能够在算法漏洞检测、模型安全验证、数据加密与防篡改等方面开展创新研究和应用。

（2）**国家关键信息基础设施安全对高端安全人才需求旺盛。**能源、电力、交通、金融、国防等领域的关键信息系统面临越来越复杂的网络攻击与入侵风险。政府与企业亟需具备网络攻防对抗、风险评估、应急响应等能力的安全专家，以保障国家基础设施的运行安全。

（3）**人工智能驱动的网络安全技术革新催生新型复合型人才需求。**

随着 AI 在网络安全防护中的广泛应用（如威胁情报分析、异常检测、入侵识别等），传统的网络安全人才已难以满足新形势下的智能防御需求。社会需要掌握深度学习、强化学习与安全防护机制融合技术的高级研究与工程人才。

（4）**数据安全与隐私保护成为社会关注焦点。**

在大数据与 AI 时代，数据的采集、共享与利用带来了重大安全与伦理风险。各行业亟需具备密码学、隐私计算、差分隐私、联邦学习等前沿技术的高层次专家，确保数据安全与用户隐私保护

的平衡。

（5）跨学科融合推动智能安全研究创新。

网络与信息安全已从单一的技术防护拓展到智能决策、行为分析和社会工程防御等综合方向。科研机构和高校需要兼具计算机科学、人工智能、统计学及社会工程学知识的复合型人才，以推动新一代智能安全体系的构建。

（6）政府与监管机构高度重视网络空间治理与安全人才储备。

国家在数字治理、网络法治、网络伦理、数据主权等方面需要既懂技术又懂政策的高层次安全专家，参与制定国家级网络安全标准和法规体系，助力形成系统化、智能化的安全治理能力。

总之，随着数字中国和智能社会建设的深入推进，网络与信息安全领域的高层次人才成为战略性稀缺资源。这些人才不仅要具备深厚的网络安全理论基础与工程实践能力，更要能够将人工智能技术与安全防护体系深度融合，支撑国家安全战略和智能化社会的可持续发展。

（二）设置该学科的目的

设置网络与信息安全学科旨在满足国家网络空间安全与数字经济高速发展背景下对高层次安全技术与管理人才的迫切需求，与南华大学学术型人才培养目标高度契合。同时，该学科的设立也为推动信息技术、人工智能、电子工程、法学等多学科的深度交叉融合提供了重要基础，促进学校在网络安全、数据保护及智能安全体系建设等领域的创新发展。

设置网络与信息安全学科是为了应对现代社会中信息化、智能化快速发展的挑战。随着人工智能、云计算、大数据、物联网、区块链等技术的广泛应用，网络空间安全问题愈加复杂，网络攻击与数据泄露事件频发，国家与社会迫切需要具备系统安全思维、创新意识和工程实践能力的高层次安全人才。该学科旨在培

养能够从理论与技术两方面推动网络空间安全创新、具备跨学科研究能力的高素质人才，为国家信息安全、数字经济建设和社会治理提供有力支撑。

网络与信息安全学科的设置与南华大学“厚基础、重交叉、强创新”的学术型人才培养目标完美契合。该学科致力于培养掌握密码学、网络攻防、数据安全、人工智能安全、隐私计算等前沿知识，具备科研能力与批判性思维的研究型人才，使其能够在学术界和产业界发挥引领作用，产出高水平科研成果，助力科技进步与社会创新。

网络与信息安全学科本身具有显著的交叉特性，涵盖计算机科学、通信工程、人工智能、控制科学、法学与管理科学等多个领域，不仅强化了学科间的融合与协同，也有助于培养兼具技术与政策视野的复合型人才，他们能够在不同领域中应用智能安全技术应对复杂问题。

（1）在**核科学与技术领域**，网络与信息安全可应用于核设施网络防护、核能监控系统的入侵检测、辐射监测数据的安全传输与加密管理，保障核能系统的运行安全与数据可靠性。

（2）在**医学与医疗健康领域**，该学科可为医学影像数据、电子病历和远程诊疗系统提供安全保护，确保医疗数据隐私与合规管理，促进“智慧医疗”与“数字健康”安全体系建设。

（3）在**矿业工程与工业控制领域**，网络与信息安全技术可用于保障矿山自动化系统、传感网络及工业控制系统的抗攻击能力，提高生产安全与应急响应水平。

（4）在**公共安全与应急管理领域**，智能安全算法可实现对舆情信息、网络威胁和社会风险的实时分析与预警，支撑国家网络安全治理体系建设。

总之，网络与信息安全学科的设置旨在培养具备坚实理论基础、创新能力与跨学科视野的高素质人才。这些人才不仅能够在科研与产业界开展前沿研究与技术创新，还能在核能安全、医疗

健康、工业控制与社会治理等关键领域应用安全技术，为国家安全战略、科技进步和社会可持续发展提供坚实的智力支撑。

（三）本单位设置该学科已具备的基础

本学科依托南华大学软件工程学科的坚实基础，充分发挥学校在核科学与技术、基础医学、临床医学以及安全科学与工程等领域的学科优势，构建起多学科交叉融合的网络与信息安全学科体系。通过跨学科协同建设，本学科形成了以智能安全、数据安全、隐私保护、关键基础设施防护为核心的研究方向，为学科的可持续发展提供了坚实基础。

在师资力量方面，本学科高度重视人才队伍建设，已形成一支结构合理、实力雄厚的高水平学术团队。现有专任教师 54 人，其中具有博士学位 47 人；包括包括国家高层次人才（千人计划）1 人，国家杰出青年基金获得者 1 人、教育部“新世纪优秀人才”1 人、教授 20 人、副教授 16 人。该师资队伍梯队完善，以国家高层次人才和杰青为核心，中青年教授为中坚，优秀青年教师为骨干，具备高水平科研创新能力和国际化的研究视野，为网络与信息安全学科的建设与发展提供了强有力的人才保障。

在科研与学科支撑平台方面，依托南华大学在工业与信息化部、生态环境部、国家卫生健康委员会、国家国防科技工业局、中国核工业集团公司及湖南省人民政府共建高校的优势，本学科拥有深厚的科研底蕴和产业应用基础。目前建有国家级与省部级科研平台 10 个，包括核能与核安全示范型国际科技合作基地、核燃料循环技术与装备湖南省协同创新中心、湖南省医疗大数据国际科技创新合作基地、湖南省智能装备软件评测工程研究中心等。同时设有 3 个省级研究生培养创新基地，协同单位涵盖核工业主要研究院、所及企业，为网络与信息安全学科的科研创新与产学研转化提供了广阔平台。

在科研成果与创新能力方面，本学科教师近5年承担国家自然科学基金重大研究计划、国家核能开发项目、国家重点研发计划等科研项目共264项，立项总经费达1.16亿元，其中纵向经费4984.6万元。发表相关学术论文458篇，获省科学技术进步奖二等奖3项、技术发明奖二等奖1项、三等奖2项、自然科学奖三等奖1项，并获得省级教学成果奖一等奖2项、二等奖1项、三等奖3项。这些成果体现了学科在网络空间安全、智能安全监测、数据防护与系统可靠性等方面的研究实力。

在教育与人才培养方面，本学科已开设“大数据理论及技术”、“知识工程”、“模式识别”、“深度学习”、“语义网技术”和“概率图模型”等多门前沿课程，建立起完善的研究生培养体系。近5年累计培养硕士研究生206人、博士研究生10人。学生国际化视野突出，研究生参与国际学术交流比例达8%，国内学术交流比例达23%，培养质量和学术影响力显著提升。

在实验与工程实践条件方面，本学科拥有完善的科研与实验支撑体系。现有激光与等离子加工设备、核应急救援作业装备、铀水冶试验平台、仿星聚变装置等专业设备，以及数控实验平台、超算中心、电镜与XRD实验系统等基础科研设备，总值达1.81亿元，实验用房面积11000平方米。这些条件完全能够支撑网络安全攻防实验、密码学计算实验、数据安全分析及系统安全性验证等研究的需求。

此外，南华大学在智能安全与应用创新方面积累了丰富成果，如研发的核应急抢险作业机器人、核设施蒸汽发生器泄漏监测系统、自主化核电DCS“龙鳞系统”安全性监测技术等，均在工程安全与网络防护中取得实际成效，并在衡阳市孵化出多个主导市场的高新技术企业。这些成果为网络与信息安全学科在智能防护、工业控制安全、关键基础设施安全等方向的应用研究提供了有力支撑。

综上，南华大学网络与信息安全学科已具备坚实的学科依

托、雄厚的师资队伍、完备的科研平台、充足的实验条件和突出的科研成果。这一系列基础保障为本学科建设成为具有国内影响力、服务国家安全战略与数字化转型需求的高水平学科奠定了坚实基础。

（四）该学科的发展前景

网络与信息安全交叉学科的研究对象是网络空间安全系统，它由密码学算法、安全协议、智能检测模型、可信计算环境以及复杂的网络基础设施构成，旨在保障信息系统的机密性、完整性、可用性与可控性。通过融合人工智能、大数据分析、量子通信、区块链和物联网等新兴技术，网络与信息安全学科不仅能够识别、预测和防御各类网络威胁，还能在复杂环境中实现系统级的智能防护与自主决策。

网络与信息安全学科的建设目标是跨学科、重基础、重应用、重实践，致力于培养兼具深厚理论素养、工程实践能力与创新精神的高层次安全技术与科研人才。

网络与信息安全作为高度交叉的战略性学科，具有在多领域支撑科技创新和国家安全的独特优势。

在复杂的社会与技术环境中，该学科能够以智能化的安全模型和技术手段，为核能设施安全监控、医疗数据隐私保护、工业控制系统防御、城市基础设施安全管理等提供系统化的解决方案。通过强化智能算法与安全体系的融合，能够有效应对跨领域、多层次的网络安全风险，支撑国家在数字治理、国防安全、能源安全、社会安全等关键领域的战略需求。

目前，全国虽已设立若干网络空间安全一级或二级学科硕士点，但在人工智能、核技术、医学、安全科学等领域深度交叉的网络与信息安全学位点仍较为稀缺。南华大学依托软件工程、核科学与技术、安全工程及医学等优势学科，在智能安全监测、数据安全防护、工业控制安全与隐私保护方面已具备扎实基础，具

备建设高水平网络与信息安全交叉学科的独特条件。

通过该学科建设，可以实现以下突破与价值：

在核能安全领域：融合智能算法与安全防护机制，实现核设施控制系统的实时监测与风险预警，提高核能利用的安全性与可靠性；

在医疗健康领域：构建基于隐私计算的医疗数据安全管理与共享体系，助力精准医疗与智慧医疗发展；

在工业与城市安全领域：发展智能入侵检测与异常识别技术，为工业互联网、智慧城市和应急管理提供安全保障；

在国家战略安全层面：形成自主可控的安全防护与技术创新体系，提升国家网络空间安全防御与治理能力。

因此，可以认为，高层次网络与信息安全专业人才的市场需求巨大且持续增长。随着数字中国和网络强国战略的深入推进，网络安全已成为国家安全体系的关键组成部分。本学科的设立将有助于推动网络与信息安全及其相关交叉学科的发展，培养具备国际竞争力的安全科研与工程人才。

网络与信息安全学科拥有广阔的发展前景和深远的社会价值。它不仅能带动人工智能、安全科学、医学信息化等领域的协同创新，还能在促进科技进步、维护国家安全、保障社会稳定与经济高质量发展方面发挥重要作用。未来，随着智能化与数字化进程的加速推进，该学科必将成为国家科技创新体系中不可或缺的重要支撑力量。

三、该学科的人才培养方案

（一）培养目标

本专业学位旨在培养德、智、体、美、劳全面发展，结合学校核、医学科优势，在网络与信息安全领域具有一定创新的应用型、复合型高层次人才。具体要求如下：

（1）坚持党的基本路线，热爱祖国，热爱人民，具有坚定的马克思主义信仰和中国特色社会主义共同理想，以及正确的世界观、人生观和价值观。

（2）掌握本领域的基础理论、先进方法和现代技术手段，具备解决网络与信息安全方向复杂技术问题的实践和创新能力，能够独立从事本领域的基础研究和应用研究及系统的分析、设计、开发等工作。恪守职业道德和工程伦理，成为具有良好职业素养的网新人才。

（3）掌握一门外国语，能熟练地阅读专业外文资料，具备一定的写作能力和国际学术交流能力。

（二）生源要求和选拔方式

1、生源要求

（1）优先招收计算机相关专业方向、信息与通信工程、数学等相关专业背景的考生，需掌握高等数学、线性代数、离散数学、概率论与数理统计等数学基础课程，熟练掌握计算机网络（如 TCP/IP 协议栈、网络分层架构）、操作系统（进程管理、内存管理、文件系统安全）、数据结构与算法（哈希表、图论、动态规划等）等核心课程知识，具备严谨的逻辑分析与抽象思维能力，为后续密码算法设计、安全协议分析等核心课程学习奠定基础。

（2）需具备至少一种编程语言（如 Python、C/C++、Java）的编程能力，能独立完成代码编写、调试与优化；熟悉常用网络安全工具（如 Wireshark 网络抓包分析、Nessus 漏洞扫描、Metasploit 渗透测试框架）的使用，可开展基础的网络流量分析、

漏洞探测与渗透测试工作；了解 Linux /Unix 操作系统的常用命令与配置，并能够在系统上搭建安全测试实验环境。

（3）需系统掌握网络安全核心知识体系，包括密码学基础（对称加密、非对称加密、哈希函数、数字签名）、网络攻击与防御技术（DDoS 攻击原理与防御、SQL 注入、XSS 跨站脚本攻击、防火墙与入侵检测系统配置）、数据安全（数据加密、脱敏、备份与恢复）、应用安全（Web 应用安全、移动应用安全）等，能准确识别常见安全风险并提出应对策略。

（4）具备一定的学术文献检索、阅读与分析能力，能使用知网、Web of Science、IEEE Xplore 等学术数据库查找领域内核心文献，理解文献的研究思路、方法与结论；拥有基础的学术写作能力，可撰写课程论文、研究报告或学术论文提纲，清晰表达研究观点与逻辑。

（5）网络与信息安全工作直接关系到个人信息安全、企业商业秘密及国家网络空间安全，学生需具备强烈的社会责任感与职业道德，严格遵守网络安全法律法规与伦理准则，坚决抵制网络攻击、数据泄露等违法违规行为，树立正确的安全防护理念。

2、选拔方式

通过报名参加全国硕士研究生招生考试，或从推免生中选拔。考核和选拔过程中，重点考查考生的综合素质、创新意识和创新能力， 把对专业有没有激情和兴趣， 作为面试考察的侧重点。优先考虑具备网络安全相关项目经历，例如参与过企业网络安全防护体系搭建、信息系统漏洞挖掘与修复、数据加密传输方案设计、安全审计与风险评估等项目；拥有网络安全领域相关竞赛经历或专业认证的考生，如全国大学生信息安全竞赛、CTF（Capture The Flag）网络安全竞赛、“强网杯”“护网杯” 等赛事获奖经历，或持有华为 HCIA、 CISAW（学生通道）等行业认可度较高的认证证书。

（三）课程体系的设计方案及依据

本学科硕士研究生培养课程体系设置结合网络与信息安全依托一级学科的特点，遵循科学理论基础与学科前沿技术的结合创新，注重学生自主研究能力和创新能力的培养。课程内容体现网络与信息安全的新进展及与依托学科的结合，拓宽知识面，注重综合性、前沿性。同时，还要结合社会发展和人才市场需求来优化课程结构，优化培养计划，完善课程体系。

硕士研究生课程体系结构分为学位课和非学位课两大类型。学位必修课包括新时代中国特色社会主义理论与实践、硕士生学术英语写译、硕士生学术交流英语、高等工程数学 A、高级计算机网络、现代密码学、网络安全协议理论与技术和高级网络安全技术。非学位课则在理论基础上，注重与依托学科的结合，以及学生分析能力，创新能力综合素质的培养。硕士研究生在完成课程学习的同时，还必须参加课题研究和学术交流活动。课程设置如下表所示。

南华大学网络与信息安全领域专业学位硕士研究生课程设置

类别	课程编号	课程名称	学分	课内学时	开课学期	考核方式	开课单位	是否新开设	课程负责人
学位课 (公共学位课) 5学分	S999101	新时代中国特色社会主义理论与实践	2	32	1	考试	马克思主义学院	否	何小英
	S999009	硕士生学术英语写译	2	36	1	考试	语言文学学院	否	刘德军
	S999010	硕士生学术交流英语	1	18	1	考试	语言文学学院	否	刘德军
学位课 (专业基础课) 8学分	S004025	高等工程数学A	2	32	1	考试	数理学院	否	郑立景
	S004026	高级计算机网络	2	32	1	考试	计算机学院	是	万亚平
	S004027	现代密码学	2	32	1	考试	计算机学院	是	田纹龙
	S004028	网络安全协议理论与技术	2	32	1	考试	计算机学院	是	罗凌云
学位课（专业课） 3学分	S1208126	网络安全技术前沿进展	1	16	2	考查	计算机学院	否	教师组
	S1208127	高级网络安全技术	2	32	2	考查	计算机学院	是	付仲明
非学位课 (公共必修课) 8学分	S1201133	自然辩证法概论	1	16	1	考查	马克思主义学院	否	尹长青
	S1201134	软件安全	2	32	2	考查	计算机学院	是	李萌
	1208127	如何写好科研论文	1	16	2	考查	计算机学院	否	欧阳纯萍
	S1201135	信息隐藏技术	2	32	2	考查	计算机学院	是	毛宁雄
	S1201136	网络攻防技术	2	32	2	考试	计算机学院	是	刘朝晖
非学位课(必修环节) 1学分	S008043	开题报告	0.5		3	考查	计算机学院	否	
	S008044	中期考核	0.5		4	考查	计算机学院	否	
计算机与核交叉课程模块 非学位课(专业选修课)	S008002	核工业软件安全测试	2	32	2	考查	计算机学院	否	阳小华
	S008035	时序大数据分析与挖掘	2	32	2	考查	计算机学院	否	朱 涛
	S008036	无线传感器网络安全技术	2	32	2	考查	计算机学院	是	聂 沛
医工交叉课程组课程模块 非学位课(专业选修课)	S1208107	模式识别	2	32	2	考查	计算机学院	否	屈爱平
	S1208108	医学大数据与人工智能(双语)	2	32	2	考查	计算机学院	否	李春权

类别	课程编号	课程名称	学分	课内学时	开课学期	考核方式	开课单位	是否新开设	课程负责人
	S1208109	隐私计算在医疗中的应用	2	32	2	考查	计算机学院	是	刘永彬
公共选修模块 非学位课(专业选修课)	S006638	人工智能与区块链安全	2	32	2	考查	计算机学院	否	田纹龙
	S006638	图像信息安全	2	32	2	考查	计算机学院	是	毛宁雄
	S006639	物联网安全与隐私保护	2	32	2	考查	计算机学院	是	胡珍珍
	S006641	信息安全技术前沿进展	2	32	2	考查	计算机学院	是	高宸
	S006642	大数据隐私保护方法	2	32	2	考查	计算机学院	是	周顺衡
本科补修课		离散数学			2		计算机学院		
		数据结构			2		计算机学院		
		计算机网络原理			2		计算机学院		
		LINUX 操作系统			2		计算机学院		

（四）培养和学位的基本要求

1、培养方式

（1）本专业学位研究生采取理论学习、科学研究及实践活动等相结合的培养方式。着重培养和加强研究生的自学能力和独立分析问题、解决问题的能力，使研究生掌握基本的科研方法，培养研究生严谨的科学作风。

（2）实行导师负责制，在导师指导下完成个人培养计划制定、课程学习、必修环节和实践环节。

（3）可实行校企协同培养，校内导师负责科研与理论把关，企业导师负责项目实践指导，共同参与论文选题与成果评价，将企业真实需求融入学位论文研究，实现“科研-产业”无缝衔接。

（4）可跨学科联合培养，与医学、核技术等学科合作开设交叉课程，培养针对特殊行业的安全人才。

2、学位学分要求

学制 3 年，全日制在校学习年限 2-4 年（不超过 4 年）。总学分不少于 32 学分，硕士研究生学位课学分不少于 16 学分，公共必修课（非学位课）不少于 8 学分，非学位课（必修环节）不少于 1 学分，专业选修课（非学位课）学分不少于 7 学分。跨学科、专业录取的研究生，要求补修本专业本科主干课程 4 门，并通过考核，取得及格成绩，不计学分。

3、学位论文要求

（1）文献阅读

要求广泛阅读本专业研究方向的权威文献资料，包括国外文献以及国内一级学会刊物等重要核心文献。在阅读文献的基础上完成一篇字数不少于 4000 字的文献综述，参考文献不少于 50 篇，其中外文文献在 1/2 以上，近 5 年文献在 2/3 以上。

（2）论文选题

论文选题应该来源于导师的研究课题、或者企业委托课题、或者学生获批的校级及其以上的研究生创新实验项目，选题必须具有明确的学术研究意义或者实际应用价值。

（3）开题报告及评价

在完成文献综述和论文选题的基础上，学生应在导师的指导下，根据所选定的课题范围按《南华大学研究生开题报告评价暂行管理规定》（附件-南华大学研究生开题报告评价暂行管理规定）要求写出完整的开题报告，并由以研究生导师为主体组成考核小组（专家由5~7组成）进行评审。评分结果严格按开题报告评价内容及分值进行综合评分，成绩70分以上为合格。开题考核不合格者，推迟半年重新开题。

从开题考核通过到论文答辩，应至少有一年的时间间隔。开题报告一经通过，应按计划进行论文工作。如因故需要改选课题时，由导师确定并在学科会议上重新报告审定。会后，可根据提出的意见和建议，在一周内修改科研和撰写论文工作计划，经导师、学科带头人签字同意后，交学院和研究生院备案。

（4）学位论文中期进展报告

在学位论文工作的中期，学生应提交学位论文中期报告，由院（系）组织考核小组公开进行学位论文中期检查（保密论文除外）。中期检查时间距离答辩时间一般不少于半年。中期检查主要内容包括：研究生的思想政治表现、综合能力、课程学习完成情况、论文工作进展情况以及工作态度和精力投入等。通过中期

检查的准予继续进行论文工作。未按时提交中期报告者以及中期检查不合格者，不能申请学位论文答辩。

（5）论文答辩资格考核

研究生在第五学期参与预答辩之前，必须先提出申请，满足如下条件，方可答辩：

• 按培养计划要求修满学分；

• 取得符合学校及本学科有关规定的成果(参见附件-计算机学院电子信息工程硕士研究生答辩资格考核要求）

（6）学位论文答辩

所有学位论文必须通过预答辩之后，方能参与论文盲审。论文由两位该领域的专家进行匿名评阅，其中至少一份由校外专家进行双向匿名评审。

4、学位论文量化标准

以南华大学为第一署名单位、研究生为第一作者、导师为第一作者且研究生为第二作者，在国内、外正式期刊或会议上发表论文至少 1 篇，论文需达到如下条件之一：

（1）SCI 期刊、EI 期刊、北大核心期刊论文 1 篇（以正式录用通知为准）

（2）CCF 推荐会议论文 1 篇（以正式录用通知为准）

（3）EI 会议论文 1 篇（以 EI 检索证明为准）

四、该学科的建设规划

（一）研究方向

该学科将立足国家网络空间安全与人工智能安全发展的重大需求，结合南华大学在智能计算、信息安全与核能安全等领域的研究基础，规划形成“可信智能、安全感知与协同防护”三大研究方向，构建交叉融合、协同推进的研究体系，形成支撑网络空间安全、人工智能安全与可信计算协同发展的研究格局。

(1) 基于置信规则库的可信 AI 多模态决策理论与形式化验证

本方向面向人工智能系统的可信性与可验证性问题，研究如何在复杂安全环境下实现可靠的智能决策与形式化保障。学科将以置信规则库为理论核心，探索人工智能在多模态信息处理中的可信推理与安全控制机制，发展具备可解释性、可追溯性与防攻击能力的 AI 算法体系。未来将建设“可信 AI 与安全验证实验平台”，推动机器学习、强化学习与形式化方法的融合应用，形成“算法–模型–验证–部署”一体化的研究体系，为智能安全防护、网络威胁识别与关键任务系统的稳定运行提供技术支撑。

(2) 多模态可信感知驱动的全域安全动态评估与智能决策

该方向聚焦关键基础设施与复杂系统的安全监测和风险预测，研究多模态感知驱动的安全动态评估与决策优化机制。学科将依托人工智能、信号处理与安全计算技术，构建集数据采集、威胁识别、风险分析与决策支持于一体的安全感知体系。重点面向核安全、工业互联网、能源网络等关键领域，建设多模态安全态势感知平台，发展基于大数据与深度学习的全域安全预测与智能响应模型。通过理论创新与工程验证相结合，形成可应用、可扩展的动态安全评估体系，支撑国家重大安全工程的智能化防护需求。

(3) 跨域数据安全流通的云链协同可信计算与动态防护

本方向面向数据安全与隐私保护的新兴挑战，研究云计算、

区块链与人工智能协同的可信计算机制，推动跨域数据安全流通与动态防护技术的发展。学科将建设“云链协同可信计算实验环境”，探索联邦学习、安全多方计算、差分隐私等关键技术，发展可验证、可追溯的云链安全信任体系。通过融合云端智能防护与链上可信记录，实现数据在不同组织与领域间的安全共享与计算协作。未来将面向医疗健康、智慧政务与公共安全等典型应用场景，打造数据安全流通示范平台，形成具有区域影响力的“云链协同可信计算”研究方向品牌。

总体而言，该学科将通过上述三大方向的协同推进，形成从理论创新、技术攻关到工程应用的系统化研究格局，构建以“可信智能—全域防护—协同计算”为核心特色的学科体系，为南华大学在网络与信息安全领域的高质量发展奠定坚实基础。

（二）师资队伍

本学科坚持“自主培养与重点引进并举”的建设方针，着力加强高层次人才队伍建设。未来5年，将通过多渠道引进与校内培养并重的方式，引进和培养约2名高水平学科带头人，培养与引进4名左右高层次学术骨干，进一步优化教师队伍的职称、学历与年龄结构，提升整体科研与教学水平。目前本学科已形成以教授、副教授为主体的结构合理、梯队完善的科研教学团队，主要骨干教师如下：

1、林文斌，博士，教授，博士生导师。教育部新世纪优秀人才。现任南华大学数理学院院长。研究领域和兴趣包括有广义相对论、宇宙学、电磁场与微波技术、科学计算、深度学习和强化学习等。迄今发表SCI论文100余篇，获授权国家发明专利3项。主持国家自然科学基金项目3项、科技部外专项目1项、省部级等其他项目10余项。指导硕士和博士研究生40余名，其中已毕业博士7名。

2、万亚平，博士，教授，硕士研究生导师。现任南华大学

计算机学院院长。ACM、CCF 会员。研究方向为分布式计算、网络存储、信息检索等。先后参与和主持国家 973、863、教育部创新团队、国家自然科学基金、湖南省教育厅科研课题、南华大学博士启动基金等多个项目，发表学术论文 20 余篇, SCIE、EI 收录 10 余篇,获得国家发明专利 1 项、软件著作版权 3 项，参与的《基于存储接口路径优化的 iSCSI 磁盘阵列》项目获得省级鉴定，达到国际先进水平。

3、刘军，博士，教授，博士生导师。入选国家级人才计划，IEEE 高级会员。在人工智能领域深耕多年，研究方向为可信人工智能模型和系统及其应用。近五年主持和参与各类项目和工程建设数千万元。已发表论文 250 余篇，其中 JCR 1 区论文 70 余篇，被引 7000 余次，多个高水平 SCI 期刊的副主编、编委。

4、宁婉仪，博士，教授，硕士生导师。2025 年 6 月在北京邮电获得博士学位；2022 年 12 月至 2023 年 12 月，在苏黎世联邦理工学院进行联合培养博士学习；2025 年 6 月至今，就职于南华大学计算机学院。以第一/共一作者身份在 JSAC、TSC、NeurIPS、TNNLS 等国际顶级期刊和会议上发表多篇论文。研究方向包括分布式深度学习、模型压缩与边缘智能。

5、刘朝晖，博士，副教授，硕士生导师。现任南华大学创新创业教育与实践中心副主任。 主要研究方向为计算机网络安全、物联网技术、人工智能应用等。在国内外重要期刊或国际会议发表学术论文数十篇，其中 SCE/EI 检索 20 余篇。出版著作或教材 3 部；主持或主要参加国家社科基金、湖南省自然科学基金、湖南省社科基金、湖南省科技计划、湖南省教育厅科学研究课题、国家重点实验室开放基金项目十余项，主持完成横向项目 10 余项，累计金额四百余万元。2016 年主要参与获得湖南省教学成果一等奖，2019 年、2022 年两次参与获得湖南省科技进步奖二等奖。现担任中国核能行业协会信息化专委会委员、湖南省信息安全标准化技术委员会委员，曾任湖南省智能装备软件评测工程

技术研究中心副主任、四川省核电仪控工程技术研究中心副主任、湖南省计算机学会第八届理事会理事等社会兼职。

6、田纹龙，博士，副教授，硕士生导师。现任南华大学计算机学院副院长。IEEE 会员、ACM 会员、中国计算机学会会员。先后在 TDSC, IOT, JPDC, CCPE, TrustCom, IPCCC, HPCC, ICPADS, 现代教育技术等国内外权威刊物和国际会议上发表学术论文 20 余篇。申请国家发明专利十余项，获 IEEE TrustCom 2018 会议最佳论文奖。现主要研究方向为云计算安全，区块链与人工智能安全，密码学分析，并行与分布式计算。

7、郑立景，博士，副教授，硕士生导师。2014 年 9 月毕业于湖南师范大学，获理学博士学位；2020 年 6 月于复旦大学博士后出站。主要从事密码学与编码学研究，在偶特征有限域上 APN 函数、具有最大 BENT 分支数的向量布尔函数、极小线性码以及置换多项式函数等方向取得了具有代表性的研究成果。以第一作者在 IEEE Transactions on Information Theory、Designs Codes and Cryptography 等国际著名学术期刊发表论文 10 余篇。主持国家自然科学基金面上项目（2024－2027）、湖南省自然科学基金面上项目（2023－2025）等科研项目 5 项。现主要研究方向为密码学与编码学。

8、毛宁雄，博士，副教授。2024 年 12 月在西南交通大学获得博士学位；2023 年 9 月至 2024 年 9 月，在意大利博洛尼亚大学进行联合培养博士学习；2024 年 12 月至今，就职于南华大学计算机学院。长期从事多媒体信息安全，可逆信息隐藏等方面的研究，目前为止在《IEEE Trans. Circuits Syst. Video Technol.》、《IEEE Trans. Multimedia》、《Signal Processing》、《J. King Saud Univ.—Comput. Inf. Sci.》、《Biomedical Signal Processing and Control》、《Appl Intell》等国内外高水平期刊、会议发表论文 20 余篇。

8、付仲明，博士，副教授，硕士生导师。于 2020 年在湖南

大学信息科学与工程学院获博士学位。目前研究方向为大数据并行分布式计算、高性能计算和人工智能，包括分布式计算框架（Hadoop/Spark 框架）和分布式机器学习以及深度学习。现为中国计算机学会 CCF 会员、IEEE 会员。在 IEEE TPDS，IEEE TCC，IEEE TKDE、ICPADS 等国际著名期刊或会议发表论文 10 余篇，获授权发明专利 5 项，出版教材 1 部，主持或参与国家级、省级科研项目 4 项，指导硕士研究生 3 名，已毕业硕士 1 名。

9、蒋方玲，博士，副教授，硕士生导师。研究领域和兴趣包括计算机视觉、模式识别、人工智能等。迄今发表 SCI 论文 10 余篇，获授权国家发明专利 3 项。主持国家自然科学基金项目 1 项、省部级及其他项目 5 项。

10、聂沛，博士，副教授，硕士生导师。2022 年-2024 年于荷兰特文特大学地理信息科学与地球观测学院（University of Twente, ITC）从事博士后研究，现为中国地理学会（GSC）会员及第二届地理大数据工作委员会委员、中国计算机学会（CCF）会员、中文信息学会（CIPS）会员。研究领域主要包括空间大数据、机器（深度）学习及地理信息学，先后在国内外权威刊物和国际会议上发表论文 10 余篇，近年来研究兴趣为结合机器（深度）学习、大模型与空间统计理论来解决地理空间中的预测与识别问题。

（三）人才培养

本学科将围绕国家网络强国与人工智能安全战略需求，立足南华大学“厚基础、重实践、强能力”的办学理念，构建网络与信息安全硕士研究生培养体系。通过“课程体系+科研实践+创新训练”三位一体的人才培养模式，注重学生的工程能力与科研素养并重，强化跨学科综合应用能力。课程体系将以网络空间安全、人工智能安全、可信计算、数据隐私保护等为核心方向，配合密码学、系统安全、机器学习安全等前沿课程模块，系统培养

学生在复杂网络环境中的安全分析、系统防护与智能安全设计能力。

同时，依托学校在智能计算与核安全等领域的科研优势，本学科将建设“可信智能与网络安全实验教学中心”，建立“研究生联合培养基地”和“产学研联合创新平台”，推进研究生与科研团队、企业及国家重点实验室的协同培养。通过科研项目参与、国际交流、学术竞赛与创新创业实践等途径，形成课程体系完备、科研实践深入、创新氛围浓厚的研究生培养生态，培养具备国际视野、工程实践能力与创新精神的高层次网络安全人才。未来五年，学科将力争形成一支具有突出的科研创新能力与社会服务能力的研究生群体，为国家关键领域的网络与信息安全保障提供坚实的人才支撑。

（四）科学研究和学术交流

本学科将坚持“基础研究与工程应用并重、科研创新与服务国家需求并行”的建设思路，聚焦网络空间安全、人工智能可信与数据隐私保护等重点方向，同时依托南华大学在核科学与核技术领域的深厚基础，面向国家核工业数字化转型过程中涌现的安全挑战，开展核工业网络安全与核设施智能防护相关研究。学科将积极承担国家自然科学基金、省部级科研计划和重点实验室建设任务。未来五年，拟重点建设“可信智能与安全防护创新研究中心”，形成集理论创新、技术攻关和系统验证为一体的科研平台，推动在可信计算、隐私保护、联邦学习、大模型安全以及核设施智能监测与防护等方向取得标志性成果。

在学术交流方面，本学科将构建多层次、国际化的合作机制，积极与国内外高水平高校和科研机构开展学术交流与联合研究，鼓励教师参与国际会议与学术组织，提升科研影响力。通过定期举办“网络与智能安全前沿论坛”“青年学者沙龙”以及“核工业数字安全研讨会”等特色活动，营造开放共享的学术生态，促

进交叉融合与创新发展，为南华大学网络与信息安全学科的持续提升提供坚实的学术支撑与外部合作基础。

（五）教学科研基本条件

本学科经过建设，已初步形成较为完善的教学与科研条件体系。团队教师在教材建设、高水平论文发表及科研项目申报方面均取得良好成绩，积累了丰富的研究经验和数据资源，为学科建设提供了坚实基础。依托国家自然科学基金、省部级科研项目以及多项横向合作课题，学科逐步形成了较为系统的理论研究框架与稳定的科研方向，具备进一步开展高水平科学研究和人才培养的能力。

目前，本学科已配备必要的教学科研仪器设备和高性能计算资源，可支撑网络攻防实验、加密算法验证、数据隐私保护等核心教学科研任务。学校同时在信息化基础设施建设方面投入持续经费，为科研数据存储、云端协作与远程教学提供有力支撑。未来，学科将继续完善科研环境，规划建设“可信智能与安全防护实验平台”，推动教学科研条件的智能化、体系化与开放化发展，保障学科高质量建设目标的实现。

（六）经费保障

本学科经费来源稳定，科研基础良好。团队成员主持和参与多项国家自然科学基金、省部级科研计划及企事业单位合作项目，形成了稳定的科研经费基础，为学科建设提供了坚实支撑。未来，学科将持续加强科研项目的组织与申报工作，积极争取国家级、省部级及市校级重点项目立项，进一步拓宽纵向经费来源。

同时，学科将依托学校科研管理与成果转化体系，深化与企事业单位产学研合作，推动技术成果转化，增强横向经费支持能力。通过研究生教育质量提升工程等政策渠道，保障教学科研活动和平台建设的持续投入，确保网络与信息安全学科建设的可持续发展与稳定经费支持，为硕士学位点建设提供长期支撑保障。