网络空间测绘技术白皮书

White Paper for Cyberspace Mapping Techniques

中关村实验室

清华大学

国防科技大学

远江盛邦安全科技集团股份有限公司

2025 年 7 月

前　言

随着全球信息化的不断深化，网络空间作为国家主权的第五疆域，其安全问题已经成为各国高度关注的重点。作为支撑网络空间安全的基础性、普适性和关键性手段，网络空间测绘在准确感知、客观度量与动态跟踪网络态势中发挥着不可替代的作用。科学刻画网络空间，是实现有效治理和构建安全防护体系的重要前提和核心支撑。

中关村实验室围绕网络空间测绘和态势感知领域开展深入研究，联合清华大学、国防科技大学等高水平研究型大学，以及远江盛邦安全科技集团股份有限公司等科技领军企业，共同撰写《网络空间测绘技术白皮书》。本白皮书全面、系统地梳理了网络空间测绘的理论基础和技术体系，深入总结国内外在该领域的研究成果和实践经验，并结合当前网络空间安全的发展趋势和实际需求，提出了网络空间测绘技术的未来发展方向。希望本白皮书能帮助读者建立对网络空间测绘技术体系的全面认识，为科研人员、产业界和政府部门提供有针对性的建议和指导，促进行业的健康与可持续发展。

目　录

第一章 引言

1.1 背景与意义

（1）网络空间作为第五疆域的战略地位及数字化时代安全需求升级

21 世纪以来，随着信息技术的飞速发展，人类社会加速迈入数字化时代。网络空间作为信息传播、存储与交互的重要载体，正深刻重塑人们的生产生活方式。从个人的日常生活，如在线购物、社交娱乐，到国家的关键基础设施运行，如能源供应、金融交易，都高度依赖网络空间。网络空间已经成为继陆、海、空、天之后的第五疆域，其战略地位日益凸显。网络空间这一概念通常是指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间，是信息时代中社会有机运行的神经指挥系统。

在军事领域，网络空间的攻防博弈已成为塑造战略平衡的关键力量。构建网络防御体系不仅需要抵御敌方对指挥控制系统的渗透攻击，更需通过常态化对抗演练持续提升防护能力。以俄乌冲突为例，攻防体系的持续对抗既暴露出关键基础设施的脆弱性，也推动了新型主动防御技术的快速迭代，这种攻防相长的螺旋演进正在重新定义现代国家安全边界。

在经济领域，网络空间是企业和金融机构支撑业务运转和数字化发展的关键依托。随着全球经济的深度融合和数字化转型的加速，企业和金融机构对网络信息系统的依赖持续加深。一次成功的网络攻击可能导致企业数据泄露、业务中断，进而造成巨大的经济损失。以金融行业为例，黑客攻击银行系统可能导致客户资金被盗、金融秩序紊乱，不仅损害相关机构的信誉，还可能引发系统性金融风险，威胁整体金融稳定。

在社会领域，网络空间成为人们获取信息、交流沟通的主要平台。网络安全问题直接影响社会稳定和公众权益。虚假信息、网络诈骗等违法犯罪活动泛滥，严重干扰了人们的正常生活，甚至可能引发社会恐慌。例如，因网络谣言传播而诱发的群体性事件，已多次在现实中出现。

然而，网络空间的开放性、虚拟性和复杂性使得其面临着诸多安全威胁。黑客组织、网络犯罪团伙以及敌对势力利用各种技术手段，如漏洞攻击、恶意软件传播、分布式拒绝服务攻击（DDoS）等，不断地对网络空间进行渗透和破坏。传统的安全防护手段主要聚焦于单点防护和被动防御，难以应对日益复杂多变的

网络安全威胁。因此，数字化时代对网络安全提出了更高的要求，迫切需要一种更加主动、全面的安全防护方式。

（2）网络空间测绘的定义

网络空间测绘是一种通过综合运用多种主动与被动探测及分析技术，对网络空间中的各类资源进行全面、深入探测和精准分析，并以可视化的方式呈现其内在结构和相互关系的技术手段。它类似于现实世界中的地理测绘，旨在绘制一张详细的网络空间地图，实现网络资产与行为的可视化、威胁感知与攻防支撑。

网络空间测绘的核心任务之一是实现资产及其行为的可视化。在庞大而复杂的网络空间中，分布着大量服务器、路由器和应用系统，资产种类繁多、分布广泛，传统管理手段难以实现全面、精细的掌控。网络空间测绘技术可以通过主被动探测等手段，识别出网络中的每一个资产节点，收集其详细属性信息，包括设备类型、IP 地址、开放端口、运行的服务等，并将这些信息整合呈现在统一的可视化平台上。借助该平台，网络管理者可以直观地了解网络资产的分布情况、网络拓扑结构，并及时发现潜在安全风险，为后续安全防护与运维决策提供有力支撑。

威胁感知是网络空间测绘的另一个重要功能。网络攻击者通常会寻找网络中的漏洞和薄弱环节进行攻击。网络空间测绘技术可以通过对网络资产的漏洞扫描和数据分析，提前发现潜在的安全漏洞和攻击迹象，实现对网络资产的风险预判。该技术还可实时监测网络中的异常流量和异常行为，精准识别出潜在的攻击源和攻击目标，为安全管理人员提供及时、准确的预警信息，辅助其快速制定有效的防御策略。

此外，网络空间测绘还能为网络攻防提供有力的支撑。在网络安全防护方面，它可以帮助安全人员了解网络的整体态势，制定合理的安全策略，优化网络拓扑结构，增强网络的抗攻击能力。在网络攻击模拟和测试方面，测绘得到的网络地图可以为攻击方提供详细的目标信息，帮助他们制定更加有效的攻击方案，从而发现网络中的潜在安全问题，实现“以攻促防”的目的。

1.2 目标与范围

（1）白皮书目标

本白皮书的主要目标是全面、系统地梳理网络空间测绘技术体系，深入总结国内外在该领域的实践经验，为相关从业者提供一个清晰、准确的技术参考框架。随着网络空间测绘技术的快速发展，新技术、新方法不断涌现，技术体系日益复

杂。本白皮书将对网络空间测绘技术的基本原理、关键技术和发展趋势进行详细阐述，帮助读者建立起对该技术体系的全面认识。

同时，通过对国内外在网络空间测绘技术应用方面的实际案例进行分析和总结，能够让读者了解不同地区、不同行业在该领域的实践路径与成果经验，从中汲取有益的经验和教训。这不仅有助于国内企业和机构更好地开展网络空间测绘工作，提升自身的网络安全防护水平，也有助于加强国际交流与合作，推动网络空间测绘技术的共同发展。

此外，本白皮书还将结合当前网络空间安全的发展趋势和实际需求，提出网络空间测绘技术的未来发展方向。面对日益复杂的网络安全形势和不断涌现的新威胁，网络空间测绘技术亟需持续创新和迭代升级。通过深入分析技术发展的挑战和机遇，本白皮书旨在为科研机构、产业界及政府部门提供有针对性的建议和指导，促进行业的健康、可持续发展。

（2）覆盖范围

1、技术原理

本白皮书将详细介绍网络空间测绘的核心技术原理，包括探测技术、数据分析技术和可视化技术等。探测技术是网络空间测绘的基础，它涉及到如何高效、准确地发现网络中的资产节点。网络测绘探测包含主动探测、被动探测以及开源情报获取等多种技术方法。

数据分析技术是对探测得到的大量原始数据进行清洗、整理和挖掘，从中提取有价值的信息。例如，通过漏洞分析技术，可以发现资产中存在的安全漏洞；通过关联分析，可以揭示资产之间的内在联系；通过异常检测，可识别网络故障或攻击行为。

可视化技术通过将分析结果以直观、易于理解的形式呈现，辅助用户高效把握网络态势并做出科学决策。常见的可视化形式包括网络拓扑图、热力图、统计报表等，并通过把网络空间映射到物理空间地图之上，实现全面展示网络资产分布、风险分布和行为模式等关键信息。

2、平台开发

网络空间测绘平台是实现网络空间测绘功能的重要载体。本白皮书将围绕平台开发中的关键问题进行探讨，包括架构设计、功能模块划分、数据存储与管理等内容。一个优秀的网络空间测绘平台需要具备高效的数据采集能力、强大的数

据分析处理能力以及友好的用户界面。同时，为应对复杂多变的网络环境和多样化的用户需求，平台还需具备良好的可扩展性与运行稳定性。

3、攻防应用

网络空间测绘在网络攻防中具有重要的应用价值。网络空间测绘通过攻击视角构建威胁模型，为防御体系提供对抗推演的战术地图。防御方基于测绘数据模拟攻击路径，可精准定位暴露面并预判入侵路线，实现“以攻验防”“以攻促防”的主动防御闭环。本白皮书将详细分析网络空间测绘在攻防应用中的具体场景和技术方法，以及面临的挑战和应对策略。

4、标准化探索

随着网络空间测绘技术的不断推广与深入应用，标准化建设已成为保障其规范化、可持续发展的关键基础。本白皮书将聚焦该领域的标准化进展，梳理当前的发展现状，分析标准体系建设的现实需求与未来演进趋势。

第二章 网络空间测绘的理论基础

2.1 网络空间的定义与特性

（1）网络空间（Cyberspace）的起源与多国定义演进

网络空间这一概念最早可追溯到 20 世纪 80 年代。1984 年，加拿大科幻小说家威廉·吉布森在其小说《神经漫游者》中，首次创造了“Cyberspace”一词，用来描述一种由计算机生成的虚拟空间，在这个空间里，人们的意识和数据能够自由流动与交互，这一设想为后续网络空间概念的发展奠定了基础。

随着信息技术的不断发展和互联网的广泛普及，各国开始从不同角度对网络空间进行定义和阐释。

- **美国**：美国在网络空间领域起步较早，对网络空间的定义也在不断发展演进。早期，美国侧重于从技术层面理解网络空间，将其视为一个由计算机系统、网络基础设施和相关数据构成的技术领域。后来，随着网络空间在国家安全、经济发展等方面的重要性日益凸显，美国在《国家网络空间政策评估报告》等文件中，将网络空间定义为一个全球范围的信息环境，它由信息技术基础设施中的相互依存的网络构成，包括互联网、电信网、计算机系统以及嵌入式处理器和控制器。这一定义强调了网络空间的全球性、信息性以及基础设施的相互依存性。
- **俄罗斯**：俄罗斯军方高度重视网络空间在国家安全中的作用，将网络空间视为一个与陆地、海洋、天空和太空同等重要的作战领域。在其相关军事理论和战略文件中，认为网络空间是一个依托信息技术装备和通信网络而存在的虚拟领域，是各种军事和民用信息系统的集合。俄罗斯注重网络空间的军事对抗属性，强调在网络空间进行战略防御和进攻的能力建设。
- **中国学者的四要素理论**：中国工程院院士方滨兴提出了网络空间的四要素理论。他认为网络空间应由物理设施、通信网络、数据信息和人四个基本要素构成。物理设施是网络空间的硬件基础，包括服务器、计算机终端、通信线路等；通信网络是连接物理设施的纽带，实现数据的传输和共享；数据信息是网络空间的核心内容，涵盖了各种类型的数字信息；而人则是网络空间的使用者和创造者，他们的行为和活动对网络空间的发展和安全产生重要影响。

该理论从较为全面的角度对网络空间进行了定义，强调了人的因素及各要素之间的相互关系，为我国深入理解和有效治理网络空间提供了重要的理论支撑。

（2）动态性、虚实融合性、跨域关联性等核心特征

- **动态性**：网络空间处于持续动态演化之中。一方面，新的网络设备、应用程序和技术不断涌现，如智能手机、物联网设备的普及，以及 5G、卫星互联网技术的应用等，使得网络空间的基础设施和资源规模持续增长和更新。另一方面，网络攻击、网络犯罪等恶意行为持续威胁网络安全，漏洞被持续发现与修复，攻防对抗呈现常态化。例如，海量新型病毒和恶意软件持续被开发并迅速传播，严重威胁网络系统安全，需持续更新防护策略与技术手段，以应对这些不断演化的网络威胁。
- **虚实融合性**：网络空间是虚拟世界与现实世界的深度融合。在网络空间中，虚拟的数据和信息代表着现实世界中的各种事物、现象和活动。例如，电子商务平台上的商品信息、用户的交易记录等虚拟数据，反映了现实世界中的商业交易活动；社交媒体上的用户动态和互动，体现了现实社会中的人际关系和社交行为。同时，网络空间中的虚拟活动也会对现实世界产生影响，如网络舆论可以引发现实社会关注和群体行动，网络攻击可能导致现实世界中的关键基础设施瘫痪。
- **跨域关联性**：网络空间跨越了地理、政治、经济、社会等多个领域，具有高度的关联性。在地理层面，网络打破了传统地域限制，实现了全球范围内的信息交流与资源共享，一个地区的网络安全事件可能迅速蔓延并波及他国。在政治层面，网络空间已成为各国开展政治宣传、舆论引导与外交博弈的重要平台。在经济领域，网络空间推动了电子商务、数字金融等新兴产业的发展，同时也引发诸如商业机密泄露、金融欺诈等新的经济安全风险。在社会层面，网络空间深刻改变着人们的生活方式、思维方式与价值观念，网络社交、在线教育等应用日益融入日常生活，重塑社会运行方式。

2.2 传统测绘理论在网络空间的应用与延伸

（1）地理测绘中的“地图-地志-对抗方针”模型在网络空间的延伸

在地理测绘中，“地图-地志-对抗方针”三层模型是一种经典的理论框架。地图是对地理空间的直观描绘，它展示了地理区域的地形、地貌、城市、道路等基本信息；地志则是对地理区域的更详细描述，包括当地的历史、文化、气候、资

源等方面的内容；对抗方针是基于地图和地志的信息，为军事作战、资源开发等活动制定的策略和方法。

在网络空间中，上述三层模型被进一步延伸和应用。网络空间地图类似于地理地图，通过对网络设备、IP 地址等网络资源的探测和分析，绘制出网络空间的拓扑结构和资源分布情况，帮助人们了解网络的基本架构和连接关系。网络空间地志则更深入地描述网络空间中的各种信息，如网络服务的类型、应用程序的功能、用户的行为模式等，这些信息有助于全面掌握网络空间的运行状态和特征。基于网络空间地图和地志的信息，可制定相应的对抗策略，如在网络安全领域部署防御机制，或在资源管理中优化分配与调度方案。

（2）情报分析四层级在网络测绘中的应用

传统的情报分析方法论为网络测绘赋予了价值挖掘能力，提供了知识提炼框架，使网络测绘可以更好的服务于网络安全、社会治理等战略需求。

- **描述性分析**：在网络测绘中，描述性分析是最基础的层级。它主要对网络空间中的各种要素进行客观的描述和记录，如网络设备的数量、类型、分布位置，网络带宽的使用情况，IP 地址的分配结构等。通过系统性的数据采集与整理，可形成网络空间现状的详细画像，为后续分析提供基础数据支撑。例如，利用网络扫描工具对一个企业的内部网络进行探测，记录所有已连接设备的名称、型号、IP 地址等信息，形成网络设备清单，这就是典型的描述性分析。
- **解释性分析**：解释性分析是在描述性分析的基础上，对网络空间中的现象和数据进行深入的解释和说明。它旨在回答“为什么”的问题，分析各种网络行为和事件发生的原因及其内在机制。例如，当网络出现异常流量时，通过解释性分析可以找出流量异常的源头设备，分析是由于网络攻击、软件故障还是用户的异常操作导致的流量变化。通过对网络日志、流量数据等进行挖掘和分析，探究事件背后的深层次原因。
- **评估性分析**：评估性分析侧重于对网络空间的安全性、可靠性、性能等方面进行量化评估。它基于预设的指标体系与评估标准，对网络系统的各组成部分进行综合评价，以判断网络空间的整体状况和风险等级。例如，评估一个企业网络的安全防护水平，可从网络边界防护、访问控制、数据加密等多个维度开展系统性评估，判断网络是否面临较高的安全风险，并给出相应的评估报告和改进建议。
- **预测性分析**：预测性分析是情报分析的最高层级，主要利用历史数据和趋势分析等方法，对网络空间的未来发展和可能出现的事件进行预测。在网络测

绘中，预测性分析可用于提前识别潜在威胁，辅助制定前瞻性防护策略。例如，通过对过去一段时间内网络攻击事件的统计分析，可预测未来一段时间内可能出现的攻击类型、攻击频率和攻击目标，从而有针对性地加强网络安全防护。

2.3 网络空间地图与网络空间坐标系

（1）地理/物理空间坐标

地理空间坐标是用于描述地球上地理位置的系统，最常见的是经纬度坐标系。通过经纬度的数值，可以精确地定位地球表面上的任意一点。在网络空间中，地理空间坐标仍然具有重要的意义，因为许多网络设备和基础设施都部署在现实的地理空间中。例如，数据中心有其具体的地理位置，通过地理空间坐标可以确定数据中心的所在地，这对于网络服务的优化、灾难恢复等方面具有重要作用。此外，一些基于位置的网络服务，如移动互联网应用中的定位服务、智能交通系统等，也依赖于地理空间坐标来提供准确的信息。

物理空间坐标则侧重于描述网络设备在物理环境中的具体位置，如服务器在机房中的机架位置、无线网络基站的安装高度和角度等。物理空间坐标对于网络设备的管理、维护和故障排除非常重要，它可以帮助网络管理人员快速定位设备，进行设备的安装、调试和维修等操作。

地理/物理空间坐标是传统空间定位的基础，主要依托于坐标系体系实现精准定位。国内互联网地图服务普遍采用加密坐标系以满足国家安全要求：

1. **WGS84**：全球通用的 GPS 标准坐标系，适用于未加密的原始定位数据。大多数手机的 GPS 模块获取的坐标通常基于该坐标系。

2. **GCJ02**（火星坐标系）：该坐标系由国测局制定，在 WGS-84 坐标基础上引入非线性偏移处理。高德、腾讯地图等主流互联网地图服务均采用该标准。该体系通过算法确保公开地图与真实地理坐标存在不可逆偏移。

3. **BD09**：百度地图在 GCJ02 坐标系基础上进行了进一步加密处理，通过二次坐标变换增强地理数据的保护强度。其坐标转换需依赖专用算法，与 WGS84 的直接兼容性较低。

这种分层加密机制体现了对物理空间坐标安全性与可控性的现实需求，也为网络空间坐标体系的设计提供了有益的技术参考。

（2）网络空间地图

网络空间地图作为数字世界的核心基础设施，正逐渐成为网络安全、信息化治理及数字化转型的关键支撑工具，也是网络空间测绘的重要输出之一。网络空间地图是以网络空间资产为核心，通过主被动测绘、大数据分析及多维度可视化技术构建的虚拟空间全景图。其核心功能包括：

1. **资产可视化**：实时感知全球网络空间中的 IT 资产（如设备、系统、服务等），并标注地理位置、运行状态及安全风险。
2. **态势感知**：动态呈现网络威胁分布（如漏洞、攻击路径），辅助制定防御策略。
3. **跨域映射**：融合地理空间域、虚拟网络域及社会空间域，构建多维度关联的“数字沙盘”。

网络空间地图在技术层面涉及节点标识、拓扑建模、服务映射等内容：

1. **节点标识**：在特定网络层级与范围内，可通过自治系统号码 ASN、IP 地址、MAC 地址等多种标识符组合标识网络设备。
2. **拓扑建模**：刻画设备间的连接关系（如路由器、服务器链路），形成动态网络图谱。
3. **服务映射**：标注关键服务（如域名服务器、内容分发网络节点）的位置与状态。

与物理地图不同，网络地图需动态更新以反映实时流量、故障节点等变化，这对数据采集与渲染技术提出了更高要求。

（3）网络空间坐标理论

网络空间坐标理论旨在通过数学方法描述网络实体的位置与关系，常见研究方向包括：

1. **多维属性坐标化**：将延迟、带宽、节点负载等参数映射为多维坐标轴，形成性能坐标系。例如，基于欧氏距离的坐标模型可优化内容分发路径。
2. **动态坐标变换**：借鉴希尔伯特空间的升维思想，将网络状态变化（如拥塞）转化为坐标变换，实现全局资源调度，或者将不同的网络节点标识作为坐标的不同维度，构建新型网络空间坐标，实现网络空间与地理空间的映射等。

3. **加密与标准化：**参考地理坐标的加密机制，设计网络坐标的隐私保护算法，防止恶意节点定位。

该领域仍面临动态性与复杂性挑战，需结合机器学习与拓扑分析进一步突破，特别是网络空间坐标理论还很不成熟，还未在更广泛的范围内形成共识。

第三章 网络空间测绘技术体系

3.1 核心技术

网络空间测绘技术体系主要包括三个大的方面，即探测技术、数据分析技术和可视化技术等，如图 3.1 所示。

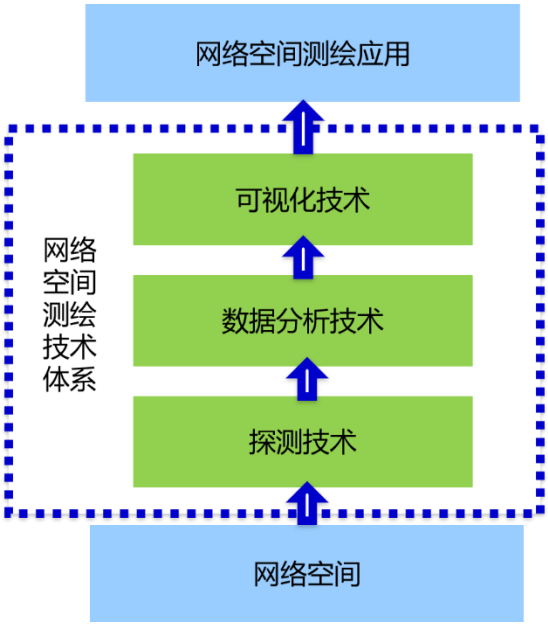


图 3.1 网络空间测绘技术体系

3.1.1 探测技术

在网络空间测绘领域，探测技术是基础性的关键环节，它如同网络空间里的“雷达”，能够主动发现目标网络中的各种资产信息，包括主机、设备、服务等。准确且高效的探测技术可以为后续的分析和决策提供坚实的数据基础。随着网络技术的不断发展，探测技术也在不断演进，涵盖了从简单的 IP 活跃性探测到复杂的资产指纹识别等多个方面，本节将对这些关键技术进行详细阐述，并结合国内外学术界和工业界的最新成果进行分析。

3.1.1.1 IP 活跃性探测/端口开放性探测

一、基本原理

1）IP 活跃性探测

IP 活跃性探测的核心目标是确定网络中某个 IP 地址是否处于活跃状态。常见的方法是使用 ICMP（Internet Control Message Protocol）协议。ICMP 是 TCP/IP 协议族中的一种控制消息协议，用于在主机与路由器之间传递网络状态信息。典型做法是向目标 IP 地址发送 ICMP Echo Request（即 Ping 报文），若目标主机处于活跃状态并允许 ICMP 响应，则会返回 ICMP Echo Reply 报文，从而确认该 IP 地址的活跃性。

2）端口开放性探测

端口开放性探测则是确定目标主机上哪些端口是开放的。在 TCP/IP 协议中，端口是应用程序与外界进行通信的出入口，不同的服务通常监听不同的端口。例如，HTTP 服务通常监听 80 或 443 端口。通过向目标主机的不同端口发送特定的数据包，根据返回的响应来判断端口是否开放。常见的端口探测方法有 TCP SYN 扫描、TCP Connect 扫描等。

二、国内外研究现状与成果

1）国外代表性成果

- **Nmap**：Nmap 是由 Fyodor 开发的一款广受欢迎的网络扫描工具，广泛应用于网络安全检测与资产发现任务中。该工具支持多种扫描技术，包括 TCP SYN 扫描、TCP Connect 扫描、UDP 扫描等，具备高效且准确的端口探测能力，可快速发现目标主机开放的端口。Nmap 还提供了丰富的脚本引擎，支持用户编写自定义脚本以实现更复杂的功能。众多国外网络安全机构和研究团队都将 Nmap 作为网络探测的重要工具，并基于其进行二次开发与功能扩展。

- **ZMap**：ZMap 是一款开源的高性能网络扫描工具，专为快速扫描大规模 IP 地址空间而设计。其核心优势在于采用无状态扫描机制，即不维护单个连接的状态信息，从而显著提升扫描效率。ZMap 可在数分钟内完成对整个 IPv4 空间中某一指定端口（如 443 端口）的全面扫描，性能远超传统工具如 Nmap。ZMap 支持模块化扩展，允许用户自定义探测协议（如 HTTP、DNS）和数据分析模块，适用于网络普查、安全漏洞检测等场景。例如，研究人员常用它发现暴露的物联网设备或评估 HTTPS 部署情况。该工具资源占用低，普通服务器即可运行，但需一定网络知识配置参数。

- **Masscan**：Masscan 是一款高速的端口扫描工具，由 Robert David Graham 开发。它采用异步扫描技术，能够在短时间内扫描大量的 IP 地址和端口。Masscan 的扫描速度比 Nmap 快得多，适用于大规模网络的快速探测。在国

外的一些大型网络安全演习和研究项目中，Masscan 被广泛应用于快速发现网络中的开放端口和活跃主机。

2）国内代表性成果

- **X-Scan**：国内一款知名的网络安全扫描器，支持 IP 活跃性探测和端口开放扫描。它具有简洁易用的界面和丰富的扫描选项，适合初学者和专业安全人员使用。X-Scan 在国内的一些企业网络安全评估和网络测绘项目中得到了广泛应用。

- **绿盟科技的 IP 探测技术**：该技术采用了多线程、多协议的探测方式，结合智能策略调度，提高了 IP 活跃性探测和端口开放扫描的效率和准确性。在一些大型的国家级网络安全监测项目中，该技术技术为及时发现网络中的异常活跃 IP 和开放端口提供了有力支持。

- SMap：SMap[1]是一款开源的国产化高性能网络扫描工具，兼具 IPv4/IPv6 双栈多场景高效探测。为支撑国家网络空间测绘能力提升，摆脱国内对国际开源扫描器的研究依赖，中关村实验室联合清华大学、中原工学院等高校协同研发了新型网络测量工具 SMap，在性能与功能上超越现有国际主流扫描器工具如 NMap、ZMap 等。SMap 针对传统工具在扩展性差、定制困难、维护成本高等问题，提出高性能、模块化、可编程的架构设计，全面支持自定义测量逻辑、多协议并发探测、IPv4/IPv6 混合扫描等功能，具备更强的灵活性和可持续演进能力。工具采用 Rust 编程语言实现，具有可扩展性强、内存安全、并发友好、无运行时依赖、可跨平台构建与部署等技术优势，并借助 Rust 的“零成本抽象”特性，在保障高性能的同时显著提升了代码可维护性。相较于传统扫描工具，SMap 集成多种前沿探测算法，在 IPv6 活跃地址探测、端口与服务识别、网络拓扑发现等关键任务中表现出更优的性能与适应性。该工具定位于替代并升级现有 ZMap 等国际扫描工具，研制国产化高水平开源扫描器，建议国内科研人员优先采用并积极参与 SMap 的后续维护与生态建设。

三、技术发展趋势

随着网络环境的日益复杂，IP 活跃性探测和端口开放性探测技术也面临着新的挑战和机遇。一方面，网络设备的防火墙和入侵检测系统不断升级，对探测行为的防范能力增强，需要发展更隐蔽、更有效的探测技术。另一方面，物联网

1 Smap github 项目:https://github.com/AddrMiner/smap

等新兴技术的发展使得网络中的设备数量急剧增加，对大规模网络的快速探测提出了更高的要求。未来，融合人工智能和大数据技术的智能探测技术将成为发展趋势，通过学习网络行为模式，实现更精准、更高效的探测。

3.1.1.2 服务扫描

一、基本原理

服务扫描是在确定目标主机的开放端口后，进一步识别每个开放端口上运行的具体服务。不同的服务在通信过程中有不同的协议和数据交互模式。通过向开放端口发送特定的请求数据，并分析返回的响应数据，就可以判断该端口上运行的服务类型。例如，对于 HTTP 服务，发送一个简单的 HTTP 请求，根据返回的 HTTP 响应头信息可以确定服务器的类型、版本等信息。响应数据的分析依赖于协议解析技术。

协议解析是网络空间测绘中非常重要的一项技术，它通过对网络中传输的数据报文进行深入分析，识别出其中所遵循的协议类型、结构以及携带的信息。在网络空间中，存在着各种各样的网络协议，如常见的 TCP、UDP、HTTP、FTP 等，不同的协议具有不同的功能和数据格式。准确地解析协议对于识别网络资产、发现潜在风险等方面具有关键作用。

以下是一个简单的 HTTP 协议报文解析示例图，展示了 HTTP 报文的基本结构，包括请求行、请求头、请求数据等。

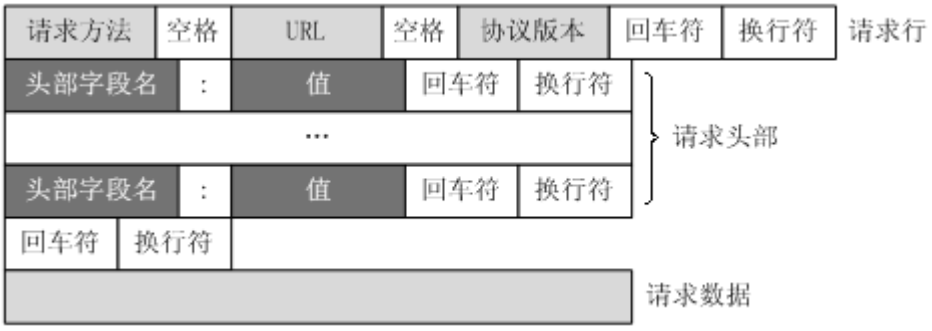


图 3.2 HTTP 协议报文解析示例

协议解析主要基于以下原理：

- **报文特征匹配**：每种协议的报文都具有特定的格式和字段特征。通过对报文的头部、数据部分等进行精确匹配，判断其所属的协议类型。例如，HTTP 请求报文以特定的请求行（如 GET、POST 等方法）开头，后续包含若干头部字段及可选的消息体，通过识别这些特征可以确定是 HTTP 协议。

- **状态机分析**：对于一些具有状态性的协议，如 TCP 协议，使用状态机来跟踪连接的不同状态变化。通过监测状态的转移，可以更准确地理解协议的执行过程和数据交互逻辑。

二、国内外研究现状与成果

1）国外代表性成果

- **ServiceScan**：这是国外一款专门用于服务扫描的工具，它结合了多种协议分析方法，能够准确识别各种常见和稀有服务。ServiceScan 采用了先进的指纹匹配技术，预先收集了大量服务的特征指纹，通过与扫描结果进行比对，快速准确地确定服务类型。在国外的网络漏洞挖掘和安全评估项目中，ServiceScan 被广泛应用于发现网络中隐藏的服务漏洞。

- **Shodan**：Shodan 是一个著名的搜索引擎，它通过扫描全球网络中的设备，建立了一个庞大的设备和服务数据库。Shodan 不仅能够扫描开放端口和识别服务类型，还能收集设备的地理位置、操作系统版本等信息。许多安全研究人员和企业利用 Shodan 来了解全球网络中的服务分布情况和安全态势。

- **LZR:** LZR 是一种高效的网络服务发现工具，旨在检测和识别运行在非标准端口上的服务。它通过与 ZMap 协同工作，能够在仅发送两个额外数据包的情况下，同时检测多达 18 种协议，并对超过 35 种协议进行指纹识别。LZR 的核心创新在于其能够快速完成协议握手并分析响应数据，从而高效识别服务类型。该工具在大规模网络扫描中具有性能优势，具备发现隐藏服务和潜在安全风险方面的能力。LZR 的应用场景包括网络安全研究、攻击面管理以及第三方依赖风险评估，为理解互联网服务的分布和安全态势提供了重要支持。

- **Nmap 的协议支持**：Nmap 是一款广泛使用的开源网络扫描工具，它支持多种协议的扫描和解析。例如，它可以通过发送不同类型的数据包来探测目标主机上的 TCP 和 UDP 端口状态，同时还能对常见服务的协议进行简单的解析。Nmap 背后的开发者社区一直在持续更新对新协议的支持，不断增强其协议解析的能力。

- **Tcpdump**：Tcpdump 作为命令行网络嗅探工具，其核心能力在于底层协议抓取与结构化解析。它通过 BPF（Berkeley Packet Filter）语法对网络流量进行细粒度过滤，支持对以太网帧、IP/TCP/UDP/ICMP 等数百种协议的头部字段进行逐层解码。在网络测绘中，该工具常用于协议特征提取、异常流量定位和跨层关联分析。

- **Wireshark 的深度解析**：Wireshark 是一款强大的网络协议分析软件，它能够对捕获的数据包进行极其详细的协议解析。该工具支持解析数百种网络协议，并提供直观友好的图形化用户界面，便于用户查看和分析各协议字段的具体内容。Wireshark 也常被科研人员用于对新发现或未知协议进行逆向分析与协议行为研究，广泛应用于网络通信解析、协议标准验证及安全研究等场景。

2）国内代表性成果

- **绿盟科技的服务扫描方法**：绿盟科技的服务扫描采用了全量探测和智能匹配相结合的方法。它不仅能够识别常见的服务，还能针对一些自定义服务进行深度检测。通过不断更新服务指纹库，绿盟科技的服务扫描技术能够适应不断变化的网络环境。

- **远江盛邦的资产探测技术**：远江盛邦的资产探测支持 IPv4、IPv6 双栈探测、域名探测，具备对指定范围 IPv4/IPv6 地址的全方位属性识别能力，能够识别包含服务、操作系统、设备类型、厂商、组件等资产属性，并可通过服务 banner 信息匹配发现资产脆弱性。

三、技术发展趋势

未来，服务扫描技术将朝着更自动化、更智能化的方向发展。随着微服务和无服务器架构的广泛应用，服务的数量和复杂度不断增加，传统的服务扫描方法将面临挑战。智能化的服务扫描技术将利用人工智能和机器学习算法，自动学习服务的行为模式和特征，实现对未知服务的快速识别和分析。同时，服务扫描与威胁情报的结合也将成为发展趋势，通过关联已知的威胁情报，及时发现潜在的服务安全威胁。

3.1.1.3 资产指纹识别

一、概念与背景

资产指纹识别是网络空间测绘中用于确定网络资产的具体信息和特征的技术。在复杂的网络环境中，存在着大量的不同类型的网络资产，如服务器、路由器设备、物联网设备等。通过资产指纹识别，可以准确地识别出这些资产的品牌、型号、操作系统版本、应用程序类型等信息，为网络资产管理、安全评估等提供重要依据。

二、技术原理

资产指纹识别主要基于以下几种原理：

- **特征码匹配**：为不同的网络资产生成唯一的特征码，这些特征码可以是资产的软件版本号、配置信息、特定文件的哈希值等。通过对目标资产进行扫描，提取其特征信息并与预先存储的特征码库进行匹配，从而确定资产的类型和详细信息。
- **行为分析**：观察资产在网络中的行为模式，如服务的响应时间、请求处理方式、协议使用习惯等。不同品牌和型号的资产在行为上可能存在差异，通过对这些行为特征的分析，可以辅助进行资产的识别。

以下是一个资产指纹识别流程的示例图，包含资产指纹识别前期的主被动信息采集与后期的风险评估分析：

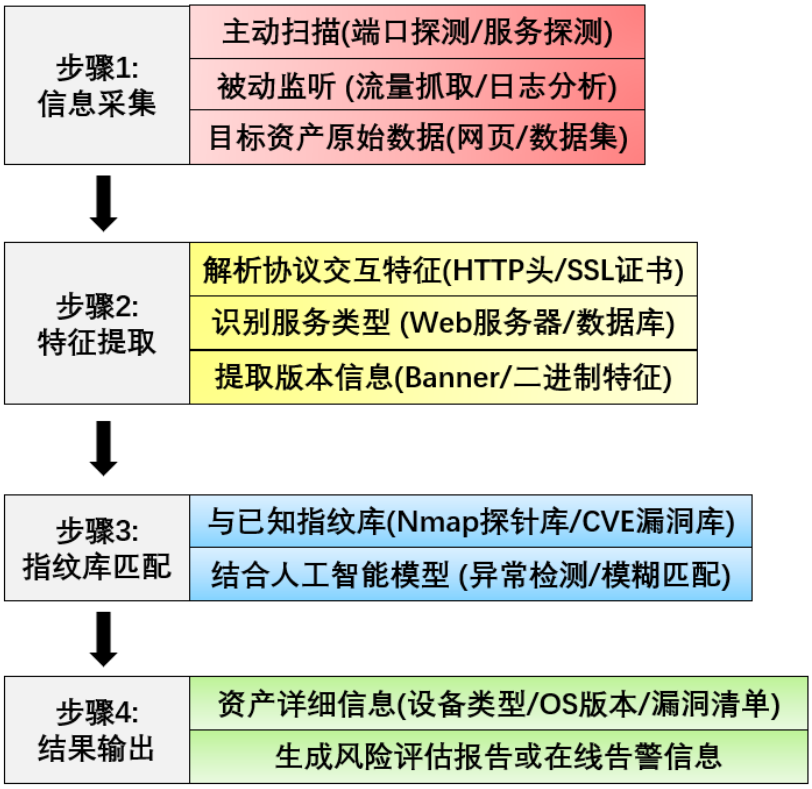


图 3.3 资产指纹识别流程示意图

该图展示了资产指纹识别的主要流程，包括信息采集、特征提取、指纹库匹配和结果输出等环节。通过这样的流程，可以逐步确定目标资产的详细信息。

三、国内外研究现状与成果

1）国外代表性成果

- **Shodan 网络空间搜索引擎**：Shodan 被称为“互联网上最可怕的搜索引擎”，它通过对大量的网络资产进行扫描和指纹识别，建立了庞大的资产数据库。

用户可以通过 Shodan 搜索特定类型的网络资产，获取其详细的信息，如地理位置、开放端口、服务类型等。Shodan 不断收集新的资产指纹信息，保持对网络空间资产的实时监测。

- **Censys 网络空间搜索引擎：**Censys 专注于网络资产的深度测绘和识别，采用了先进的机器学习和深度学习算法来提高资产指纹识别的准确性。它不仅可以识别常见的网络资产，还能对一些隐蔽的、使用自定义协议的资产进行精准识别，为网络安全研究和情报收集提供了有价值的数据。

2）国内代表性成果

- **绿盟科技的全量探测方法：**绿盟科技提出了一种全量探测的资产指纹识别方法，该方法通过对目标网络进行全方位的扫描和探测，收集资产的各种特征信息。同时，利用大数据和人工智能技术对这些特征信息进行分析和处理，构建了一套完善的资产指纹库。通过不断更新和优化指纹库，能够提高对新型资产和未知资产的识别能力。

- **ZoomEye 网络空间搜索引擎：**ZoomEye 是由知道创宇开发的网络空间测绘搜索引擎，具备较强的资产指纹识别能力，广泛应用于网络安全态势感知和威胁情报分析。该平台特别注重资产的安全特性与漏洞关联性，通过对网络设备和服务指纹的深度提取与分析，能够快速发现潜在安全风险，辅助用户识别存在漏洞的资产，并提供相应的防护建议。ZoomEye 的探测体系融合主动扫描与安全指纹匹配机制，可有效支撑攻击面管理和漏洞监测等任务。

- **FOFA 网络空间搜索引擎：**FOFA 是由华顺信安推出的网络空间搜索引擎，专注于网络资产的指纹识别与分类，通过大规模数据采集与智能分析，构建了全面的资产指纹库。其技术核心在于对网络设备、服务、应用等特征的深度提取与匹配，能够精准识别 IP、端口、协议、服务版本等信息。FOFA 利用主动探测与被动流量分析相结合的方法，持续更新指纹规则，支持对复杂网络环境的资产发现与分类。该平台广泛应用于网络安全、漏洞扫描、攻击面管理等领域，为企业和安全团队提供高效的资产测绘与风险识别能力。

- **DayDayMap 网络资产测绘平台：**DayDayMap 是由盛邦安全推出的新一代网络空间测绘引擎，尤其是在 IPv6 网络资产指纹识别方面表现出色。该平台在资产指纹识别方面，依托其强大的自动化指纹提取技术和深度协议解析能力，能够精准识别网络资产信息，包括设备类型、操作系统、应用服务、厂商及版本等多维属性。其指纹库覆盖 23 万+硬件指纹，涵盖安防、工控、物联网等 30+类别，支持 IPv4/IPv6 双栈探测，并通过动态匹配专属口令库，提升弱

口令检测的精准性。平台还结合 AI 技术，实现了资产识别与风险评估的智能化优化，广泛服务于政企机构的网络防护与攻防演练。

3.1.2 分析技术

3.1.2.1 资产关联分析

一、资产关联分析的意义

资产关联分析旨在挖掘不同网络资产之间的潜在关联关系，包括物理连接、逻辑连接、业务依赖等多种形式。通过构建资产间的关联模型，可更全面地理解网络的整体架构，识别关键节点与依赖链条，评估单点故障可能引发的连锁影响，进而揭示潜在的安全风险传播路径。

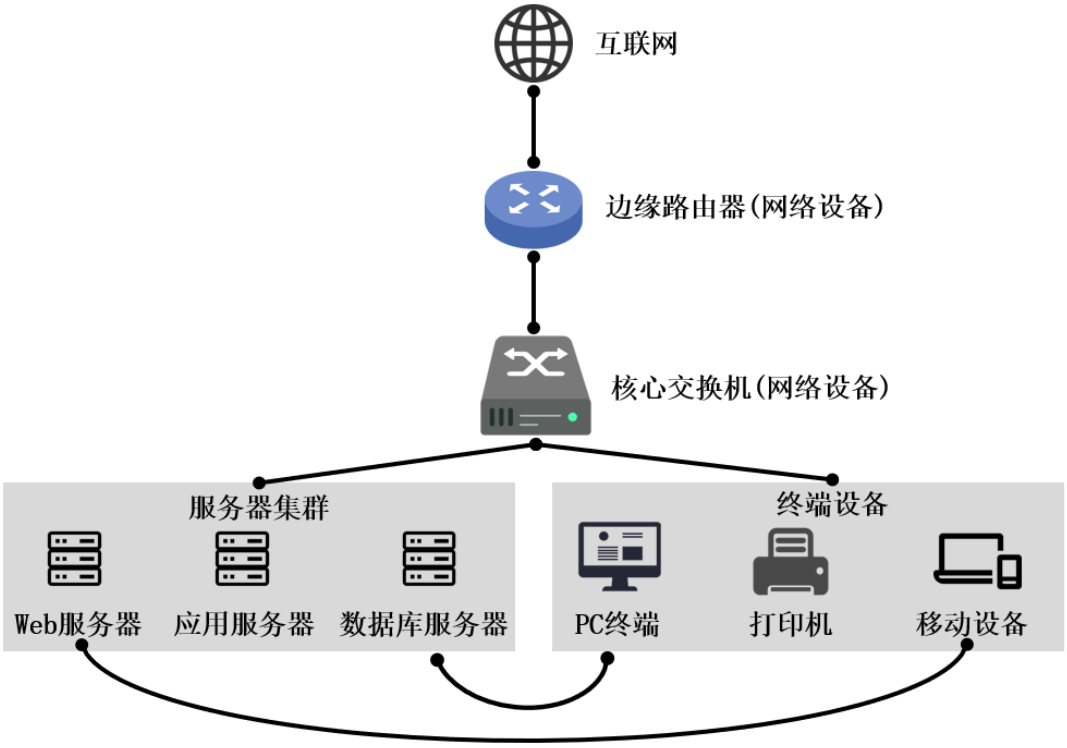


图 3.4 资产关联分析的示例图

以图 3.4 为例，展示了某企业网络中各类资产的关联关系。图中使用不同形状的图标区分服务器、终端、网络设备等资产类型，并通过连线表示它们之间的物理或逻辑连接。该可视化图示有助于直观理解资产间的依赖关系与网络结构。

二、国内外学术界研究成果

1）国外研究成果

- **英国剑桥大学研究团队：**提出了基于图论的资产关联分析方法。该方法将网络中的每个资产看作图中的节点，资产之间的关系看作边，构建资产关系图。通过图的遍历和社区发现算法，识别出资产的不同群落和关键连接节点。例如，使用 Louvain 算法对资产关系图进行社区划分，将相关性强的资产划分到同一个社区中，便于后续的针对性分析。
- **美国斯坦福大学、CMU 等的研究：**专注于基于机器学习的资产关联预测。利用历史的资产连接数据和业务操作记录，训练深度学习模型（如 LSTM 长短期记忆网络）来预测资产之间未来的关联关系。

2）国内研究成果

- **清华大学的科研团队：**研发了基于知识图谱的资产关联分析系统。该系统整合了网络配置信息、资产属性信息和安全事件信息，构建了一个大规模的知识图谱。通过图神经网络（GNN）对知识图谱进行推理，挖掘出隐藏的资产关联关系。例如，在一个大型企业网络中，该系统能够发现不同部门的服务器之间由于共享存储资源而产生的关联。
- **中国科学院信工所的研究：**提出了基于信息论的资产关联度量方法。该方法通过计算资产之间的互信息和条件熵，量化资产关联的强度。以数据中心为例，通过该方法可以准确评估服务器与存储设备、网络设备之间的关联紧密程度。

三、国内外工业界研究成果

1）国外公司成果

- **IBM：**提供的安全信息和事件管理（SIEM）系统中包含资产关联分析模块。该模块结合威胁情报和资产信息，对资产之间的关联关系进行分析，发现潜在的攻击传播路径。例如，当检测到某个端点设备被入侵时，系统能够通过资产关联分析预测可能被攻击的其他相关资产。
- **Splunk：**依托大数据分析平台，根据通用安全分组技术和计算（包括相似实体、累积风险评分、MITRE ATT&CK 阈值等），基于预定规则将海量日志与资产信息融合，通过自适应关联分析算法识别跨系统的攻击传播链条。

2）国内公司成果

- **阿里云：**在其云计算平台上推出了资产关联洞察服务。利用大数据和人工智能技术，对云环境中的各种资产（如虚拟机、容器、数据库等）进行关联分

析。通过建立资产关联模型，能够帮助用户快速定位故障的根源和影响范围。例如，当某个云数据库出现性能问题时，系统可以通过资产关联分析找出可能导致问题的上游服务。

- **奇安信**：其网络空间测绘平台具备资产关联分析能力。通过深度扫描和数据挖掘技术，分析企业网络中各种资产的关联关系，为企业提供全面的网络拓扑视图和资产依赖关系图。例如，帮助企业发现办公网络中员工电脑与服务器、网络设备之间的关联，识别潜在的安全风险。

3.1.2.2 资产与组织关联映射分析

一、资产与组织关联映射分析的概念与重要性

资产与组织关联映射分析旨在将网络资产与所属的组织实体（如部门、业务单元、公司等）进行关联和映射。通过这种分析，可以更好地了解组织对资产的使用和管理情况，评估不同组织部门的安全风险，以及在发生安全事件时能够快速定位责任主体。

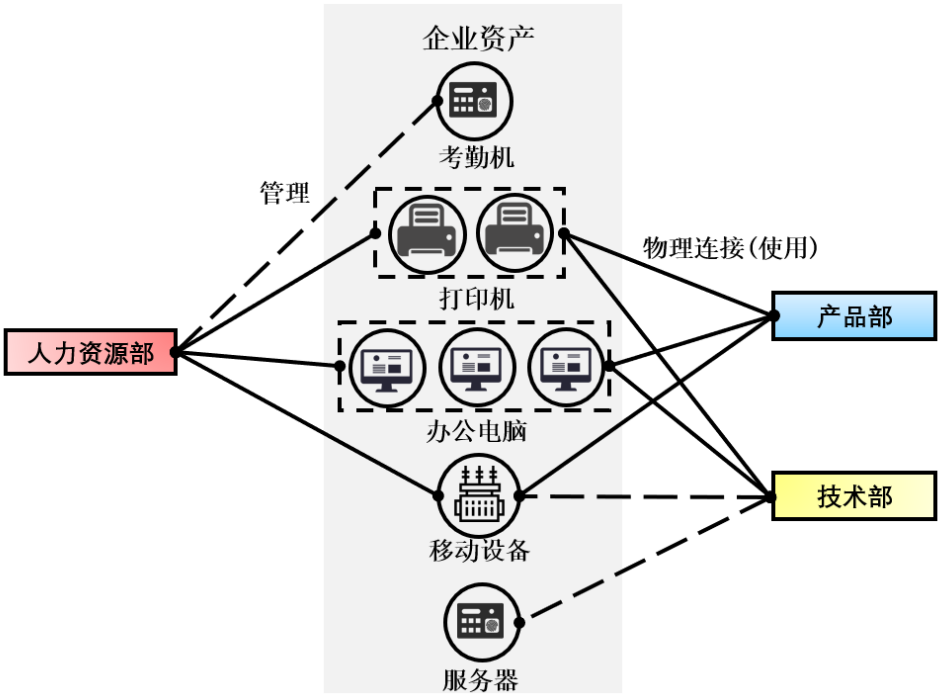


图 3.5 资产与组织关联映射分析的示例图

以图 3.5 为例，展示了一个企业的组织架构和资产的关联映射。不同颜色的方块表示不同的组织部门，圆形表示资产。通过线条将资产与所属的组织部门连接起来，直观地展示了资产与组织的关联关系。

二、国内外学术界研究成果

1）国外研究成果

- **澳大利亚悉尼大学：**开展了基于身份认证和访问控制数据的资产与组织关联研究。通过分析用户的身份认证信息和对资产的访问权限，建立资产与用户所属组织的关联关系。例如，通过 LDAP（轻量级目录访问协议）和 Kerberos 认证系统的数据，确定每个员工所属的部门以及他们可以访问的资产，从而实现资产与组织的映射。

- **德国慕尼黑工业大学：**提出了基于社会网络分析的资产与组织关联模型。将组织内的人员和资产看作社会网络中的节点，人员对资产的操作关系看作边，通过社会网络分析方法（如中心性分析、传播分析等）揭示资产与组织之间的潜在关联。例如，发现某个关键资产在组织内的重要性和影响力。

2）国内研究成果

- **上海交通大学：**研究了基于区块链技术的资产与组织关联映射方法。利用区块链的不可篡改和分布式账本特性，记录资产的归属和使用信息，确保资产与组织关联信息的真实性和完整性。例如，在一个跨部门的项目中，通过区块链记录每个部门对项目相关资产的投入和使用情况，实现资产与组织的精确映射。

- **复旦大学：**开展了基于大数据挖掘的资产与组织关联分析。通过收集和分析组织的各种业务数据（如财务数据、项目管理数据等），挖掘资产与组织部门之间的隐藏关系。例如，通过分析项目成本数据，发现某个部门在特定项目中对资产的使用成本，从而建立资产与组织的关联。

三、国内外工业界研究成果

1）国外公司成果

- **甲骨文（Oracle）：**在其企业资产管理系统中提供了资产与组织关联映射功能。通过集成企业的人力资源管理系统和资产清单系统，将资产分配到相应的组织部门，并跟踪资产在组织内的使用和流转情况。例如，当员工离职时，系统能够自动更新与该员工相关的资产与组织的关联关系。

- **微软（Microsoft）：**其 Azure 云服务平台支持资产与组织单元的关联映射。企业可以在平台上创建不同的组织层次结构（如部门、团队等），并将云资产（如虚拟机、存储账户等）分配到相应的组织单元，方便企业进行资源管理和安全控制。

2）国内公司成果

- **华为**：在其企业网络解决方案中提供了资产与组织关联分析功能。通过整合企业的园区网络、办公系统和人员信息，实现资产与组织部门的精确映射。例如，在一个大型企业园区中，能够实时掌握每个部门所拥有的网络设备和办公终端的使用情况。
- **深信服**：其安全管理平台具备资产与组织关联映射能力。通过收集企业的网络拓扑信息、用户认证信息和资产信息，建立资产与组织的关联模型。在发生安全事件时，能够迅速定位受影响的组织部门和相关资产，为应急响应提供有力支持。

3.1.2.3 资产定位

一、定义及重要性

资产定位是指在网络空间中准确确定网络资产的物理位置、逻辑位置以及所属组织等信息的过程。准确的资产定位有助于网络安全管理者了解资产分布，制定合理的安全策略，提高应急响应效率。

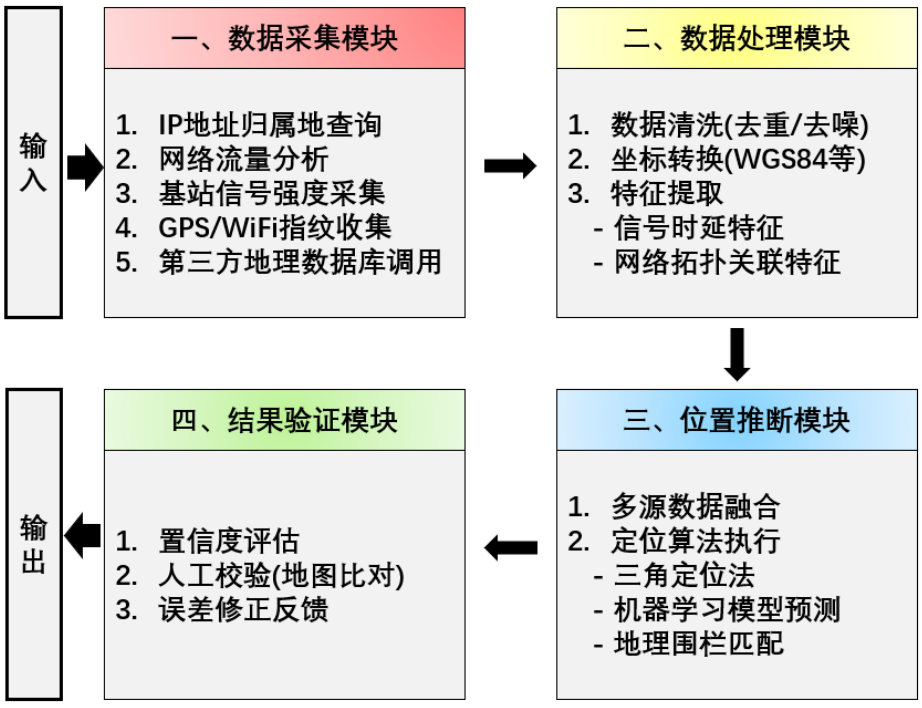


图 3.6 资产定位总体流程

图 3.6 为资产定位的总体流程，包括数据采集、数据处理、位置推断和结果验证等环节。数据采集模块负责收集各种与资产位置相关的信息，如 IP 地址、网络流量、基站信号等；数据处理模块对采集到的数据进行清洗、转换和特征提

取；位置推断模块根据处理后的数据，利用各种定位算法确定资产的位置；结果验证模块对定位结果进行准确性评估和修正。

二、国内外学术界成果

1）国外学术界

- **基于地理位置指纹的资产定位：**美国部分大学的研究团队利用全球 IP 地址分配规则以及网络流量的地理路由特征，结合基站位置、卫星定位等信息，通过机器学习算法构建地理位置指纹库，实现对网络资产物理位置的高精度定位。例如，一些学者通过分析 DNS 解析响应中的 IP 信息以及网络延迟等参数，设计了基于贝叶斯网络的地理位置推断模型，能够在一定程度上规避 IP 代理等干扰因素。

- **基于网络拓扑的资产逻辑定位：**欧洲的研究机构开展了关于网络拓扑结构与资产逻辑位置关系的研究。他们提出了利用图论和复杂网络理论，对网络中的节点和链路进行建模和分析，以确定资产在网络拓扑中的精确位置。通过挖掘网络设备之间的通信关系和数据流向，使用图嵌入算法将网络拓扑信息转化为低维向量，从而实现对资产逻辑位置的快速准确识别。

2）国内学术界

- **多源数据融合的资产定位方法：**国内一些高校结合地理信息系统（GIS）数据、域名系统（DNS）数据、网络流量数据等多源数据，提出了融合多模态信息的资产定位算法。通过构建数据关联模型，充分挖掘不同数据源之间的互补信息，提高资产定位的准确性和可靠性。例如，某高校研究团队将网络扫描数据与运营商的基站位置数据进行融合，利用深度学习算法实现对移动终端资产的高精度定位。

- **基于区块链的资产定位安全验证：**为保障资产定位信息的安全性和可信性，国内部分研究机构开展了基于区块链技术的资产定位研究。通过将资产定位信息存储在区块链上，利用区块链的不可篡改和分布式共识机制，确保资产位置信息在传输和存储过程中的完整性和真实性。同时，采用智能合约对资产定位信息进行自动化验证和审计，有效防止信息被恶意篡改。

- **基于大规模地标挖掘及图神经网络的定位方法：**为了实现全球范围内的高精度 IP 地理定位，清华大学研究团队从定位地标和定位算法的角度研究基于大规模地标挖掘及基于图神经网络的定位方法。通过挖掘地标网页的特征，利用搜索引擎在全网范围内检索定位地标，确保定位的过程中有足够的定位

约束输入。基于这些地标节点，在全球范围内构建地理定位图结构，并引入图神经网络（GNN）对目标资产的地理位置进行预测。该方法有效缓解了因约束信息分布不均而导致的区域性误差，同时依托高密度地标覆盖与图神经网络的强表征能力，显著提升了定位精度。

三、国内外工业界成果

1）国外工业界

- **网络安全厂商的资产定位解决方案：**国外一些知名的网络安全公司，如 Fortinet、CrowdStrike 等，推出了基于云平台的资产定位服务。他们通过在全球范围内部署探测节点，收集网络资产的相关信息，并结合大数据分析和机器学习技术，实现对资产的实时定位和监控。这些解决方案支持多维度的资产搜索和筛选功能，能够为企业提供全面的资产分布视图。

- **互联网服务提供商的资产定位技术：**像 Google、Amazon 等互联网巨头，在其数据中心和云服务平台中采用了先进的资产定位技术。他们利用自研的网络管理系统和自动化工具，对分布在全球各地的数据中心资产进行精确管理和定位。通过实时监测网络设备的状态和性能，能够快速准确地定位网络故障和异常资产，保障云服务的稳定性和可靠性。

- **专业的 IP 定位服务 Maxmind、IP2Location：**MaxMind 是一家提供 IP 定位和在线欺诈检测服务的公司，其核心产品 GeoIP 数据库通过分析 IP 地址的地理位置信息（如国家、城市、经纬度等），广泛应用于广告定向、内容本地化和网络安全等领域。MaxMind 提供的 IP 地理定位数据库覆盖全球主要地区，具有较高的数据更新频率，并支持多种编程语言的集成调用，是当前业界广泛采用的主流 IP 定位解决方案之一。IP2Location 提供基于 IP 地址的地理位置和网络属性数据库，支持查询国家、地区、城市、ISP、经纬度等信息。其数据库广泛应用于电子商务、网络安全、数字版权管理等领域。IP2Location 提供多种数据格式和 API，支持灵活集成，并以高精度和频繁更新著称，是 IP 定位领域的重要工具之一。

2）国内工业界

- **安全态势感知平台的资产定位功能：**国内的网络安全厂商，如奇安信、深信服等，在其安全态势感知平台中集成了资产定位模块。这些模块通过与多种安全设备和数据源进行对接，实现对企业内部网络资产的全面扫描和定位。同时，利用可视化技术将资产位置信息以地图或拓扑图的形式展示出来，为安全管理人员提供直观的决策支持。

- **运营商的物联网资产定位服务：**中国移动、中国联通等国内运营商在物联网领域开展了资产定位业务。他们依托自身的通信网络优势，为物联网设备提供基于基站定位、GPS 定位等多种方式的资产定位服务。通过建立物联网资产数据库，实现对物联网设备的实时跟踪和管理，为智慧城市、智能交通等领域的应用提供了有力支持。

- **专业的 IP 定位服务埃文科技、IPIP.net：**埃文科技是一家全球领先的 IP 地址定位服务提供商，专注于高精准实时 IP 定位技术。其数据库覆盖全球 43 亿 IPv4 和 2^{128} IPv6 地址，支持城市级、区县级甚至街道级定位，广泛应用于广告投放、网络安全、反欺诈等领域。埃文科技通过大数据挖掘和网络探测技术，结合多层神经网络算法，提供高精度的 IP 地理位置信息和丰富的 IP 风险画像。IPIP.net 提供基于 IP 地址的地理位置查询服务，支持 IPv4 和 IPv6 地址的定位。其数据库覆盖全球，能够精确到城市级别，部分数据可细化到区县。IPIP.net 的数据更新频率较高，广泛应用于网络管理、广告投放和网络安全等领域。其服务形式包括在线 API 和离线数据库，适合多种应用场景。

- **清华大学融合定位服务：**清华大学研究团队构建了一套具备高精度、高覆盖度和高可靠性的 IP 地址定位服务，覆盖对象包括 IPv4 全地址空间及超过 12 亿长期活跃的 IPv6 地址。该定位系统整体精度达到城市级及以上，其中部分数据可精确至街道级，少量数据可实现楼宇级定位，显著提升了大规模网络空间测绘中的地理感知能力。定位库能实现日频率的动态更新，支持在线定位计算和批量 IP 位置查询，相比其他定位库具有更高的精度、覆盖度和可靠度。该定位库来源于高精度 IP 定位算法和 IP 定位库的智能融合。一方面，基于大规模的地标挖掘和图神经网络定位算法，实现全球 IP 的高精度定位。另一方面，通过全面、广泛的定位库测量，对当前主流的定位库进行评估和量化融合。基于强化学习框架融合定位算法和定位库的定位结果，实现多来源定位结果的智能融合和校验，进一步提升定位库的质量。其服务形式包括在线 API 和离线数据库，适合不同场景的定位应用。

3.1.2.4 威胁建模

一、定义及重要性

威胁建模是一种识别、评估和分析网络系统面临的潜在威胁的过程。通过构建威胁模型，网络安全人员可以更好地了解系统的安全弱点，提前制定应对措施，降低安全风险。

图 3.7 展示了威胁建模的基本流程，主要包括系统分析、威胁识别、威胁评估和模型建立四个步骤。系统分析阶段主要对目标系统的架构、功能、资产分布等进行全面了解；威胁识别阶段通过各种手段收集和分析潜在的威胁信息；威胁评估阶段对识别出的威胁进行量化评估，确定其严重程度和影响范围；模型建立阶段根据前三个阶段的结果，构建威胁模型，并将其应用于安全决策和防护措施的制定。

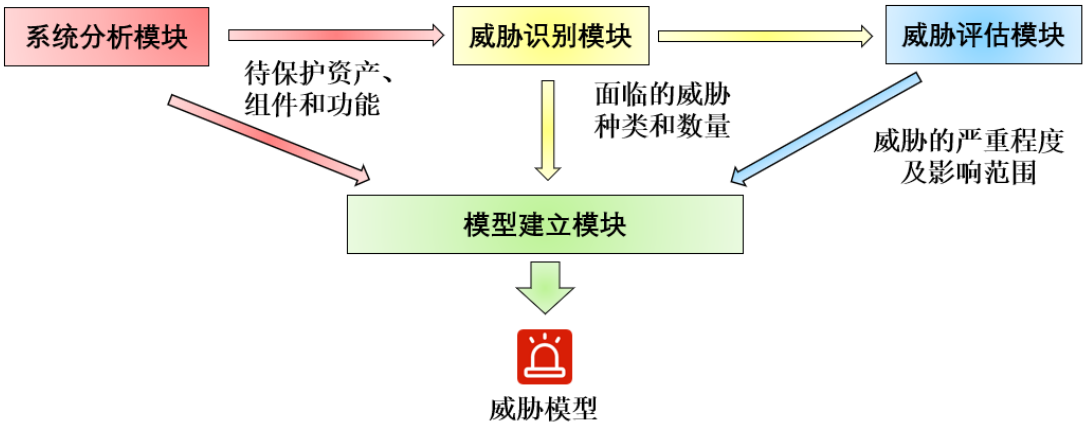


图 3.7 威胁建模的基本流程

二、国内外学术界成果

1）国外学术界

- **基于攻击图的威胁建模：**美国的一些研究团队提出了基于攻击图的威胁建模方法。攻击图是一种描述攻击者可能采取的攻击路径的有向图，通过对网络系统的拓扑结构、资产配置信息和安全策略进行分析，构建攻击图模型。研究人员利用模型检测技术和图搜索算法，对攻击图进行分析和评估，识别系统中的关键漏洞和潜在攻击路径。

- **基于机器学习的威胁态势预测：**欧洲的学者开展了利用机器学习算法进行威胁态势预测的研究。他们收集了大量的网络攻击数据和系统安全日志，使用深度学习模型对攻击行为进行建模和分析。通过学习攻击行为的特征和模式，实现对未来攻击事件的预测和预警。例如，利用循环神经网络（RNN）和长短时记忆网络（LSTM）对网络流量的时间序列数据进行分析，能够提前发现异常的攻击行为。

2）国内学术界

- **基于知识图谱的威胁建模：**国内部分高校和科研机构提出了基于知识图谱的威胁建模方法。知识图谱是一种将网络安全领域的知识和信息以图的形式进

行表示和存储的技术。通过整合各种安全漏洞信息、攻击手法、资产信息等，构建网络安全知识图谱。在威胁建模过程中，利用知识图谱中的丰富信息进行推理和分析，能够更全面地识别潜在威胁和攻击场景。

- **多属性威胁建模与量化评估：**为了更准确地评估威胁的严重程度和影响范围，国内研究人员提出了多属性威胁建模与量化评估方法。该方法综合考虑了威胁的可能性、影响程度、攻击成本等多个属性，采用模糊数学和层次分析法等技术，对威胁进行量化评估。通过建立多属性威胁评估模型，为安全决策提供更加科学的依据。

三、国内外工业界成果

1）国外工业界

- **安全情报平台的威胁建模功能：**国外的安全情报公司，如 FireEye、Recorded Future 等，在其安全情报平台中集成了先进的威胁建模工具。这些工具能够实时收集和分析全球范围内的安全威胁情报，结合企业自身的网络环境和资产信息，为企业量身定制威胁模型。通过对威胁模型的动态更新和可视化展示，帮助企业及时发现潜在的安全威胁。

- **云服务提供商的威胁建模与防护：**像 Microsoft Azure、Amazon Web Services 等云服务提供商，为其用户提供了全面的威胁建模和防护解决方案。他们利用云计算的强大计算能力和大数据分析技术，对云环境中的各种资产和服务进行实时监控和威胁建模。通过自动化的安全策略配置和应急响应机制，有效抵御各种网络攻击。

- **ATT&CK 模型：**MITRE 公司提出 ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）模型，将攻击行为分解为战术（Tactics）、技术（Techniques）和过程（Procedures），为威胁分析、防御策略制定和红蓝对抗提供标准化参考。ATT&CK 模型通过标准化攻击行为描述，成为网络威胁分析的核心模型。其价值在于从攻击者视角重构防御逻辑，推动检测能力从“基于特征”向“基于行为”升级。

2）国内工业界

- **态势感知平台的威胁建模与分析：**国内的网络安全厂商，如绿盟科技、天融信等，在其态势感知平台中实现了威胁建模与分析功能。这些平台通过采集和整合企业内部的各种安全数据，如入侵检测系统（IDS）日志、防火墙日志

等，利用机器学习和关联分析技术，构建威胁模型。同时，通过可视化界面展示威胁的分布和发展态势，为安全管理人员提供决策支持。

- **物联网安全厂商的威胁建模解决方案：**随着物联网技术的广泛应用，国内的物联网安全厂商也开始重视威胁建模工作。如信锐技术、三六零安全等公司，针对物联网设备的特点和安全需求，提出了专门的威胁建模解决方案。通过对物联网设备的通信协议、数据传输模式等进行分析，识别潜在的安全威胁，并制定相应的防护策略。

3.1.2.5 漏洞与暴露面分析

一、概述

漏洞与暴露面分析是网络空间测绘的重要组成部分，其主要目标是识别网络中存在的安全漏洞以及系统对外暴露的攻击面，从而为网络安全防护提供有力支持。在当今复杂多变的网络环境中，新的漏洞不断涌现，攻击者利用暴露面进行攻击的手段也日益多样化，因此准确、高效的漏洞与暴露面分析至关重要。图 3.8 展示了从多源数据采集到最终生成分析报告的整个过程，有助于读者更直观地理解漏洞与暴露面分析的方法。下面将从国内外的学术界与工业界分别阐述其最新研究成果。

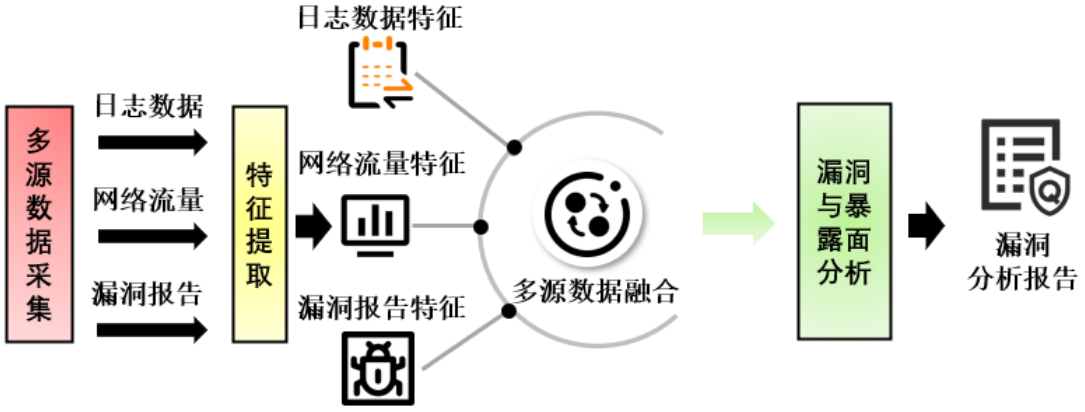


图 3.8 多源数据融合的漏洞与暴露面分析过程

二、国内外学术界成果

1）国外学术界

- **多源数据融合的漏洞分析方法：**国外一些学术机构通过融合多种数据源，如系统日志、网络流量数据、漏洞扫描报告等，来更全面地进行漏洞分析。这种方法可以弥补单一数据源的局限性，提高漏洞发现的准确率。美国某大学

的研究团队提出了一种基于多源数据融合的深度学习模型。该模型将网络流量特征和主机系统日志数据进行融合，利用卷积神经网络（CNN）提取特征，通过长短期记忆网络（LSTM）对特征进行序列分析，从而更精准地预测漏洞的存在和风险等级。实验结果表明，该模型在漏洞检测准确率上比传统方法有一定提高。

- **基于图神经网络的暴露面分析：**图神经网络（GNN）可以很好地表示网络中的节点（如设备、用户）和边（如连接关系），因此被应用于暴露面分析中。通过构建网络拓扑图，分析节点之间的关系和信息传播，能够发现潜在的暴露路径和攻击可能性。欧洲某研究机构利用图神经网络对大型企业网络的暴露面进行分析。他们将网络中的设备、服务、用户等元素抽象为图中的节点，将它们之间的连接关系表示为边，然后通过 GNN 模型学习节点的特征和图的结构信息。实验发现，该方法能够发现一些传统方法难以察觉的隐蔽暴露面，从而为企业的安全防护提供了新的思路。

2）国内学术界

- **基于知识图谱的漏洞与暴露面分析：**国内学术界部分研究认为知识图谱能够整合各类网络安全知识，包括漏洞信息、资产信息、攻击手法等，通过构建知识图谱并进行推理分析，可以更深入地理解网络中的安全状况。山东大学的研究团队提出了一种基于知识图谱的多源数据融合方法，用于漏洞与暴露面分析。他们将不同来源的漏洞数据、资产数据以及安全事件数据整合到知识图谱中，利用图嵌入和知识推理技术，实现对漏洞关联分析和暴露面的精准定位。该方法在实际应用中取得了较好的效果，提高了对复杂网络环境下安全风险的感知能力。

- **大数据驱动的网络暴露面分析原理：**随着大数据技术的发展，国内学者开始利用大数据分析方法来研究网络暴露面。通过收集和分析大量的网络数据，挖掘数据中的潜在信息，从而发现隐藏的暴露面和安全威胁。某高校研究团队基于大数据平台，对海量的网络流量数据、设备日志数据进行存储和分析。他们采用数据挖掘算法，如关联规则挖掘、聚类分析等，发现了一些潜在的暴露模式和风险因素。实验结果表明，该方法能够有效地扩展网络暴露面的监测范围，为网络安全防护提供了有力支持。

三、国内外工业界成果

1）国外工业界

- **自动化漏洞扫描与分析平台：**国外一些安全厂商开发了先进的自动化漏洞扫描与分析平台，这些平台集成了多种扫描工具和分析算法，能够快速、全面地扫描网络资产，发现漏洞并评估其风险。知名安全厂商 Rapid7 的 Nexpose 平台，它可以对各类网络设备、应用程序进行漏洞扫描，利用其庞大的漏洞数据库和智能分析引擎，能够准确识别漏洞类型，评估漏洞的严重程度，并提供详细的修复建议。该平台还支持自动化的漏洞管理流程，大大提高了企业的安全运维效率。

- **实时暴露面监测系统：**一些工业界企业推出了实时暴露面监测系统，通过对网络流量的实时监测和分析，及时发现新出现的暴露面，并向企业安全团队发出警报。FireEye 的 Helix 平台，它利用机器学习和行为分析技术，对网络中的异常流量和新出现的服务进行实时监测。一旦发现可能的暴露面，系统会立即发出告警，并提供详细的分析报告，帮助企业快速响应和处理安全事件。

2）国内工业界

- **绿盟科技的漏洞扫描与分析解决方案：**绿盟科技利用其自研的漏洞扫描技术和智能分析引擎，对企业网络资产进行全面扫描和漏洞分析。该方案结合了多种扫描策略和规则，能够准确识别各类漏洞，并根据漏洞的风险程度进行分级处理。绿盟科技的漏洞扫描器可以对不同操作系统、应用程序进行深度扫描，利用其强大的漏洞特征库和实时更新机制，及时发现新出现的漏洞。同时，该方案还提供了漏洞分析报告和修复建议，帮助企业快速解决安全隐患。

- **奇安信的网络暴露面管理系统：**奇安信的网络暴露面管理系统通过对网络资产的全面梳理和监测，结合大数据分析和机器学习技术，实现对网络暴露面的实时监测、分析和预警。该系统可以自动发现企业网络中的未知资产和潜在暴露面，通过对资产的属性、行为和关联关系进行分析，评估其安全风险。一旦发现异常情况，系统会及时发出告警，并提供应对措施建议，帮助企业降低网络安全风险。

3.1.3 可视化技术

3.1.3.1 地理空间强/弱相关模型

一、地理空间强相关模型

- **概念**：地理空间强相关模型是指网络空间资产与地理空间位置具有明确且紧密联系的一种可视化表达模型。在这种模型中，网络资产的地理位置信息是可视化的重要基础，它能够将网络空间中的资产直观地映射到现实地理空间中，使得用户可以清晰地看到不同地区的网络资产分布情况。

- **实现方式**：该模型通常结合地理信息系统（GIS）技术实现网络资产的空间可视化。首先，收集网络资产的地理位置信息，这可能包括 IP 地址对应的地理坐标（可以通过专业的 IP 地理定位数据库获取）、数据中心的实际物理地址等。然后，将这些信息与地理地图相结合，在地图上以不同的图标、颜色或标记来表示不同类型的网络资产。例如，大型数据中心可能用大型的图标表示，而普通企业的服务器则用较小的图标表示；安全等级高的资产用绿色表示，存在安全风险的资产用红色表示。

- **应用场景**：该模型在网络安全策略制定方面具有重要应用价值。通过观察不同地区网络资产的分布和安全状态，安全决策者可以根据地理区域来制定针对性的安全策略。例如，对于网络资产密集且安全风险较高的地区，可增加安全防护资源的投入，部署更多的入侵检测设备或防火墙。同时，在应急响应中，也可快速定位受影响资产的地理位置，调配就近的技术人员进行处理。

图 3.9 是一张全球性资产分布示意图，不同国家和地区分布着代表各种网络资产的图标。美国西海岸地区，由于聚集了大量的科技公司和数据中心，图标分布密集，且颜色多为不同亮度的绿色，表示这些资产相对安全；而在某些战乱地区，图标颜色较多为红色或橙色，表明这些地区的网络资产存在较高的安全风险。

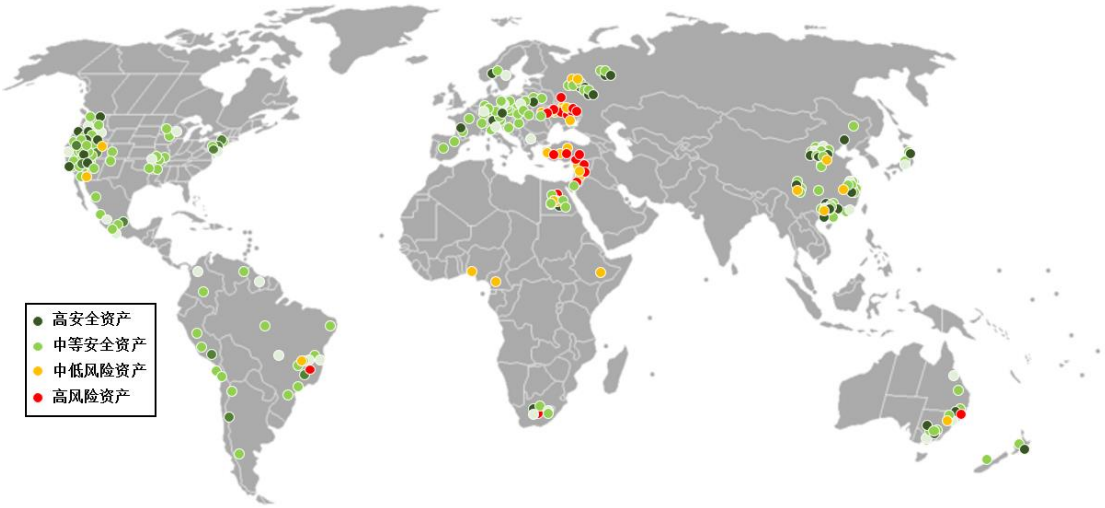


图 3.9 全球资产安全等级评估示意图

二、地理空间弱相关模型

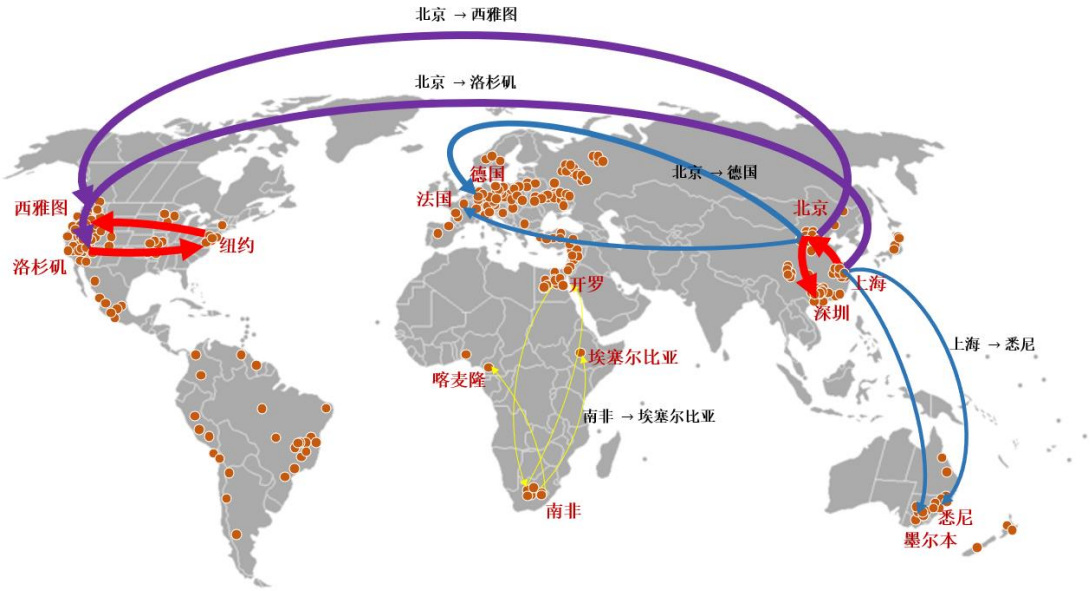
- **概念**：地理空间弱相关模型并不强调网络空间资产与具体地理位置的精确映射关系，而是侧重于展示网络资产之间的某种抽象的、与地理空间有一定关联的关系。例如，它可能关注的是不同地区网络资产之间的流量交互关系、业务关联关系等，而不是资产具体位于哪个经纬度。
- **实现方式**：这种模型通常采用图论和数据挖掘的方法来处理和表示资产之间的关系。通过分析网络流量数据、业务访问日志等，构建资产之间的关联图。在关联图中，节点代表网络资产，边代表资产之间的关系，边的粗细、颜色等属性可以表示关系的强度、类型等。然后，在可视化展示时，可以将这些关联图与简化的地理空间背景相结合，例如只显示大洲、国家的轮廓，以提供一种相对宏观的地理参照。
- **应用场景**：该模型在分析网络流量走向和业务协作方面具有重要作用。例如，在跨国企业的网络中，可以通过地理空间弱相关模型观察不同地区子公司之间的网络流量交互情况，判断业务协作的有效性。同时，在网络攻击溯源中，也可以利用这种模型来分析攻击流量在不同地理区域之间的传播路径。
- 

图 3.10 资产关联图

图 3.10 显示地理空间弱相关模型的示意，在各大洲轮廓的地图上，分布着许多节点和连接节点的边。节点代表不同地区的网络资产，边表示资产之间的流量交互关系。例如，从亚洲到北美洲的边比较粗，说明这两个地区之间的网络流量较大；而一些非洲内部的节点之间边比较细，表明这些资产之间的交互较少。

3.1.3.2 拓扑图与隐喻表达

一、拓扑图

拓扑图是用于表示网络中各个组件之间连接关系的图形化工具。在网络空间测绘中，拓扑图可以展示网络资产（如服务器、路由器、交换机等）之间的物理或逻辑连接关系，帮助用户直观地理解网络的结构和布局。

类型及应用：

1. **物理拓扑图**：反映网络中设备的实际物理连接情况，例如通过网线、光纤等直接连接的设备关系。这种拓扑图在网络基础设施建设和维护中非常有用，网络工程师可以根据物理拓扑图快速定位设备故障和进行线缆维护。
2. **逻辑拓扑图**：侧重于展示网络中各组件之间的逻辑关系，如数据流向、通信协议等。逻辑拓扑图在网络安全分析中更为重要，它可以帮助安全人员识别网络中的关键路径和潜在的安全弱点。

一个典型的企业网络设备连接拓扑图可能包括核心交换机、服务器群、接入层交换机和客户端设备，如图 3.11 所示。核心交换机位于图的中心位置，通过高速链路连接到各个服务器群；接入层交换机则连接到客户端设备，并与核心交换机相连。服务器群之间可能存在不同的网络连接，以实现数据的备份和共享。

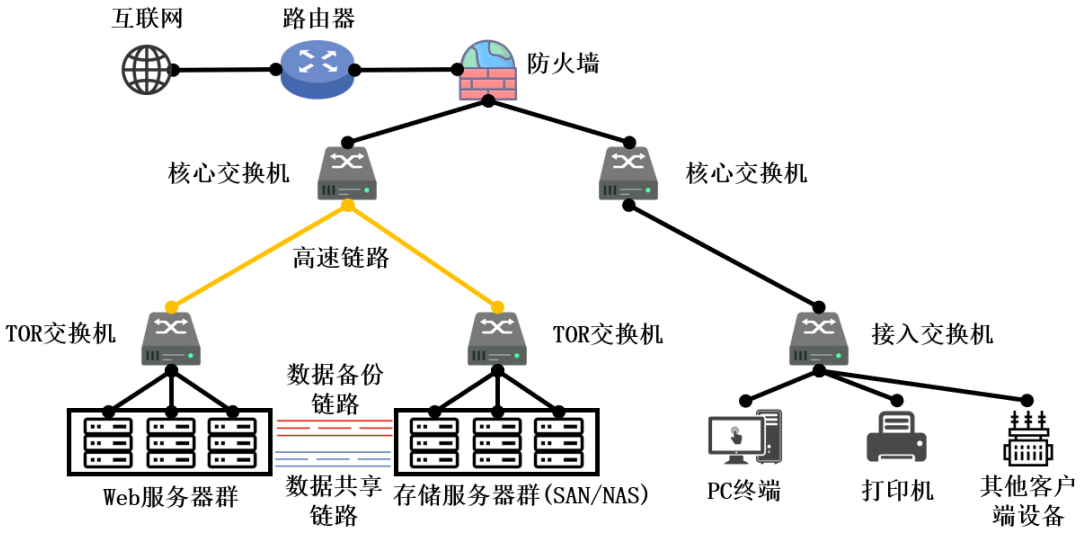


图 3.11 企业网络设备连接拓扑图示例

二、隐喻表达与 DAVA 循环体系

隐喻表达是指在可视化过程中，将抽象的网络概念和关系用更直观、形象的方式进行表示。通过隐喻，用户可以更容易地理解复杂的网络信息，例如将网

络中的节点隐喻为城市，将连接节点的边隐喻为公路，从而使网络结构更具有场景感和亲和力。

DAVA 循环体系（Data - Abstraction - Visualization - Analysis，数据-抽象-可视化-分析）是一种基于隐喻表达的可视化设计方法。它强调数据从原始状态经过抽象处理后转化为可视化表示，再通过分析反馈来优化整个过程。其基本循环步骤包括：

1. **数据（Data）**：首先是收集网络空间测绘中的各种原始数据，包括设备信息、流量数据、配置信息等。这些数据是整个循环的基础。
2. **抽象（Abstraction）**：对收集到的数据进行处理和提炼，去除冗余信息，提取关键特征，并将这些特征转化为适合可视化的形式。例如，将复杂的网络流量数据抽象为流量的大小、频率等指标。
3. **可视化（Visualization）**：利用隐喻表达等方法将抽象后的数据以直观的图形、图表等形式展示出来。例如，将网络中的节点隐喻为星球，节点之间的边隐喻为星际航线，通过这种形象的方式展示网络结构。
4. **分析（Analysis）**：用户对可视化结果进行分析，发现其中的规律、问题和趋势。分析结果可以反馈到前面的步骤中，如调整抽象方法或优化可视化展示方式，形成一个闭环的迭代过程。
5. **应用价值**：DAVA 循环体系能够有效地将复杂的网络空间数据转化为易于理解和分析的可视化信息，提高用户对网络状况的认知和决策能力。同时，通过不断的迭代优化，可以使可视化结果更加准确地反映网络的实际情况。

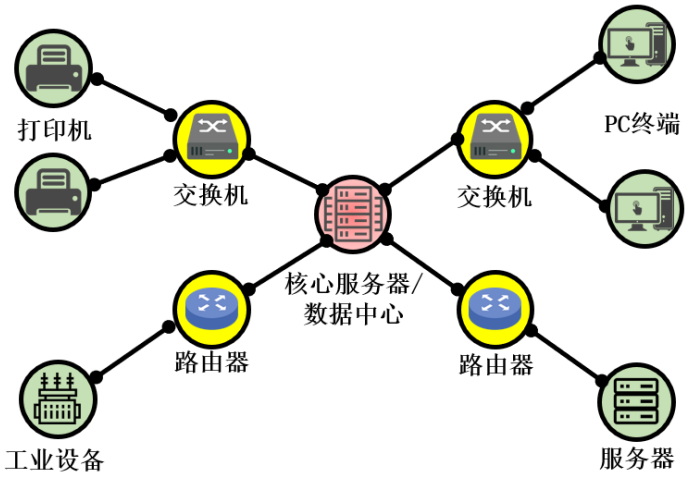


图 3.12 企业网络星型拓扑结构图

如图 3.12 所示，在一个以星球隐喻网络节点的可视化图中，每个星球代表一个网络设备，星球之间的光线代表设备之间的连接关系。不同大小和颜色的星球表示不同类型和重要性的设备，例如，中心的大星球可能代表核心服务器，周围的小星球代表客户端设备。通过这种隐喻方式，网络的层次结构和连接关系一目了然。

3.1.3.3 可视化技术前沿探索

增强现实（AR）融合：增强现实技术将虚拟信息叠加到现实世界中，为网络空间测绘带来全新的交互与认知方式。在网络可视化领域，增强现实技术可以将网络拓扑结构、攻击路径、威胁指标等信息，直接呈现在用户所处的真实空间中，提升决策效率与空间理解能力。例如，网络运维人员可以佩戴 Microsoft HoloLens 眼镜，查看三维网络拓扑中主机、交换机、攻击路径的实时状态，了解设备的运行负载、连接关系与告警等级等，从而快速定位异常区域并进行针对性排查，提升响应效率与精准度。此外，增强现实技术提供对手势识别、语音控制和空间定位的支持，便于在多源数据中高效切换与分析，可用于辅助开展实景化的态势演示与攻防演练。例如，华为 Cyberverse 通过 AR 技术将网络空间实体叠加到真实物理环境中，具体包括设备、数据流、攻击路径等，实现虚实融合的网络拓扑可视化。

知识图谱驱动可视化：知识图谱技术为网络测绘提供了语义层次的可视化基础。传统网络可视化往往基于底层数据并且缺少数据关联，而知识图谱引入实体关系建模，将主机、应用、攻击行为、安全事件等网络元素转化为语义节点，并通过属性关系图展示它们之间的联系。其核心优势是可实现“从数据到知识”的认知跃迁。实际应用中，安全运维人员可以基于图谱查询某一攻击行为所关联的资产路径、受影响业务与外部威胁源。例如，可结合 MITRE ATT&CK 构建攻击模式知识库，通过力导向图、圆弧依赖图等具体可视化方式实现对攻击链、战术-技术-程序（TTPs）的可视化，支持行为路径查找与上下文多跳交互操作。例如，基于 Neo4j 图数据库将知识图谱用于展示 APT 攻击路径，将攻击节点、时间、攻击阶段以图结构呈现，帮助用户快速识别高危路径和潜在落地资产。另外，Graphistry 基于 GPU 加速的图计算平台支持大规模实体图谱的实时可视分析，用户只需上传数据即可自动生成交互式图谱视图，以更便捷地开展威胁追踪与事件溯源。

三维时空融合可视化：三维时空融合可视化是将三维建模、地理空间定位与时序数据驱动相结合的一种先进可视表达方式，能够实现网络空间中“逻辑结构

—物理空间—时间演变”的一体化呈现。在技术实现层面，首先借助如 Cesium.js、Three.js 等 WebGL 渲染引擎构建网络资产与物理位置的三维模型，将主机节点、交换机、机房空间或云平台资源以三维图形方式布局。其次，将滑动时间窗口、事件回放模块等时序数据引擎对安全事件、数据流、攻击路径等动态信息进行同步驱动，从而在时间轴上展现攻击扩散趋势、通信行为演变等变化过程。再者，利用空间语义绑定机制，将 IP 地址、子网段、组织结构等逻辑网络信息映射至实际地理区域或拓扑结构中，实现逻辑与空间的融合表达。此外，三维可视化系统通常支持多层渲染与交互操作，用户可在不同视角切换下查看网络层级结构、资产关联关系、攻击链路径等内容，并通过路径高亮、流向动画、热力闪烁等方式突出关键威胁节点或异常传播过程。

生成式 AI 增强的仪表布局：生成式 AI 在智能仪表布局、图形摘要生成、自然语言转可视界面等方面表现出较强潜力，有望实现“对话式数据可视化”的新范式。传统界面中的仪表盘设计往往需要手动选择图表类型、布局逻辑及交互方式，效率低、适应性差。而生成式 AI 可基于用户意图、历史数据特征与知识库，自动构建适应任务的可视化面板。例如，用户输入“展示某时间段内全网异常连接与攻击来源分布”指令，生成式 AI 可根据历史攻击频率、地理分布特征与可视组件优选规则分析，输出包含地图热力图、时间序列折线图与攻击行为雷达图的组合仪表，完成数据映射与布局排序。此外，生成式 AI 具有推理增强的能力，可将图表中复杂指标以自然语言方式辅助解读，或结合领域知识辅助分析，提供决策支持。目前，多个平台已开展实用研究与集成探索。例如，LangChain 通过自定义 Tools 整合数据源与可视化库，可实现折线图、柱状体、热力图等多种图表输出，打造“问答式数据可视化助手”。Tableau GPT 整合生成式语言模型至数据分析平台，实现“Ask Data”功能升级，支持自然语言提问生成图表，并自动提供统计摘要。

数字孪生可视化技术：数字孪生技术是指在虚拟空间中创建物理系统的高保真数字镜像，用以实时同步状态、预测行为、优化控制。在网络空间测绘中，数字孪生技术可被用于构建真实网络的动态映射模型，通过 3D 场景或多层网络架构呈现网络资产、通信路径、业务流程及安全态势。与传统可视化技术相比，数字孪生不仅可视，还“可感、可控、可推演”。其关键能力包括：实时同步流量、告警等数据流、实现机房、设备、链路等多维度资产重构、攻击路径预测与回放、虚拟部署演练等。例如，Unity 3D、Unreal Engine 结合 IoT 数据流平台与可视中台系统，构建工业网络的可视孪生平台，重现 PLC 控制网络的状态变化与入侵轨迹，实现“边运维边仿真”的新模式。该类系统已应用于电力、化工、轨道交通等行业，通过孪生模拟与回放技术评估风险响应策略，推动网络运维、态势评估

和演练推演的全面革新。

高速数据流动态渲染：在网络空间测绘中，高速数据流带来的数据吞吐量和时效性挑战对可视化系统提出了更高要求。传统静态图表难以适应高速更新的数据场景，容易出现延迟、卡顿或可读性下降的问题。为此，动态渲染技术正逐步成为测绘系统可视化“实战级”的核心组件。其主要技术包括 GPU 加速渲染、增量式数据绑定、滑动窗口渲染算法、WebSocket/ZeroMQ 实时推送等手段，构建低延迟、高并发、动态更新的可视界面。这类技术可以在百万级数据吞吐下保持毫秒级刷新响应，支持攻击波动、流量突变、地理热力等动态视觉表达。现代技术栈如 WebGL 提供了浏览器端的高性能图形渲染能力，Deck.gl 支持大规模地理数据的动态可视化，Plotly Dash 提供 Python 驱动的交互图表平台，而 Apache ECharts 5 引入了基于 Canvas 的异步渲染优化，提升大数据场景下的图表刷新效率。这些模块广泛用于态势大屏、告警监控平台和高速入侵检测系统的可视化前端，可为网络运维与安全决策提供了高实时、高准确度的视觉支持。

3.1.3.4 技术对比与选型建议

可视化技术的技术对比与选型建议如表 3.1 所示。

表 3.1 技术对比与选型建议

技术类型	适用场景	优势	局限性
地理空间强相关模型	精准定位、应急响应	高精度、支持物理联动	依赖高质量 GIS 数据
拓扑图分层布局	大型复杂网络	结构清晰、可扩展性强	手动配置复杂度高
DAVA 隐喻表达	攻防推演、决策支持	直观易懂、闭环反馈	需定制化开发成本高

3.2 平台架构设计

3.2.1 分层架构示例

网络空间测绘平台的分层架构设计有助于将不同功能模块进行解耦，提高系统的可维护性和可扩展性。以下将详细介绍常见的四层架构，并结合国内外学术界和工业界的成果进行分析。

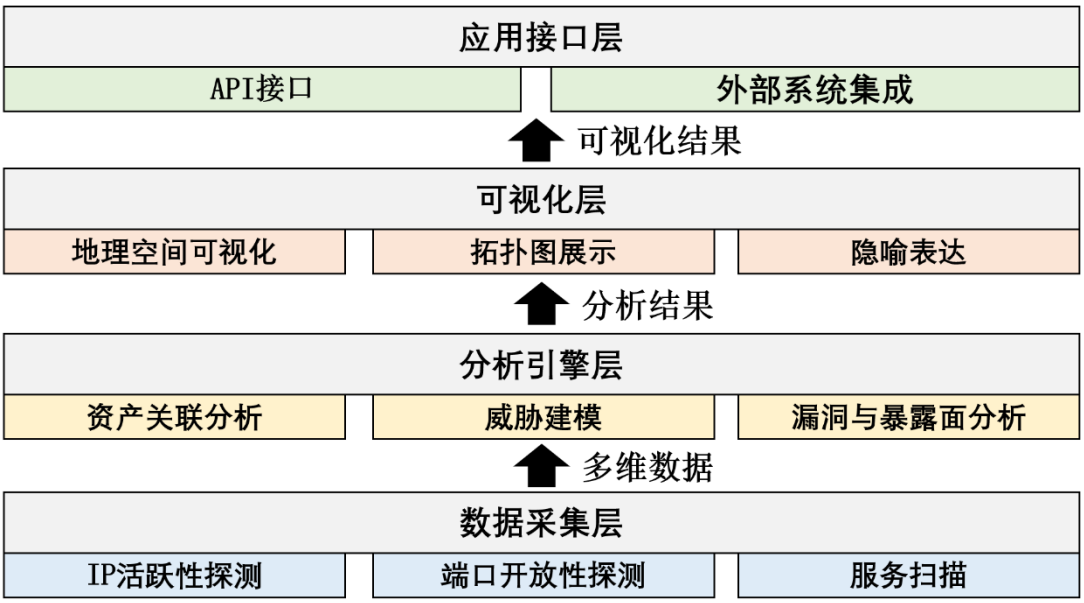


图 3.13 网络空间测绘平台的分层架构图

如图 3.13 所示，测绘平台四层架构包括数据采集层、分析引擎层、可视化层和应用接口层：

一、数据采集层

- **功能**：该层是平台数据的来源，主要负责对目标网络空间的资产进行探测和数据收集。它使用各种探测技术，如 IP 活跃性探测、端口开放性探测、服务扫描等，收集网络设备和系统的基础信息。
- **成果举例**：国外的 Shodan、Censys 搜索引擎，它可以在全球范围内进行大规模的网络资产扫描，收集设备的 IP、端口、应用信息等。国内的 ZoomEye、FoFa 等采用全量探测方法，能够对网络空间中的资产进行全面、细致的扫描，为后续分析提供丰富的数据基础。

二、分析引擎层

- **功能**：对采集到的数据进行深度挖掘和分析。运用资产关联分析、资产与组织关联映射分析、威胁建模、漏洞与暴露面分析等技术，从海量数据中提取有价值的信息，发现潜在的安全威胁和资产关系。
- **成果举例**：国外的学术界有许多关于数据挖掘和机器学习在网络安全分析中的应用研究，通过建立复杂的模型，对网络行为和资产特征进行分析，发现隐藏在数据背后的安全风险。国内某高校的网络空间安全平台采用多源数据融合技术，将不同类型、不同来源的数据进行整合分析，提高了资产识别和威胁检测的准确性。

三、可视化层

- **功能：**将分析结果以直观的方式展示给用户。利用地理空间强/弱相关模型、拓扑图与隐喻表达等可视化技术，让用户能够快速理解网络资产的分布、关系和安全态势。
- **成果举例：**国外的 DAVA 循环体系将数据的采集、分析、可视化和评估形成一个循环，通过不断地迭代优化可视化效果，帮助用户更好地掌握网络信息。国内一些安全厂商也开发了自己的可视化平台，如奇安信的天眼威胁感知系统，通过直观的图表和地图展示，让用户能够一目了然地了解网络威胁的来源和分布。

四、应用接口层

- **功能：**为外部系统和用户提供访问和调用平台功能的接口。通过 API 等方式，实现与其他安全系统、业务系统的集成，方便用户根据自己的需求进行定制开发和应用拓展。
- **成果举例：**国外的一些开源网络空间测绘平台提供了丰富的 API 接口，方便开发者将其融入到自己的项目中。国内的部分网络安全企业也逐渐重视接口层的开发，为企业客户提供定制化的解决方案，实现与企业内部安全管理系统的无缝对接。

3.2.2 动态更新机制与实时性保障

在网络空间中，资产的状态和安全态势是不断变化的，因此平台需要具备动态更新机制和实时性保障能力。以下结合数智安公司平台技术实践进行分析。

一、动态更新机制

动态更新机制主要体现在数据采集和分析结果的更新上。

1）数据采集更新

- **方式：**定期自动扫描和实时触发扫描相结合。定期扫描可以按照预设的时间间隔对目标网络进行全面扫描，保证数据的及时更新。实时触发扫描则可以在检测到网络变化（如设备上线、下线）时立即进行扫描，获取最新的资产信息。
- **成果举例：**国外的一些商业网络空间测绘平台采用了智能调度算法，根据网络的动态变化调整扫描频率，提高数据更新的效率。国内的数智安平台也通

过优化扫描策略，结合分布式扫描技术，实现了对大规模网络资产的快速、定期更新。

2）分析结果更新

- **方式：**基于数据流处理技术，对新采集到的数据进行实时分析，并更新原有分析结果。当发现新的威胁或资产变化时，及时调整威胁建模和资产关联关系。
- **成果举例：**国内外学术界都有关于流式数据分析的研究，通过引入实时计算框架（如 Apache Flink、Spark Streaming），实现对网络数据的实时处理和分析结果的动态更新。工业界的一些安全产品也开始集成这些技术，提高平台的实时性和响应能力。

二、实时性保障

1）数据传输优化

- **方式：**采用高速网络传输协议和分布式存储技术，减少数据采集和传输的时间延迟。同时，对数据进行预处理和压缩，减少传输的数据量。
- **成果举例：**国外的一些大型网络空间测绘项目采用了分布式文件系统（如 Ceph）和高速网络接口（如 100Gbps 以太网），提高了数据传输的速度。国内的企业也在不断优化数据传输架构，通过采用 SDN（软件定义网络）技术，实现对网络带宽的灵活分配和优化，保障数据的实时传输。

2）分析处理加速

- **方式：**利用并行计算和硬件加速技术（如 GPU 计算），提高分析引擎的处理速度。对复杂的分析任务进行分解，并行处理多个子任务，加快分析结果的生成。
- **成果举例：**学术界的研究人员提出了许多并行计算算法和模型，在大规模数据处理和分析方面取得了显著的成果。工业界的一些安全厂商也开始引入 GPU 计算技术，提高威胁建模和漏洞分析的速度，实现对网络安全态势的实时监测和响应。

3.2.3 不同架构的比较

这里将分层架构与其他常见的微服务、云计算架构进行比较。

一、分层架构

1）优点

- **易于理解和维护**：分层结构清晰，每个层次的职责明确，开发人员和维护人员可以更容易地理解系统的整体架构和各部分的功能。例如，数据采集层出现问题，维护人员可以专注于该层进行排查和修复，而不会影响其他层的正常运行。
- **可扩展性强**：每层可以独立进行扩展和升级。例如，随着数据采集需求的增加，可以添加新的采集工具或数据源到数据采集层；当需要更复杂的分析模型时，可以对分析引擎层进行优化和扩展。
- **可复用性高**：各层可以被不同的系统复用。例如，数据采集层的采集工具和方法可以应用于多个类似的网络空间测绘项目中，降低了开发成本。

2）缺点

- **性能瓶颈**：层与层之间的数据交互可能会导致性能瓶颈。例如，当数据采集层采集到大量数据时，传输到分析引擎层进行处理可能会出现延迟，影响系统的实时性。
- **分层过多导致系统复杂**：如果分层设计不合理，层数过多，会增加系统的复杂性，导致开发和维护难度增加。

二、微服务架构

如图 3.14 所示，微服务架构将网络空间测绘平台拆分成多个小型、自治的服务。每个微服务专注于单一的业务功能，例如数据采集微服务、资产关联分析微服务、可视化展示微服务等。这些微服务可以独立开发、部署和扩展。微服务之间通过轻量级的通信机制（如 RESTful API、消息队列等）进行交互。例如，数据采集微服务负责采集网络空间数据，并将数据发送到消息队列中；分析引擎微服务从消息队列中获取数据进行处理和分析，然后将结果存储到数据库中；可视化微服务通过调用分析引擎微服务的 API 获取分析结果并进行展示。

1）优点

- **高可扩展性**：每个微服务可以独立进行扩展，根据不同服务的负载情况合理分配资源。例如，在网络流量高峰期，数据采集微服务需要处理更多的数据，可以单独增加该微服务的实例数量，提高采集效率。

- **快速迭代和部署**：微服务的独立性使得开发团队可以更快地对单个服务进行迭代和部署。例如，当需要对资产关联分析微服务进行功能优化时，只需更新该服务，而不会影响其他服务的正常运行。
- **技术异构性支持**：不同的微服务可以使用不同的技术栈。例如，数据采集微服务可以使用 Python 编写，分析引擎微服务可以使用 Java 并结合机器学习框架，而可视化微服务可以使用 JavaScript 和前端框架，充分发挥各种技术的优势。

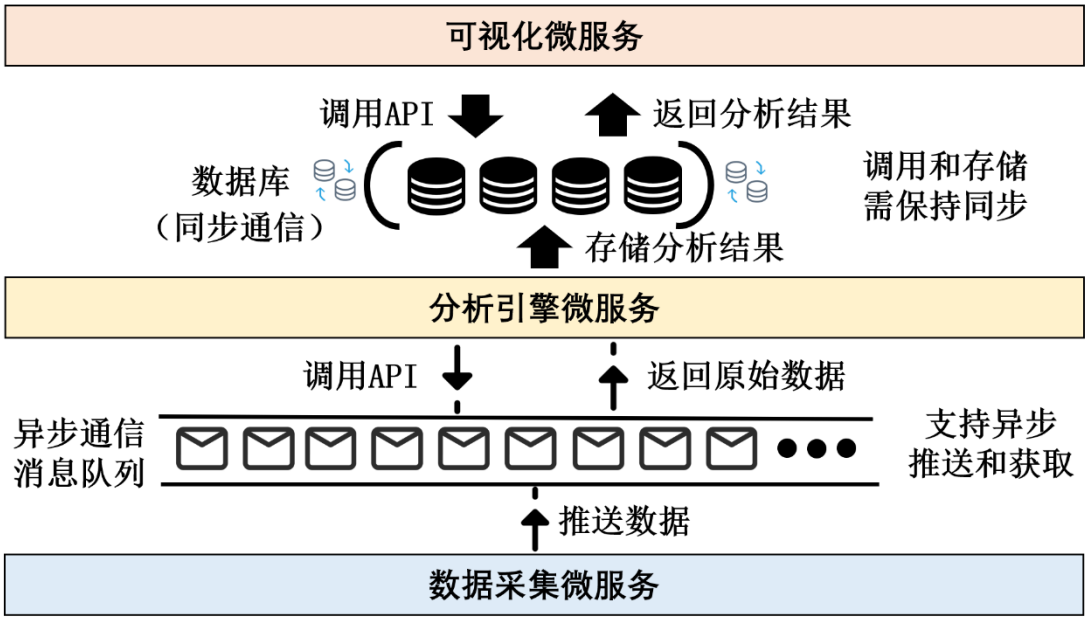


图 3.14 微服务架构

2）缺点

- **服务间通信成本**：微服务之间的通信需要额外的开销，包括网络延迟、序列化和反序列化等。例如，当分析引擎微服务从数据采集微服务获取数据时，需要通过网络进行数据传输，可能会影响系统的整体性能。
- **服务管理和协调复杂度高**：随着微服务数量的增加，服务的管理和协调变得更加复杂。例如，如何发现和调用其他微服务、如何保证服务之间的一致性等问题都需要额外的机制来解决。

三、云计算架构

云计算架构借助云计算平台的强大计算资源和存储能力来构建网络空间测绘平台。常见的云计算模式包括基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。在网络空间测绘中，可以使用 IaaS 提供的虚拟服务器、

存储设备等资源来部署数据采集、分析和存储系统；使用 PaaS 提供的开发和运行环境来开发和运行分析算法和应用程序；使用 SaaS 模式向用户提供网络空间测绘服务。例如，利用 Amazon Web Services（AWS）的 EC2 实例来运行数据采集工具和分析引擎，使用 S3 存储采集到的数据和分析结果，用户可以通过浏览器访问基于 SaaS 的网络空间测绘平台获取相关信息。如图 3.15 所示。

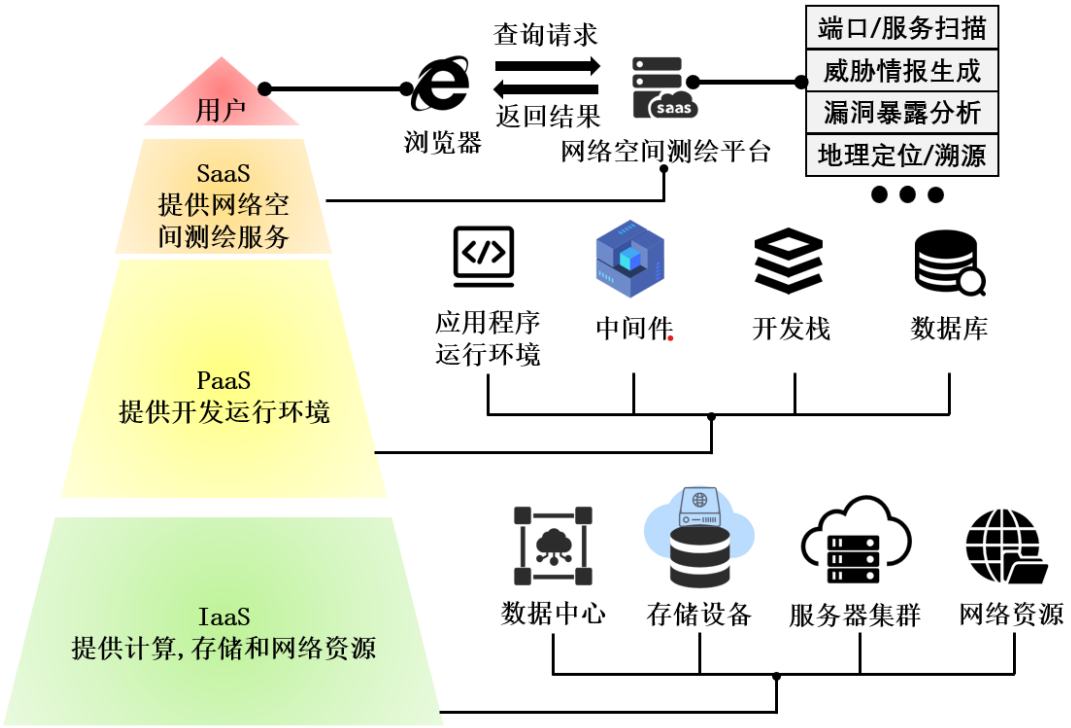


图 3.15 云计算架构示意图

1）优点

- **资源弹性伸缩**：可以根据平台的负载情况灵活调整云计算资源的使用量。例如，在进行大规模网络测绘时，可以增加虚拟服务器的实例数量；在低峰期，可以减少资源的使用，降低成本。
- **无需前期大量投资**：无需购买和维护昂贵的硬件设备和软件许可证，降低了建设网络空间测绘平台的门槛。例如，小型企业或研究机构可以通过租赁云计算资源来开展网络空间测绘工作。
- **高可用性和可靠性**：云计算平台通常提供了高可用性和数据冗余机制，确保平台的稳定运行和数据的安全性。例如，亚马逊 AWS 的 S3 提供了多副本存储，即使某个存储节点出现故障，数据也不会丢失。

2）缺点

- **对网络依赖度高**：由于数据的处理和存储都依赖于云计算平台，网络连接的稳定性和速度会直接影响平台的性能。例如，如果网络出现故障，用户可能无法访问平台或获取数据。
- **数据安全和隐私问题**：将敏感的网络空间数据存储和处理在云计算平台上，可能存在数据泄露和隐私侵犯的风险。例如，云服务提供商的安全措施不当可能会导致用户数据被非法获取。

通过比较可以看出，分层架构在大型、复杂的网络空间测绘平台中具有明显的优势，能够满足系统的可维护性、可扩展性和集成性要求；而微服务架构在小型、简单的应用场景中可能具有一定的优势，但在面对大规模数据处理和复杂业务需求时，其局限性也较为明显。因此，在实际设计网络空间测绘平台时，需要根据具体的应用场景和需求选择合适的架构，或者进行不同架构的有机组合。

第四章 国内外研究与实践进展

4.1 国际动态

4.1.1 相关国家网络空间测绘项目简介

4.1.1.1 美国“藏宝图计划”

一、背景概述

“藏宝图计划”是美国出于国家安全和军事战略需求而开展的一个大型网络空间态势感知项目。该计划没有暴露具体的起止时间，但据推断可能在 2000 年代初期已启动雏形，且因网络空间监控的长期需求和技术迭代，目前可能仍处于活跃状态。随着信息技术的飞速发展，网络空间的战略意义日益凸显，各国都在加强对网络空间的掌控。美国希望通过该计划全面掌握全球网络空间的资产分布、通信关系以及潜在的安全威胁等信息，以便在网络空间冲突中占据优势地位，保护自身关键基础设施和国家利益，同时具备攻击敌方网络的能力。图 4.1 给出了该项目的框架示意图。

二、项目框架结构

表 4.1 总结了该架构各层次的主要功能。

1）数据收集层

这一层主要负责从各种渠道收集网络空间的数据，包括但不限于互联网上的 IP 地址、域名、端口信息等。收集手段可能包括主动扫描、被动监听以及与不同机构的数据共享等。例如，利用低速率的扫描器对全球范围内的 IP 地址段进行定期扫描，获取开放的端口和正在运行的服务信息。

2）数据处理与分析层

对收集到的大量原始数据进行清洗、分类和整合。运用机器学习和数据挖掘技术，挖掘数据背后的关联和模式。例如，通过数据分析可以发现某一地区大量异常的网络连接行为，可能暗示着存在网络攻击的迹象。

3）可视化与决策支持层

将处理和分析后的数据以直观的地图形式呈现出来，形成网络空间的“藏宝图”。地图上可以标记出各种网络资产的地理位置、安全状况等信息。同时，为决策者提供分析报告和决策建议，帮助他们制定网络安全战略和应对措施。

表 4.1 藏宝图计划层级功能

层级	主要功能
数据收集层	从多种渠道收集网络空间各类数据，如 IP、域名、端口等
数据处理与分析层	清洗、分类、整合数据，运用机器学习和数据挖掘技术挖掘数据关联和模式
可视化与决策支持层	将数据以地图形式可视化展示，为决策者提供分析报告和决策建议

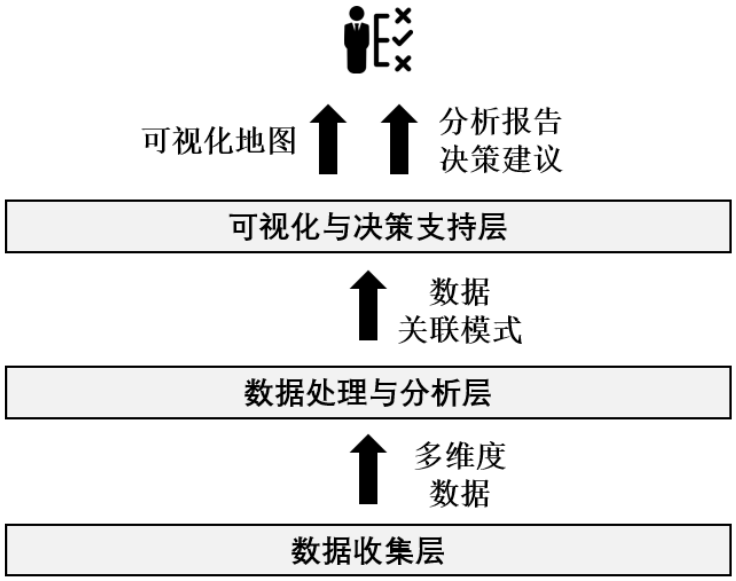


图 4.1 藏宝图计划项目框架示意图

三、主要功能介绍

1、网络资产发现

能够识别全球范围内的各类网络资产，包括服务器、终端设备等。这有助于美国了解其他国家的网络基础设施分布，为网络攻击或防御做好准备。

2、威胁预警

通过对网络流量和行为的分析，实时监测潜在的网络安全威胁，提前发出预警信号，使美国能够及时采取措施应对攻击。

3、战略决策辅助

为美国政府和军队的决策者提供全面的网络空间态势信息，支持他们制定网络作战计划和国家安全战略。

4.1.1.2 美国“X 计划”

一、背景概述

随着网络空间成为新的作战领域，传统的作战方式在网络空间难以有效实施。“X 计划”（2012 年-2019 年）旨在开发一套全面的网络战管理系统，使美军能够像在陆、海、空、天等传统作战领域一样，高效地规划、执行和评估网络作战行动。该计划有助于提升美国在网络空间的作战能力，确保在网络冲突中的优势地位。图 4.2 给出了该项目的框架示意图。

二、项目框架结构

表 4.2 总结了该架构各层次的主要功能。

1）网络作战规划模块

该模块允许作战人员根据任务目标和网络态势，制定详细的网络作战计划。包括选择攻击或防御的目标、确定作战时机、规划攻击路径等。例如，作战人员可以根据情报预先设定针对敌方某一关键网络基础设施的攻击流程。

2）执行与控制模块

根据制定好的作战计划，自动调度和执行各种网络作战行动。实时监控作战进度，对执行过程中的异常情况进行及时处理和调整。比如，在攻击过程中如果发现目标网络的防御策略发生变化，系统可以自动调整攻击手段。

3）态势感知与评估模块

持续收集网络空间的态势信息，对作战效果进行实时评估。通过各种指标和模型，分析作战行动是否达到预期目标，为后续的作战决策提供依据。

表 4.2 美国 X 计划模块功能

模块	主要功能
网络作战规划模块	根据任务目标和网络态势制定详细网络作战计划，包括选择目标、确定时机和规划路径等
执行与控制模块	自动调度和执行网络作战行动，实时监控进度并处理异常情况，可动态调整攻击手段
态势感知与评估模块	持续收集网络态势信息，实时评估作战效果，为后续决策提供依据

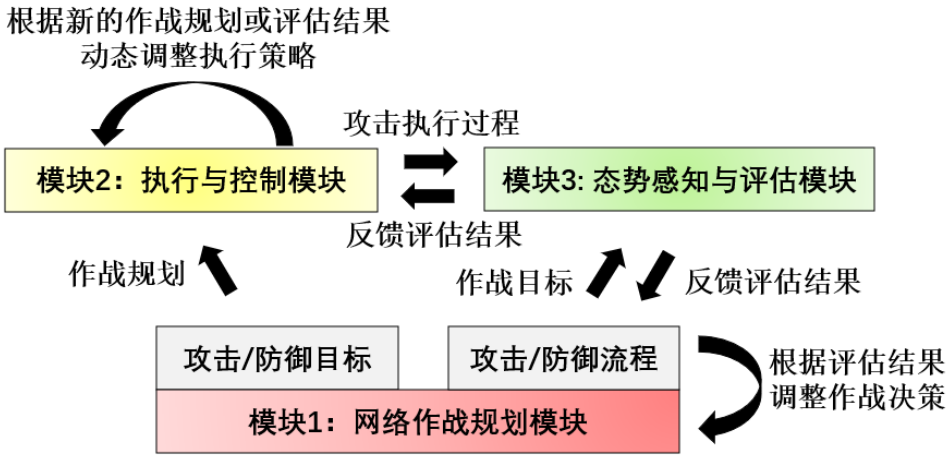


图 4.2 美国 X 计划项目框架示意图

三、主要功能介绍

1）网络作战协同

实现不同部门和作战单元之间的网络作战协同，打破信息壁垒。例如，军队的情报部门、通信部队和网络攻击部队可以通过“X 计划”系统实现信息共享和协同作战。

2）模拟和演练

提供网络作战的模拟环境，允许作战人员进行战前演练和战术验证。通过模拟不同的作战场景和对手策略，提高作战人员的应对能力。

3）实时监控和调整

在作战过程中实时监控网络态势，根据实际情况及时调整作战计划和行动。确保作战行动能够适应复杂多变的网络环境。

4.1.1.3 美国“SHINE 计划”

一、背景概述

美国国土安全部 DHS 下属 ICS-CERT（工业控制系统应急小组）为关注美国本土关键基础设施相关设备网络可达及安全态势而制定的项目，代号为“SHINE 计划 (Shodan Intelligence Extraction)”，参与人员为 Bob Radvanovsky 和 Jake Brodsky（Shodan 的两位开发者），起止时间为 2008 年中期至 2014 年 1 月 31 日。“SHINE 计划”的目标是基于开放情报源，根据可定义、可搜索的术语集进行设备搜索，并进行进一步数据分析，改善、降低互联网中 ICS 系统的安全风险。

二、项目/系统框架结构

表 4.3 总结了该项目架构各层次的主要功能。

1）数据采集层

主要负责从 Shodan 等类似的互联网设备搜索引擎中提取设备和服务的相关信息，涵盖设备开放端口、使用的服务协议、服务版本、操作系统及其他相关信息。

2）数据分析与威胁识别层

通过分析采集到的 Shodan 数据，结合现有的安全威胁数据库和漏洞情报，执行智能化的威胁分析。利用机器学习、模式识别等技术，识别潜在的安全威胁。

3）风险评估与响应层

基于分析层的输出结果，负责评估潜在的安全威胁，生成攻击优先级，执行相应的防护措施。该层结合上下游数据，动态调整防御策略，并向用户或安全团队提供实时的攻击预警。

4）可视化与报告层

提供实时的图形化展示，帮助用户理解网络中设备的安全状态。可视化界面不仅显示设备风险状况，还可以展示相关的安全事件历史，帮助决策者做出响应。

表 4.3 美国 SHINE 计划层级功能

层级	主要功能
数据采集层	从 Shodan 等互联网设备搜索引擎中提取设备和服务的相关信息
数据分析与威胁识别层	对分析采集到的数据进行智能化的威胁分析，并识别潜在的安全威胁
风险评估与响应层	评估潜在的安全威胁，执行相应的防护措施，并提供实时的攻击预警
可视化与报告层	提供实时的图形化展示，以及相关的安全事件历史，帮助决策者做出响应。

三、主要功能介绍

1）智能数据提取与设备信息聚合

SHINE 计划的核心功能之一是通过 Shodan 平台，自动化提取并聚合来自全球范围内的设备信息。这些信息不仅包括设备暴露的端口和协议，还包括设备的具体型号、运行服务、版本信息等，有助于精确识别暴露的攻击面。

2）高效的漏洞挖掘与风险识别

通过结合已知的漏洞数据库（如 CVE、NVD 等）以及学习模型，SHINE 计划能够高效地对已提取的设备信息进行漏洞挖掘。系统会根据设备类型、服务版本等信息，对潜在的漏洞进行优先级排序，帮助安全人员迅速定位高风险设备。

3）跨平台、跨设备的安全分析

SHINE 计划设计了一种跨平台的安全分析框架，可以整合不同网络环境、操作系统、协议栈的数据，生成统一的安全态势感知模型。这样，能够有效识别由不同设备间的互动所带来的安全风险。

4.1.1.4 俄罗斯卡巴斯基威胁地图

一、背景概述

在全球化的网络环境下，网络安全威胁日益严峻且呈现出国际化的特点。卡巴斯基作为全球知名的网络安全公司，为了帮助企业、政府和个人更好地了解全

球网络安全态势，开发了卡巴斯基威胁地图。该项目为用户提供及时准确的威胁信息，提高用户的安全防护意识，也有助于进一步研究和应对网络安全威胁。图 4.3 给出了该项目的框架示意图。

二、项目/系统框架结构

表 4.4 总结了该项目架构各层次的主要功能。

1）数据采集源

主要来自卡巴斯基分布在全球各地的用户设备和安全网关。这些设备和网关实时收集本地的网络安全事件数据，如恶意软件攻击、网络入侵尝试等。

2）数据传输与整合

将采集到的大量分散数据通过安全的通信链路传输到数据中心。在数据中心，对这些数据进行整合和处理，去除重复和无效信息。

3）分析与可视化模块

运用先进的数据分析技术，对整合后的数据进行深入分析。包括分析攻击的来源地、目标地、攻击类型和趋势等。然后将分析结果以直观的地图形式展示出来，地图上用不同的颜色和图标表示不同的威胁信息。

表 4.4 俄罗斯卡巴斯基威胁地图层级功能

层级	主要功能
数据采集源	全球各地用户设备和安全网关实时收集本地网络安全事件数据，如恶意软件攻击、网络入侵尝试等
数据传输与整合	将采集数据安全传输到数据中心，整合处理，去除重复和无效信息
分析与可视化模块	运用数据分析技术深入分析数据，分析攻击来源、目标、类型和趋势等，以地图形式直观展示结果

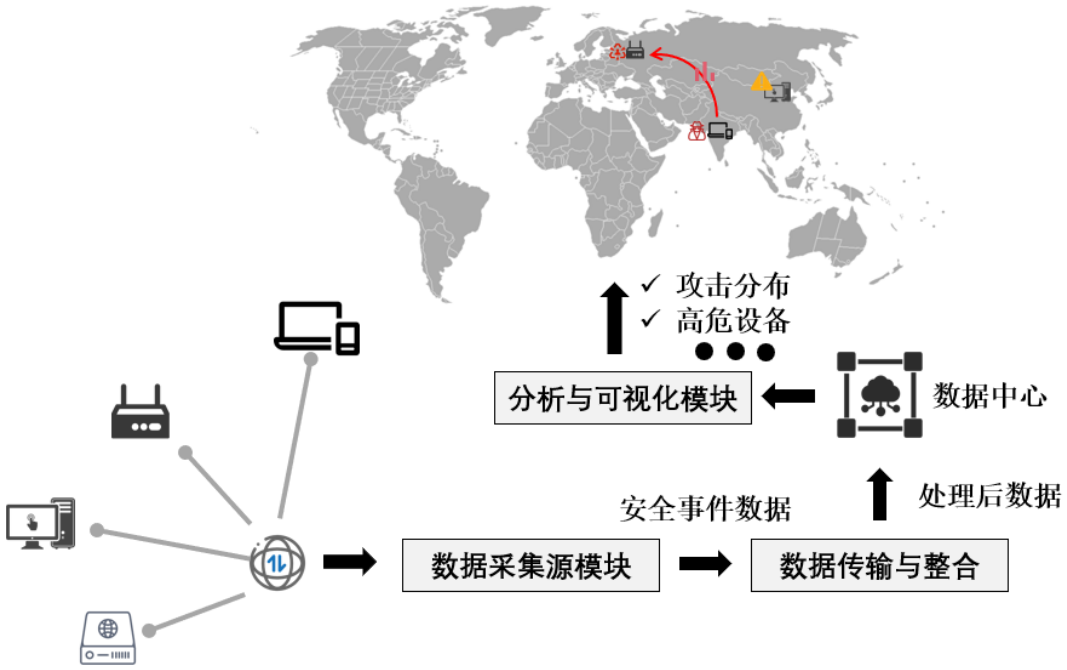


图 4.3 俄罗斯卡巴斯基威胁地图项目框架示意图

三、主要功能介绍

1）实时威胁展示

通过地图实时展示全球范围内正在发生的网络安全威胁，用户可以直观地了解各个地区的威胁分布情况。例如，能看到某个时段内东南亚地区遭受恶意软件攻击的频率较高。

2）趋势分析

对一段时间内的威胁数据进行分析，呈现出网络安全威胁的发展趋势。帮助用户预测未来可能面临的威胁类型和高发地区，提前做好防范措施。

3）情报共享

为全球用户提供网络安全情报共享平台。用户可以根据威胁地图上的信息，及时调整自身的安全策略，共同应对网络安全挑战。

4.1.2 工业界平台-国外情况

4.1.2.1 Shodan 平台

一、基本背景概述

Shodan 由 John Matherly 在 2009 年创建，与 Google 等常规搜索引擎搜索网页不同，Shodan 专门搜索联网设备，例如摄像头、路由器、工控设备等。它通过持续不断地扫描全球互联网，收集各类设备暴露的信息，构建了一个庞大的设备数据库，使人们能够了解各种联网设备的分布、配置和安全状况。Shodan 的出现为网络安全研究人员、企业和政府机构等提供了宝贵的信息资源，同时也引发了人们对设备暴露风险的广泛关注。

二、平台框架结构

Shodan 的平台框架主要由数据采集层、数据处理层和数据展示层构成：

1）数据采集层

Shodan 拥有大量分布式的扫描节点，这些节点不断对全球范围内的 IP 地址空间进行扫描，收集设备主动开放的服务信息，如端口号、服务类型、软件版本等，并将数据发送回中央服务器。

2）数据处理层

中央服务器接收到扫描数据后，对其进行清洗、分类和存储。系统会对数据进行分析，提取关键信息，并建立索引，以便后续快速查询。

3）数据展示层

用户通过 Web 界面或 API 接口访问 Shodan 的数据库。搜索结果以可视化的方式呈现，用户可以根据不同的筛选条件（如国家、城市、设备类型等）对搜索结果进行细化和分析。以下是一个简单的 Shodan 平台框架结构示意图：

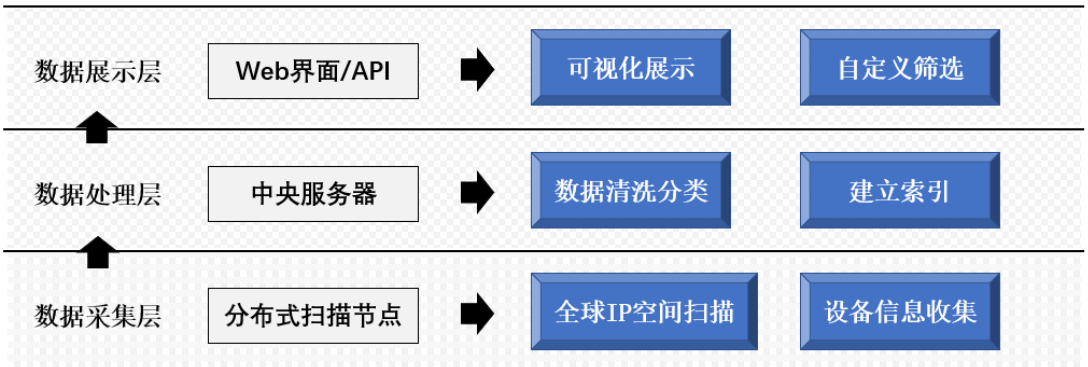


图 4.4 Shodan 平台框架结构示意图

三、主要功能介绍

1）设备搜索功能

用户可以输入各种搜索关键词，如设备类型（如“camera”搜索摄像头设备）、服务端口（如“port:80”搜索开放 80 端口的设备）等，Shodan 会根据关键词在其数据库中进行搜索，并返回相关设备的详细信息，包括地理位置、IP 地址、设备制造商、使用的软件版本等。

2）地理定位功能

Shodan 可以将搜索到的设备在地图上进行标记，直观地展示设备的地理位置分布。这对于了解特定地区的设备部署情况和安全状况非常有帮助。

3）安全漏洞检测

Shodan 可以识别一些已知的安全漏洞，某些情况下会提示设备是否存在特定的安全风险。研究人员可以利用这一功能发现潜在的易受攻击的设备，及时采取措施进行防范。

4）数据统计分析

平台提供对搜索结果的统计分析功能，例如可以统计某种设备在不同国家或地区的分布数量，不同类型服务的使用比例等。这有助于用户从宏观层面了解全球联网设备的整体情况。

4.1.2.2 Censys 平台

一、基本背景概述

Censys 由安全专家 Zakir Durumeric、Eric Wustrow 和 J Alex Halderman 在 2013 年创立。Censys 的目标是对整个互联网进行全面的测绘，通过持续扫描互联网上的各种协议（如 HTTP、HTTPS、SMTP 等），收集和分析设备和服务的信息。它为安全研究人员、企业和政府机构提供了丰富的网络空间数据，帮助他们评估网络安全态势、发现潜在威胁和进行合规性检查。

二、平台框架结构

Censys 的平台框架主要包括以下几个部分：

1）扫描基础设施

Censys 构建了一套分布式的扫描系统，利用多个扫描节点从全球不同位置对互联网进行全方位扫描。这些节点按照特定的规则和频率对 IP 地址进行探测，收集各种协议的响应信息。

2）数据存储与处理系统

扫描得到的数据被存储到大规模的数据库中，同时进行清洗、解析和标注，提取有价值的信息。系统采用先进的数据处理技术，确保数据的准确性和及时性。

3）用户接口

用户可以通过 Web 界面、API 接口或命令行工具访问 Censys 的数据库。用户可以根据自己的需求提交查询请求，并获取相关的数据和分析结果。以下是 Censys 平台框架结构的示意图：

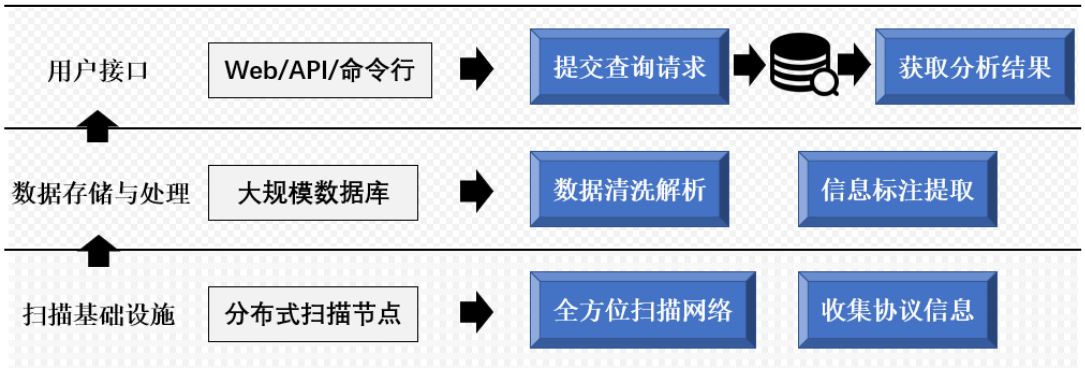


图 4.5 Censys 平台框架结构的示意图

三、主要功能介绍

1）全面的互联网测绘

Censys 对整个互联网进行持续扫描，不仅覆盖常见的端口和协议，还关注一些小众或自定义的服务。这使得用户能够获得关于互联网上各种设备和服务的最全面信息。

2）证书分析功能

Censys 专门对 SSL/TLS 证书进行深入分析，可提供证书的详细信息，如证书颁发机构、有效期、域名关联等。这有助于发现潜在的中间人攻击、非法证书使用等安全问题。

3）历史数据查询

平台保存了大量的历史扫描数据，用户可以查询特定时间范围内的互联网状态。这对于研究网络的演化、安全事件的追溯和趋势分析非常有价值。

4）API 服务

Censys 提供丰富的 API 接口，方便开发者将 Censys 的数据集成到自己的应用程序中，实现自动化的网络安全监测和分析。例如，企业可以利用 API 自动发现内部网络中暴露的敏感设备和服务。

4.1.2.3 RIPE Atlas 平台

一、基本背景概述

RIPE Atlas 是由 RIPE NCC（欧洲 IP 网络资源协调中心）创建的一个全球性网络测量平台，旨在提供全球互联网的性能和连通性数据。RIPE Atlas 自 2010 年推出以来，已经发展成为全球最为广泛部署的互联网测量平台之一，拥有大量的分布式测量探针。RIPE Atlas 主要通过使用分布在全球各地的测量探针（小型硬件设备）进行网络性能监测。测量数据由这些探针收集并传回系统，用户可以通过平台对数据进行查询和分析。该平台不仅帮助用户监控和评估网络的质量，还能提供关于全球互联网拓扑、路径、延迟、流量等重要信息，辅助解决网络故障、优化网络路由等问题。

二、平台框架结构

RIPE Atlas 的架构是由多个层次构成的，主要包括以下几个层次：

1) 物理层（测量探针）

测量探针是 RIPE Atlas 的核心组件，它们通过全球分布的硬件设备（通常是路由器或专用设备）采集网络的相关数据。每个探针通过开放测量协议与 RIPE Atlas 平台进行交互，定期或实时上传数据。

2）数据采集与存储层（数据传输和存储）

探针采集到的数据会通过互联网传输回 RIPE Atlas 的中心平台，平台对其进行存储和处理。数据包括延迟、带宽、路径、丢包率等网络性能指标。这些数据会被存储在高效的数据库中，供后续分析使用。

3）数据分析与处理层（实时分析与查询）

负责对收集到的数据进行实时分析与处理。用户可以通过平台的查询界面，获取网络性能的数据，进行深度的统计分析、故障定位、路由优化等操作。该层利用算法和机器学习技术帮助分析网络状况并提供报告。

4）用户接口与可视化层（Web 界面与 API）

为用户提供交互界面，支持通过 Web 界面、API 或命令行进行数据访问、查询和可视化展示。用户可以方便地查看网络性能的各种数据、生成分析报告、执行定制化的测量任务。

5）外部服务与集成层（合作与共享）

该层允许与其他第三方平台和工具的集成，提供数据共享和合作分析的功能。通过合作伙伴的支持，RIPE Atlas 能够拓展其应用场景，如与网络安全平台、流量分析工具等系统的接口对接。

三、主要功能介绍

1）网络路径与连通性分析

RIPE Atlas 能够实时监测互联网的路径，并为用户提供从一个探针到另一个探针之间的网络路径分析。这对于网络故障诊断、路由优化和连通性分析非常有用。

2）延迟和带宽测量

RIPE Atlas 提供实时的网络延迟和带宽测量，用户可以通过平台查询不同地区、不同路由的延迟情况。对于 ISP 或企业来说，了解网络延迟和带宽利用情况是优化网络性能的重要手段。

3）数据开放与研究

RIPE Atlas 提供了一个开放的数据平台，研究人员、学术界和企业都可以访问和利用这些数据。平台支持定制化的测量任务，可以根据特定需求进行定制的网络测量实验。

4.2 国内成果 - 学术研究

4.2.1 “三层三空间映射”理论

一、基本背景

在网络空间不断发展与演变的过程中，网络空间结构日益复杂，传统的分析和认知方法难以全面、准确地描述网络空间的本质特征和内在规律。网络空间包含多种要素，如物理设备、逻辑关系以及信息内容等，它们之间相互交织且关系复杂。为了更好地理解网络空间结构，实现对网络空间的有效治理、安全防护和资源管理，解放军信息工程大学提出了“三层三空间映射”理论。

二、主要思路/思想

该理论将网络空间抽象为物理层、逻辑层和信息层三个层次，以及物理空间、逻辑空间和信息空间三个空间（如图 4.6）。

1）物理层与物理空间

物理层主要涉及网络空间中的硬件设备，如服务器、计算机、网络通信设备等，这些硬件设备所处的现实世界构成了物理空间。物理层设备是网络空间存在和运行的基础，它们之间通过物理连接和地理位置关系形成了物理拓扑结构。

2）逻辑层与逻辑空间

逻辑层描述了网络中设备之间的逻辑关系，如网络协议、路由规则、数据传输路径等。逻辑空间则是由这些逻辑关系构建而成的抽象空间，它反映了网络系统的功能和行为模式。逻辑层与物理层相对独立，但又相互关联，逻辑规则决定了数据在物理设备之间的流动方式。

3）信息层与信息空间

信息层关注网络中传输和存储的各种信息，包括文本、图像、视频等。信息空间是信息在网络中存在和传播的虚拟空间，信息的产生、传播和处理受到逻辑层规则和物理层设备的制约。

“三层三空间映射”理论强调这三个层次和三个空间之间存在着复杂的映射关系。物理层为逻辑层和信息层提供了物质基础，逻辑层对物理层进行管理和控制，同时影响信息的流动和处理，信息层则是物理层和逻辑层活动的结果体现。通过研究这些映射关系，可以深入理解网络空间的复杂性和内在规律。

三、主要成果和结论

该理论为网络空间结构的研究提供了一种全新的视角和方法框架，有助于构建更加准确的网络空间模型。基于此理论开发的相关分析工具和技术，能够更全面地对网络空间进行可视化展示和分析，为网络空间的安全评估、态势感知等应用提供了有力支持。

“三层三空间映射”理论揭示了网络空间的层次性和复杂性，表明网络空间是一个由多种要素相互作用的有机整体。通过对各层空间映射关系的研究，可以更好地把握网络空间的动态变化，为网络空间的规划、管理和安全保障提供科学依据。

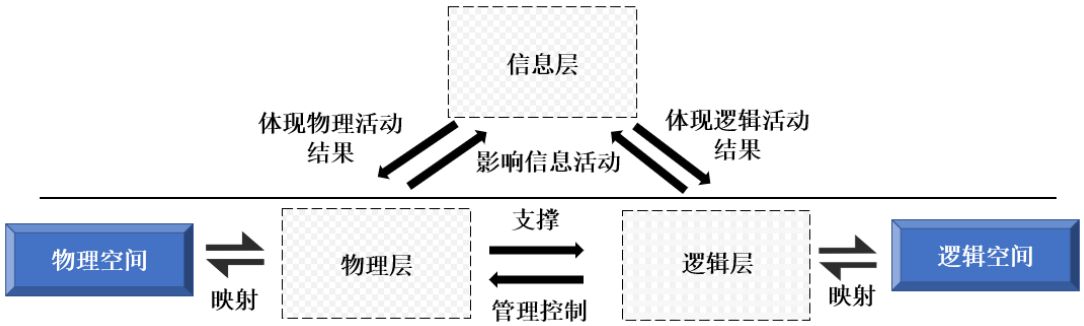


图 4.6 三层三空间映射示例图

4.2.2 网络空间主权框架

一、基本背景

随着信息技术的飞速发展，网络空间已经成为国家主权延伸的新领域。网络空间的虚拟性、跨国性和开放性等特点，使得传统的国家主权理论面临挑战。同时，国际上对于网络空间主权的认知和界定存在分歧，网络攻击、信息泄露、隐私侵犯等问题频发，严重威胁到国家的安全和利益。在这样的背景下，方滨兴院士提出了网络空间主权框架（如图 4.7），旨在明确网络空间主权的内涵和范围，为维护国家网络空间主权提供理论支持和实践指导。

二、主要思路或思想

方滨兴院士认为网络空间主权是国家主权在网络空间的自然延伸，它涵盖了网络空间的管辖权、控制权和发展权等多个方面。

1）管辖权

国家对其领土范围内的网络基础设施、网络活动和网络用户拥有管理和执法的权力。这包括制定网络空间的法律法规，对网络犯罪进行打击，以及对网络内容进行监管等。

2）控制权

国家有权对其关键网络基础设施进行保护和控制，确保网络系统的安全稳定运行。在面对外部网络攻击时，国家可以采取必要的防御措施，保障网络空间的国家安全。

3）发展权

国家在网络空间具有自主发展的权力，包括推动网络信息技术创新、发展网络产业、提高国民网络素养等，以增强国家在网络空间的综合实力。

该框架强调网络空间主权的相对性和相互性，各国在行使网络空间主权时，应遵循国际法和国际关系基本准则，尊重他国的网络空间主权，通过合作共同维护全球网络空间的和平与安全。

三、主要成果和结论

该框架为我国制定网络空间战略和政策提供了重要的理论基础，可促进我国网络安全产业的发展，激发了企业在网络安全技术研发和应用方面的积极性。该框架明确了网络空间主权的重要性和具体内涵，指出维护网络空间主权是保障国家主权、安全和发展利益的必然要求。同时，强调国际合作在网络空间治理中的重要性，只有通过各国之间的合作与协调，才能实现全球网络空间的可持续发展和安全有序。

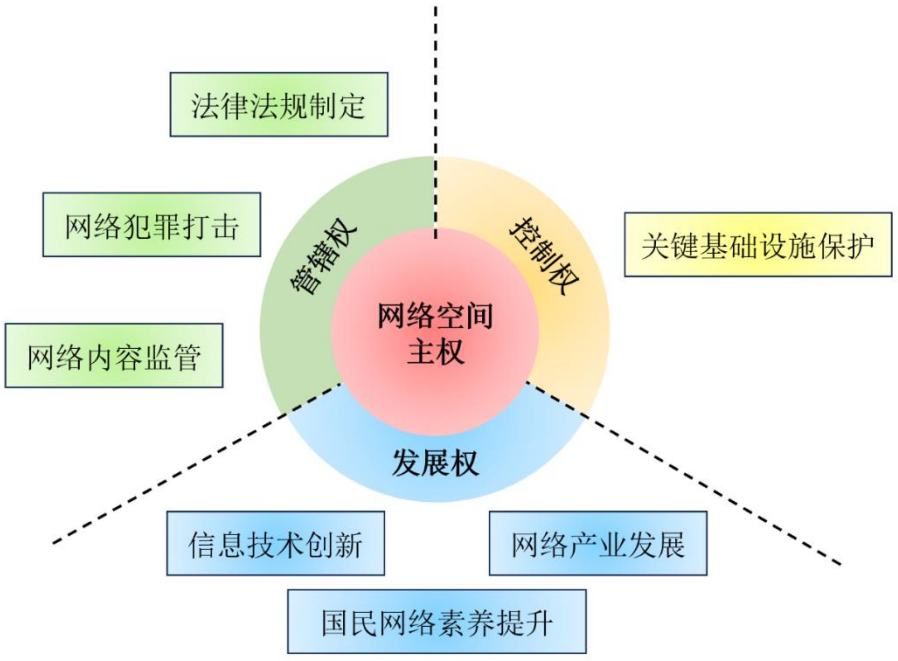


图 4.7 网络空间主权框架

4.2.3 中科院信工所的研究

一、基本背景

随着网络空间安全威胁日益复杂多样，包括恶意软件攻击、数据泄露、网络诈骗等问题不断涌现，对国家的政治、经济、社会等各个领域的安全构成了严峻挑战。

二、主要思路或思想

中科院信工所在网络空间安全研究方面采用多学科交叉融合的方法，综合运用数学、计算机科学、密码学、控制论等多个学科的理论和技术，从多个维度对网络空间安全问题进行深入研究。其研究思路强调主动防御和智能化防控，通过对网络空间的大数据分析、态势感知和风险评估，提前发现潜在的安全威胁，并制定相应的防御策略。同时，注重产学研用相结合，与企业和政府部门合作，将科研成果转化为实际的安全产品和解决方案，服务于国家和社会的网络安全需求。

三、主要成果和结论

中科院信工所在网络安全和网络测绘领域取得了众多重要成果。在地址空间测绘方面，中科院信工所提出了一种基于泄露信息的对抗训练的主动 IPv6 地址生成方法 6GAI, 由生成对抗网络（GAN）和卷积瓶颈注意力模块（CBAM）集成而成；面向不同类型的 IP 设备分析了适用的 IP 定位技术，并且从定位逻辑上对各个定位技术进行了拆解, 提出了一个普适的 IP 定位理论。在域名系统（DNS）测绘方面，中科院信工所设计了一种基于 IPv4 和 IPv6 的合作解析关系，通过跨栈服务关联发现 IPv6 DNS 服务的方法；提出了一种利用孪生网络(Siamese Network)在 IPv6 上支持 TLS1.3 的大规模加密流量中发现加密 DNS 解析器唯一服务提供商的方法；此外，中科院信工所针对公共 DNS 解析器进行探测，提出公共解析器、开放解析器、解析器缓存、解析器选择策等 DNS 解析器测量方法。在密码学方面，开展了新型密码算法的研究，为保障信息的机密性和完整性提供了先进的技术手段。在人工智能安全领域，研究了对抗攻击和防御方法，提高了人工智能系统的安全性。此外，还开发了一系列网络安全监测和预警系统，能够实时监测网络中的异常行为，及时发现和防范安全威胁。

通过多年的研究实践，中科院信工所得出多学科交叉融合是解决复杂网络安全问题的有效途径的结论。强调主动防御和智能化防控在网络安全保障中的重要性，认为只有不断加强技术创新和应用，提高网络安全的自主可控能力，才能有效应对日益增长的网络安全威胁。

4.2.4 中科院地理所的研究

一、基本背景

随着信息技术的飞速发展，网络空间逐渐成为与陆、海、空、天并列的第五大战略空间。网络空间具有高度的复杂性、动态性和虚拟性，其拓扑结构和资源分布等对于国家的网络安全、经济发展和社会稳定至关重要。中科院地理所利用其在地理信息技术和空间分析等方面的优势，将地理空间的研究方法引入网络空间领域，以更好地理解和掌握网络空间的规律和特征。在网络攻击日益频繁、网络空间国际竞争加剧的背景下，对网络空间进行精准、全面的测绘和分析具有迫切的现实需求。

二、主要思路或思想

中科院地理所的研究主要基于地理信息技术中的空间建模、数据分析和可视化等方法。其核心思想是将网络空间中的各种元素，如 IP 地址、网络节点、网络服务等，映射到地理空间中，构建网络空间的地理空间模型。通过对网络流量数据、IP 地址注册信息等多源数据的收集和整合，分析网络空间的拓扑结构、节点分布和流量流动规律等。同时，利用地理信息技术的可视化手段，将抽象的网络空间信息以直观的地图形式呈现出来，以便研究人员和决策者更好地理解和把握网络空间的态势。

例如，通过构建网络空间的“地理图层”，将不同类型的网络节点（如服务器、终端设备等）用不同的符号或颜色在地图上表示出来，清晰地展示网络节点的分布特征。利用空间分析方法，分析网络节点之间的连接关系和距离，研究网络的连通性和脆弱性。

三、主要成果或主要结论

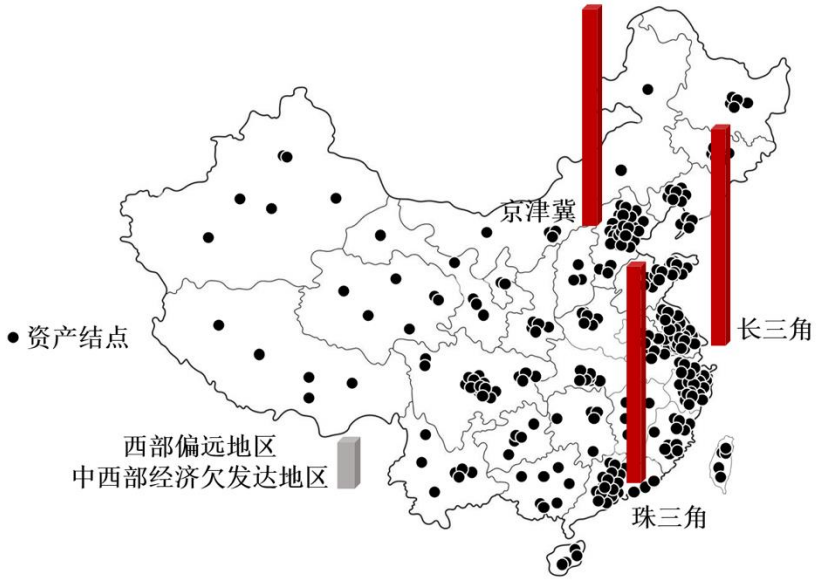


图 4.8 某地区网络节点分布地图

构建了网络空间地理信息系统（NSGIS）：该系统集成了网络空间的多源数据，实现了网络空间信息的高效管理和可视化分析。通过 NSGIS，研究人员可以快速查询和分析网络节点的地理分布、服务类型和连通状态等信息，为网络安全监测、网络规划和决策提供了有力的支持。图 4.8 展示了基于 NSGIS 生成的某地区网络节点分布地图。

揭示了网络空间的空间分布规律：研究发现网络空间中的节点分布并非随机的，而是呈现出一定的聚集性和层次性。在地理空间上，一些经济发达地区和大城市往往是网络节点的集中分布区域，形成了网络空间的“核心区”。而在一些偏远地区和经济欠发达地区，网络节点相对较少，形成了网络空间的“边缘区”。这种分布规律对于理解网络空间的发展不平衡性和制定网络普及政策具有重要的意义。

提出了网络空间脆弱性评估方法：结合地理信息和网络拓扑结构，中科院地理所的研究团队提出了一种基于空间分析的网络空间脆弱性评估方法。该方法考虑了网络节点的地理位置、连接关系和服务重要性等因素，能够准确地识别网络中的脆弱节点和关键链路。通过对网络脆弱性的评估，可以有针对性地制定网络安全防护策略，提高网络的抗攻击能力。

构建网络空间地理图谱的概念和方法，设计了网络空间地理图谱的构建方法，包括三个步骤，网络空间地理要素的信息获取、网络空间关系的识别与空间化以及图谱构建和更新。并以网络空间地理学理论为指导，紧密围绕“人-地-网”纽带关系，结合网络安全工作的实战需求，提出了包含地理环境层、网络环境层、行为主体层和业务环境层的四层网络空间层次模型。此外，还针对天基信息系统设计了网络空间地理图谱的构建方法。首先通过梳理天基信息系统中的网络体系结构，获得网络空间实体与虚拟资源在地理空间和网络空间内的相关属性，实现网络空间各类要素的绘制上图。之后针对天基信息网络拓扑具有链路复杂、高度动态性等特征，采用知识图谱技术，构建网络空间知识图谱，存储、更新和分析网络要素关系，同时依据天基信息网络空间的结构特性，在网络空间信息要素可视化的基础上，对网络要素之间的拓扑关系进行空间化。

4.2.5 哈尔滨工业大学的研究

一、基本背景

在网络空间安全领域，面对日益复杂的网络攻击和安全威胁，准确地掌握网络态势、及时发现网络安全漏洞和入侵行为变得至关重要。传统的网络安全监测方法主要依赖于基于规则的检测和特征匹配，对于新出现的未知攻击和复杂攻击

模式的检测能力有限。哈尔滨工业大学针对网络空间安全领域的新需求和新挑战，开展了一系列创新性的研究工作。

二、主要思路或思想

哈尔滨工业大学的研究主要围绕网络空间的态势感知和安全防护展开。其主要思想是利用大数据分析、机器学习和人工智能等先进技术，对网络流量数据、系统日志数据等进行深度挖掘和分析，以实现对网络安全态势的实时监测和准确预测。通过构建数据驱动的网络安全模型，自动学习网络攻击的模式和特征，提高对未知攻击的检测能力。同时，将网络安全态势感知与网络控制相结合，实现对网络资源的动态配置和优化，增强网络的安全性和可靠性。

例如，利用深度学习算法对网络流量进行建模，将正常的网络流量模式和异常的攻击流量模式进行区分。通过实时监测网络流量的变化，及时发现潜在的安全威胁。同时，根据网络安全态势的评估结果，动态调整网络访问控制策略，阻止非法入侵和恶意攻击。

三、主要成果或主要结论

在地址空间测绘方面，提出了一种基于多接口信息的路由器地理定位方法，利用同一台路由器上不同接口 IP 地址位置相同、相连路由器间地理位置相近的事实，提升了定位的覆盖率和准确率。在路由系统测绘方面，设计了一个通用框架以解决多瓶颈网络拓扑探测中的缓冲膨胀问题，提升实时交互应用的性能；提出了一种不相交路径路由算法，旨在提高无线传感器网络中路由的可靠性，适用于多 Sink 节点的网络结构的拓扑探测。在域名系统测绘方面，提出非公共 DNS 服务器的主动测量方法；设计实现了开放 DNS 服务器缓存测量与风险评估系统，从而掌握全国开放 DNS 服务器缓存的部署与风险状况；并对中国境内部署的根 DNS 服务器的根任播节点的服务性能进行了分析。在证书系统测绘方面，应用不同的机器学习模型并通过验证提取 (VFE) 来区分恶意 X.509 证书和良性 X.509 证书。

开发了基于深度学习的网络安全态势感知系统：该系统利用卷积神经网络（CNN）和循环神经网络（RNN）等深度学习模型，对网络流量数据进行实时分析和处理。通过对大量的网络流量数据进行训练，系统能够自动识别各种类型的网络攻击，包括 DDoS 攻击、恶意软件入侵、SQL 注入等。实验结果表明，该系统在网络攻击检测的准确率和召回率方面都取得了较好的性能，能够有效地提高网络的安全性。图 4.9 展示了该系统的工作流程示意图。

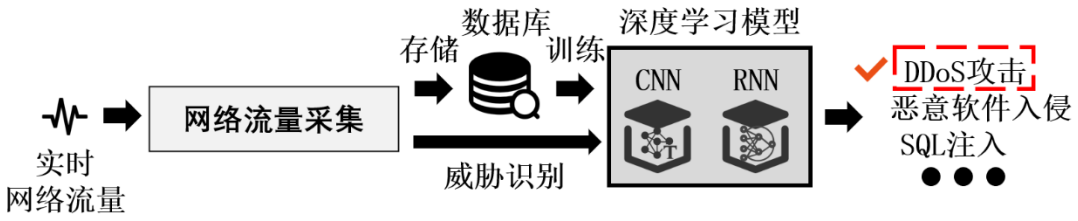


图 4.9 基于深度学习的网络安全态势感知系统工作流程

提出了多源数据融合的网络安全分析方法：为了提高网络安全态势感知的准确性和全面性，哈尔滨工业大学的研究团队提出了一种多源数据融合的网络安全分析方法。该方法将网络流量数据、系统日志数据、威胁情报数据等多种来源的数据进行融合，综合分析网络中的各种安全信息。通过数据融合，可以更全面地了解网络的运行状态和安全态势，发现潜在的安全威胁和漏洞。

实现了网络安全态势的可视化展示：将复杂的网络安全信息以直观的图表、地图等形式展示出来，有助于安全管理人员快速理解和掌握网络的安全态势。哈尔滨工业大学的研究团队开发了一套网络安全态势可视化系统，该系统能够实时展示网络中的攻击事件、安全漏洞分布、网络流量变化等信息。通过可视化展示，可以及时发现网络中的安全隐患，为安全决策提供有力的支持。

4.2.6 清华大学的研究

一、基本背景

清华大网络研究院在网络空间安全态势感知和面向 IPv6 的网络空间测绘方面开展了大量深入的研究。这里重点对该团队在 IPv6 网络空间测绘及 IP 端口开放性智能化预测方面进行介绍。

随着互联网的迅猛发展，IPv4 地址资源日益枯竭，难以支撑物联网、工业互联网等大规模设备接入需求。IPv6 作为新一代互联网协议应运而生，凭借其巨大的地址空间，为未来的网络扩展提供了坚实基础。然而，IPv6 的大规模部署也带来了诸多新挑战，例如地址编排多样性导致的活跃地址分布不可预测，以及网络拓扑结构日趋复杂难以探测等。

在网络安全领域，对 IPv6 网络的精确探测和了解是保障网络安全的基础。准确探测活跃 IPv6 地址有助于发现潜在的攻击目标和漏洞，而端口开放性预测可以帮助评估网络设备的安全风险。同时，清晰的 IPv6 拓扑结构对于网络规划、流量管理以及故障排除都具有重要意义。但是，由于 IPv6 地址空间的巨大，传

统的网络探测和分析方法在 IPv6 网络中面临效率和准确性的问题，因此需要新的技术和方法来适应 IPv6 网络的特点。

二、主要思路或思想

1）面向 IPv6 的网络空间探测（活跃地址探测）

鉴于 IPv6 地址空间的规模极为庞大，传统的全空间暴力扫描方法在时间与资源开销上不可行，因此团队摒弃了该策略。针对 IPv6 地址空间的庞大性和复杂性，团队提出了一套系统、全面且高效的 IPv6 活跃地址探测方法 AddrMiner（如图 4.10），将 IPv6 地址空间划分为**三种场景**：无种子地址的区域、只有少量种子地址的区域和丰富种子地址的区域，并针对每种场景设计了相应的探测方案，构建了全球化的主动探测体系，实现了活跃 IPv6 地址从无到有、由少到多的积累。

无种子地址的区域：在无种子地址的区域，结合 IPv6 地址结构规律和外部信息（如组织、所属等），提出了一种基于多级关联策略的活跃 IPv6 地址探测方法。该方法通过挖掘有种子区域中种子地址的通用模式，构建通用地址模式库，并设计多级关联策略将其迁移至无种子区域以生成目标地址，实现跨区域的高效探测。算法设计了多熵值并行分裂、基于贪心策略的游离点去除、多级关联迁移和动态反馈引导等四项关键机制，有效克服了无种子区域探测效率低下的难题，极大程度扩展了活跃 IPv6 地址探测的边界。

只有少量种子地址的区域：在种子地址较少的区域，团队提出了相似性匹配策略。该策略基于平衡空间模式表示技术（Balanced Space Pattern Representation, BSPR）对种子地址模式进行建模，并构建通用模式库。随后，利用该区域内有限的种子地址，从通用模式库中筛选出更相关的候选模式列表。为提升探测效果，方法进一步引入动态反馈机制，以规避模式迁移失效问题，从而实现对少量种子区域中活跃 IPv6 地址的高效探测。

有足量种子地址的区域：在有足量种子地址的区域，团队提出一种基于强化学习的动态反馈探测方法。该方法首先采用最小熵值分裂策略，在近线性时间内构建种子地址的密度空间树，以识别高密度聚集区域。随后引入强化学习框架，根据探测反馈动态修正种子地址的密度分布，纠正抽样偏差，从而引导目标地址生成更加贴近真实活跃分布。该方法显著提升了 IPv6 活跃地址的探测效率与发现速率，避免了传统暴力扫描的低效问题。

这些研究成果已在 IPv6 网络测量和安全分析中得到广泛应用，特别是在**网络空间态势感知和网络安全防御**领域。例如，团队的研究为 IPv6 网络中的资产

发现、漏洞管理和攻击溯源提供了重要工具，推动了我国 IPv6 网络的规模化部署和安全保障。

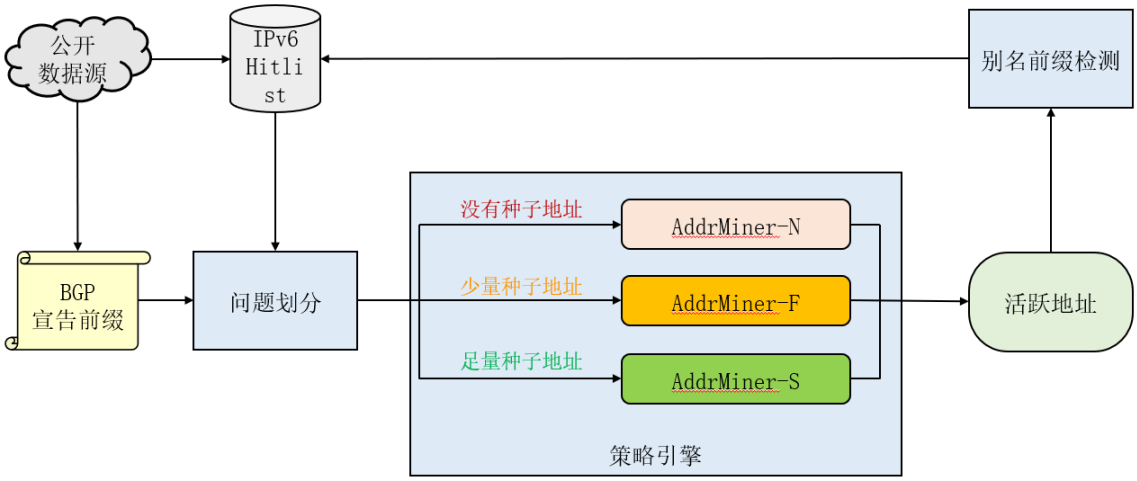


图 4.10 IPv6 活跃地址探测框架 AddrMiner

2）端口开放性预测

团队运用机器学习的方法来进行端口开放性预测，以使用少量的探测资源发现足量的开放端口，该方法对于 IPv4 和 IPv6 地址空间均适用（如图 4.11）。首先，在各个子网内部随机选取一部分地址作为种子地址，并获取种子地址的全量端口开放性信息，利用这些信息初始化决策模型。然后，收集目标主机的特征信息，如已知的开放端口、主机所属的子网、主机所属的自治域和组织等，并根据特征信息作用范围的大小，将它们分类为局部特征与全局特征。接着，利用目标主机的全局特征与局部特征，决策模型能够计算得到目标主机上各个端口的开放概率。探索模块进一步对各端口的开放概率进行调整，以避免模型陷入局部最优的困境之中。得到各端口最终的开放概率后，选择其中开放概率最高的若干端口进行扫描，得到真实的开放端口信息。反馈模块能够利用扫描得到的真实开放端口信息更新已知的主机特征和决策模型，并据此进行下一轮的预测——扫描循环，直至达到预设的轮次上限。通过上述的算法，团队实现了端口开放性预测系统，能够大幅节省发现网络空间中开放端口所需的时间和扫描资源，在预测覆盖度和预测耗时等指标上明显超越了前人工作的结果。

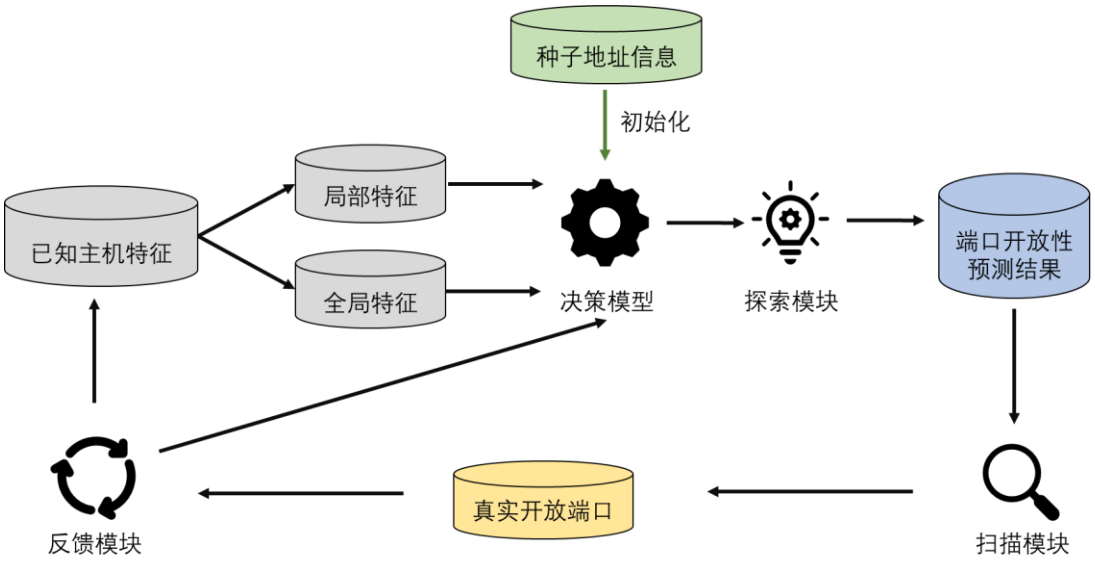


图 4.11 端口开放性预测架构图

3）IPv6 拓扑发现

在 IPv6 拓扑发现方面，团队综合利用主动探测和被动监测的方法（如图 4.12）。主动探测主要通过发送特定的网络数据包，如 Ping 包、Traceroute 包等，来获取网络节点之间的连接信息。被动监测则通过监听网络中的路由信息、邻居发现消息等，来补充和修正拓扑结构。同时，采用图论的方法对拓扑结构进行建模和分析，识别网络中的关键节点、链路和子网，从而清晰地描绘出 IPv6 网络的拓扑结构。

基于强化学习的主动探测方法：IPv6 地址空间十分庞大，且具有更加严格的 ICMPv6 响应限速策略——这限制了我们使用较高的发包速率进行探测。因此，为了实现高效的 IPv6 拓扑发现，对探测包的选取进行了精心的设计，这包括两点：1）通过强化学习的方法找到具有高探测收益的目标区域，并给这些区域分配更多探测资源；2）在确定目标地址后，结合 DoubleTree, Yarrp6 等多种优化技术，尽可能减少对同一拓扑（接口、边）的重复探测，从而节约探测包。通过上述的策略，实现了高效的 IPv6 拓扑发现主动探测方法，在探测效率、探测结果覆盖广度等指标上都超过前人的方法。

多来源被动监测方法：主动探测方法受限于探针本身的数量和位置，并且互联网中的路由器普遍存在抗拓扑测绘的现象（例如不响应 ICMPv6 探测包），因此，需要尽可能多来源的被动监测方法的数据进行补充。我们使用了 RouteViews 公开的路由信息、IXP 们公开的 AS peering 关系等被动收集的数据，与主动探测的结果相互融合印证。

拓扑结构分析：通过持续收集 IPv6 拓扑信息，对得到的结果采用图论的方法进行建模和分析。通过对结点的度的分析，能够识别网络中的关键节点、链路和子网，为网络安全监测提供信息。此外，还对 IPv6 拓扑的动态变化进行了记录和分析，发现存在大量靠近互联网边缘的路由器呈现出很高的动态性，其活跃周期非常短（数小时）。

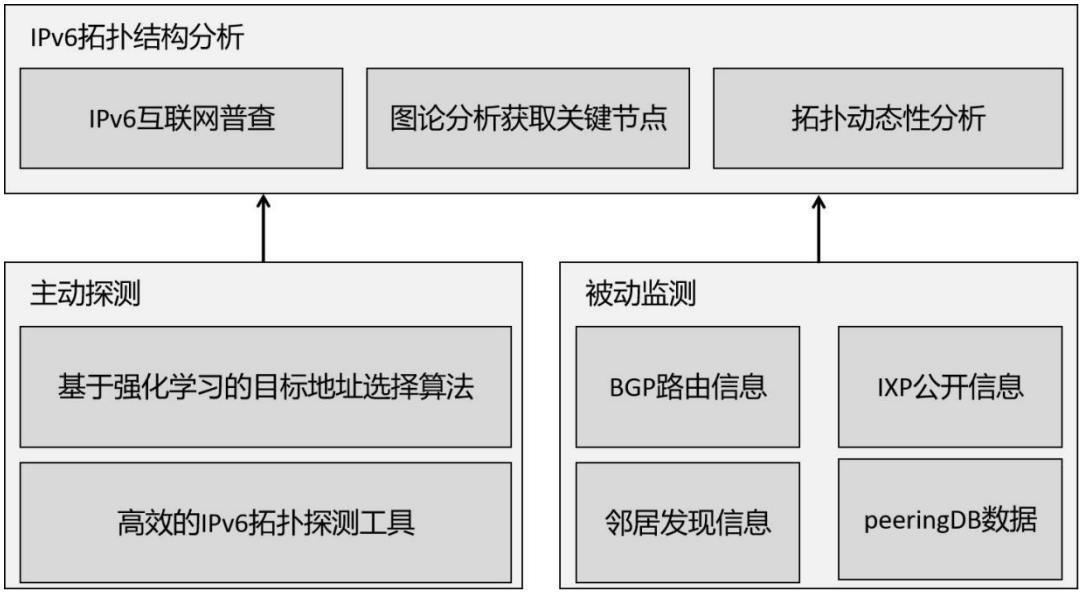


图 4.12 IPv6 拓扑发现方法

三、主要成果

1）面向 IPv6 的网络空间探测（活跃地址探测）

高效探测算法：团队提出了一套系统、全面且高效的 IPv6 活跃地址探测方法，构建了全球化的主动探测体系，有效应对传统扫描技术在超大地址空间下失效的问题，显著降低探测开销并提升探测效率。并在此基础上，研制新型地址探测工具 AddrMiner。

活跃 IPv6 地址库：通过持续探测，团队累计发现超过 21 亿高质量活跃 IPv6 地址，形成全球规模更大、质量更高、覆盖最广的公开 IPv6 地址库，已广泛支撑国内外知名科研机构的 IPv6 网络安全研究，并成功应用于国内主流测绘平台。

2）端口开放性预测

高精度预测模型：团队训练的机器学习模型在端口开放性预测方面取得了较高的准确率。通过对多种模型的比较和优化，选择了最适合 IPv6 网络端口预测

的模型，预测覆盖率最高可达 98%。这使得安全管理人员可以提前了解网络设备的端口状态，及时发现潜在的安全风险。

特征重要性分析：在特征提取和选择的过程中，分析了各个特征对端口开放性预测的重要性。发现设备的操作系统类型、服务类型等特征对端口状态的影响较大。这一结论有助于在实际应用中更加有针对性地收集和分析相关特征，提高预测的效率和准确性。

3）IPv6 拓扑发现

准确的拓扑模型：通过综合利用主动探测和被动监测的方法，构建了准确的 IPv6 网络拓扑模型。该模型能够清晰地展示 IPv6 网络中节点之间的连接关系、子网结构以及关键节点和链路的位置。为网络规划、流量管理和故障排除提供了重要的依据。

拓扑变化规律：对不同时间段的 IPv6 拓扑结构进行分析，揭示了 IPv6 网络拓扑的动态变化规律。发现 IPv6 网络拓扑的变化主要受到新设备接入、网络升级和路由策略调整等因素的影响。这一结论有助于网络管理人员及时掌握网络拓扑的变化情况，采取相应的措施保障网络的稳定运行。

4.3 国内成果 - 工业界平台

4.3.1 知道创宇 ZoomEye

一、基本背景概述

知道创宇是国内知名的网络安全企业，长期专注于网络安全技术研究与服务。ZoomEye 是知道创宇自主研发的一款网络空间搜索引擎，它被广泛应用于网络资产探测、安全情报收集、漏洞扫描发现等多个领域。通过对全球范围内的网络资产进行大规模的扫描和数据收集，ZoomEye 帮助企业、安全研究人员和政府机构更好地了解网络空间中的资产分布和安全状况。

自推出以来，ZoomEye 随着网络技术的发展不断更新和完善。它适应了 IPv6 网络的普及趋势，能够对 IPv4 和 IPv6 网络资产进行全面探测，为网络空间安全建设提供了有力的支持。在网络安全检测和防护方面，广泛用于发现企业潜在的安全风险，提前发现可能被攻击的目标，辅助企业完善安全策略。ZoomEye 是唯一入选“全球 25 大 OSINT 工具”的中国产品，兼具公有云与私有化部署能力，服务于漏洞应急响应和国家级网络安全保障。

二、平台框架结构

ZoomEye 主要由数据采集层、数据存储层和数据检索层构成，其框架结构示意图如图 4.13 所示：

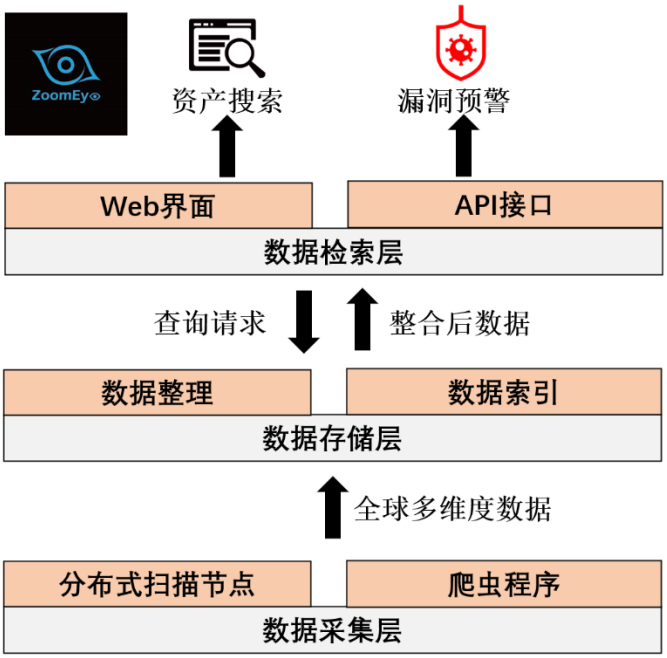


图 4.13 ZoomEye 平台框架示意图

1）数据采集层

分布式扫描节点：ZoomEye 拥有大量分布在全球各地的扫描节点，这些节点持续对网络空间进行扫描，通过发送各种类型的网络请求（如 HTTP、HTTPS、FTP 等），收集目标资产的响应信息，包括开放端口、服务类型、应用程序版本等。

爬虫程序：除了主动扫描，ZoomEye 还利用爬虫程序从互联网上收集公开的网络资产数据，例如网站的 HTML 内容、DNS 记录等。这些数据来源多样化，可以更全面地获取网络资产信息。

2）数据存储层

采集到的大量数据会被存储在高性能的分布式数据库中。数据库会对数据进行分类、整理和索引，以方便快速检索和查询。同时，为了保证数据的安全性和可靠性，数据库采用了数据备份和冗余机制。

3）数据检索层

Web 界面：用户可以通过浏览器访问 ZoomEye 的 Web 界面，使用简单易懂的搜索语法进行资产查询。Web 界面提供了直观的搜索框、筛选条件和结果展示，方便用户快速定位所需的网络资产。

API 接口：对于开发者和企业用户，ZoomEye 提供了丰富的 API 接口，允许他们集成到自己的系统中，实现自动化的资产搜索和数据挖掘。

三、主要功能介绍

1）网络资产搜索

用户可以根据 IP 地址、域名、端口、服务类型等多种条件进行资产搜索。例如，用户可以搜索全球范围内开放特定端口（如 8080 端口）的服务器，或者查找运行特定软件（如 Apache 服务器）的设备。

2）资产详情查询

当用户找到感兴趣的资产后，可以查看详细的资产信息，包括开放端口列表、服务指纹、操作系统信息、应用程序版本等。这些详细信息有助于安全研究人员进一步分析资产的安全状况。

3）安全漏洞预警

ZoomEye 会对收集到的资产数据进行分析，结合已知的安全漏洞数据库，为用户提供与资产相关的安全漏洞预警信息。例如，如果某个服务器使用的软件版本存在已知漏洞，ZoomEye 会及时提醒用户。

4）资产可视化展示

平台提供了直观的可视化界面，将搜索结果以地图、图表等形式展示出来。用户可以通过地图快速了解不同地区的网络资产分布情况，通过图表对比不同类型资产的数量和比例。

5）产品特色

通过全球分布式测绘节点和 AI 技术（如集成 DeepSeek 大模型），支持多语言智能搜索，显著提升搜索精准度与用户体验，覆盖 IPv4/IPv6 及多协议资产。

4.3.2 华顺信安 Fofa

一、基本背景概述

华顺信安是一家专注于网络空间测绘技术创新的企业。Fofa 作为其核心产品，是一款具有强大搜索能力的网络空间资产搜索引擎。Fofa 的目标是帮助企

业、安全机构和研究人员更深入地了解网络空间中的资产信息，通过整合海量的网络资产数据，为用户提供全方位的网络安全情报服务。

Fofa 在网络安全领域具有广泛的应用，无论是在安全威胁预警、漏洞扫描，还是在安全策略制定方面都发挥着重要作用。它能够快速准确地定位目标资产，为安全人员节省大量的时间和精力，在国内网络安全市场上占据重要地位。

二、平台框架结构

Fofa 的平台框架主要包括数据采集模块、数据挖掘与分析模块、数据存储与索引模块和用户交互模块，其框架结构示意图如 4.14 所示：

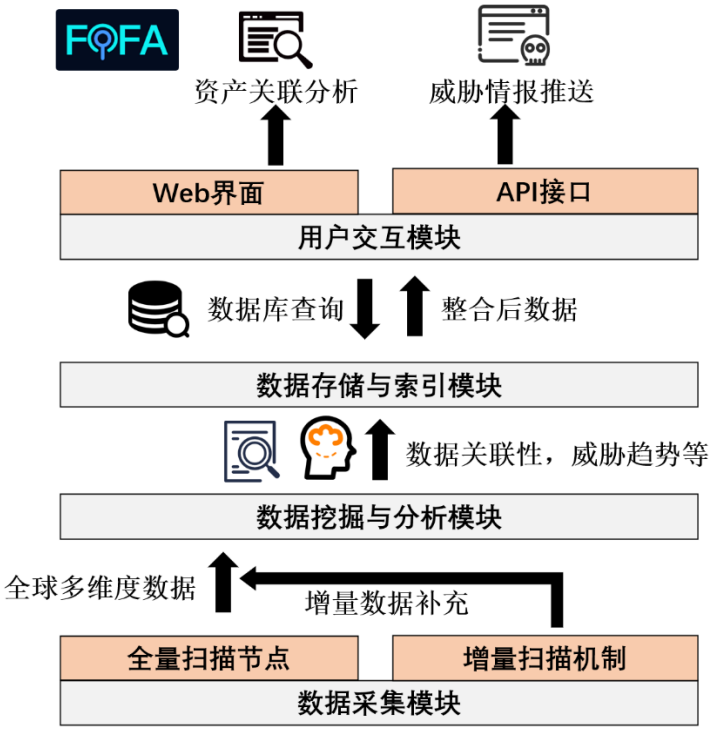


图 4.14 Fofa 平台框架示意图

1）数据采集模块

全量扫描节点：Fofa 部署了大量的全量扫描节点，对全球范围内的网络资产进行周期性的全面扫描。扫描内容包括各种网络协议、应用程序和设备信息，确保能够覆盖尽可能多的网络资产。

增量扫描机制：除了全量扫描，Fofa 还采用了增量扫描机制，对新出现或发生变化的资产进行实时监测和更新。这种机制可以保证数据的及时性和准确性。

2）数据挖掘与分析模块

该模块通过先进的数据挖掘算法和机器学习技术，对采集到的数据进行深度分析。它可以从海量数据中挖掘出有价值的信息，例如资产的关联性、安全威胁趋势等，并为用户提供相应的分析报告和建议。

3）数据存储与索引模块

采集和分析后的数据会被存储在高性能的数据库中，并进行详细的索引。这样，当用户进行查询时，可以快速定位到所需的数据。同时，该模块还具备数据备份和恢复功能，以确保数据的安全性和可靠性。

4）用户交互模块

Web 搜索界面：用户可以通过 Fofa 的 Web 搜索界面输入搜索语法进行资产搜索。界面简洁易用，同时提供了丰富的帮助文档和示例，方便新用户快速上手。

API 开发接口：Fofa 为开发者提供了 API 开发接口，允许他们将 Fofa 的搜索功能集成到自己的应用程序中，实现个性化的开发需求。

三、主要功能介绍

1）高级搜索语法

Fofa 支持复杂的搜索语法，用户可以根据多种条件组合进行资产搜索。例如，用户可以使用逻辑运算符（如 AND、OR、NOT）和正则表达式来精确筛选目标资产，大大提高了搜索的灵活性和准确性。

2）资产关联分析

Fofa 能够对搜索到的资产进行关联分析，找出不同资产之间的潜在联系。例如，它可以发现同一企业在不同地区的多个服务器之间的关系，帮助安全人员全面了解企业的网络资产布局。

3）威胁情报推送

结合实时的安全威胁情报，Fofa 会为用户推送与搜索结果相关的安全威胁信息。例如，如果某个资产可能受到近期流行的网络攻击威胁，Fofa 会及时通知用户。

4）历史数据查询

用户可以查询指定时间段内的网络资产信息，了解资产的变化情况。这对于分析网络发展趋势和安全事件的历史演变具有重要意义。

5）产品特点

资产数据与白帽子生态：独特的域名爬虫技术，域名资产数据积累丰富，持续性更新探测数据，保证数据的时效性、可用性。构建攻防双向应用的白帽子社群生态。

攻击面管理创新：通过“线索融合-资产关联-风险评估”三步自动化流程，以攻击者视角发现未知资产，支持滚雪球式资产扩展与分类管理。

4.3.3 360Quake

一、基本背景概述

360Quake 是 360 公司旗下一款全面且强大的网络空间搜索引擎和资产测绘平台。在当前复杂多变的网络安全形势下，网络空间中存在着大量的资产和漏洞，各类黑客攻击、数据泄露等安全事件频发。360 作为国内知名的网络安全企业，凭借其多年来在网络安全领域的技术积累和丰富经验，推出了 360Quake 平台。其目标是帮助企业、安全研究人员和相关机构更好地掌握网络空间的资产分布状况，及时发现潜在的安全风险，从而有效进行安全防护和漏洞修复，保障网络空间的安全稳定。

二、平台框架结构

360Quake 的平台框架结构主要由数据采集层、数据处理层、数据分析层和用户交互层四个部分组成，下面详细介绍各部分及其作用。

1）数据采集层

这是平台的基础层，负责从广阔的网络空间中收集各类资产信息。该层拥有多种数据采集渠道和方法，包括但不限于：

主动扫描：通过部署大量的扫描节点，主动对网络中的 IP 地址段进行周期性的扫描，获取资产的开放端口、服务信息、应用程序版本等基础信息。

被动监听：在网络关键节点部署监听设备，被动收集网络中的数据包信息，从中提取关于资产的相关线索，如域名解析记录、设备通信信息等。

2）数据处理层

数据处理层主要对采集到的原始数据进行清洗、整理和存储。其具体功能包括：

数据清洗：去除采集数据中的噪声、重复信息以及错误数据，确保数据的准确性和一致性。例如，过滤掉由于网络干扰产生的无效扫描结果。

数据标准化：将不同来源、不同格式的数据进行统一的标准化处理，以便后续的分析和查询。例如，将不同操作系统返回的服务信息进行规范格式化。

数据存储：采用分布式存储技术，如 HBase、MongoDB 等，将处理后的数据高效地存储在数据仓库中，以便快速查询和访问。

3）数据分析层

这是平台的核心层，运用多种分析算法和技术对处理后的数据进行深度挖掘和分析。主要功能有：

资产关联分析：将采集到的各种资产信息进行关联，构建资产之间的关系图谱。例如，将域名、IP 地址、服务器端口等信息关联起来，形成一个完整的资产视图，帮助用户了解资产的整体分布和相互关系。

漏洞发现与分析：结合已知的漏洞库和安全规则，对资产信息进行分析，发现潜在的安全漏洞。通过对资产的软件版本、开放端口等信息进行比对，判断是否存在已知的可利用漏洞。

威胁情报分析：融合外部的威胁情报数据，对采集到的资产信息进行实时监测和分析，识别潜在的威胁源。例如，根据情报数据判断某个 IP 地址是否与恶意组织有关联。

4）用户交互层

用户交互层为用户提供了友好的界面和便捷的操作方式，使用户能够方便地访问和使用平台的功能。具体包括：

搜索查询：提供多样化的搜索方式，用户可以根据资产的 IP 地址、域名、端口号、服务类型等多个维度进行精确或模糊查询，快速定位目标资产。

可视化展示：以直观的图表、地图等形式展示资产的分布情况、安全状况等信息。例如，通过世界地图展示全球范围内的资产分布热力图，让用户一目了然地了解资产的分布密集程度。

API 接口：为开发者和企业用户提供 API 接口，允许他们将 360Quake 的功能集成到自己的系统中，实现自动化的资产监测和安全分析。

三、主要功能介绍

1）资产搜索功能

360Quake 具备强大的资产搜索能力，用户可以根据各种条件进行灵活搜索。

多维度搜索：支持按 IP 地址、域名、端口号、服务类型（如 HTTP、FTP、SSH 等）、设备类型（如服务器、路由器、摄像头等）进行搜索。例如，用户可以输入特定的 IP 段，查询该网段内所有开放 HTTP 服务的资产信息；或者输入某个域名，查找该域名对应的所有 IP 地址及相关资产详情。

高级搜索语法：提供丰富的高级搜索语法，支持逻辑运算符（如 AND、OR、NOT）、通配符等。用户可以通过复杂的搜索表达式进行精确的资产筛选。例如，使用“port:80 AND title:财务系统”这样的搜索表达式，就可以快速定位所有开放 80 端口且页面标题包含“财务系统”的资产。

2）漏洞发现功能

通过对采集到的资产信息与已知漏洞库进行比对和分析，360Quake 能够及时发现潜在的安全漏洞。

漏洞精准识别：利用先进的漏洞匹配算法，准确识别资产中存在的已知漏洞。对于每一个发现的漏洞，平台会提供详细的漏洞信息，包括漏洞名称、漏洞类型、严重程度、影响范围以及修复建议等。

漏洞实时监测：对资产进行持续监测，一旦发现新的漏洞或已有漏洞的利用情况发生变化，及时向用户推送警报信息。例如，当某个关键资产发现了高危漏洞时，系统会立即通过短信、邮件等方式通知用户。

3）威胁情报分析功能

360Quake 融合了丰富的外部威胁情报数据，为用户提供全面的威胁情报分析服务。

威胁源识别：通过对资产信息和流量数据的分析，识别潜在的威胁源，如恶意 IP 地址、恶意域名等。平台会对这些威胁源进行实时跟踪和监控，及时发现异常活动。

攻击态势感知：结合安全事件数据和威胁情报，为用户提供网络空间的攻击态势感知服务。通过直观的可视化界面，用户可以了解不同地区、不同行业的攻击分布情况，以及攻击趋势的变化，从而提前做好安全防范措施。

4）资产报表与可视化展示功能

平台提供详细的资产报表和直观的可视化展示功能，帮助用户更好地了解资产状况。

资产报表生成：用户可以根据自己的需求生成各种类型的资产报表，如资产清单、漏洞统计报表、安全态势报告等。报表内容丰富、格式规范，可以方便地导出为 PDF、Excel 等常见文件格式，便于用户进行存档和分享。

可视化展示：以图表、地图、拓扑图等形式对资产信息进行可视化展示，让用户更加直观地了解资产的分布、关联关系和安全状况。例如，通过资产拓扑图，用户可以清晰地看到各个资产之间的网络连接关系，及时发现潜在的安全隐患。

5）产品特点

实时威胁情报联动：结合 360 安全大脑的威胁情报库，提供动态漏洞关联与攻击链分析，侧重实时风险预警。

轻量化与低侵扰探测：优化扫描策略减少网络负载，适用于高敏感场景的资产发现与漏洞验证。

4.3.4 盛邦安全 Daydaymap

一、基本背景概述

盛邦安全是一家专注于网络安全领域的企业，在网络安全技术研发和应用方面拥有丰富的经验和深厚的技术积累。Daydaymap 是盛邦安全推出的一款网络空间测绘平台，旨在帮助用户全面、精准地掌握网络空间资产信息，及时发现潜在的安全风险。

在当今数字化时代，网络攻击日益频繁和复杂，企业和组织面临着越来越多的安全挑战。网络空间测绘技术能够通过主动扫描和探测，发现网络中的各种资产，包括服务器、设备、应用程序等，并对其进行详细的信息采集和分析。Daydaymap 平台正是为了满足这一市场需求而开发的，它可以为政府、企业、金融、能源等各个行业的用户提供专业的网络空间资产测绘服务。

二、平台框架结构

Daydaymap 平台主要由数据采集层、数据处理层、数据分析层和应用服务层四个部分组成，以下是各层的详细介绍：

1）数据采集层

数据采集层是 Daydaymap 平台的基础，它负责通过多种方式收集网络空间中的资产信息。主要的采集方式包括：

主动扫描：对指定的 IP 地址段、域名等进行全面的扫描，收集开放的端口、运行的服务、操作系统信息等。

被动监听：通过监听网络流量，获取设备之间的通信信息，发现潜在的资产。

第三方数据整合：整合来自各种公开数据源和合作伙伴的数据，丰富平台的资产信息。

数据采集层使用了先进的扫描技术和网络监听工具，确保能够高效、准确地收集到全面的网络空间资产信息。

2）数据处理层

数据处理层负责对采集到的原始数据进行清洗、去重、归一化等处理，以提高数据的质量和可用性。同时，该层还会对处理后的数据进行存储，建立完善的数据索引，便于后续的查询和分析。

数据处理过程中，会运用大数据处理技术，如分布式存储和计算框架，确保能够处理大规模的数据。

3）数据分析层

数据分析层是 Daydaymap 平台的核心，它运用机器学习、深度学习、关联分析等技术，对处理后的数据进行深入挖掘和分析。主要的分析内容包括：

资产关联分析：分析不同资产之间的关联关系，如设备之间的网络连接、应用程序与服务器的依赖关系等。

漏洞风险分析：结合已知的漏洞信息和资产数据，评估资产面临的漏洞风险等级。

威胁情报分析：与外部威胁情报源进行关联，及时发现潜在的安全威胁。

通过数据分析层的处理，可以为用户提供有价值的安全洞察和决策依据。

4）应用服务层

应用服务层为用户提供了一系列的应用和服务接口，方便用户根据自己的需求进行使用。主要的应用包括：

资产可视化：通过直观的图表和地图等形式，展示网络空间资产的分布和状态。

安全监测与预警：实时监测资产的安全状态，当发现异常情况时及时发出预警。

报告生成：根据用户的需求，生成详细的资产测绘报告和安全分析报告。

应用服务层还支持开放 API 接口，方便与其他企业内部系统进行集成，实现数据的共享和业务流程的自动化。整个平台的框架如图 4.15 所示。

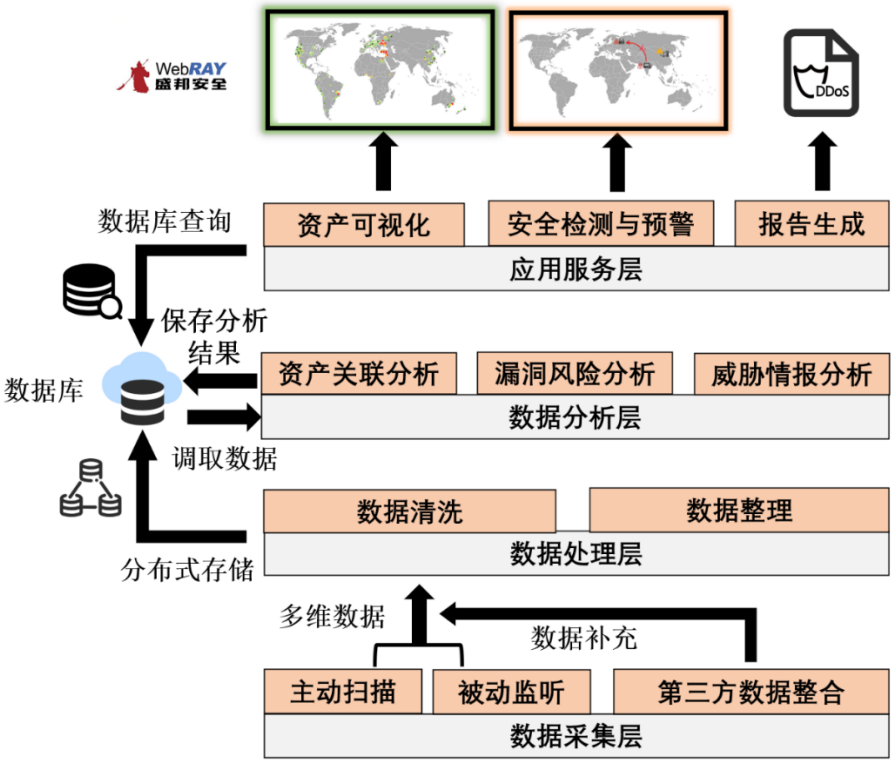


图 4.15 盛邦安全 Daydaymap 平台框架示意图

三、主要功能介绍

1）资产发现与识别

全面扫描：Daydaymap 平台可以对指定的网络范围进行全面的扫描，发现各种类型的资产，包括路由器、交换机、服务器、工控设备等。

资产识别：准确识别资产的类型、操作系统、应用程序等详细信息，帮助用户全面了解网络中的资产状况。

资产分类与管理：对发现的资产进行分类管理，方便用户按照不同的维度进行查看和筛选，如按地理位置、业务部门、资产类型等。

2）漏洞管理

漏洞检测：结合漏洞数据库和先进的漏洞检测技术，对资产进行漏洞检测，发现潜在的安全漏洞。

漏洞评估：对检测到的漏洞进行风险评估，给出漏洞的严重程度和修复建议，帮助用户优先处理高风险漏洞。

漏洞跟踪与修复管理：跟踪漏洞的修复进度，提醒用户及时修复漏洞，确保资产的安全性。

3）安全态势感知

实时监测：实时监测网络空间资产的安全状态，及时发现异常行为和安全事件。

威胁情报整合：整合国内外的威胁情报源，为用户提供最新的安全威胁信息，提高用户的安全防范能力。

可视化展示：通过直观的图表和报表，展示网络空间的安全态势，帮助用户快速了解整体安全状况。

4）合规性检查

合规标准支持：支持多种国内外的合规标准，如等保、PCI DSS 等，帮助用户检查网络资产是否符合相关标准的要求。

合规报告生成：根据合规检查结果，生成详细的合规报告，为用户提供改进建议和参考。

5）API 接口与集成

开放 API：提供开放的 API 接口，方便用户将 Daydaymap 平台与其他安全系统、业务系统进行集成，实现数据的共享和业务流程的自动化。

定制化开发：支持根据用户的特定需求进行定制化开发，满足不同用户的个性化需求。

通过以上功能，盛邦安全 Daydaymap 平台可以帮助用户全面掌握网络空间资产信息，及时发现安全漏洞和威胁，提高网络安全防护能力。同时，平台的可视化界面和丰富的报表功能也方便用户进行管理和决策。

6）产品特色

合规导向的资产测绘：聚焦等保 2.0 要求，提供资产暴露面收敛与合规性评估，适配政府及金融行业需求。目前数据对学术界开放，支撑学术研究。

丰富的 IPv6 资产数据：盛邦安全联合清华大学，长期深耕 IPv6 网络空间探测，攻克多项关键技术难题，积累了丰富的高质量 IPv6 资产数据，其平台在 IPv6 数据的广度与深度方面具有明显优势。

4.3.5 奇安信天眼

一、基本背景概述

奇安信作为国内领先的网络安全公司，长期致力于为政府、企业等各类组织提供全方位的网络安全解决方案。奇安信天眼是奇安信倾力打造的一款针对网络空间资产进行全面监测、分析和管理的平台。在当前复杂多变的网络安全形势下，企业和组织面临着日益增多的网络攻击威胁，网络空间中的资产暴露面不断扩大，亟需一个强大的工具来帮助发现潜在的安全风险，加强对自身网络资产的掌控能力。奇安信天眼正是顺应这一需求而生，它融合了先进的大数据、人工智能和网络探测等技术，旨在为用户提供准确、及时的网络空间资产信息和安全态势感知。

二、平台框架结构

奇安信天眼的平台框架结构主要由数据采集层、数据处理层、数据分析层和应用展示层构成，以下是各层的详细介绍：

1）数据采集层

此层负责从各种渠道收集网络空间中的资产数据。其数据源广泛，包括但不限于网络扫描，通过主动扫描网络中的 IP 地址段、端口以及服务，获取资产的开放端口、运行的服务版本等信息；还会收集域名解析数据，了解域名与 IP 的对应关系；同时也会整合第三方数据源的信息，例如一些公开的安全漏洞库信息等。这些收集到的数据将作为后续处理和分析的基础。

2）数据处理层

该层主要对采集到的原始数据进行清洗、归一化和存储等操作。由于采集到的数据可能存在格式不一致、重复、错误等问题，数据处理层会对这些数据进行清理，去除噪声和无用信息。归一化处理则是将不同来源的数据转换为统一的格式，便于后续的分析和整合。经过处理后的数据将被存储在奇安信专门的数据仓库中，以便后续的查询和使用。

3）数据分析层

数据分析层是奇安信天眼的核心部分，它运用多种分析技术和模型对处理后的数据进行深度挖掘和分析。其中包括风险评估模型，根据资产的漏洞情况、暴露程度等因素评估其面临的安全风险；关联分析技术，通过分析资产之间的关联关系，发现潜在的安全威胁链。同时，还会结合机器学习算法对数据进行实时分析和预测，提前发现潜在的安全隐患。

4）应用展示层

应用展示层将分析结果以直观易懂的方式呈现给用户。它提供了丰富的可视化界面，例如资产地图，用户可以直观地看到全球范围内自己的网络资产分布情况；安全态势仪表盘，展示整体的安全风险等级和各类安全事件的统计信息。此外，还提供了报表生成功能，用户可以根据自己的需求生成详细的安全报告，为决策提供有力的支持。

图 4.16 是一个简化的奇安信天眼平台框架结构示意图：

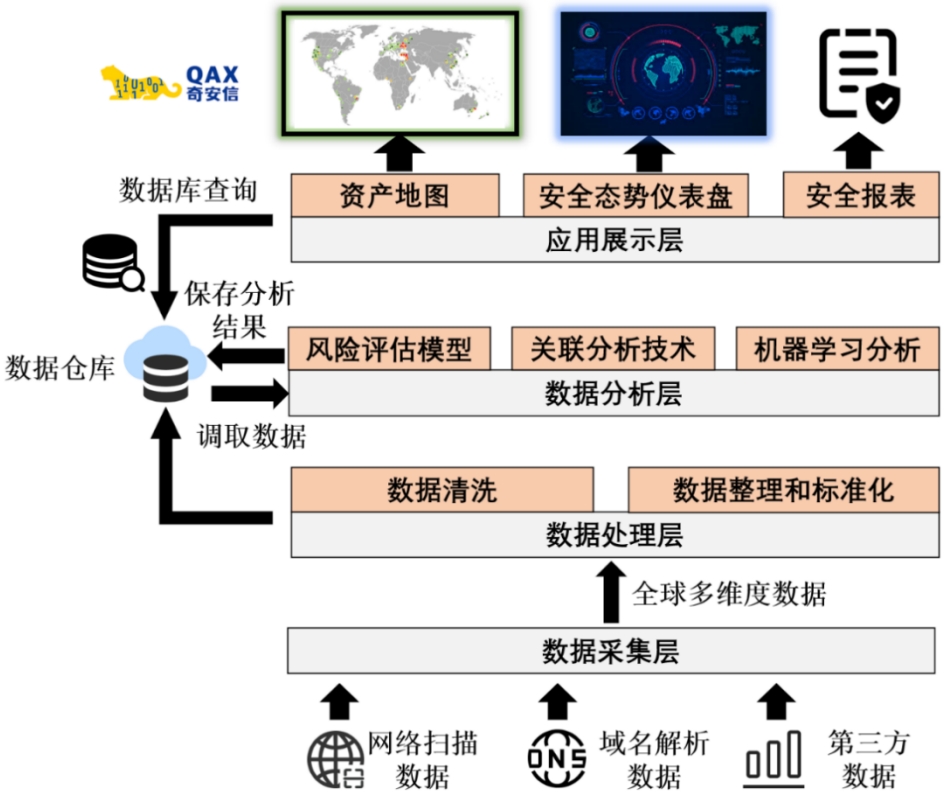


图 4.16 奇安信天眼平台框架结构示意图

三、主要功能介绍

1）网络资产发现与管理

奇安信天眼能够全面扫描和识别用户网络中的各种资产，包括服务器、主机、网络设备、物联网设备等。它可以发现隐藏在网络中的未授权设备，帮助用户掌握网络资产的真实情况。同时，平台会建立详细的资产档案，记录资产的基本信息、配置信息、安全状态等，方便用户进行资产的统一管理和维护。例如，用户可以通过平台查看某台服务器的操作系统版本、安装的软件应用以及开放的端口等信息，及时进行软件升级和端口管理，降低安全风险。

2）安全漏洞监测与预警

天眼平台会实时监测网络资产中的安全漏洞情况，通过与权威的漏洞库进行对比分析，及时发现资产存在的已知漏洞。一旦发现漏洞，平台会立即发出预警信息，告知用户漏洞的严重程度、影响范围以及修复建议。同时，平台还会提供漏洞修复的进度跟踪功能，帮助用户确保漏洞得到及时有效的修复。例如，当发现某企业的 Web 服务器存在一个高危的 SQL 注入漏洞时，平台会第一时间通知企业安全团队，并提供相应的补丁下载链接和修复指导。

3）网络攻击检测与溯源

奇安信天眼具备强大的网络攻击检测能力，通过对网络流量的实时监控和分析，能够识别各类攻击行为，如 DDoS 攻击、恶意扫描、漏洞利用等。当检测到攻击发生时，平台不仅会及时发出告警，还会对攻击的来源、攻击路径、攻击手段等进行详细分析和溯源。这有助于用户快速定位攻击者，采取相应的应对措施，并且可以为后续的安全调查和法律追责提供有力证据。例如，在检测到一次 DDoS 攻击后，平台可以分析出攻击流量的来源 IP 地址、攻击的峰值流量等信息，帮助企业安全团队采取限流、封堵等措施进行应对。

4）安全态势感知与评估

平台通过收集和分析大量的网络安全数据，能够全面、实时地展示用户的网络安全态势。它会以直观的图表和报表形式展示安全威胁的分布情况、趋势分析以及不同业务系统的安全风险等级。同时，还会根据用户设定的安全策略和行业标准，对网络安全状况进行全面评估，为用户提供专业的安全改进建议。例如，企业可以通过平台了解到自己在不同时间段受到的攻击类型和数量的变化趋势，以及与同行业相比的安全风险水平，从而有针对性地加强安全防护措施。

5）合规性检查与管理

随着网络安全法规和标准的不断完善，企业需要确保自身的网络安全措施符合相关的合规要求。奇安信天眼可以根据国家和行业的相关法规、标准，对企业的网络资产和安全策略进行全面检查，发现不符合合规要求的地方，并提供详细的整改建议。这有助于企业避免因合规问题而面临的法律风险和声誉损失。例如，平台可以依据《网络安全法》《等级保护制度》等法规标准，检查企业的网络安全管理制度、数据保护措施等是否达标。

6）产品特色

全流量分析与 APT 防御：基于流量探针的资产识别与异常行为检测，强化 APT 攻击追踪能力。

攻防演练集成：结合红蓝对抗场景，提供资产暴露面仿真与实战化防御演练支持。

4.3.6 绿盟科技网络空间地形图

一、基本背景概述

绿盟科技作为国内领先的网络安全解决方案提供商，拥有深厚的安全技术积累和丰富的行业经验。绿盟科技网络空间地形图是其在网络空间资产测绘领域的重要产品，旨在帮助企业、政府机构等用户全面、精准地掌握自身网络空间资产的分布和安全状况。随着网络攻击的日益复杂和频繁，企业对自身网络资产的清晰认知成为保障网络安全的基础，该平台应运而生以满足市场需求。

二、平台框架结构

绿盟科技网络空间地形图的框架结构可以分为数据采集层、数据处理层、数据分析层和应用展示层，具体如下：

1）数据采集层

利用多种主动探测和被动监听技术，从互联网中收集各类网络资产信息，包括 IP 地址、域名、端口、服务等。例如，它可以通过扫描技术对目标网络进行全端口扫描，发现开放的服务；同时，也会收集网络流量中的资产相关信息。

2）数据处理层

对采集到的原始数据进行清洗、去重和标准化处理。例如，去除无效的、重复的 IP 地址记录，统一端口映射规则等，以提高数据质量。同时，将处理后的数据存储到数据库中，便于后续的查询和分析。

3）数据分析层

运用机器学习、关联分析等技术对数据进行深入挖掘。例如，通过机器学习算法识别异常的网络服务和资产关联关系，帮助用户发现潜在的安全隐患。该层还可以对资产的安全态势进行评估和预测。

4）应用展示层

以可视化的界面将分析结果呈现给用户，包括网络空间资产地图、资产清单、安全漏洞报告等。用户可以根据自己的需求进行查询、筛选和分析，以直观地了解网络资产的状况。

图 4.17 是一个简化的框架结构示意图：

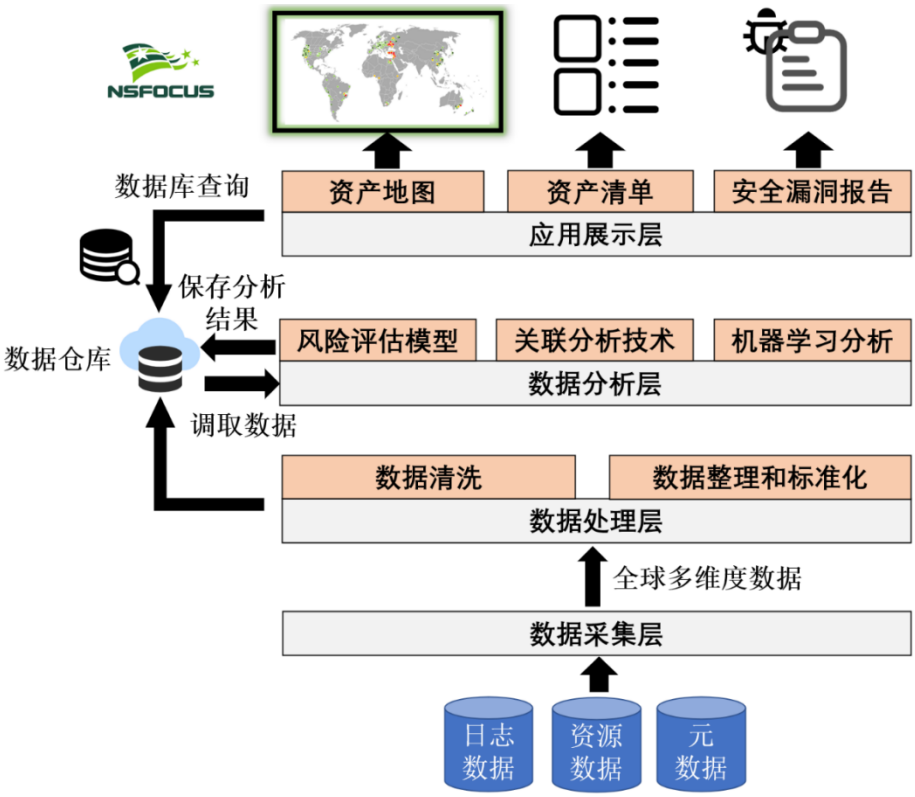


图 4.17 绿盟框架结构示意图

三、主要功能介绍

1）资产全面发现

可以发现不同类型的网络资产，包括办公网络设备、工业控制系统设备、物联网设备等。例如，它能够发现隐藏在企业内部网络中的老旧打印机、摄像头等设备，避免因这些设备的安全漏洞而带来的潜在风险。

2）资产关联分析

通过分析资产之间的关联关系，如 IP 地址与域名的映射关系、设备与服务的依赖关系等，帮助用户了解网络的拓扑结构和资产的逻辑关系。例如，当某一关键服务器出现故障时，能够迅速定位受影响的其他相关设备和服务。

3）安全漏洞检测

结合绿盟科技的漏洞库，对发现的资产进行漏洞扫描和评估。例如，检测设备是否存在已知的高危漏洞，如远程命令执行漏洞、SQL 注入漏洞等，并及时生成漏洞报告，为用户提供修复建议。

4）态势感知与预警

实时监测网络资产的安全态势，当发现异常的攻击行为或安全事件时，能够及时发出预警。例如，当检测到大量的异常登录尝试时，系统会自动触发预警信息，提醒用户及时采取防范措施。

5）产品特色

态势感知与大数据融合：集成网络流量、漏洞库及威胁情报，构建三维空间资产态势地图，支持宏观决策。

工控场景专项优化：针对工控网络低性能设备设计轻量探测策略，减少扫描对业务的影响。

4.3.7 数智安安全测绘平台

一、基本背景概述

数智安是专注于网络空间安全测绘领域的新兴企业，数智安安全测绘平台是其核心产品。在数字化转型的大背景下，各行各业对网络安全的重视程度不断提高，而准确掌握网络资产信息是网络安全防护的关键。该平台聚焦于网络空间资产的深度测绘和安全分析，为用户提供全面、精准的资产安全解决方案。

二、平台框架结构

数智安安全测绘平台的框架结构主要包括前端采集模块、数据存储与管理模块、核心分析引擎模块和可视化展示模块，具体如下：

1）前端采集模块

采用分布式采集节点，对不同区域、不同网络环境下的资产进行数据采集。采集方式包括主动探测和被动嗅探，能够快速、准确地收集网络资产的各类信息，如设备型号、操作系统版本、运行服务等。

2）数据存储与管理模块

建立大规模的数据仓库，对采集到的海量数据进行高效存储和管理。采用数据库集群技术，确保数据的高可用性和读写性能。同时，对数据进行分类和索引，便于后续的快速查询和分析。

3）核心分析引擎模块

集成多种分析算法和模型，如机器学习模型、关联规则引擎等。对存储的数据进行深度挖掘和分析，以发现潜在的安全风险和资产之间的复杂关系。例如，通过机器学习算法识别异常的数据访问模式，判断是否存在数据泄露的风险。

4）可视化展示模块

以直观、交互性强的界面将分析结果呈现给用户。支持多种可视化方式，如地图可视化、表格可视化、图表可视化等。用户可以根据自己的需求自定义展示内容和方式，方便快捷地获取所需信息。

图 4.18 是平台框架结构的示意图：

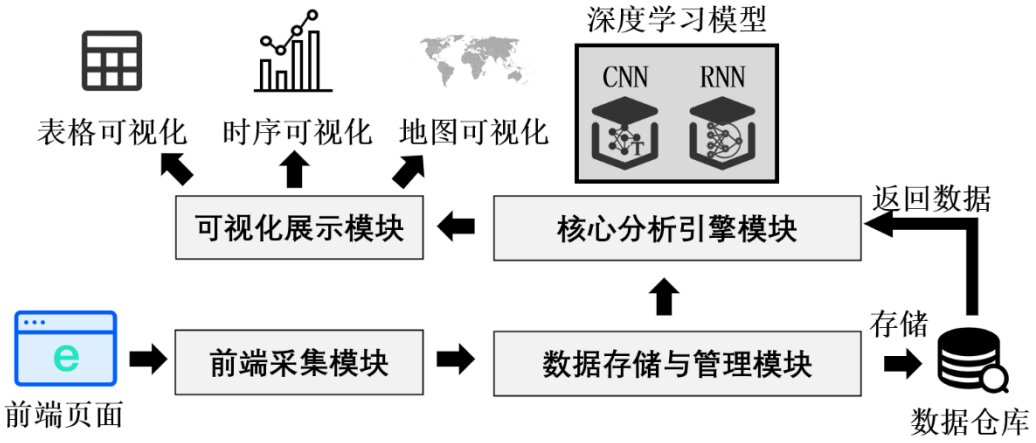


图 4.18 数智安安全测绘平台框架结构示意图

三、主要功能介绍

1）精细资产识别

能够精确识别各类网络资产的详细信息，包括设备的硬件参数、软件版本、应用程序等。例如，对于一台服务器，不仅可以识别其操作系统和运行的服务，还能准确判断服务器中安装的数据库版本和中间件类型。

2）供应链安全分析

分析资产的供应链关系，识别潜在的供应链安全风险。例如，检测企业所使用的第三方软件和服务是否存在安全漏洞或恶意代码，避免因供应链环节的安全问题而影响整个企业的网络安全。

3）漏洞精准研判

结合多源漏洞情报，对检测到的漏洞进行精准研判。不仅能够判断漏洞的严重程度，还能分析漏洞的利用难度和可能造成的影响。例如，对于一个存在漏洞的工业控制器，能够分析该漏洞被利用后可能对工业生产造成的影响范围和程度。

4）动态监测与预警

对网络资产进行实时动态监测，及时发现资产的变化情况和安全事件。当资产的配置发生改变、出现异常流量或遭受攻击时，系统能够迅速发出预警，并提供相应的应急处置建议。

5）产品特色

AI 驱动的资产聚类：利用机器学习自动归类资产属性，识别影子 IT 与未知设备。

云原生架构适配：支持多云环境资产同步探测，结合容器与微服务技术实现动态资产管理。

第五章 技术挑战与未来趋势

5.1 当前技术挑战

5.1.1 数据规模与实时性矛盾

在网络空间测绘领域，数据规模与实时性矛盾是一个关键挑战，主要体现在全网扫描的效率瓶颈、IPv6 网络空间探测和全端口探测等方面。下面将详细分析这些方面的技术难点以及可能的解决方法。

一、全网扫描的效率瓶颈

1）技术难点

巨大的数据量：当前全球互联网规模极其庞大，包含数以亿计的设备和 IP 地址。对全网进行扫描意味着需要处理海量的数据，从数据的收集、传输到存储和分析，每一个环节都面临巨大压力。例如，进行全网 IP 扫描时，即使每次扫描仅针对特定的几个端口，扫描所产生的数据量也会呈指数级增长，处理这些数据需要极高的计算资源和存储容量。

扫描时间过长：为了完整地对全网进行扫描，需要遍历大量的网络节点。由于网络带宽、设备响应速度等因素的限制，完成一次全网扫描可能需要数天甚至数周的时间。在扫描过程中，网络环境是动态变化的，扫描所得到的数据可能在完成扫描时已经过时，无法反映当前网络的真实情况。

目标的动态性：网络中的设备和服务具有动态特性，新的设备不断加入网络，旧的设备可能随时下线，服务的端口和配置也可能频繁变化。这使得全网扫描难以跟上网络变化的节奏，增加了保证扫描结果实时性的难度。

扫描策略的复杂性：制定高效的扫描策略需要考虑多个因素，如扫描的频率、扫描的范围、扫描的深度等。不合理的扫描策略可能导致某些重要的网络节点被遗漏，或者对某些节点进行不必要的重复扫描，从而降低扫描效率。

2）可能的解决之道

分布式扫描架构：采用分布式系统进行全网扫描，将扫描任务分配到多个扫描节点上并行执行。每个扫描节点负责扫描一部分网络范围，然后将扫描结果汇总到中央服务器进行处理。这种架构可以显著提高扫描效率，减少扫描时间。例

如，一些研究机构采用基于云计算平台的分布式扫描系统，利用多个云服务器同时进行扫描，大大缩短了全网扫描的周期。

增量扫描技术：在完成一次全网扫描后，后续的扫描只关注网络中发生变化的部分。通过记录上一次扫描的结果，对比当前网络状态，只对新增、删除或修改的设备和服务进行扫描。这种方法可以避免对未变化的部分进行重复扫描，提高扫描效率，同时保证扫描结果的实时性。

智能扫描策略：利用机器学习和数据分析技术，根据网络的历史数据和实时状态，动态调整扫描策略。例如，根据网络节点的活跃度和重要性，合理安排扫描的频率和深度；对于频繁变化的节点，增加扫描次数；对于相对稳定的节点，可以适当降低扫描频率。

二、IPv6 网络空间探测

1）技术难点

地址空间巨大：IPv6 的地址空间达到 2^{128}，比 IPv4 的地址空间大得多。这使得对 IPv6 网络空间进行全面探测变得极其困难，传统的扫描方法在面对如此庞大的地址空间时效率极低，甚至无法在合理的时间内完成扫描。尽管当前方法在一定程度上缓解了活跃 IPv6 地址探测的困难，但受限于主动探测手段，国内尚缺乏覆盖全球的系统性地址发现方案，所获取的活跃地址边界仍较受限。

网络拓扑复杂：IPv6 网络的拓扑结构更加复杂，采用了更多的子网划分和地址分配方式。此外，IPv6 支持移动性、自动配置等特性，使得网络节点的位置和状态更加动态多变。这增加了探测 IPv6 网络拓扑结构和设备分布的难度。

路由多样性：IPv6 网络中的路由协议和策略更加多样化，不同的网络服务提供商可能采用不同的路由配置。这使得数据在传输过程中的路径更加复杂，增加了探测数据的收集和分析难度。

安全机制增强：IPv6 引入了更加严格的安全机制，如 IPsec 协议，用于保护网络通信的安全性。这些安全机制可能会对探测数据的获取造成阻碍，例如防火墙可能会阻止探测数据包的传输，导致无法准确获取网络信息；ICMPv6 协议引入了限速机制，使得扫描发包速率受到很大限制。

2）可能的解决之道

分层探测策略：为实现全球活跃 IPv6 地址的高效发现，可采用主动探测、被动监测与公开数据获取等多种方式。例如，在无种子区域设计更高效的主动地

址探测算法，扩大探测边界；基于公开服务全球部署探测节点，监测公开服务流量提取活跃 IPv6 地址；基于 DNS 等公开数据反向解析活跃 IPv6 地址等。

基于代理的探测：利用网络中的代理节点进行探测。代理节点可以部署在不同的网络区域，负责收集周围的网络信息，并将数据传回中央服务器进行处理。这种方法可以减少直接探测的范围，提高探测效率，同时避免一些安全机制的限制。

数据分析和机器学习：利用大数据分析和机器学习技术，对探测到的 IPv6 网络数据进行挖掘和分析。通过学习 IPv6 网络的规律和特征，预测可能存在的网络节点和服务，提高探测的准确性和效率。例如，可以使用聚类算法对 IPv6 地址进行分类，找出潜在的活跃网络区域。

三、全端口探测

1）技术难点

端口数量众多：每个网络设备通常有 65535 个端口，对全端口进行探测意味着需要发送大量的探测数据包，增加了网络负担和扫描时间。同时，大量的端口扫描可能会被网络防火墙或入侵检测系统视为恶意攻击行为，从而被阻止。

目标设备响应差异：不同的目标设备对端口扫描的响应方式不同，有些设备可能会对所有端口扫描都进行响应，而有些设备可能只对部分端口扫描进行响应。此外，目标设备的处理能力和响应时间也存在差异，这使得准确判断端口的开放状态变得困难。

网络延迟和丢包：在进行全端口探测时，由于网络延迟和丢包的存在，可能会导致探测数据包无法及时到达目标设备，或者目标设备的响应数据包无法正确返回。这会影响对端口状态的判断，增加误报和漏报的概率。

2）可能的解决之道

优化扫描算法：采用优化的扫描算法，减少不必要的端口扫描。例如，可以先对常用的端口进行扫描，根据扫描结果判断目标设备的类型和服务情况，然后有针对性地对可能开放的非常用端口进行扫描。

随机扫描顺序：采用随机的扫描顺序，避免被网络防火墙或入侵检测系统识别为恶意扫描。通过打乱扫描顺序，可以降低被检测到的概率，提高扫描的成功率。

多次扫描和验证：为了减少因网络延迟和丢包导致的误判，对同一端口进行多次扫描，并对比扫描结果。如果多次扫描结果一致，则可以较为准确地判断端

口的开放状态。同时，可以结合其他网络信息，如目标设备的操作系统类型、服务指纹等，对端口状态进行验证。

5.1.2 隐蔽资产探测、虚假信息干扰、隐私合规风险

一、隐蔽资产探测挑战

1）技术难点

资产隐藏技术多样化：现代网络攻击者和企业网络管理员会采用各种技术隐藏资产。例如，利用网络地址转换（NAT）技术将内部资产的真实 IP 地址隐藏在公共 IP 之后，使得外部难以直接探测到内部网络的真实拓扑和资产信息。此外，还有采用虚拟专用网络（VPN）、代理服务等方式，将资产的访问信道进行加密和隐蔽，大幅增加了探测的难度。

动态变化的资产特性：在云计算和容器化环境中，资产的创建、销毁和迁移非常频繁。例如，采用微服务架构的应用可能会根据业务负载动态创建和销毁容器实例，这些临时的、动态的资产很难被传统的静态扫描工具及时发现。而且，一些企业为了提高抗攻击能力，会定期变更资产的配置和网络位置，进一步加大了探测的复杂性。

深网资源探测难题：深网（Deep Web）是指搜索引擎无法索引到的网络内容，其中包含大量受访问限制的企业数据库、内部文档系统等隐蔽资产。这些资源通常需要身份验证才能访问，普通的扫描工具难以突破访问权限进行探测。

2）解决之道

多源数据融合分析：综合利用网络流量数据、DNS 数据、安全设备日志等多源数据进行关联分析。例如，通过分析网络流量中的异常连接模式，找出可能隐藏的内部资产。同时，结合 DNS 解析记录，发现那些未公开备案但在网络中实际使用的域名和资产。

机器学习和 AI 技术应用：利用机器学习算法对网络协议和行为进行建模，识别异常的流量特征和资产行为模式。例如，基于深度学习的异常检测算法可以学习正常网络流量的模式，从而发现那些隐藏在正常流量下的隐蔽资产。此外，还可以利用强化学习技术指导扫描策略，根据扫描结果动态调整扫描方向和重点。

渗透测试与主动探测结合：采用自动化渗透测试工具对目标网络进行模拟攻击，尝试发现隐藏的资产和漏洞。同时，结合主动探测技术，如端口扫描、服务探测等，对整个网络进行全面的摸排。例如，通过缓慢、隐蔽的端口扫描方式，减少被目标网络发现的概率，提高探测的成功率。

二、虚假信息（抗测绘）干扰挑战

1）技术难点

伪造信息的逼真性：攻击者可以使用工具和技术伪造非常逼真的网络信息，如虚假的 IP 地址、端口状态、服务信息等。例如，利用蜜罐技术设置虚假的服务器，模拟正常的业务服务，使得探测工具误判其为真实的资产，从而干扰探测结果。而且，随着技术的发展，伪造信息的手段越来越高明，很难通过简单的规则匹配进行识别。

海量信息的甄别难度：在大规模的网络空间中，每天都会产生海量的网络信息。探测工具需要处理和分析如此庞大的数据量，从中甄别出虚假信息是一项极具挑战性的任务。传统的信息筛选方法往往效率低下，无法及时准确地排除虚假信息。

信息动态变化导致的误判：网络环境中的信息是动态变化的，一些正常的网络配置变更或业务调整可能会被误判为虚假信息。例如，服务器的暂时故障或维护可能导致端口状态发生变化，使得探测工具误解为虚假信息干扰。

2）解决之道

基于行为特征的信息验证：除了对信息内容进行分析外，还可以结合网络行为特征进行验证。例如，分析服务器的响应时间、流量模式、服务调用关系等行为信息。如果某个服务器的响应时间异常、流量模式不符合常规业务需求，那么很可能是虚假信息。通过建立行为特征模型，对探测到的信息进行多维度验证，提高识别虚假信息的准确性。

关联分析和交叉验证：将不同渠道获取的信息进行关联分析和交叉验证。例如，同时利用扫描工具、网络监控系统和安全情报平台的数据，对比同一资产在不同数据源中的信息。如果某个信息在多个数据源中不一致，那么就需要进一步核实其真实性，从而有效排除虚假信息的干扰。

基于机器学习的异常检测：运用机器学习算法建立异常检测模型，对网络信息的正常模式进行学习和建模。当检测到不符合正常模式的信息时，将其标记为可能的虚假信息。例如，使用无监督学习算法对网络信息进行聚类分析，发现那些远离正常聚类的异常信息。

三、隐私合规风险挑战

1）技术难点

复杂的法规要求：不同国家和地区的隐私法规存在差异，如欧盟的《通用数据保护条例》（GDPR）、美国加利福尼亚州的《加州消费者隐私法案》（CCPA）等。这些法规对数据收集、存储、使用和共享等方面都有严格的规定，企业在进行网络资产测绘时需要确保符合所有相关法规的要求，这增加了合规难度。

数据收集与隐私保护的平衡：网络资产测绘过程中，不可避免地需要收集一些与个人隐私相关的数据，如 IP 地址、设备标识等。如何在获取必要信息的同时，保护用户的隐私不被泄露，是一个关键的技术挑战。例如，在进行大规模扫描时，如何确保不收集过多的敏感信息，避免造成隐私侵权。

数据安全存储和处理：收集到的测绘数据需要进行安全存储和处理，以防止数据泄露和滥用。然而，随着数据量的不断增加，数据存储和管理的难度也在加大。一旦数据存储系统遭受攻击，可能会导致大量用户隐私信息泄露。

2）解决之道

合规管理体系建设：企业应建立完善的隐私合规管理体系，制定详细的合规政策和流程。例如，设立专门的合规岗位，负责跟踪和研究最新的隐私法规，确保企业的测绘活动符合法规要求。同时，对员工进行隐私合规培训，提高员工的合规意识。

隐私增强技术应用：采用隐私增强技术，如差分隐私、同态加密等，在不泄露敏感信息的前提下进行数据处理和分析。差分隐私技术可以在数据中添加一定的噪声，使得攻击者无法从数据分析结果中推断出具体的个人信息。同态加密则允许在加密数据上进行计算，而无需先解密，从而在数据处理过程中保护隐私。

数据最小化原则：在进行网络资产测绘时，严格遵循数据最小化原则，只收集必要的信息，并对收集到的数据进行严格的访问控制和审计。例如，对数据访问进行分级管理，只有经过授权的人员才能访问和处理隐私数据。同时，定期对数据进行清理，删除不再需要的信息，降低数据泄露的风险。

5.1.3 云服务动态资源探测

一、技术难点

1）资源动态性与不透明性

云上部署的第三方服务通常具有高度动态性。其资源会根据负载自动伸缩，服务实例可能随时启动、停止或迁移，这使得传统的静态探测方法难以跟踪。例

如，在云平台上，弹性计算服务会根据业务流量自动调整虚拟机的数量，探测系统很难实时准确地捕捉到这些变化。

云服务商为了保障用户隐私和安全，往往对底层基础设施进行了封装，提供的是抽象化的服务接口。这导致探测系统无法直接获取服务的底层物理信息，增加了探测的难度。例如，云存储服务的实际存储位置和具体存储架构通常对外部探测系统不透明。

2）多租户环境干扰

云平台采用多租户架构，多个用户的服务可能共享同一物理资源。这会造成探测结果的干扰，因为不同租户的网络流量、服务行为等可能相互交织。例如，在共享网络中，一个租户的高流量业务可能会掩盖另一个租户服务的真实网络特征，使得探测系统难以准确识别和区分各个服务。

多租户环境下，为了保障租户之间的隔离性，云平台会采取各种安全机制，如虚拟专用网络（VPN）、网络访问控制列表（ACL）等。这些机制会限制探测系统对服务的访问权限，导致部分信息无法获取。

3）第三方服务多样性与协议兼容性

云上第三方服务种类繁多，涵盖了各种不同的业务领域，如数据库服务、消息队列服务、机器学习服务等。每种服务都有其独特的运行模式和通信协议，探测系统需要具备广泛的协议解析能力才能对其进行有效探测。然而，新的服务和协议不断涌现，使得探测系统的协议库更新和维护面临巨大挑战。

不同云服务商提供的第三方服务在接口定义、数据格式等方面存在差异，这增加了探测系统的适配难度。例如，不同云平台的数据库服务在连接方式、命令语法等方面可能各不相同，探测系统需要针对每个云平台进行定制化开发才能实现精准探测。

4）安全与合规限制

为了保护用户数据安全和隐私，云平台和第三方服务通常会采取严格的安全措施，如加密通信、身份认证、访问控制等。这些安全措施会对探测系统的正常运行造成阻碍，因为探测系统可能无法绕过这些安全机制来获取所需信息。例如，部分服务采用端到端加密技术，探测系统无法解析加密后的通信内容。

不同国家和地区的法律法规对数据收集、存储和使用有不同的要求，探测云上第三方服务可能会涉及到合规问题。例如，某些地区要求在收集用户数据前必

须获得用户明确同意，并且对数据的跨境传输有严格限制。探测系统在设计和实施过程中需要充分考虑这些合规要求，否则可能会面临法律风险。

二、可能的解决之道

1）基于 API 的探测方法

云服务商通常会提供丰富的 API 接口，用于管理和监控云上资源。探测系统可以通过调用这些 API 来获取服务的实时信息，从而实现对动态资源的跟踪。例如，通过云平台的计算服务 API 可以获取虚拟机的创建、删除和迁移信息，通过存储服务 API 可以获取存储资源的使用情况。

与第三方服务提供商合作，获取其开放的 API 接口。一些第三方服务提供商会为合作伙伴提供特定的 API，用于获取服务的运行状态、性能指标等信息。探测系统可以利用这些 API 来提高探测的准确性和实时性。

2）多维度数据融合与机器学习算法

整合多种来源的数据，包括网络流量数据、系统日志数据、API 调用数据等，通过多维度数据分析来提高对服务的识别和监测能力。例如，结合网络流量的特征信息和系统日志中的事件记录，可以更准确地判断服务的状态和行为。

利用机器学习算法对海量数据进行分析和建模，识别服务的动态模式和特征。例如，使用聚类算法对网络流量进行聚类，将具有相似特征的流量归为同一类，从而分析不同服务的流量特点；使用异常检测算法实时监测服务的运行状态，及时发现服务的异常变化。

3）协议解析与适配技术

建立一个通用的协议解析框架，对常见的服务协议进行集中管理和解析。该框架可以不断更新和扩展协议库，以适应新出现的服务和协议。例如，使用开源的协议解析工具（如 Scapy 等），实现对多种网络协议的解析。

采用插件式架构设计探测系统，使其能够方便地适配不同云服务商的第三方服务。通过为每种云平台和服务开发相应的插件，实现对不同服务接口和数据格式的支持。这样，当出现新的云平台或服务时，只需开发对应的插件即可将其纳入探测范围。

4）安全合规策略设计

在探测系统的设计过程中，充分考虑安全和合规要求。采用安全的通信协议和加密技术，确保探测过程中数据的安全性和隐私性。例如，使用 SSL/TLS 协议对通信数据进行加密传输，防止数据被窃取或篡改。

与云服务商和第三方服务提供商密切合作，了解其安全策略和合规要求。在合法合规的前提下，通过协商或申请授权的方式获取必要的探测权限。同时，建立完善的数据管理和审计机制，确保探测过程符合相关法律法规和行业标准。

通过以上方法，可以在一定程度上克服对云上部署的第三方服务等动态资源探测的技术难点，提高探测的准确性和可靠性。然而，随着云计算和第三方服务的不断发展，新的挑战可能会不断涌现，需要持续关注和研究相关技术的发展动态。

5.2 未来发展趋势

5.2.1 技术融合

网络空间测绘面临着诸多挑战，如数据规模与实时性的矛盾，在全网扫描时存在效率瓶颈，IPv6 网络空间范围庞大、结构复杂，全端口探测的数据量极为巨大；还有隐蔽资产探测难度高，易受虚假信息干扰，以及需要面对隐私合规风险等问题。同时，动态资源尤其是云上部署的第三方服务的探测也存在许多不确定性。不过，随着相关领域技术的不断进步，新型测绘技术正呈现出一些显著的发展趋势，其中 AI 驱动的自动化测绘和区块链技术保障数据可信度是重要方向。

一、AI 驱动的自动化测绘

1）解决数据规模与处理效率难题

网络空间中数据规模呈指数级增长，传统的测绘方法在面对庞大的数据源时效率低下，难以满足实时性要求。而 AI 强大的数据处理和分析能力为解决这一难题提供了有效途径。首先，利用机器学习算法，特别是深度学习算法中的卷积神经网络（CNN）、循环神经网络（RNN）及其变种长短时记忆网络（LSTM）等，可以对大规模的网络空间数据进行高效处理。CNN 擅长处理具有网格结构的数据，例如网络拓扑图，能自动提取其中的特征信息；LSTM 则适用于处理序列数据，如网络中的流量信息，可学习流量的变化规律，从而预测网络状态。

同时，AI 算法还可以对全网扫描进行智能优化。传统的全网扫描是一种地毯式的搜索方式，耗费大量的时间和资源。通过深度学习和 LLM（大语言模型）等 AI 技术，可以根据历史数据和当前已知的网络信息，分析出高风险区域和潜在有价值的目标，有针对性地进行扫描，避免不必要的扫描操作，极大地提高扫描效率。例如，使用强化学习算法，让扫描策略不断地与环境进行交互，根据扫

描结果获得奖励或惩罚信号，从而优化扫描路径和顺序，使扫描效率达到最优；利用 LLM 技术自动生成服务扫描代码，提升对新型服务的探测能力。

2）提升隐蔽资产发现能力

隐蔽资产往往采用各种手段隐藏自身的存在，使得传统的探测方法难以发现。AI 技术能够通过对网络行为模式、异常流量等多维度数据的深度分析，发现潜在的隐蔽资产。例如，利用无监督学习算法，如 DBSCAN（基于密度的空间聚类算法）和自编码器（Autoencoder），对网络流量进行聚类分析和异常检测。DBSCAN 可以将具有相似特征的流量点聚集在一起，通过分析这些聚类结果，识别出与正常业务流量模式不同的异常流量，这些异常流量很可能与隐蔽资产相关。自编码器则可以学习正常流量的特征表示，当输入异常流量时，其重构误差会增大，从而检测出异常情况。

此外，自然语言处理（NLP）技术也可以在隐蔽资产发现中发挥作用。网络中的各种服务和设备会产生大量的文本信息，如日志文件、配置文件等。通过 NLP 技术对这些文本信息进行分析，提取其中的关键信息，挖掘潜在的隐蔽资产线索。例如，利用命名实体识别（NER）技术或 LLM 识别出文本中的设备名称、IP 地址、服务类型等信息，然后通过关联分析，找出隐藏在正常业务流程中的隐蔽资产。

3）增强测绘的适应性和智能决策能力

网络空间是动态变化的，新的网络技术、设备和应用不断涌现，传统的测绘方法难以快速适应这种变化。AI 驱动的自动化测绘具有良好的自适应能力，能够根据网络环境的变化自动调整测绘策略。例如，使用迁移学习技术，当面临新的网络架构或应用场景时，可以利用在已有数据集上训练好的模型，通过少量的新数据进行微调，快速适应新环境，减少重新训练模型的时间和成本。

同时，在面对复杂的测绘任务时，AI 能够实现智能决策。例如，当探测到网络中的异常活动时，AI 系统可以综合多方面的信息，如异常活动的类型、发生频率、可能造成的影响等，自动判断是否需要进一步深入探测或采取相应的安全措施。这种智能决策能力可以大大提高网络空间测绘的效率和准确性，及时发现潜在的安全威胁。

二、区块链技术保障数据可信度

1）防止数据篡改和虚假信息干扰

在网络空间测绘中，数据的真实性和可信度至关重要。然而，测绘过程中可能会受到虚假信息的干扰，例如恶意攻击者可能会伪造设备信息、网络拓扑结构

等，影响测绘结果的准确性。区块链技术具有去中心化、不可篡改和可追溯的特点，可以有效地防止数据被篡改和虚假信息的干扰。

区块链通过分布式账本的方式，将测绘数据记录在多个节点上。每个数据块都包含前一个数据块的哈希值，形成一个链条，任何对数据的篡改都会导致哈希值的变化，从而被其他节点察觉。这样，所有参与测绘的节点都可以共同维护数据的真实性和一致性，确保测绘数据不被恶意修改。例如，在进行网络资产探测时，每个节点将自己探测到的资产信息记录在区块链上，其他节点可以对这些信息进行验证和监督，一旦发现数据异常，就可以追溯到数据的源头，查明问题所在。通过区块链技术，可以联合多个测绘机构/测绘点共同完成对网络空间的可信测绘，提升测绘的覆盖率。

2）保护隐私和合规性

隐私合规是网络空间测绘中需要重点关注的问题。区块链的密码学技术可以为数据隐私保护提供有效的解决方案。在区块链网络中，数据可以采用加密算法进行加密处理，只有授权的节点才能访问和查看相应的数据。例如，对于涉及用户个人信息和敏感业务数据的测绘内容，可以使用对称加密或非对称加密算法进行加密，确保数据在传输和存储过程中的安全性。

同时，区块链的智能合约功能可以实现自动化的合规管理。智能合约是一种自动执行的合约代码，它可以根据预设的规则和条件，对测绘过程中的数据访问、共享和使用进行自动化管理。例如，在数据共享场景下，智能合约可以规定数据的使用范围、使用期限和使用权限等，只有满足这些条件的节点才能获取相应的数据，从而保证测绘活动符合相关的法律法规和行业规范。

3）建立可信的数据共享机制

网络空间测绘往往需要多个参与方之间的数据共享和协作，例如不同的安全机构、企业等需要共享测绘数据以实现更全面的安全防护。然而，数据共享过程中存在信任问题，各参与方担心数据泄露和被滥用。区块链可以建立一个可信的数据共享平台，通过智能合约和共识机制，实现数据的安全共享。

在区块链数据共享平台上，每个参与方作为一个节点，通过数字签名和身份验证机制进行身份确认。智能合约可以规定数据共享的条件和方式，例如数据提供者可以设置数据的使用费用、共享范围等，当其他节点满足这些条件时，才能获取相应的数据。同时，共识机制确保了数据的一致性和可靠性，只有通过大多数节点验证的数据才能被记录到区块链上。这样，各参与方可以在信任的基础上进行数据共享和协作，共同推动网络空间测绘技术的发展。

5.2.2 应用深化

一、结合 APT 防御的战术级地图

在当今复杂的网络安全环境下，高级可持续威胁（APT）攻击因其隐蔽性、长期性和针对性，对政府机构、大型企业以及关键基础设施部门构成了严重威胁。网络空间测绘与 APT 防御相结合，生成战术级地图，是有效应对 APT 攻击的关键手段。下面详细阐述其相关内容及应用场景。

首先，战术级地图可全面识别潜在攻击面。网络空间测绘技术能够扫描和发现组织内部及外部的所有联网资产，涵盖服务器、网络设备、物联网终端等。通过构建这些资产的详尽清单，战术级地图能够精准定位可能被 APT 攻击者利用的薄弱环节，如开放的端口、存在漏洞的服务等。例如，某金融机构利用网络空间测绘生成的战术级地图，发现了一个未被授权接入互联网的老旧业务服务器，该服务器存在高危漏洞，可能成为 APT 攻击的突破口。及时对该服务器进行加固和隔离，避免了潜在的重大安全事件。

其次，映射攻击路径也不容小觑。结合历史 APT 攻击案例和实时情报，战术级地图能够模拟攻击者可能采取的入侵路径。它可以分析从初始的网络侦查、漏洞利用，到横向移动、数据提取等各个阶段的攻击方式，并在地图上清晰展示出来。安全团队可以根据这些模拟路径，制定针对性的防御策略，提前部署防护措施。比如，在军事网络防御中，战术级地图可以模拟敌方 APT 攻击可能经过的网络节点和通信链路，军方可以据此加强关键节点的防护，设置诱饵和监控机制，以有效抵御攻击。

最后，能够实时监测与预警。基于网络空间测绘的持续监测能力，战术级地图可以实时更新资产状态和网络活动信息。一旦检测到与 APT 攻击相关的异常行为，如异常的网络流量、未知的设备连接等，系统能够立即发出预警，安全团队可以迅速响应，采取应急措施。例如，某能源企业的网络监控系统在战术级地图的支持下，及时发现了来自境外的异常流量，经过分析确认是一起针对能源控制系统的潜在 APT 攻击，通过自动阻断和溯源，成功挫败了攻击企图。

二、数字孪生网络空间建模

数字孪生网络空间建模是将现实网络空间中的物理设施、逻辑关系、数据流动等要素进行数字化映射，构建出一个与现实网络高度相似的虚拟模型。这种建模方式为网络空间的管理和安全保障带来了全新的视角和方法。下面阐述其特点及应用场景。

在网络规划与优化方面，数字孪生网络空间模型可以准确模拟不同网络拓扑结构、设备配置和业务流量下的网络性能。通过对模型进行各种场景的仿真实验，网络工程师可以提前评估网络升级、新业务部署等方案的可行性和效果，从而进行优化调整。例如，在建设 5G 网络时，运营商可以利用数字孪生模型模拟不同基站布局、频率分配和用户分布情况下的网络覆盖和容量，合理规划基础设施建设，提高资源利用效率。

对于故障诊断与修复来说，当网络出现故障时，数字孪生模型可以实时反映故障发生时的网络状态，并通过对比正常状态下的模型数据，快速定位故障点和原因。同时，模型还可以模拟不同修复方案的效果，帮助运维人员选择最优的解决方案。比如，在企业数据中心网络中，当发生网络拥塞或设备故障时，数字孪生模型可以迅速分析出是哪个链路或设备出现问题，并推荐合适的修复措施，如调整路由策略、更换故障设备等，减少故障修复时间和对业务的影响。

在安全态势感知中，数字孪生网络空间建模可以为安全分析提供一个虚拟的实验环境。安全团队可以在模型中模拟各种攻击场景，评估网络的脆弱性和抗攻击能力，制定相应的安全策略。同时，通过实时监测模型与现实网络的状态差异，能够及时发现潜在的安全威胁。例如，在政府网络安全防护中，利用数字孪生模型模拟黑客的渗透攻击，分析网络的安全漏洞和防护薄弱环节，为加强网络安全建设提供依据。

三、更多网络空间测绘的应用场景

1）工业互联网安全保障

工业互联网融合了大量的工业设备、生产系统和网络技术，其安全状况直接关系到企业的生产运营和国家的经济安全。网络空间测绘可以全面识别工业互联网中的各类资产，包括工业控制系统、智能生产线、传感器等，并绘制详细的资产地图。通过对资产的实时监测和分析，能够及时发现潜在的安全漏洞和异常行为，如非法设备接入、数据异常传输等，保障工业生产的连续性和稳定性。例如，在汽车制造企业的工业互联网中，利用网络空间测绘技术可以监测生产线上的机器人、PLC 等设备的运行状态，及时发现设备故障和网络攻击，避免生产停滞和质量问题。

2）智慧城市建设

智慧城市涵盖了交通、能源、环保、医疗等多个领域的数字化系统，网络空间测绘可以为智慧城市的建设和管理提供有力支持。通过测绘城市中的网络基础设施、物联网终端和各种信息系统，构建城市网络空间的全景视图。这有助于城

市管理者合理规划网络资源，优化城市运行效率。例如，在城市交通管理中，利用网络空间测绘可以实时掌握交通信号灯、智能停车系统等设备的联网状态和运行情况，实现交通流量的精准调控，减少拥堵。同时，在应对自然灾害和公共安全事件时，网络空间测绘可以帮助快速评估城市网络的受损情况，为应急救援和恢复工作提供决策依据。

3）供应链安全管理

现代供应链涉及众多供应商、制造商、物流商等，其网络安全状况相互关联。网络空间测绘可以对供应链中的各个环节进行全面扫描和分析，识别潜在的安全风险。通过测绘供应商的网络资产和安全措施，评估其对整个供应链的安全性影响。例如，在电子产品供应链中，对芯片供应商的网络进行测绘，发现其存在安全漏洞可能导致芯片被植入恶意代码，及时采取措施更换供应商或督促整改，保障产品的安全性。此外，网络空间测绘还可以监测供应链中的物流信息系统，防止货物运输过程中的信息泄露和供应链中断事件。

4）金融科技风险防控

金融科技领域涉及大量的在线交易、支付系统和客户信息，网络安全至关重要。网络空间测绘可以帮助金融机构全面了解自身的网络资产和外部攻击面，识别潜在的安全威胁。通过对金融网络的实时监测，及时发现异常的网络流量和交易行为，如盗刷、洗钱等犯罪活动。例如，银行可以利用网络空间测绘技术对网银系统、移动支付平台等进行持续监测，发现异常的登录行为和资金转移，及时采取风险防控措施，保障客户资金安全。同时，测绘结果还可以为金融机构的合规性检查提供依据，确保其符合监管要求。

5.2.3 标准化建设

一、网络空间测绘当前标准化现状

目前，网络空间测绘领域的标准化程度整体偏低，尚处于发展阶段。不同的测绘技术提供商和研究机构在数据采集、处理、存储和呈现等环节都有各自的一套方法和标准。

数据格式不统一：各测绘系统生成的数据格式多样，缺乏通用的数据交换和存储格式。例如，有的系统采用 XML 格式来记录设备信息和网络拓扑结构，而有的则偏好 JSON 格式。甚至在一些情况下，为了特定的应用场景，还会使用自定义的二进制格式。这种数据格式的差异使得不同系统之间的数据共享和整合变得极为困难。

接口规范缺失：在接口方面，由于缺乏统一的标准，各个平台的接口规则各不相同。从数据读取接口到控制接口，每个系统都有自己独特的输入输出参数和调用方式。这导致当用户需要集成多个测绘系统的数据或功能时，不得不为每个系统单独开发适配代码，大大增加了开发成本和复杂度。

缺乏行业规范引导：网络空间测绘作为一个新兴领域，目前还没有形成一套完整的行业规范。在数据采集的合法性、隐私保护、数据质量评估等方面，没有明确的标准和准则。这使得测绘市场存在一定的混乱，不同的测绘产品和服务在质量和可靠性上参差不齐。

二、相关部门及用户单位的需求

随着网络空间测绘技术的广泛应用，相关部门及用户单位对测绘技术与平台的互联互通互操作提出了更为迫切的需求。

政府监管部门：政府监管部门需要整合多个测绘系统的数据，以便全面掌握国家网络空间的态势，进行有效的安全监管。例如，在国家关键信息基础设施保护方面，需要将不同行业、不同地区的测绘数据进行融合分析，及时发现潜在的安全威胁。统一的数据格式和接口规范可以大大提高数据整合的效率，为政府决策提供更准确、更及时的支持。

企业用户：企业在进行自身网络空间安全管理时，往往会同时使用多个测绘工具和平台，以获取更全面的资产信息。例如，一家大型企业可能会使用国内外不同厂商的测绘系统，对其内网和外网资产进行扫描。然而，由于各系统之间缺乏互操作性，企业需要花费大量的人力和物力来整合数据。因此，企业期望有统一的标准来实现不同测绘系统的互联互通，提高工作效率和管理水平。

科研机构：科研机构在进行网络空间相关研究时，通常需要收集来自不同数据源的测绘数据。统一的数据格式和接口规范可以方便科研人员获取和处理数据，促进学术交流和合作，推动网络空间测绘技术的发展。

三、网络空间测绘标准化发展趋势

1）数据格式标准化

制定通用数据模型：未来，行业将逐步制定出一套通用的数据模型，用于描述网络空间中的各种资产和关系。这个模型将涵盖设备信息、网络拓扑、服务信息等各个方面，并且具有良好的扩展性，能够适应不同类型的网络和应用场景。例如，借鉴地理信息系统（GIS）中的通用数据模型，将网络空间中的节点和链路进行抽象和分类，以统一的方式进行表示和存储。

推广标准数据文件格式：为了实现数据的有效交换和共享，行业将推广使用标准化的数据文件格式。这些格式将具有良好的可读性和可解析性，能够被不同的系统和工具所识别和处理。JSON-LD（JSON for Linking Data）这种具有语义表达能力的格式是潜在的选择之一，在存储网络空间测绘数据的同时，保留数据之间的语义关联，方便数据的查询和分析。

2）接口规范标准化

定义通用接口协议：制定一套通用的接口协议，规定数据读取、写入、更新等操作的标准流程和调用方式。这个协议将涵盖 HTTP、TCP、MQTT 等多种常见的网络协议，以适应不同的应用场景。例如，采用 RESTful API 的方式，定义统一的资源定位和请求方法，使得不同的测绘系统可以方便地进行数据交互和功能调用。

制定统一接口参数标准：明确接口的输入输出参数标准，包括参数的名称、类型、含义和取值范围等。这样可以避免因参数不统一而导致的兼容性问题。例如，在资产查询接口中，统一规定查询条件的参数格式和返回结果的格式，使得不同系统之间的查询结果可以直接进行对比和整合。

3）行业规范与标准体系建设

建立数据质量评估标准：制定一套数据质量评估标准，用于衡量网络空间测绘数据的准确性、完整性、一致性和时效性。通过定期对测绘数据进行质量评估，可以提高数据的可靠性和可用性。例如，规定设备信息的准确率应达到 95%以上，网络拓扑的更新周期不应超过 24 小时等。

规范数据采集与使用规则：明确数据采集的合法性和合规性要求，保护用户的隐私和权益。同时，规范数据的使用范围和方式，防止数据的滥用和泄露。例如，规定在进行网络扫描时，必须获得目标对象的授权，并且对采集到的数据进行严格的加密和访问控制。

推动国际标准合作：随着网络空间的全球化发展，网络空间测绘的标准化也需要进行国际合作。积极参与国际标准制定，与国际组织和其他国家共同制定全球适用的标准和规范，有利于提高我国在网络空间测绘领域的国际影响力，促进全球网络空间的安全和稳定。

5.2.4 面向新形态网络空间的测绘

一、新形态网络空间的特点

1）云网络

动态性：云网络中的资源具有高度的动态性。云服务提供商根据用户的需求动态分配和释放计算、存储和网络资源。例如，企业在业务高峰时段可能会临时增加虚拟机实例，在业务低谷时减少实例数量。这种动态变化导致云网络的拓扑结构和设备状态不断改变。

多租户性：多个租户共享同一云基础设施，不同租户的网络之间存在逻辑隔离。每个租户可能有不同的安全策略和网络配置，这增加了云网络的复杂性。例如，电商企业和金融机构可能会在同一云平台上运行，但它们对数据安全性和网络性能的要求差异很大。

弹性伸缩：云网络可以根据业务负载自动进行弹性伸缩。当业务流量增大时，自动增加服务器数量；当流量减小时，减少服务器数量。这种弹性伸缩使得云网络的规模和性能具有很大的可变性。

2）物联网

设备多样性：物联网涉及大量不同类型的设备，包括传感器、执行器、智能家电等。这些设备具有不同的通信协议、计算能力和数据格式。例如，智能家居中的温度传感器和智能门锁可能使用不同的无线通信协议进行数据传输。

分布广泛：物联网设备分布在世界各地，从家庭环境到工业场所，从城市到农村。这种广泛的分布使得对物联网设备的管理和监控变得更加困难。例如，农业中的远程土壤湿度传感器可能部署在偏远的农田中，网络连接不稳定。

数据海量：物联网设备不断产生大量的数据，这些数据需要进行实时处理和分析。例如，智能交通系统中的传感器每天会产生数以亿计的交通数据，包括车辆速度、流量等信息。

3）内容分发网络（CDN）

节点分布广泛：CDN 网络由分布在全球各地的节点服务器组成，这些节点服务器可以缓存网站的内容，提高用户的访问速度。例如，全球最大的 CDN 提供商 Akamai 在世界各地拥有数千个节点服务器。

内容分发动态性：CDN 会根据用户的地理位置和网络状况动态地选择最合适的节点服务器进行内容分发。例如，当用户访问某一网站时，CDN 会自动选择距离用户最近且网络连接最好的节点服务器提供内容。

流量波动大：CDN 网络的流量会随着时间和业务需求的变化而波动。例如，在热门视频发布时，相关网站的流量会急剧增加，CDN 需要能够快速响应并提供足够的带宽。

4）暗网

匿名性强：暗网使用诸如洋葱路由（如 TOR 网络）等技术，通过多层加密和代理转发，将用户的网络流量分散和混淆，使得追踪用户的真实 IP 地址和身份变得极其困难。这一特性吸引了大量追求隐私保护和进行非法活动（如军火交易、毒品贩卖、个人信息贩卖等）的人群，加剧了对其监管和探测的难度。

内容高度隐蔽：暗网网站的访问需要特定的软件、配置或授权才能进行。通常，这些网站使用特殊的域名（如.onion 域名），无法通过传统的搜索引擎和网络发现工具找到，它们隐藏在普通互联网的背后，为恶意活动提供了避风港。

网络结构复杂：暗网的网络拓扑结构与明网截然不同，它由大量分布式的节点构成，节点之间的连接关系动态多变。新的节点可能随时加入或离开网络，使得整个暗网的网络结构呈现出高度的动态性和不确定性，加大了对其进行全面测绘的难度。

二、新形态网络空间测绘研究现状

1）云网络

目前，关于云网络测绘的研究主要集中在云平台的资源发现和拓扑结构绘制方面。一些研究提出了通过分析云平台的 API 接口来获取云网络的资源信息的方法，但这种方法需要与云服务提供商进行合作，且受到 API 接口权限的限制。另外，对于云网络中多租户环境的测绘研究还相对较少，尤其是如何准确区分不同租户的网络边界和安全策略。

2）物联网

物联网测绘的研究主要关注物联网设备的发现和识别。一些研究通过分析物联网设备的通信协议来识别设备类型，但由于物联网设备的通信协议种类繁多，这种方法的准确性和通用性有待提高。此外，对于物联网设备的地理位置和拓扑结构的测绘研究还处于起步阶段，如何有效地对大规模分布式物联网设备进行测绘仍然是一个挑战。

3）内容分发网络

CDN 网络测绘的研究主要集中在节点发现和性能评估方面。通过向 CDN 网络发送探查请求，分析响应时间和带宽等指标来评估节点的性能。然而，CDN

网络的动态性和复杂性使得节点的实时发现和性能监测存在一定的困难，如何准确地获取 CDN 网络的全局拓扑结构和流量分布仍然是研究的热点。

4）暗网

基于流量分析的探测方法：通过监测网络流量中的特殊特征和行为模式，识别可能通往暗网的流量。一些研究工作利用机器学习算法对网络流量进行分类和识别，但由于暗网流量与正常流量存在一定的重叠，且暗网用户不断采用新的加密和混淆技术，这种方法的准确率和召回率仍有待提高。

主动探测与蜜罐技术：主动在暗网中投放蜜罐节点，吸引暗网用户的访问，并记录其行为和交互信息。蜜罐技术可以获取到暗网内部的部分信息，但由于暗网用户具有较高的安全防范意识，蜜罐容易被识别和绕过，导致获取的数据有限。

基于情报共享的探测：不同的安全组织和研究机构之间共享暗网相关的情报和数据，通过整合多方信息，扩大对暗网的监测范围。然而，情报共享存在数据格式不统一、隐私保护和信任问题，限制了其效果的进一步提升。

三、新形态网络空间测绘需求

1）云网络

安全评估：了解云网络的拓扑结构和设备状态，有助于发现潜在的安全漏洞和威胁，评估云服务的安全性。例如，检测云网络中是否存在被非法入侵的虚拟机实例。

资源管理：通过测绘云网络，可以准确掌握云资源的使用情况，合理分配和调度资源，提高资源利用率。例如，优化云服务器的配置，避免资源浪费。

合规性检查：确保云网络的配置符合相关的法规和标准要求，例如 GDPR（通用数据保护条例）等。

2）物联网

安全监测：及时发现物联网设备中的安全隐患，如设备被恶意攻击、数据泄露等问题。例如，检测智能摄像头是否被非法入侵。

故障诊断：当物联网系统出现故障时，能够快速定位故障设备和故障原因，提高系统的可靠性和可用性。例如，在智能电网中，快速定位故障的传感器节点。

网络优化：了解物联网设备的拓扑结构和通信状况，优化网络布局和通信协议，提高物联网系统的性能。例如，优化智能家居网络的拓扑结构，减少网络延迟。

3）内容分发网络

性能优化：通过了解 CDN 网络的拓扑结构和节点性能，优化内容分发策略，提高用户的访问速度和体验。例如，根据节点的实时性能动态调整内容缓存策略。

故障排查：当 CDN 网络出现故障时，快速定位故障节点和故障原因，减少故障对用户的影响。例如，在网站访问异常时，快速确定是哪个 CDN 节点出现了问题。

竞争分析：了解竞争对手的 CDN 网络布局和性能情况，为企业制定合理的 CDN 选择和使用策略提供参考。

4）暗网

安全保障需求：暗网是各类非法活动的温床，对国家安全、社会稳定和个人隐私构成了严重威胁。准确测绘暗网网络空间，有助于执法部门打击网络犯罪，维护社会秩序。

威胁情报收集需求：了解暗网中的恶意活动趋势和黑客技术动态，为企业和政府机构提供及时有效的威胁情报，从而采取相应的防范措施，降低安全风险。

学术研究需求：暗网作为一个特殊的网络空间，对其进行深入研究有助于推动网络科学、信息安全等领域的发展，为解决网络匿名性、隐私保护和安全监管等问题提供理论和实践基础。

四、新形态网络空间测绘基本思路

1）云网络

- **数据采集：**

利用云平台提供的 API 接口获取云资源的基本信息，如虚拟机实例的数量、状态、配置等。同时，部署网络探针，监测云网络中的数据包流量，分析网络拓扑结构和通信关系。最后，可结合用户的业务需求信息，了解云服务的使用情况和分布情况。

- **数据分析：**

运用数据挖掘和机器学习算法，对采集到的数据进行分析和处理，识别云网络中的节点和链路。在此基础上，建立云网络的拓扑模型，描述云网络的结构和动态变化。最后，分析云网络中的安全威胁和风险，评估云服务的安全性。

- **结果呈现：**

以可视化的方式呈现云网络的拓扑结构和资源使用情况，为用户提供直观的网络视图。生成云网络的安全报告和性能评估报告，为用户的决策提供支持。

2）物联网

- **设备发现：**

利用蓝牙、WiFi 等无线通信协议进行设备扫描，发现周围的物联网设备。分析物联网设备的通信数据包，识别设备的类型和身份信息。结合物联网平台的注册信息，获取设备的详细信息和地理位置。

- **拓扑绘制：**

根据设备之间的通信关系，构建物联网的拓扑结构。考虑物联网设备的移动性和动态性，实时更新拓扑结构。

- **数据整合与分析：**

将设备发现和拓扑绘制的数据进行整合，建立物联网的整体模型。运用大数据分析和人工智能算法，对物联网数据进行挖掘和分析，发现潜在的安全隐患和业务价值。

3）内容分发网络

- **节点发现：**

利用 DNS 解析和网络探测技术，发现 CDN 网络中的节点服务器。也可以通过与 CDN 提供商的合作，获取节点的地理位置和网络配置信息。

- **性能评估：**

向 CDN 节点发送测试请求，测量节点的响应时间、带宽、丢包率等性能指标。同时，分析不同地理位置和网络环境下的节点性能差异，评估 CDN 网络的整体性能。

- **拓扑构建：**

根据节点发现和性能评估的结果，构建 CDN 网络的拓扑结构。同时，考虑 CDN 网络的动态性，实时更新拓扑结构，反映 CDN 网络的变化情况。

4）暗网

- **多模态数据融合**

在未来的暗网探测中，单一的数据来源往往难以满足全面测绘的需求。融合多种数据源，如网络流量数据、节点行为日志、暗网论坛文本信息等。通过多模态数据融合，可以从不同角度对暗网进行分析和理解，提高对暗网节点和活动的识别准确性。例如，将流量特征与暗网论坛中的文本语义分析相结合，能够更精准地判断一个暗网节点是否涉及非法活动，以及活动的具体类型。

- **AI 与机器学习的深度应用**

利用深度学习模型，如卷积神经网络（CNN）、循环神经网络（RNN）及其变体（LSTM、GRU）等，对暗网数据进行深度挖掘和分析。深度学习模型可以

自动学习暗网数据中的复杂模式和特征，从而提高对暗网节点和活动的分类、识别和预测能力。

强化学习可用于优化暗网探测策略，根据实时反馈调整探测路径和方法，提高探测效率和效果。例如，通过强化学习算法，智能控制蜜罐的投放位置和策略，以获取更多有价值的信息。

- **跨国合作与国际标准制定**

暗网不受地理边界的限制，其活动范围往往涉及多个国家和地区。因此，加强国际间的合作与交流，建立跨国的暗网监测和打击机制至关重要。不同国家的执法部门、安全机构和研究组织可以共享情报和技术资源，共同应对暗网带来的挑战。

制定国际统一的暗网测绘标准和规范，包括数据采集、处理、存储和共享等方面的标准。这有助于提高不同组织和国家之间的数据兼容性和互操作性，促进暗网测绘工作的规范化和科学化。

- **与区块链技术结合**

利用区块链技术的去中心化、不可篡改和可追溯等特性，为暗网测绘数据的存储和共享提供安全可靠的解决方案。将测绘数据存储在区块链上，可以保证数据的完整性和可信度，防止数据被篡改和伪造。基于区块链的智能合约可以实现数据共享的自动化和规范化，在保护数据隐私的前提下，促进不同机构之间的数据交换和合作。

- **面向新涌现暗网技术的适应性探测**

随着技术的不断发展，暗网也在不断涌现新的匿名技术和网络形态。未来的暗网探测技术需要具备快速适应和应对这些新变化的能力。例如，针对可能出现的新型匿名通信协议和隐藏服务技术，及时研发相应的探测方法和工具。持续跟踪暗网技术的发展动态，建立技术预警机制，提前做好技术储备和应对准备，确保在新的暗网技术出现时能够迅速开展有效的测绘工作。

- **可视化与交互技术的应用**

开发先进的可视化工具，将复杂的暗网网络结构和活动信息以直观易懂的图形、图表等形式展示出来。通过可视化技术，安全分析人员和决策者可以更清晰地了解暗网的整体态势和关键信息，提高决策效率和准确性。

引入交互技术，允许用户与可视化界面进行互动，如查询特定节点信息、分析节点之间的关联关系等。这有助于用户深入挖掘暗网数据背后的潜在价值，更好地应对暗网带来的威胁。

当前，以星链（Starlink）为代表的卫星互联网已经开始规模性应用，特别是在一些特定的场景下（如俄乌冲突等）发挥着其他网络形态不可替代的作用。目前学术界已经有一些面向 Starlink 等卫星互联网的测量测绘研究，以盛邦安全的 Daydaymap 为代表的部分网络空间测绘平台已经专门针对星链卫星互联网进行了一些测绘实践。限于篇幅，本白皮书暂不对此展开论述，留待下次更新白皮书版本的时候再做专题研究。

第六章 典型应用场景与案例

6.1 攻防对抗支撑

6.1.1 攻击面管理（ASM）

一、应用场景描述

在当今数字化时代，网络攻击无处不在且手段日益复杂多样，企业和组织面临着巨大的安全威胁。对于各类组织机构而言，无论是金融机构、企业集团还是政府部门，其网络环境中存在着大量的资产，这些资产如同战场上的阵地，若防护不当就容易被攻击者利用，进而造成严重的损失。具体来说，在攻防对抗场景下，攻击者会通过各种手段寻找目标组织网络中的薄弱环节并发起攻击，而组织则需要尽可能全面地了解自身的攻击面，以便采取有效的防护措施。

攻击面管理（ASM）作为一种全面性的安全策略，旨在识别、评估和降低组织的攻击面。它不仅关注传统的网络边界，还涵盖了所有可能成为攻击入口的资产和漏洞，例如云服务中的未授权访问点、物联网设备的安全隐患等。与传统的网络安全策略不同，ASM 是一种主动的、全面的安全方法，更加注重对整个攻击面的动态管理，能够帮助组织及时发现潜在的安全威胁并进行处理。

二、网络空间测绘对识别暴露资产的作用

网络空间测绘是一种通过各种技术手段对网络资产进行全面探测和定位的方法。在攻击面管理中，它对于识别暴露资产起着至关重要的作用。

全面资产发现：网络空间测绘能够运用多种技术手段，如主动探测、被动监听等，对组织内外的各种网络资产进行扫描和识别。这包括服务器、网络设备、物联网设备、云服务资源等。例如，在一个大型企业网络中，可能存在大量未被直接管理或记录的老旧设备，这些设备可能由于长期缺乏维护而存在安全漏洞，成为潜在的攻击入口。通过网络空间测绘，能够将这些隐藏的资产逐一发现出来，避免因资产信息不完整而导致的安全隐患。

实时动态监测：网络环境是动态变化的，新的资产会不断加入，旧的资产可能会被淘汰或重新配置。网络空间测绘可以实时地对网络进行监测，及时发现资产的变化情况。比如，当企业内部新接入一台未经授权的物联网设备时，测绘系

统能够迅速检测到该设备并将其纳入到资产清单中，以便安全团队进行进一步的评估和管理。

资产属性识别：除了发现资产本身，网络空间测绘还能够识别资产的各种属性，如设备类型、操作系统版本、开放端口和服务等。这些属性信息对于评估资产的安全风险至关重要。例如，通过识别服务器的操作系统版本，安全团队可以判断该服务器是否存在已知的安全漏洞，并及时采取相应的补丁升级措施。

三、基于测绘结果的防护策略优化

通过网络空间测绘识别出暴露资产后，组织可以利用这些数据来优化自身的防护策略，从而在攻防对抗中占据更有利的位置。

风险评估与排序：根据测绘结果中的资产属性和资产的重要性，对暴露资产进行风险评估和排序。例如，对于存储敏感客户信息的数据库服务器，其风险级别通常较高；而对于一些内部使用的普通办公设备，风险级别相对较低。通过对风险的量化评估，安全团队可以优先处理高风险的资产，确保有限的安全资源得到合理利用。

漏洞修复与补丁管理：结合测绘得到的资产系统版本等信息，安全团队可以及时发现存在的漏洞，并制定相应的漏洞修复和补丁管理计划。同时，根据资产的业务需求和风险级别，合理安排修复时间，避免因修复操作对正常业务造成影响。例如，对于关键业务系统的服务器，在进行补丁升级之前，需要进行充分的测试和评估，以确保系统的稳定性。

访问控制策略调整：基于测绘发现的暴露资产和资产的访问权限情况，优化访问控制策略。例如，如果发现某个服务器开放了不必要的端口和服务，安全团队可以通过配置防火墙规则，关闭这些不必要的访问通道，减少潜在的攻击途径。同时，加强对内部网络中不同资产之间的访问控制，防止攻击者利用内部网络的信任关系进行横向移动。

应急响应预案完善：根据网络空间测绘的结果，进一步完善组织的应急响应预案。了解到哪些资产可能成为攻击的重点目标以及资产之间的关联关系后，安全团队可以制定更加针对性和可操作性的应急处置流程。例如，当某个关键资产受到攻击时，能够迅速采取相应的措施，如隔离受攻击资产、恢复备份数据等，将损失降到最低。

四、网络空间测绘结果对攻防对抗场景的支撑作用总结

在攻防对抗场景中，网络空间测绘结果为攻击面管理提供了坚实的基础，极大地增强了组织的安全防护能力。具体来说，它的支撑作用体现在以下几个方面：

提前预警与防御：通过及时发现暴露资产和潜在的安全漏洞，网络空间测绘能够帮助组织在攻击发生之前采取相应的防护措施，将攻击风险消除在萌芽状态。例如，在攻击者发现并利用某个漏洞之前，组织已经对该漏洞进行了修复，从而避免了安全事件的发生。

精确打击攻击源头：在遭受攻击后，测绘结果可以用于分析攻击路径和攻击者的可能来源。通过对资产之间的关联关系和访问日志的分析，安全团队能够追踪攻击者的活动轨迹，定位攻击源头，并采取相应的反制措施，如封锁攻击源 IP 地址等。

提升安全决策的科学性：网络空间测绘提供的全面、准确的资产信息和安全风险数据，为安全决策提供了有力的支持。安全团队可以基于这些数据制定更加合理、有效的安全策略和计划，避免盲目投入安全资源，提高安全投资回报率。

持续改进安全态势：随着网络环境的不断变化，攻击手段也在不断演变。网络空间测绘的实时监测和动态分析功能，能够帮助组织及时了解自身攻击面的变化情况，持续改进安全措施，保持对攻击的有效防御，从而在长期的攻防对抗中占据优势地位。

综上所述，网络空间测绘在攻击面管理中起着关键作用，能够帮助组织全面识别暴露资产并优化防护策略，有效应对复杂多变的网络攻击威胁。

6.1.2 防御案例

一、案例背景

随着数字化转型的加速，金融行业对信息技术的依赖程度日益加深，供应链的复杂性也大幅增加，这使得金融机构面临的供应链攻击风险与日俱增。供应链攻击通过渗透金融机构的供应商或合作伙伴网络，利用其系统漏洞或薄弱环节，最终达成对金融机构核心系统的入侵，造成数据泄露、资金损失等严重后果。本文所涉及的金融机构，简称为 F 银行，它是一家业务广泛、客户众多的大型银行，在日常运营中与大量科技供应商、外包服务商等存在紧密的合作关系，因此供应链安全成为了其信息安全的重要关注点。

二、供应链攻击形势与金融机构脆弱性分析

1）供应链攻击现状

近年来，全球范围内针对金融行业的供应链攻击事件呈上升趋势。攻击者利用金融机构供应链的复杂性和依赖性，通过感染供应商软件、植入恶意代码等方

式绕过传统的安全防护机制。例如，一些攻击者通过控制金融机构外部合作伙伴的服务器，获取对银行内部网络的初始访问权限，进而发动进一步的攻击。

2）F 银行面临的风险

F 银行在日常运营中使用了众多供应商提供的软件和服务，涵盖了核心业务系统、办公自动化系统、安全防护设备等多个方面。其中一些供应商的安全管理水平参差不齐，部分软件可能存在未修复的漏洞，这给攻击者提供了可乘之机。此外，随着业务的拓展，F 银行与更多的第三方合作伙伴建立了联系，供应链的范围不断扩大，潜在的安全风险也相应增加。

三、测绘平台的引入与功能

1）测绘平台的选择

为了有效应对供应链攻击风险，F 银行经过全面评估，引入了专业的数字化资产测绘平台 S。该平台具备全面的资产发现、漏洞扫描、风险评估等功能，能够实时监测金融机构及其供应链中的资产状况。平台采用先进的网络探测技术，能够在不影响业务正常运行的前提下，高效、准确地发现各种隐藏的资产和潜在的安全漏洞。

2）平台核心功能

资产全面识别：平台 S 能够对 F 银行自身的各类资产，包括服务器、终端设备、网络设备等进行详细的识别和分类。同时，还能对供应链中的供应商和合作伙伴的资产进行梳理，建立完整的资产清单。

漏洞精准扫描：针对发现的资产，平台 S 采用多种扫描技术，包括端口扫描、漏洞利用工具扫描等，检测资产中存在的已知漏洞，并生成详细的漏洞报告。报告中不仅包含漏洞的基本信息，如漏洞类型、严重程度，还会提供对应的修复建议。

风险动态评估：根据资产识别和漏洞扫描的结果，平台 S 实时评估金融机构及其供应链的安全风险水平。通过建立风险评估模型，综合考虑资产的重要性、漏洞的严重程度等因素，为管理者提供直观的风险评估结果和可视化的风险展示。

四、基于测绘平台的防御实践

1）建立供应链资产基线

在引入测绘平台 S 后，F 银行首先利用平台对自身和供应链中的所有资产进行了全面测绘，建立了初始的资产基线。通过对资产的详细信息和配置进行记录，为后续的实时监测和异常发现提供了基础。在测绘过程中，平台发现了一些

未被纳入管理的供应商服务器，这些服务器存在潜在的安全隐患，F 银行及时与供应商沟通，将其纳入统一的安全管理体系。

2）实时监测与预警

平台 S 对供应链中的资产进行 7×24 小时的实时监测，一旦发现资产状态的异常变化或新的安全漏洞，立即发出预警。例如，当监测到某个供应商的软件更新包中包含异常的网络连接行为时，平台及时通知 F 银行的安全团队。安全团队通过深入分析，发现该更新包被植入了恶意代码，可能会导致银行核心系统的信息泄露。F 银行迅速采取措施，暂停使用该供应商的软件更新服务，并要求供应商进行全面的安全排查。

3）阻断供应链攻击的具体过程

攻击迹象发现：在一次日常监测中，测绘平台 S 发现 F 银行某重要供应商的一个业务系统出现异常的网络流量。该流量指向一个境外的可疑 IP 地址，且流量模式与正常业务流量存在明显差异。平台立即发出预警，提示可能存在供应链攻击。

深入调查分析：F 银行的安全团队接到预警后，迅速展开深入调查。通过对供应商系统的日志分析和网络流量溯源，发现攻击者通过利用供应商系统中的一个未修复的漏洞，植入了后门程序，并通过该后门与境外服务器进行通信，企图窃取 F 银行的客户账户信息和交易数据。

应急响应处理：安全团队立即启动应急响应预案，一方面，断开供应商系统与 F 银行内部网络的连接，防止攻击进一步扩散；另一方面，通知供应商对其系统进行紧急修复，消除系统中的漏洞和后门程序。同时，F 银行加强了自身网络的访问控制和安全防护措施，防止攻击者绕过阻断措施，对银行系统进行二次攻击。

后续整改与预防：在成功阻断攻击后，F 银行与供应商共同对事件进行了总结和反思。双方制定了详细的整改计划，加强了对供应链系统的安全审查和定期评估。同时，F 银行要求供应商建立更加完善的安全管理体系，及时修复系统漏洞，加强对软件供应链的安全控制。此外，F 银行还利用测绘平台 S 加强了对供应链的持续监测，建立了更加敏捷的应急响应机制，以应对可能出现的类似攻击。

五、防御实践的成效与经验总结

1）成效评估

通过引入测绘平台 S 并实施基于该平台的防御措施，F 银行成功阻断了供应链攻击，有效保护了银行的核心系统和客户数据安全。在攻击阻断后，未发生客户信息泄露和资金损失等情况，银行的正常业务运营未受到明显影响。同时，通过对供应链资产的全面管理和实时监测，F 银行提高了自身和供应链的整体安全水平，增强了应对供应链攻击的能力。

2）经验总结

重视供应链安全：金融机构应充分认识到供应链攻击的潜在风险，将供应链安全纳入整体安全战略，加强对供应商和合作伙伴的安全管理。

利用先进技术手段：引入专业的资产测绘平台等先进技术工具，能够有效提高金融机构对供应链资产的可见性和安全管控能力。通过实时监测和预警，及时发现和处理潜在的安全威胁。

建立应急响应机制：制定完善的应急响应预案，在发现供应链攻击后能够迅速采取有效的措施进行阻断和处理，减少攻击造成的损失。同时，加强与供应商的合作与沟通，共同应对供应链安全挑战。

持续监测与改进：供应链安全是一个动态的过程，金融机构应建立持续监测和评估机制，不断改进安全管理措施。定期对供应链进行安全审查和漏洞扫描，及时发现和解决潜在的安全问题，确保供应链的长期安全稳定。

6.2 国家安全与关键基础设施保护

6.2.1 国家级网络地形图构建（参考美国 SHINE 计划）

一、国家级网络地形图的概念与意义

国家级网络地形图是一种全面、精准描绘国家范围内网络空间资产、连接关系、脆弱性分布等信息的综合视图，就如同传统地理地形图对地理环境的呈现一样，它为国家网络空间安全管理、战略决策和应急响应提供了基础支撑。其意义主要体现在以下几个方面：

战略规划：有助于国家制定长期的网络安全战略，明确网络安全的重点区域和关键节点，合理分配安全资源。

态势感知：使国家能够实时掌握网络空间的动态变化，及时发现潜在的威胁和攻击迹象，为网络安全预警提供依据。

应急响应：在发生网络安全事件时，网络地形图可以帮助快速定位受影响的区域和资产，制定有效的应急处置方案，减少损失。

国际合作：在国际网络安全合作中，国家级网络地形图可以作为交流和协作的基础，提升国家在网络安全领域的国际影响力。

二、国家级网络地形图构建的步骤与方法

1）数据采集阶段

资产发现：利用主动扫描（如端口扫描、服务识别）和被动监测（如流量分析）相结合的方式，发现国家范围内的网络资产，包括服务器、终端设备、物联网设备等。同时，与各行业主管部门、企业和机构合作，收集其自行上报的网络资产信息，确保全面覆盖。

连接关系确定：通过分析网络流量、路由信息和设备配置数据，确定各个网络资产之间的连接关系，构建网络拓扑结构。例如，使用网络流量分析工具识别不同网段之间的通信流量，确定网络边界和内部子网的连接情况。

脆弱性评估：采用漏洞扫描工具、渗透测试等手段，对网络资产进行脆弱性评估，发现可能存在的安全漏洞。同时，收集公开的漏洞信息和威胁情报，结合网络资产的实际情况，对脆弱性进行分类和分级。

2）数据整合与分析阶段

数据清洗与标准化：对采集到的多源数据进行清洗，去除重复、错误和无效的数据，并将数据进行标准化处理，确保数据的一致性和可比性。

关联分析：将资产信息、连接关系和脆弱性数据进行关联分析，发现潜在的安全风险和攻击路径。例如，通过关联分析可以发现某个存在安全漏洞的服务器可能影响到哪些其他系统和业务。

趋势分析：利用历史数据进行趋势分析，预测网络空间的发展变化和潜在的安全威胁。例如，分析网络资产的增长趋势、漏洞的发现和修复情况等。

3）可视化展示阶段

地图设计：根据国家的行政区划、网络层次结构等因素，设计合理的网络地形图布局。可以采用分层、分区的方式进行展示，方便用户查看不同层次和区域的网络信息。

信息呈现：将网络资产、连接关系、脆弱性等信息以直观的图形元素（如节点、连线、颜色标记等）进行展示，同时提供详细的信息查询功能，使用户可以获取每个节点和连线的具体信息。

交互设计：设计友好的用户交互界面，支持用户进行缩放、平移、筛选等操作，方便用户根据自己的需求查看和分析网络地形图。

三、面临的挑战与解决方案

数据隐私与安全问题：在数据采集和处理过程中，涉及到大量的敏感信息，如用户个人信息、企业商业机密等。为了保护数据隐私和安全，需要采取严格的技术和管理措施，如数据加密、访问控制、数据匿名化等。

数据质量与完整性问题：由于网络环境的复杂性和多样性，采集到的数据可能存在不准确、不完整的情况。为了提高数据质量和完整性，需要建立完善的数据验证和补充机制，加强与数据源的沟通和协作。

跨部门协调与合作问题：国家级网络地形图的构建需要政府部门、企业、科研机构等多方面的参与和合作。为了解决跨部门协调与合作问题，需要建立有效的沟通机制和协调平台，明确各部门的职责和分工。

技术创新与发展问题：随着网络技术的不断发展和变化，网络地形图的构建技术也需要不断创新和发展。为了应对技术创新与发展问题，需要加强科研投入，培养专业的技术人才，推动相关技术的研究和应用。

四、应用前景与展望

国家级网络地形图的构建将为国家网络安全保障提供有力的支持。未来，随着技术的不断进步和应用的深入，网络地形图的应用前景将更加广阔，可能在以下几个方面得到进一步发展：

融合更多数据维度：除了现有的网络资产、连接关系和脆弱性信息外，将融合更多的数据维度，如舆情信息、社交媒体数据等，为网络安全分析提供更全面的视角。

支持智能化决策：利用人工智能和机器学习技术，对网络地形图进行深度分析和挖掘，为网络安全决策提供智能化的建议和方案。

促进国际合作与交流：各国之间可以通过共享网络地形图的相关信息，加强国际网络安全合作与交流，共同应对全球性的网络安全挑战。

6.2.2 电力、通信等行业的脆弱性测绘与应急响应

一、电力、通信等行业关键基础设施的重要性

电力和通信行业作为国家关键基础设施的重要组成部分，对于社会的正常运转和经济的稳定发展起着至关重要的作用。

在电力行业，电力供应是现代社会各领域发展的基础。无论是工业生产、商业运营还是居民日常生活，都离不开稳定的电力支持。一旦电力系统遭受破坏或出现故障，将导致工厂停工、交通混乱、医疗系统受影响等一系列严重后果，甚至可能引发社会动荡。

通信行业则承担着信息传递和交流的重任。它连接着政府、企业和民众，保障着金融交易、公共安全、国防安全等重要事务的顺利进行。在全球化和信息化的时代，通信网络的畅通无阻对于国家的竞争力和国际地位也具有重要影响。一旦通信网络遭受攻击或出现故障，将严重影响信息的流通和共享，给国家安全和经济发展带来巨大损失。

二、脆弱性测绘的概念与方法

脆弱性测绘是指对电力、通信等行业的关键基础设施进行全面、深入的扫描和分析，以识别其潜在的安全漏洞和薄弱环节。通过脆弱性测绘，可以清晰地了解基础设施的资产情况、系统架构、安全状况等信息，为后续的安全防护和应急响应提供有力支持。

脆弱性测绘的主要方法包括：

资产清查：对电力、通信行业的各类资产进行详细的梳理和登记，包括网络设备、服务器、通信线路、电力设施等。通过资产清查，可以建立完整的资产清单，为后续的脆弱性扫描提供基础。

漏洞扫描：利用专业的漏洞扫描工具，对电力、通信系统进行自动化的漏洞检测。这些工具可以检测出系统中存在的已知漏洞，如操作系统漏洞、应用程序漏洞等，并生成详细的漏洞报告。

渗透测试：模拟黑客的攻击行为，对电力、通信系统进行真实的攻击测试。通过渗透测试，可以发现系统中潜在的安全漏洞和薄弱环节，评估系统的抗攻击能力。

协议分析：对电力、通信系统中使用的各种协议进行分析，检测协议实现中存在的安全漏洞。例如，分析通信协议中的认证机制、加密算法等，发现可能存在的安全风险。

威胁情报分析：收集和分析国内外的威胁情报，了解针对电力、通信行业的最新攻击手段和趋势。通过威胁情报分析，可以提前发现潜在的安全威胁，为脆弱性测绘提供参考。

三、电力行业的脆弱性测绘与应急响应

1）电力行业的脆弱性分析

电网结构脆弱性：电力系统的电网结构存在着一定的脆弱性，如线路过载、节点故障等。一旦电网中的关键线路或节点出现故障，可能会导致大面积停电事故。

设备老化与故障：随着电力设备的使用年限增加，设备老化和故障的风险也会不断提高。例如，变压器、发电机等设备的故障可能会影响电力供应的稳定性。

网络安全漏洞：电力系统的数字化和智能化发展，使得电力企业越来越依赖网络信息技术。但是，网络安全漏洞也成为了电力行业面临的重要威胁之一。黑客可能会通过攻击电力企业的信息系统，窃取关键数据、控制电力设备，从而引发电力安全事故。

自然灾害影响：自然灾害如地震、洪水、台风等可能会对电力设施造成严重破坏，导致电力供应中断。

2）应急响应措施

建立应急指挥体系：成立专门的应急指挥中心，负责统一指挥和协调电力行业的应急响应工作。应急指挥中心应具备快速决策、资源调配、信息共享等功能。

制定应急预案：制定完善的应急预案，明确应急响应的流程、职责和措施。应急预案应包括停电预警、电力抢修、人员疏散等方面的内容，并定期进行演练和修订。

加强设备维护和管理：定期对电力设备进行检查、维护和更新，及时发现和排除设备故障。建立设备故障预警机制，对设备的运行状态进行实时监测和预警。

强化网络安全防护：加强电力企业的网络安全建设，采取防火墙、入侵检测、加密技术等措施，防止黑客攻击和数据泄露。建立网络安全应急响应机制，及时处置网络安全事件。

储备应急物资和资源：储备足够的应急物资和资源，如发电设备、抢修工具、燃料等，以应对突发停电事故。同时，建立应急物资和资源的调配机制，确保在需要时能够快速、有效地进行调配。

与其他部门协同合作：加强与气象、水利、公安等部门的协同合作，及时获取自然灾害等相关信息，提前做好防范和应对措施。同时，在停电事故发生后，与其他部门共同开展应急救援和恢复工作。

3）典型案例：某电网公司，网络空间资产测绘让治理工作更清晰、高效

应用场景：该电网公司面临资产不清，且缺乏有效发现手段，资产画像信息不足，资产风险识别和快速定位能力不足，缺乏高效的资产检索能力等问题。

解决方案：盛邦安全基于 Daydaymap 平台周期性测绘构建全量存活资产清单，深度测绘形成全面资产画像，提供多维检索条件与漏洞快速排查资产风险。

应用效果：完成对互联网大区以及信息内网的资产摸排与治理工作，形成了完备的资产台账清单和漏洞风险发现能力；大幅提升资产和漏洞检测覆盖面、检测效能和自动化程度，高效应对常态化漏洞隐患治理与漏洞通报及应急处置等资产管理工作。

四、通信行业的脆弱性测绘与应急响应

1）通信行业的脆弱性分析

网络拥塞：随着通信业务的不断增长，通信网络面临着日益严重的拥塞问题。网络拥塞可能会导致通信质量下降、数据传输延迟等问题，影响用户的正常使用。

设备故障：通信设备如基站、交换机、服务器等可能会出现故障，导致通信中断。设备故障的原因可能包括硬件损坏、软件漏洞、电力故障等。

网络攻击：通信网络是黑客攻击的重要目标之一。黑客可能会通过攻击通信网络，窃取用户信息、干扰通信服务、破坏网络基础设施等。常见的网络攻击手段包括拒绝服务攻击、中间人攻击、病毒攻击等。

自然灾害和人为破坏：自然灾害如地震、洪水、台风等可能会对通信设施造成破坏，导致通信中断。此外，人为破坏如盗窃、蓄意破坏等也可能会影响通信网络的正常运行。

2）应急响应措施

构建应急通信体系：建立完善的应急通信体系，包括卫星通信、无线电台通信、应急通信车等，以确保在自然灾害、网络攻击等突发事件发生时，能够迅速恢复通信服务。

优化网络架构：优化通信网络的架构，提高网络的可靠性和容错能力。采用多路由、冗余备份等技术，降低因设备故障或网络拥塞导致的通信中断风险。

加强网络安全防护：加强通信企业的网络安全建设，采取防火墙、入侵检测、加密技术等措施，防止黑客攻击和数据泄露。建立网络安全应急响应机制，及时处置网络安全事件。

建立监测和预警系统：建立通信网络的监测和预警系统，实时监测网络的运行状态和安全状况。当发现异常情况时，及时发出预警信号，采取相应的措施进行处理。

制定应急预案：制定完善的应急预案，明确应急响应的流程、职责和措施。应急预案应包括通信中断预警、故障抢修、用户安抚等方面的内容，并定期进行演练和修订。

与电力等行业协同合作：加强与电力、交通等行业的协同合作，确保在突发事件发生时，能够相互支持和配合。例如，在电力中断时，通信部门可以与电力部门协同工作，优先恢复通信设施的电力供应。

3）典型案例：某大型国有通信基础设施服务提供商，通过互联网资产发现与整治实现资产暴露面可管可控

应用场景：该公司需求包括在现有资产安全防护体系的基础上，应对用户总部及各省属分公司的网络资产暴露面进行全面梳理，发现更多的企业资产；排查老旧、未知、隐形资产及应用等相关信息，快速建立资产台账，发现资产存在的漏洞风险并进行整改。

解决方案：盛邦安全基于 Daydaymap 平台在公司总部部署一套网络空间资产探测系统，通过远程扫描、联动互联网资产大数据平台的方式对用户互联网暴露面的 IT 资产进行持续发现，形成完整、及时更新的资产数据库。同时，通过互联网资产测绘技术收集用户互联网 IT 资产的设备信息和服务信息，动态获取更多的资产指纹信息。

应用效果：梳理出客户互联网资产暴露面全景图，最终达到对网络资产暴露面的可管可控。切实提升客户的网络安全防护能力与管理水平；通过互联网资产测绘技术收集客户互联网 IT 资产的设备信息和服务信息，动态获取更多的资产指纹信息；将互联网资产测绘数据与本地资产数据进行比对核查及漏洞影响范围分析。

五、脆弱性测绘与应急响应的持续改进

脆弱性测绘和应急响应是一个持续的过程，需要不断地进行改进和完善。

定期评估和更新脆弱性测绘结果：随着电力、通信行业的技术发展和业务变化，其脆弱性也会不断发生变化。因此，需要定期对脆弱性测绘结果进行评估和更新，及时发现新的安全漏洞和薄弱环节。

根据演练和实际应急处置情况改进应急预案：定期组织应急预案的演练，通过演练发现应急预案中存在的问题和不足，并及时进行修改和完善。同时，在实际应急处置过程中，总结经验教训，进一步改进应急响应措施。

加强技术创新和人才培养：不断引进和应用新的技术和工具，提高脆弱性测绘和应急响应的效率和准确性。加强对相关人员的技术培训和应急演练，提高应急响应队伍的专业素质和应急处置能力。

通过对电力、通信等行业的脆弱性测绘和应急响应，可以有效降低关键基础设施面临的安全风险，保障国家的安全和社会的稳定发展。

第七章 总结与倡议

7.1 网络空间测绘技术的战略价值

网络空间测绘技术作为数字时代的新型基础设施，其战略价值已从单一技术工具跃升为国家网络安全体系的核心支撑，主要体现在以下维度：

一、国家安全与主权的数字化延伸

网络空间已成为继陆、海、空、天之后的"第五疆域"，其安全直接关系到国家关键信息基础设施的稳定性。

威胁感知与防御前置：通过高精度 IP 定位、网络拓扑测绘和动态波动监测（如 BGP 劫持事件识别），可提前数小时发现针对能源、金融等核心领域的网络攻击意图。例如，我国某省级电力系统通过部署网络空间地图平台，实现了对境外 APT 组织攻击路径的实时追踪，防御响应效率提升 40%以上。

主权数据资产化：构建自主可控的全球网络空间地理信息库，可缓减西方国家在域名根服务器、IP 地址分配等领域垄断带来的影响，为我国参与国际网络治理规则制定提供数据话语权。

二、数字经济发展的新型生产要素

2025 年全球数字经济规模预计突破 50 万亿美元，网络空间测绘技术正在重构数据要素的价值链：

产业数字化转型基石：实景三维中国与网络空间地图的融合（如雄安新区试点），为智慧城市提供厘米级精度的时空基准。

跨域价值释放：在某港口案例中，基于网络空间测绘的港口数字孪生系统，实现了船舶调度、货物装卸的毫秒级协同，经济效益显著。

三、技术自主创新的战略高地

当前全球网络空间测绘技术呈现"中美双极"竞争格局，关键技术突破关乎产业安全：

核心算法突破：比如，盛邦安全"坤舆图"系统采用动态 IP 多区域定位算法，将街道级定位精度从传统技术的 75%提升至 92%；埃文科技通过 UNDNS 解析聚簇技术，实现 AS 级拓扑测绘误差率低于 0.3%。

硬件生态构建：比如，盛科通信的“CTC8180”以太网交换芯片，提供从 1000M 到 400G 的全速率端口能力，具备智能网络可视化技术、确定性网络技术以及榫卯可编程技术。

7.2 产学研协同创新倡议

为应对技术碎片化、标准缺失等挑战，需构建"政产学研用"五位一体的创新生态系统：

一、技术研发共同体建设

在技术研发共同体建设方面，建议采取如下措施：

跨部门合作平台建设： 通过政府牵头、企业和高校联合搭建网络空间测绘研发平台，如北京市政府联合主要网络安全企业、高校和科研机构共同成立“自主可控网络安全技术创新中心”，有助于整合各方资源，实现技术协同创新。

示范项目与试点工程： 在区域或行业内推广网络空间测绘示范工程，验证技术与标准的可行性，如中央网信办、国家发改委、工信部、教育部等十二个部门共同组织开展 IPv6 技术创新和融合应用试点工作，提供了成功案例。

开放共享机制与激励措施：构建网络空间测绘数据共享平台和联合创新基金，为持续研发和人才培养提供支持。如国家数据局发布《可信数据空间发展行动计划（2024—2028 年）》，鼓励开展可信数据共享平台建设。

二、人才培养与流动机制

学科交叉培养：在目前已经被遴选为网络空间安全示范学院和一流网安学院建设高校中开展网络空间测绘的教学，招收专班进行培养。在 38 所"双一流"高校开设网络空间地理信息工程专业，课程覆盖网络协议分析（占 30%）、地理信息系统（占 25%）、社会计算（占 20%）等模块。

人才共享计划：在有条件的企业建立和网络空间安全、态势感知及网络空间测绘相关的专门博士后工作站；畅通人才流动通道，比如允许企业技术骨干可担任高校产业教授，高校科研人员可保留编制参与企业项目等。

三、政策保障体系优化

资金支持：设立千亿级国家网络空间测绘发展基金，对研发投入占比超 15%的企业给予 150%加计扣除。

标准引领：2025 年前发布《网络空间地图数据分级分类规范》《测绘服务安全评估指南》等多项团体标准，推动 ISO/TC211 国际标准提案。

伦理约束：建立"数据采集负面清单"，禁止对医疗、教育等民生领域敏感节点进行商业测绘，研发差分隐私保护算法提升位置数据匿名化处理效率。

四、全球化协同路径

技术输出：依托"数字丝绸之路"项目，向东盟国家输出网络空间测绘解决方案（典型案例如中泰铁路项目）。

数据互通：推动建立金砖国家网络空间测绘数据交换中心，实现非涉密数据的跨境安全流动。

风险联防：与欧盟合作开发全球网络波动态势感知和预警系统，对跨境 DDoS 攻击实现快速协同响应。

主要参考文献

[1] Cyberspace,[EB/OL]. https://en.wikipedia.org/wiki/Cyberspace.

[2] 方滨兴, 邹鹏, 朱诗兵. 网络空间主权研究 [J]. 中国工程科学,2016,18(06):1-7.

[3] 罗向阳, 刘琰, 尹美娟. 网络空间测绘 [M]. 北京：科学出版社. 2020 年 10 月.

[4] 杨家海, 吴建平, 安常青. 互联网络测量理论与应用 [M]. 北京：人民邮电出版社. 2009 年 10 月.

[5] 杨家海, 何林, 李城龙. 网络空间测绘——原理、技术与应用[M]. 北京：人民邮电出版社. 2023 年 9 月.

[6] 王继龙, 庄姝颖, 缪葱葱等. 网络空间信息系统模型与应用 [J]. 通信学报，Vol. 41, No. 2, 2020 年 2 月.

[7] SMap, [EB/OL]. https://github.com/AddrMiner/smap.

[8] Durumeric Z, Wustrow E, Halderman J A. ZMap: Fast Internet-wide Scanning and Its Security Applications[C]// The 22nd USENIX Security Symposium (USENIX Security 13), 2013: 605-620.

[9] Lyon G F. Nmap network scanning: The official Nmap project guide to network discovery and security scanning[M]. Insecure. Com LLC (US), 2008.

[10] Graham R D. MASSCAN: Mass IP port scanner[J]. URL, https://github. com/robertdavidgraham/masscan, 2014.

[11] Izhikevich L, Teixeira R, Durumeric Z. LZR: Identifying Unexpected Internet Services[C]//30th USENIX Security Symposium (USENIX Security 21). 2021: 3111-3128.

[12] 郭莉, 曹亚男, 苏马婧等. 网络空间资源测绘：概念与技术[J]. 信息安全学报，Vol. 3, No. 4, 2018 年 7 月.

[13] 郭启全, 高春东, 郝蒙蒙等. 发展网络空间可视化技术支撑网络安全综合防控体系建设. 中国科学院院刊，Vol. 35, No. 7, 2020 年第 7 期.

[14] Song G, et al. AddrMiner: A Comprehensive Global Active IPv6 Address Discovery System[C]//2022 USENIX Annual Technical Conference (USENIX ATC 22). 2022.

[15] Zhang W, et al. 6vision: Image-encoding-based ipv6 target generation in few-seed scenarios[C]//2024 IEEE 32nd International Conference on Network Protocols (ICNP). IEEE, 2024.

[16] Luo Y, Li C, Wang Z, et al. IPREDS: Efficient prediction system for Internet-wide port and service scanning[C]//2024 ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2024).

[17] Song G, et al. PMap: Reinforcement Learning-Based Internet-Wide Port Scanning[J]. IEEE/ACM Transactions on Networking (2024), vol. 32, no. 6, pp. 5524-5538.

[18] Pan L, Yang J, He L, et al. Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels[C]// NDSS 2023.

[19] Matherly J. Complete guide to shodan[EB/OL]. Shodan, LLC, 2015.

[20] Durumeric Z, et al. A search engine backed by Internet-wide scanning[C]// Proceedings of the 22nd ACM SIGSAC conference on computer and communications security (CCS 2015).

[21] Staff, RIPE Ncc. Ripe atlas: A global internet measurement network[J]. Internet Protocol

Journal 18.3 (2015): 2-26.
[22] Zoomeye, [EB/OL]. https://www.zoomeye.org/.
[23] Fofa, [EB/OL]. https://fofa.info/.
[24] Quake, [EB/OL]. https://quake.360.net.
[25] Daydaymap, [EB/OL]. https://www.daydaymap.com/.
[26] 奇安信，奇安信天眼威胁监测与分析系统产品技术白皮书 [EB/OL]. https://www.qianxin.com/product/detail/pid/328.
[27] 绿盟科技，网络空间地图测绘理论体系白皮书 [EB/OL]. https://www.nsfocus.com.cn/index.php?m=content&c=index&a=show&catid=92&id=203.
[28] Microsoft's HoloLens 2 Puts a Full-Fledged Computer on Your Face. Wired. 2019-02-24. [EB/OL]. https://www.wired.com/story/microsoft-hololens-2-headset.
[29] 华为. CyberVerse：开启数字新世界. 华为. [EB/OL].[2025-04-17]. https://developer.huawei.com/consumer/cn/training/course/video/101567475249831573
[30] 唐思宇,李赛飞,张丽杰.基于 Neo4j 的网络安全知识图谱构建分析[J].信息安全与通信保密,2022(8):60-70.
[31] GRAPHISTRY INC. Threat Hunting[EB/OL]. [2025-04-17].https://www.graphistry.com/use-cases/threat-hunting.
[32] CESIUM GS INC. 3D Tiles for Network Infrastructure Visualization [R]. [2025-04-17]. https://cesium.com/learn/3d-tiles/.
[33] THREE.JS COMMUNITY. Three.js Documentation: WebGL-based 3D Rendering [EB/OL]. (2023-08-20) [2023-10-28]. https://threejs.org/docs/.
[34] LANGCHAIN. LangChain Tools: Integrating Data Sources and Visualization Libraries [EB/OL].[2025-04-17]. https://python.langchain.com/docs/modules/agents/tools/custom_tools.
[35] Tableau. Preparing data for natural language interaction in Ask Data[EB/OL]. [2025-04-17]. https://www.tableau.com/learn/whitepapers/preparing-data-nlp-in-ask-data.
[36] Metz C. Gaming Giant Unity Wants to Digitally Clone the World[J]. Wired, 2022-01-18. Available: https://www.wired.com/story/gaming-giant-unity-wants-to-digitally-clone-the-world
[37] Samwoo Immersion uses a digital twin for efficient port logistics management[EB/OL]. Unreal Engine, 2022-11-03. Available: https://www.unrealengine.com/en-US/spotlights/samwoo-imersion-completes-an-efficient-port-logistics-with-digital-twins
[38] Plotly. Network graphs in Python[EB/OL]. [2025-04-17]. https://plotly.com/python/network-graphs/.Data Apps for Production | Plotly
[39] Apache ECharts. Dynamic Data - Data - How To Guides - Handbook - Apache ECharts[EB/OL]. [2025-04-17]. https://echarts.apache.org/handbook/en/how-to/data/dynamic-data/.
[40] 韩丁康,朱宇佳,赵蕾,等.基于动态域名水印的 IPv6 DNS 服务发现方法[J].网络与信息安

全学报,2024,10(05):56-70.(中国科学院信息工程研究所)
[41] 李超群,唐纯莹,韩言妮. DNS 公共解析服务可用性研究[C]//中国指挥与控制学会（Chinese Institute of Command and Control）.第十届中国指挥控制大会论文集（下册）.中国科学院信息工程研究所;中国科学院大学网络空间安全学院;,2022:193-199.DOI:10.26914/c.cnkihy.2022.018862.
[42] 刘文峰,张宇,张宏莉,等.域名系统测量研究综述[J].软件学报,2022,33(01):211-232.DOI:10.13328/j.cnki.jos.006218.
[43] Jiao L, Li J, Zhang W, et al. Measuring Encrypted DNS Service with TLS1. 3 Support over IPv6[C]//2024 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2024: 1-7.
[44] 王志豪,张卫东,文辉,等.IP 定位技术研究[J].信息安全学报,2019,4(03):34-47.DOI:10.19363/J.cnki.Cn10-1380/tn.2019.05.03.
[45] Jiao L, Zhu Y, Zhang W, et al. 6GAI: Active IPv6 Address Generation via Adversarial Training with Leaked Information[C]//2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE, 2024: 1079-1085.
[46] 陈帅,郭启全,高春东,等.网络空间地理图谱的概念与方法[J].科技导报,2023,41(13):14-22.
[47] 卓君,郭启全,高春东,等.面向天基信息系统的网络空间可视化表达技术体系[J].科技导报,2023,41(13):32-40.
[48] 郭启全,高春东,孙开锋,等.基于“人-地-网”关系的网络空间要素层次体系建设[J].地理研究,2021,40(01):109-118.
[49] 朱金玉,张宇,曾良伟,等.一种多接口路由器地理定位方法[J].信息安全学报,2018,3(04):15-24.DOI:10.19363/J.cnki.cn10-1380/tn.2018.07.02.
[50] Ye J, Leung K C, Low S H. Combating bufferbloat in multi-bottleneck networks: Theory and algorithms[J]. IEEE/ACM Transactions on Networking, 2021, 29(4): 1477-1493.
[51] 孙晶瑜.无线传感器网络中的自适应 2-不相交多路径路由算法[D].哈尔滨工业大学,2009.
[52] 苏新勇.非公共 DNS 服务器发现及分析系统设计与实现[D].哈尔滨工业大学,2022.DOI:10.27061/d.cnki.ghgdu.2022.002518.
[53] 李冷文婷.开放 DNS 服务器缓存测量与风险评估系统设计与实现[D].哈尔滨工业大学,2022.DOI:10.27061/d.cnki.ghgdu.2022.002669.
[54] Sun G Y, Ye F, Chai T, et al. Gambling domain name recognition via certificate and textual analysis[J]. The Computer Journal, 2023, 66(8): 1829-1839.
[55] Li C, Cheng Y, Men H, et al. Performance analysis of root anycast nodes based on active measurement[J]. Electronics, 2022, 11(8): 1194.
[56] Li J, Zhang Z, Guo C. Machine learning-based malicious X. 509 certificates’ detection[J]. Applied Sciences, 2021, 11(5): 2164.

附录　编写组成员名单

中关村实验室 411 项目组成员:尹霞、杨家海、李城龙、董聪、何林、宋光磊、王之梁、董恩焕、李振宇、林海、龚闻文、林金磊、张文健、罗一睿。

国防科技大学电子对抗学院施凡、薛鹏飞、许成喜。

远江盛邦安全科技集团股份有限公司权晓文、李新征、孙勇。

特别支持单位：第七届“纵横”网络空间安全创新论坛组委会。