## 网络空间测绘技术调研

*huangkai2024/01/25*

### 网络空间

构建在信息通信技术基础设施之上的人造空间，用以支撑人们在该空间中开展各类与信息通信技术相关的活动。组成四要素：载体、资源、主体、操作。

### 网络空间测绘

绘制一份网络空间地图，对网络空间中的各类虚实资源及其属性进行探测、分析和绘制的全过程。

### 国内外发展现状

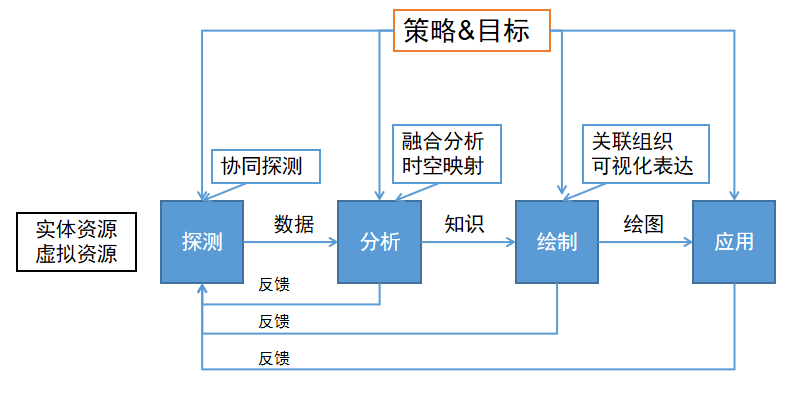
全球主流测绘平台76个,2008年以来，国内外相继出现了网络空间资源测绘方面的相关工作。

基本内容如下：

|  |  |
| --- | --- |
| 机构 | 描述 |
| 国外政府 | 2008年启动的SHINE（SHodan INtelligence Extraction）计划关注于美国本土关键基础设施相关设备的网络和安全态势，搭建本国关键基础设施安全保护框架的基础支撑。 |
| 2012年11月发布的DARPA“PLAN X”计划（已改名为“Project IKE”），构建了面向网络空间作战支撑的数字地图，使军事人员可以通过可视化的方式建立、执行并增强其网络空间的作战方案。 |
| 2013年曝光的“藏宝图计划”以全网数据为对象，实现了多层次大规模信息探测和分析，目标是将整个网络空间的所有设备在任何地点、任何时间的动态都纳入该计划监控中，绘制近乎实时的、交互式的多维度全球网络空间地图。 |
| 国内平台 | 360空间测绘平台（Quake），能够对全球IPv4、IPv6地址持续性探测、实施感知全球各类资产并发现安全风险。  功能介绍：<https://360.net/product-center/360-dns-safe/surveying-system-Saas>  平台：<https://quake.360.net/quake/> |
| Fofa是白帽汇推出的一款强大的网络空间资产搜索引擎。通过进行网络空间测绘,能够帮助研究人员或者企业迅速进行网络资产匹配。  平台：<https://fofa.info/> |
| ZoomEye（“钟馗之眼”）知道创宇旗下404实验室驱动打造的网络空间搜索引擎。通过分布在全球的大量测绘节点，针对全球范围内的IPv4、IPv6地址库及网站域名库进行24小时不间断探测、识别，根据对多个服务端口协议进行测绘，最终实现对整体或局部地区的网络空间画像。  平台： <https://www.zoomeye.org/> |
| Hunter(鹰图平台)：奇安信网络空间测绘平台（简称HUNTER平台），可对全球暴露在互联网上的服务器和设备进行：资产探测、端口探活、协议解析、应用识别。通过网络空间测绘技术，将地理空间、社会空间、网络空间相互映射，将虚拟的网络空间绘制成一幅动态、实时、有效的网络空间地图，实现互联网资产的可查、可定位，帮助客户解决互联资产暴露面梳理的难题。  平台：<https://hunter.qianxin.com/> |
| 国外平台 | Shodan堪称黑暗版Google，可以搜索几乎所有联网设备，包括服务器、摄像头、打印机、路由器等。  平台：<https://www.shodan.io/> |
| Censys是一个广泛使用的互联网搜索引擎和网络安全平台，旨在帮助用户发现和分析互联网上的设备、服务和漏洞。它提供了丰富的互联网数据和强大的搜索功能，使用户能够对全球范围内的网络进行详细的探索和分析。  平台：<https://search.censys.io/> |
| ****BinaryEdge：****不断收集和关联来自互联网可访问设备的数据，使组织能够了解他们的攻击面以及他们向攻击者暴露的内容  平台：[https://www.binaryedge.io](https://www.binaryedge.io/) |

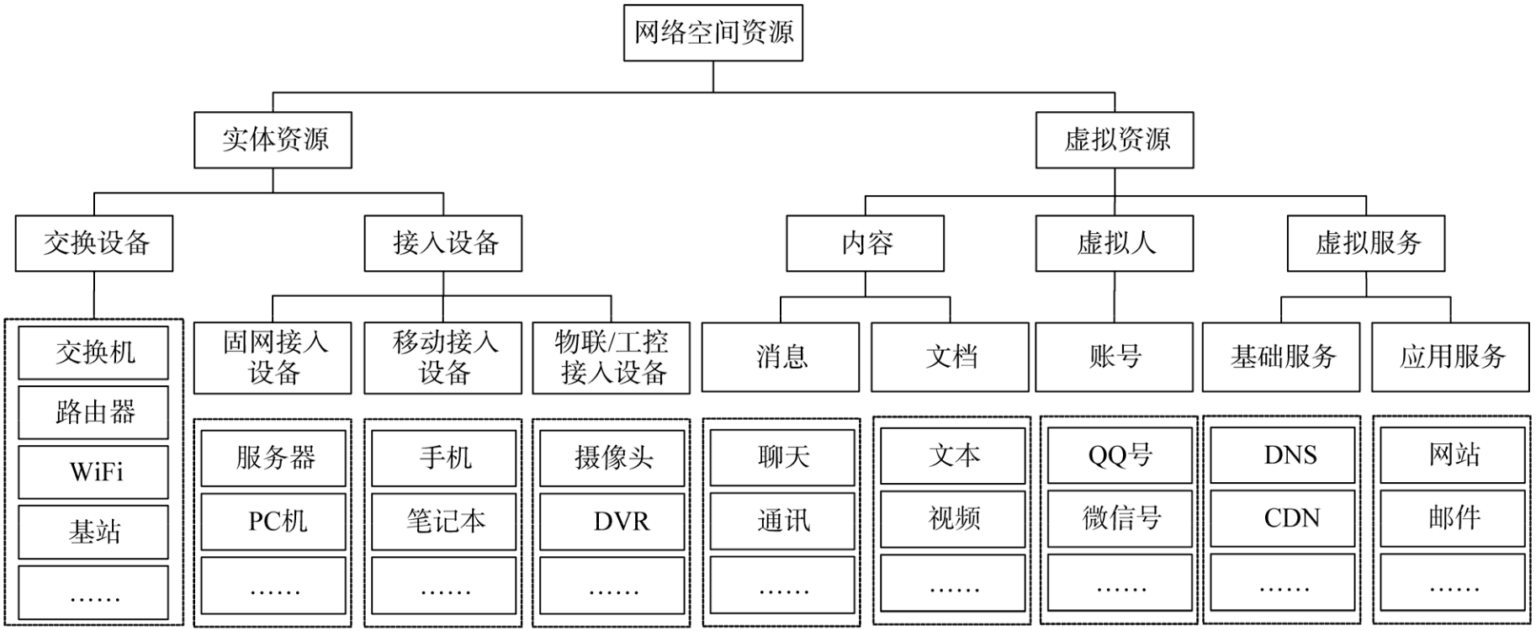
### 理论框架

探测-->分析-->绘制-->应用

****

### 测绘目标

把网络空间的组成元素，作为测绘对象；把组成网络空间的资源，分为实体资源和虚拟资源。实体资源是指服务器、设备等看得见、摸得着的硬件资源；虚拟资源则是指网站、服务、账号等电子资源。

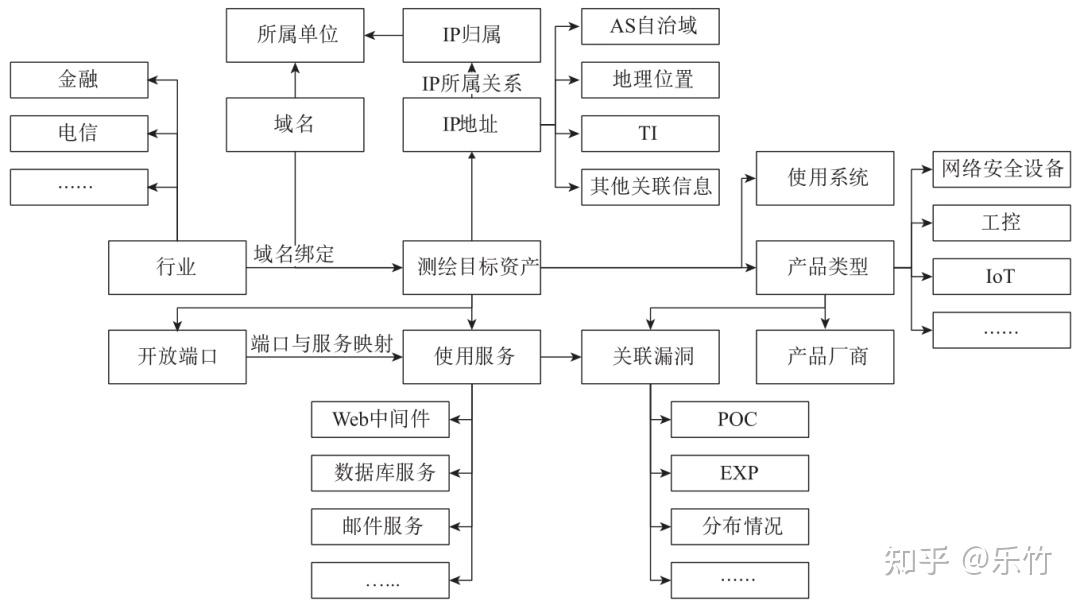


**映射分析：**虚拟资源的关联分析、实体资源定位与关联分析

**展示绘制：**强相关、弱相关、非相关

### 技术领域

**产品识别：**



网络空间中探测到的数据主要有组件资源数据和服务资源数据，如何能够对一个IP的整个攻击暴露面进行识别，主要依赖于以下技术和策略。

（1）端口策略：对多少个端口进行探测。

（2）协议识别：对多少种协议进行探测。

（3）产品识别：能够识别多少设备或组件。

（4）服务识别：能够识别多少应用服务。

最终，网络空间测绘系统在应用中形成了端口策略、协议库以及产品的特征鉴定库，后者也是这类系统的最重要指标之一，或称为产品指纹特征库。在产品识别的基础上，部分系统通过资产数据属性关联，就能得到资产对象库。(如何探测端口和协议，如何识别产品和服务)

**漏洞感知：**漏洞验证技术

**数据分析：**

（1）不同数据维度：可以结合地域属性、管理属性和组织属性等进行关联分析。

（2）数据时间维度。

**地图绘制：**可视化表达

### 主要应用场景调研

1. 安全研究支撑服务

系统采用互联网SaaS服务的交付模式，为用户开放查询检索服务。用户根据权限级别和购买积分的不同，获得不同的查询和下载权限，同时为用户提供了知识贡献奖励。这些用户主要是各企事业单位与网络安全公司的安全研究人员，从事广泛的安全研究和安全管理工作。而系统厂商除了可以获取订阅和积分销售的收益，还能获得用户提供的查询数据和贡献的代码和知识。常用四种网络空间资产搜索引擎包括：[FOFA](https://fofa.info/)、[ZoomEye](https://www.zoomeye.org/)、[360Quake](quake.360.net)、[Shodan](http://www.shodan.io) 。

1. 全网测绘分析报告服务

这种应用场景与最早的2012互联网普查一文中的应用模式非常相似，系统运营者以重要系统、重要厂商、重要漏洞、重要安全事件等不同维度为切入口，对全网资源数据进行探测和分析，在分析结果的基础上提供全网的专题测绘分析报告。

参考：

<https://zhuanlan.zhihu.com/p/466326989>

<https://zhuanlan.zhihu.com/p/336721424>

1. 区域资产评估和测绘服务

这种应用场景通过主动扫描结合流量监控的资产采集方式，对关注区域内的联网资产进行分析和统计。

<https://www.gjbmj.gov.cn/n1/2022/0422/c411145-32406257.html>

1. 企业内外网暴露面评估服务（重点）

由于攻防能力的不对等，在于攻防双方资源和信息的不对等。因此，很多企业级用户需要从攻击视角出发，利用空间测绘技术，对内网和外网暴露在攻击面的资产进行整体排查、统计、梳理和处置。目前，这方面的应用已经成为了很多大型企业和事业单位在执行攻防对抗演习工作中不可或缺的环节。

<https://blog.51cto.com/u_9652359/6539148>

<https://www.baishan.com/pages/security/IES-Detection-Service/>

1. 面向特定区域的情报数据分析挖掘业务

场景定位目标是根据用户需求应用目标标注及资产发现引擎，对重点目标进行体系性资产关联分析和迭代拓展。并对重点目标资产进行目标体系关联挖掘，发现目标资产关联性。在此基础上，对目标网络资产变化态势进行监测分析及研判，及时发现并识别目标资产变化情况，为制定合理的军事决策提供数据及技术支撑。

1. 关基监管和态势感知业务

在关基监管和态势感知业务中，一方面网络空间测绘系统可以直接为系统提供大网测绘数据、互联网暴露资产及其脆弱性的数据等，有助于网络资产云监测、漏洞响应等业务的开展；另一方面，将挂图和作战相耦合，改变传统安全监管依靠文字和图标的信息传递方式，实现人—资产—业务打通管理，全面助力于安全运营工作的升级。

1. 攻防演练和靶场业务

在攻防演练和靶场业务方向上，网络空间测绘系统有助于实战攻防视角下的训练、评估和管控等业务开展。首先，测绘系统可以对渗透资产进行远程探测，并提供对应的产品信息和脆弱性信息；其次，可以对武器和训练的效果，在多次持续性探测的基础上进行即时评估；最后，可以在网络拓扑测绘的基础上，对网络状况、蜜网防护等业务指标进行整体分析和管控。

### 反测绘技术

1. 非法请求、探测、扫描行为感知技术研究

基于IP地理位置库、扫描器指纹库、探测指纹库结合流量行为分析技术，精准感知非法请求、敌对网络测量、测绘以及非法探测行为，阻断资源泄露风险，提升网络空间防控预警能力。

1. 如何识别协议：ICMP、TCP、UDP的协议识别 [应用层协议识别算法综述](https://www.jslab6.edu.cn/media/jslab/paper/6D/6DUFD4REfzIuA9pPoaHMBYkZKwc052hr.pdf)
2. 如何识别网络探测行为：拓扑探测、资源探测
3. 如何识别扫描遍历行为。[网络扫描与防御技术](https://zhuanlan.zhihu.com/p/341605469?utm_id=0)
4. 如何结合网络行为分析  [网络安全中的实体异常行为分析技术](https://www.wangan.com/p/7fy7fx64decbed78)
5. 虚假响应技术研究

对于测绘节点及探测扫描行为，研究并利用虚假响应模型，反馈虚假信息；研究并基于虚假指纹模型，隐藏真实指纹，减少真实信息暴露风险。

1. 虚假响应模型的构建：根据访问请求协议类型和内容，保留静态资源+随机替换动 态资源。
2. 虚假指纹模型的构建：混淆指纹技术 [指纹混淆技术与实战场景](https://mp.weixin.qq.com/s/53lqy8BefY2qLu0Gw4Pyig)
3. 诱骗和扰乱技术研究

基于情报和蜜罐、欺骗网络和隐蔽陷阱等技术识别异常访问者，扰乱其探测和扫描等行为。同时结合自学习能力和关联分析能力，进一步分析访问者的异常行为。

1. 蜜罐技术 <https://zhuanlan.zhihu.com/p/535254759?utm_id=0>
2. 如何构建隐蔽陷阱并模拟真实环境
3. 如何提供虚假拓扑响应

[基于欺骗防御技术的网络安全攻击检测与技术实现](https://mp.weixin.qq.com/s/i-vdzMHygunYBOJIQS-79g)

[青藤云安全：一种基于欺骗防御的入侵检测技术研究](https://zhuanlan.zhihu.com/p/81415814)

1. 工程实现与服务包装等

其他参考资料：

*安全运营之暴露资产探测 <https://blog.51cto.com/u_9652359/6539148>*

*资产测绘学习笔记 <https://blog.csdn.net/qq_53207309/article/details/125914923>*

*网御星云拟相防御系统 <https://www.leadsec.com.cn/news/220610-632.html>*

*网络空间测绘技术的实践与思考 <https://www.secrss.com/articles/33824>*

*网络空间测绘理论体系概述 <https://blog.nsfocus.net/cyberspace/>*