## 2024子课题：关键暴露面资产反测绘技术研究：

1. **网络空间测绘国内外发展及现状调研**

对全球主流测绘平台的发展和现状进行调研，具体包括全球主流测绘平台的区域分布、区域分布、重点国家分布、主流平台名称及应用和部署情况。

调研国内外主流资产测绘厂商技术异同与差距，调研资产测绘技术所产生的附加价值，以及其技术的主要应用领域。

1. **反测绘技术技术调研**

5G、云计算技术发展带来的“网络空间泛化”使企业数字资产数量和类型激增，另一方面，随着物联网（IoT）的逐步 普及、工控系统的广泛互联，直接暴露在网络空间的联网设备数量大幅增加，随之可能面对更多的风险。当前网络空间测绘被用来管理和监控资产的同时，也极有可能被攻击者当作“窥探”网络内部的工具， 并被泄露、滥用以及利用，从而对个人、企业、国家造成巨大的内外损失。通过对反测绘技术的研究，进而研究如何提升功能反扫描能力，进一步减少国家和企业网络暴露面风险所带来的损失。

**3、反测绘技术能力研究**

反测绘技术研究按照三个阶段进行研究和实验：

1. 拦截和禁止，按照禁ping、禁止探测的手段，强制实现地址隐藏，实现反探测能力，如针对不同国家、区域、组织禁Ping、 针对不同组织、个人禁止探测等效果。
2. 迷惑和欺骗，通过指纹混淆、诱骗扰乱探测agent，通过判断请求是否来自测绘节点，定向进行错误服务的反馈，进行服务、资源、网络情况的伪造和扰乱。建立虚假指纹模型、虚假响应模型，隐藏真实指纹，减小业务暴露风险。
3. 隐匿和保护，对已知确定的测绘节点进行隐匿，保护重要系统资产，实现测不到、测不准、测不对。采用虚假的设备、服务应用、资源数据及网络陷阱欺骗非法访问者；扰乱其探测和扫描等行为，使其得到错误的结果。

**4、成果转化**

反测绘技术的相关成果转发，包括不限于技术方案、专利、原型系统等。