网络空间测绘系统分类及应用综述

刘　红，姚旺君，孙　彻，刘旭东，包正晶，贾召鹏
（中国电子信息产业集团有限公司第六研究所，北京 102209）

摘　要： 随着万物互联时代的到来以及5G、IPv6、云计算、边缘计算、物联网、区块链等新兴技术的蓬勃发展，网络空间中的联网设备呈现爆炸式增长，网络空间中的目标对象形态也多种多样，同时暴露的网络资产安全风险随之提高。如何摸清网络空间中的资产底数，感知网络资产的风险，进而保障网络空间资产安全，已成为当下领域内尤为关心的问题。简要描述了网络空间测绘系统的发展历程和相关概念，然后从网络空间资源类型、网络资产探测方法、网络空间测绘应用场景等角度对网络空间测绘系统进行分类和阐述，提出了不同维度的测绘系统评价指标体系，以及网络空间测绘面临的问题、难点及其未来发展趋势。

关键词： 网络空间测绘；分类方法；评价指标
中图分类号： TP393　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2021.10.003
引用格式： 刘红，姚旺君，孙彻，等. 网络空间测绘系统分类及应用综述[J].信息技术与网络安全，2021，40(10)：16-21，28.

Classification and application of cyberspace surveying and mapping system

Liu Hong，Yao Wangjun，Sun Che，Liu Xudong，Bao Zhengjing，Jia Zhaopeng
（The 6th Research Institute of China Electronics Corporation，Beijing 102209，China）

Abstract： With the advent of the era of Internet of Everything and the vigorous development of 5G，IPv6，cloud computing，edge computing，Internet of Things，blockchain and other emerging technologies，the network equipment in cyberspace has shown explosive growth，and the target object forms in the network space are also diversified，the security risks of network assets exposed are also increased. How to find out the base number of assets in cyberspace，to perceive the risk of network assets，and to ensure the security of network space assets has become a special concern in the current field. This paper describes the development process and related concepts of cyberspace surveying and mapping system，then classifies and expounds the network space mapping system from the perspectives of network space resource type，network asset detection method and application scene of cyberspace surveying and mapping industry. It also puts forward the evaluation index system of different dimensions，and the problems faced by cyberspace surveying and mapping，as well as the difficulties and the future development trend.

Key words： cyberspace surveying and mapping；classification method；evaluation index

0 引言

随着计算机网络及通信技术的发展，世界即将进入万物互联的时代，新兴互联网通信技术方兴未艾，联网设备种类和数量都呈现爆发式增长，网民规模与日俱增，据CNNIC发布的第47期《中国互联网发展统计报告》，截至2020年12月，中国互联网用户数达到9.89亿，占总人口的70.7%，网络空间已成为亿万民众的精神家园。为推进网络空间治理，就需要摸清网络空间的“家底”。网络空间测绘是对网络空间中的各类资源进行探测，获取网络空间资源的基本属性、应用属性和扩展属性，将获取到的各类数据进行融合处理、关联分析，绘制形成一张网络空间资源的地图，以全面掌握网络空间基本特性及其分布特征，为网络空间治理、网络安全风险防御提供参考和依据。

本文从网络空间测绘的发展历程、相关概念出发，按网络空间资源类型、探测方法、行业应用等方向对网络空间测绘进行分类，并提出网络空间测

绘系统评价体系以及发展趋势，为网络空间测绘体系理论和技术研究贡献力量。

1 发展历程

互联网，始于1969年的美国，它的兴起给人们的工作、生活、社交、娱乐、消费带来了诸多便利。起初为了解决网络中存在的问题，更好地利用网络，研究者们更多关注的是网络性能，通过研究网络测量与分析技术[1]，周期性、连续地测量网络的性能参数，包括丢包率、RTT、流量、路径的平均跳数等，通过对一系列参数的量化，来考察网络的稳定性、可达性、可靠性及网络服务质量等。随着互联网技术的成熟以及应用的普及，互联网不再仅仅作为实验室技术研究对象存在，而是越来越成为人们生产生活中的“第二类空间”[2]存在。

2001年美国《保护信息系统的国家计划》首次提出“网络空间”(cyberspace)概念，随着美国国家安全局(National Security Agency，NSA)的藏宝图计划、美国国防部先进研究项目局(Defense Advanced Research Projects Agency，DARPA)的X计划以及美国国土资源部(United States Department of Homeland Security，DHS)的SHINE计划[3]的披露，进一步推动了网络空间测绘及其应用的发展。2016年12月27日，中国国家互联网信息办公室发布了《国家网络空间安全战略》，将网络空间安全提升到一个重要的层次，加快推动了我国网络空间测绘工作的发展。

在网络空间测绘领域的起步阶段，主要集中于理论和概念的研究，结合网络测量技术和地理测绘知识，在资产探测、拓扑测量、IP定位层面逐步发展。现阶段更注重的是在海量多源异构数据的基础上进行信息同化和融合分析，根据不同应用场景和需求，应用可视化技术，结合人工智能，对所有信息分门别类地进行展示。在进行全网资产探测的同时，实现对网络空间的态势感知、规律探寻，致力于将网络空间、地理空间和社会空间进行相互映射，将虚拟、动态的网络空间测绘成一份动态、实时、可靠、有效的网络空间数据地图，支撑监管机构、网络安全部门、关键基础设施行业、互联网金融行业及互联网广告等典型行业应用。网络空间测绘系统发展历程如图1所示。

图1 网络空间测绘系统发展历程

2 相关概念

目前，国内研究主要从狭义和广义两个角度阐述网络空间测绘的基本内涵[2-4]，狭义的网络空间是指覆盖互联网，建立于各类基础设施、设备及软硬件基础上的一个抽象、虚拟、数字化的空间；广义的网络空间是指不仅覆盖互联网，还有电信网、工业控制网等，将传统物理空间中的各对象，以及其关联的信息(即社会空间信息)映像到网络空间中。本文所探讨的是广义的网络空间。

方滨兴院士将网络空间组成要素分为4种类型[5]：载体、信息、主体和操作，基于此4要素网络空间测绘的目的是获取网络空间中各个要素的全面完整信息，具体包括网络空间目标软硬件资产属性信息、网络拓扑地图绘制、目标地理位置信息、目标账号信息以及各个要素之间的信息融合和关联分析。

网络空间目标软硬件资产属性信息包括目标设备、目标软件及其属性信息，如识别目标为路由器、交换机、安全防护设备、服务器、终端、物联网设备等，进一步包括目标设备的型号、厂商等；另外，目标软件信息包括目标系统软件、应用软件、中间件等，进一步包括目标软件的名称、版本号、网络协议及版本；目标资产属性信息包括目标IP地址、MAC地址、主机名称、域名、端口开放情况、服务组件、行业属性、脆弱性匹配情况等。

网络拓扑地图绘制包含全球级别、国家级别、AS级别(AS域内和AS域间)和IP级别的绘制，分析全球网络连接情况。从物理拓扑和逻辑拓扑两个层面对指定地区下AS域内拓扑，返回路由器连接关系、路由器接口IP和路由器详细信息(如路由器位置、在网络中的角色及带宽等)。

目标IP地理位置信息包括地理位置、应用场景、所属运营商、定位精度、定位方式、定位准确度和一致性。

目标账号信息包括社交媒体账号基本信息、账号好友关系、账号发文信息，以及消息的点赞、转发、评论等。

网络空间测绘重在“测”与“绘”，以地理空间为基础，绘出网络空间中所有资产的位置，展示资产的属性特征，以资产为载体，向上扩展到社会空间，呈现所有资产的社会属性。地理空间是现实世界中可以看到的，如山川、河流、土地、城市、道路等；网络空间是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信息通信技术相关的活动[3]；社会空间原本是社会活动和社会组织所占据的空间，而基于网络空间所形成的社会空间是指虚拟的行为空间、社区、生活圈等。

本文主要从“测”的角度，通过不同的分类方法描述网络空间测绘系统，如图 2 所示；然后介绍目前网络空间测绘相关产品，并从不同维度总结其评价指标体系，提出对网络空间测绘技术的几点思考及其存在的难点、问题；最后阐述了网络空间测绘的发展趋势。

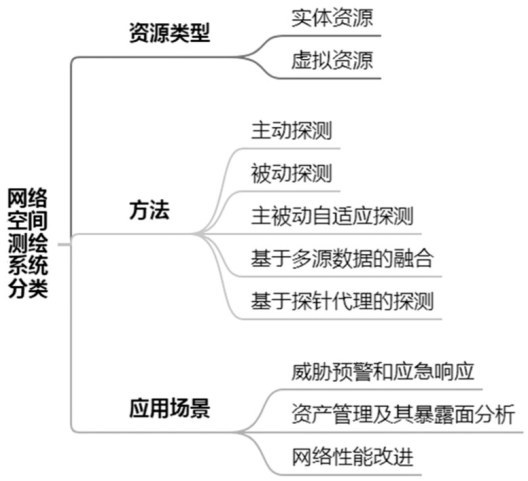

图 2 网络空间测绘系统分类

3 网络空间测绘系统分类

3.1 按资源类型分类

广义的网络空间资源是网络空间中“载体”、“信息”、“主体”等各类要素的总和，不仅覆盖通信基础设施、IP 网络、覆盖网络、应用支撑系统等互联网基础设施实体资源，而且覆盖承载在实体设施之上的信息内容、用户等虚拟资源[6-7]，如图 3 所示。

(1)实体资源

所谓实体性是指网络的组成及其在网络中能够实际体验的，即“看得见摸得到”的，它以网络本身为基础，是网络产生后才随之产生的。网络空间的实体资源[8]分为硬件和软件，硬件即能连上网络的设备，它们占据了虚拟网络空间中的某一位置，一旦设备掉电，就脱离网络空间，所以实体资源是动态变化的，如服务器、路由交换设备、物联网设备、终端设备、区块链等；软件即以硬件为载体以求达到某种目的的一系列代码，如操作系统、中间件、数据库、安全软件等。

对实体资源的“测”，主要是对实体资源属性信息的获取、地理位置的识别及其与其他实体资源的关联拓扑关系的获取。将实体资源的地理位置向地理空间映射，明确目标地址；拓扑关系向网络空间映射，绘制出目标网络的连接情况；实体资源的行业属性、组织结构等向社会空间映射，得到资源的社会属性分类和地域分布情况[9]。

(2)虚拟资源

所谓虚拟性是指网络世界的存在形态是无形的，它以图像、声音、信息等电子文本作为自己的存在形式。网络空间中的虚拟资源，划分到社会空间

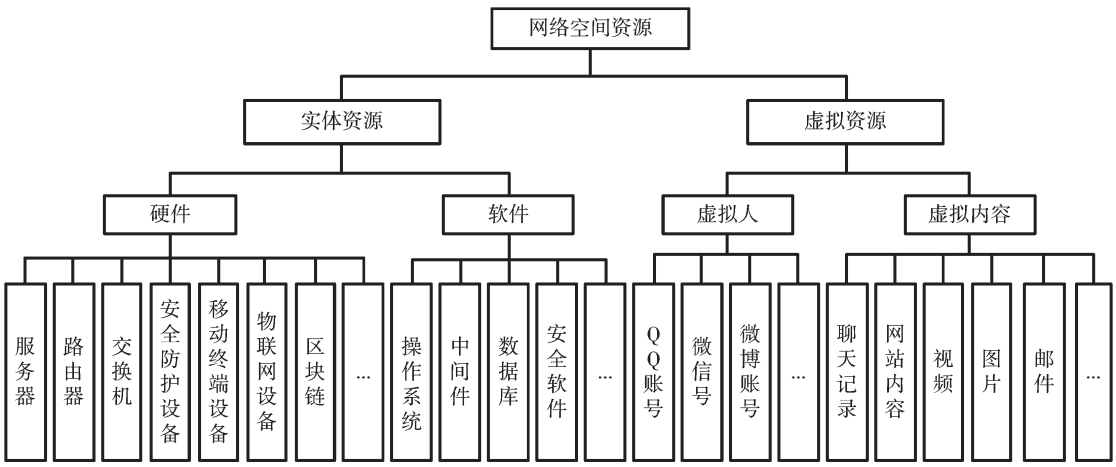

图 3 网络空间资源分类图

中，是由虚拟人(如各种社交账号等)、虚拟内容(如网页信息、聊天记录、视频等)构成的不同社区、不同群体组成的。在网络中人们可以用匿名或虚拟身份进行交流，不同于现实世界，网络空间中不存在身体属性、阶级属性以及地域属性所造成的各种沟壑。

对虚拟资源的“测”主要是对目标账号及内容信息的获取，例如对微信公众号、微博等社交媒体账号基本信息，账号好友关系和账号发文信息，以及关注的网站内容数据的提取，并在提取的数据基础上进一步关联分析，进行可视化绘制。

3.2 按方法分类

对网络空间资产进行摸底，基于网络传输技术可以应用多种手段，来获取网络空间资源的属性、地理位置、拓扑关系、社交内容等信息。

(1)主动探测

主动探测[10]是指通过主动向目标网络资产发出探测信号，包括端口扫描、指纹服务扫描、路由跟踪技术、Spider 爬虫[11]等探测网络的服务协议类型、IP 存活、社交媒体内容、网站内容等信息，从返回数据包的相关信息(包括各层协议内容、包重传时间等)中分类提取目标指纹或内容信息，将指纹与指纹库中的指纹进行比对，来实现对开放端口、操作系统、服务、应用类型、端到端间的网络性能信息、网络的路径分布及路由信息的探测；Spider 爬虫搜集目标网站域名或社交通道的诸如漏洞信息、开放服务信息、作者公司、关联关系、文本内容资产等信息[12]。主动探测方法相比于传统方法便捷且高效，其通过目标网络内的一个节点进行探测数据包的收发和响应分析实现，不需要在所有网络资产上安装客户端。但同时也存在不足之处，例如大量非正常通信的网络流量噪声易对正在运行的系统造成影响等。

(2)被动探测

被动探测是采用监听的方式，被动地接收当前网络中的流量包[13]，通过对数据包的分析和处理，获取资产信息。这种方法对网络当前状态影响较小，没有增加网络的负载，但不足之处是需要进行大量的分析工作，因为在所有流经网络的数据包中，可能只有部分具有分析价值，所以针对大规模网络，采用被动监听的方式效率较低。另一方面，对于在线但不工作的网络设备，无法监听其流量，此时采用主动探测方式比较有效。

(3)主被动自适应探测

主被动自适应探测顾名思义是依据目标类型和状态，将主动探测和被动探测两种方式自动进行优劣势互补，针对不主动产生流量的目标节点，自动采用主动探测方式，获取所需信息，针对网络性能要求较高且敏感的网络，自动采用被动探测方式采集、解析流量包，或者先通过被动方式初步判断目标节点的情况后，再自适应利用主动探测方式进一步深入地探索和分析。总之，主被动自适应探测的目的是在不影响网络性能、不增加网络负载的前提下，尽可能全面准确获取网络空间资源属性信息。

(4)基于多源数据的融合

网络空间资源属性多源数据融合分析方法包括：开源网络情报(OSINT)，即通过对公开的信息或其他开源工具进行收集、分析后所得到的情报，如公共记录数据库、政府报告、文件、网站、大众媒体、暗网等公共信息；专业网络空间资产测绘产品提供的源数据，包括 FOFA、Shodan、ZoomEye、RaySpace、360 Quake、BinaryEdge、Sumap、全球鹰等；专用数据资源库，如 Maxmind、Whois、pDNS、高精度 IP 地理位置库、漏洞库、指纹库、资产信息库、行业属性关系库、社工库；威胁情报类服务商，如 FireEye、Infoblox、LookingGlass、McAfee、RSA、SecureWorks、Symantec 和 Verisign 等。

多源网络空间资源属性数据覆盖面广、碎片化、数据异构、数据量大，需要经验丰富的大数据处理分析师以及高效的智能分析处理算法，融合分析出网络空间测绘所需要的数据。此方法为纯粹的数据分析绘制可视化技术，不主动地针对目标进行探测获取数据，需要非常明确的应用场景需求进行支撑，才能形成有针对性有特色的专业网络空间测绘系统。

(5)基于探针代理的探测

基于探针代理的探测主要针对于可协作的专网(私网)应用场景的网络空间资产的测绘。运营商或者大型企业为了更好地实现自身网络或者设备的监管能力，通过安全数据分析、可视化监管和精细化运营管理，掌握运营状况，快速监控节点状态、排查节点故障。一般会将探针部署在相关的网络节点中或者 ISP&IDC 出口，通过探针主动传回目标节点网络层及应用层的属性信息到服务器，服务器进行分析展示监控。

基于探针代理的探测方法也是网络空间测绘应用的一类场景需求，结合国内外各类开源威胁情报库，对于私网资产的精细化运营管理、实时监控、异常报警、未知威胁发现有现实应用价值。

3.3 按应用场景分类

研究网络空间测绘系统，了解空间资产分布、属性、脆弱性信息，归根结底是基于攻击与防御的目的，目前各行业主要以防御为主，实时掌握自身所属资产的公网暴露面，及时修补漏洞，进行脆弱性分析，做好主动防御，防止威胁事件的发生。

(1)威胁预警和应急响应

网络空间测绘将资产数据融合与威胁风险关联叠加后，可以提升安全应急响应时效。例如在监管部门层面，监管区域内的设备众多，分布甚广，难以统一管理，利用网络空间测绘系统梳理区域内的资产，获取资产位置信息，识别资产属性特征及其脆弱性，进一步通过态势的察觉、评估和预测，提前主动感知可能出现的威胁情况，有助于避免网络威胁事件的发生，降低网络威胁事件带来的损失，特别是针对关键基础设施的态势预测尤为重要。利用工具进行监控，以工具代替人工，自动地全天候监控与侦察，抵御外部入侵，有助于扩大监管范围，起到降本增效的效果。

(2)资产管理及其暴露面分析

网络空间测绘可以应用于梳理目标资源的暴露面，对目标进行跟踪管理。例如在企业层面，通过资产探测，清晰地了解任意时段的企业内部资产状况，检测可能被遗忘的设备，识别设备可能安装的旧版本软件，根据暴露出的该版本存在的漏洞情况，执行版本升级操作，预防网络威胁的发生。同时通过资产探测，可了解企业产品的地域分布情况，结合地理位置以及用户搜索内容的大数据分析，可以向其推送个性化的信息，包括服务、广告等，作为营销策略。通过资产识别，进一步对企业内部资产暴露面自查，对企业外部互联网资产暴露面自查，及时修复漏洞，加固自身，不给攻击方可乘之机。

(3)网络性能改进

当前网络结构复杂，设备种类和业务系统较多，网络拓扑及上层覆盖网络的组网和性能等情况，是应用开发者和网络维护者关注的重点。通过跟踪网络资源的拓扑以及流量的变化趋势，监控网络运行状态，发现网络自身问题，对网络健壮性和脆弱性等进行评估，对新型网络应用等的分布情况进行摸底，了解网络状况，进而改进网络性能，优化网络配置。

4 评价体系

目前全球已有众多网络空间测绘产品(也称网络空间搜索引擎)，如美国的 Shodan[14]，它主要针对服务器、网络摄像头等网络基础设备进行扫描识别，且具有丰富的支持多种编程语言的 API 接口代码库；Censys[15]是密歇根大学的研究者开发的，它采用自研的扫描工具 ZMap，收集 IP、证书、网站的详细信息，帮助用户梳理所属组织的攻击暴露面；BinaryEdge 是瑞士一家公司的产品，它进行全网范围内的扫描，将近 50 亿设备的因特网攻击暴露面与 1 500 万个商业团体进行映射，致力于为企业组织提供实时威胁情报信息以降低它们被攻击的风险。

国内的网络空间测绘产品也相继产生，包括知道创宇公司的 Zoomeye，其通过两大探测引擎：Xmap 和 Wmap，分别针对网络空间中的设备及网站，每天 24 小时不间断地探测、识别，标识出互联网设备及网站所使用的服务及组件，除了设备指纹的扫描外，相比 Shodan 它增加了对域名和 Web 服务器的指纹扫描。华顺信安的网络空间搜索引擎 FOFA，其资产数据按照 host:port 的方式进行存储，对资产特征收集比较完善，具备支持图标搜索、蜜罐识别等功能。360 网络安全响应中心自主研发设计的全网空间测绘系统 Quake，使用自研的 Quake Vscan 扫描引擎，支持 5 个不同层面，数 10 万种产品识别、产品类型识别，数百种常见网络协议识别，具备全网资产设备发现识别能力。盛邦安全的 RaySpace 平台，应用自主研发的安全操作系统 RayOS，支持全球 IPv4、IPv6 双协议栈，使探测的范围更广更全面。安数网络的 Oshadan 网络安全监测系统，专为网络安全监管人员设计开发，用于监测关键信息基础设施网络安全风险。威努特做为国内工控安全领域的领军者，提供防护和检测两大类完善的产品线和多行业解决方案，包括工业安全态势感知平台、工业互联网雷达、漏洞库平台等进行工业互联网的资产探测及威胁预警。东北大学研发的谛听(ditecting)，侧重搜寻暴露的工控联网设备，定位其位置，捕捉开放端口，发现安全漏洞，展示全球工控安全形势。

面对众多的网络空间测绘产品，目前国内没有统一的评价标准来定量评价各产品的优劣势，本文提出从以下不同维度进行评价，如表 1 所示。

表 1 不同维度的评价体系

序号	指标名称	指标含义	评价方法
1	识别目标规模	可识别到的目标对象的规模	在指定统计方法下,统计目标对象的数量
2	识别目标类型	可识别到的网络空间资源的目标种类,如路由交换设备、网络摄像头、防火墙、网络打印机、工控设备、数据库、服务器等	统计测绘系统能够探测识别到的目标种类数量
3	识别目标属性	可识别各类目标的属性要素,包括物理属性、应用属性、社会属性等	统计识别到的目标属性要素数量
4	目标覆盖率	识别的目标节点比例	计算识别的目标节点数量与实际的目标节点的总数比
5	识别准确率	在全部目标资源中,测绘系统能够准确识别或映射的资产比例	测算识别或映射正确的资产数占总资产数的比例(通常采用抽样方法)
6	探测速率	获取单位数据所需的时间	测算采集的数据项数与所花费时间的比例
7	数据时效性	数据更新时间距离当前时间的间隔	计算数据更新到当前时间的时间间隔
8	数据更新周期	数据更新的时间间隔	计算连续两次对同一目标对象进行探测的时间间隔
9	数据变化感知时延	目标发生变化到获取更新数据的时间间隔	计算目标发生变化到数据更新的时间间隔

当然,产品相关的参数不止上述所列出的维度,不同测绘产品的侧重点也不尽相同,后续可在此基础上进行扩充。

5 存在的问题和难点

网络空间测绘面临的问题和难点主要如下:

(1)网络空间的资产分布广,数量大且种类多,需要分析所有在网设备的特征、协议信息,才能达到全面探测识别的程度。

(2)受虚假识别、网络防护等影响,易造成设备识别不准确,同样设备位置准确性、威胁准确性均有待提高。

(3)网络中的资产是动态的、瞬时变化的,当前看到的数据结果不一定就是设备的实际状态,存在偏差,要达到实时跟踪效果有待技术的提高。

(4)如何将实体资源向地理空间映射,如何在地理空间中描绘出不同形态的实体资源及其拓扑关系,如何将虚拟资源向社会空间映射,均存在一定难度。对虚拟资源的关联分析也有待研究和实现。

(5)网络空间测绘没有特定行业标准规范和资质种类规范要求,领域内缺少统一的网络空间资产数据表示方法、展示方法、资产分类分级的标准,导致不同产品的数据连通性差,也缺少测绘产品的评价标准来指导各单位测绘产品的开发。

(6)支持工业控制设备/协议等服务数量不足、感知深度不够。因工控设备携带的更多的是私有协议,且种类多,所以需要大量的分析成本和技术积累。

(7)目前各国加大 IPv6 推广力度,不同于对 IPv4 地址的探测,对 IPv6 地址探测用轮询的方法是不可能的,如何安全地、准确定位并识别 IPv6 资产,有待进一步研究。

(8)对新一代网络的探测技术,需与时俱进,如 SDN 网络、云网络、加密网络等。

(9)需加强对网络蜜罐的识别技术,防范探测目标的网络诱捕行为。

6 结论

现阶段国内网络空间测绘领域对网络空间资产的“摸底”已初具规模,覆盖了全网大部分设备,积累了大量资产数据,但相比国外网络空间测绘系统,从技术和应用方面均有较大的差距。据预计,到 2025 年全球连接到互联网的设备将达到 416 亿台,由此可见对网络空间的探索任重道远。未来需要做的一是在探测方面,要精益求精,对未知的协议资产进一步分析、探索,提高资产覆盖率、准确率,在提高探测速度的同时,引入高效的人工智能算法技术,注重探测的安全性、无感知、无影响、无风险、防溯源;二是在探测数据的基础上,将实体和虚拟资源数据进行融合分析,基于地理地图,将网络设备的地理位置、所属组织、拓扑关系、设备属性、网络人的属性等进行多维度绘制,形成面向设备/域名、面向关键基础服务、面向内容和服务、面向网络人和社会人映射的画像,形成高度集成的网络空间

(下转第 28 页)

104.

[13] DEVLIN J, CHANG M W, LEE K, et al. BERT: Pre-training of deep bidirectional transformers for language understanding[C]//Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technolo-zgies, 2019, 1: 4171-4186.

[14] 谢润忠, 李烨. 基于 BERT 和双通道注意力的文本情感分类模型[J]. 数据采集与处理, 2020, 35(4): 642-652.

[15] MIKOLOV T, SUTSKEVER I, CHEN K, et al. Distributed representations of words and phrases and their compositionality[C]//Advances in Neural Information Processing Systems, 2013: 3111-3119.

[16] MIKOLOV T, CHEN K, CORRADO G, et al. Efficient estimation of word representations in vector space[J]. arXiv preprint arXiv: 1301.3781, 2013.

[17] BAHDANAU D, CHO K, BENGIO Y. Neural machine translation by jointly learning to align and translate[C]//Proceedings of the 3rd International Conference on Learning Representations, ICLR 2015, 2015.

(收稿日期: 2021-08-12)

作者简介:

陈旭(1993-), 男, 硕士研究生, 主要研究方向: 网络舆情分析。

潘峰(1967-), 男, 博士, 教授, 主要研究方向: 多媒体安全。

韩益亮(1977-), 通信作者, 男, 博士, 教授, 主要研究方向: 信息安全、抗量子密码。E-mail: 790767691@qq.com。

(上接第 21 页)

全产业生态链的画像。同时期待国内多家网络空间测绘领域的企业, 可共享资源、共享补丁、高效协同、强强联合、合作共赢, 为国家安全战略同奋斗。

参考文献

[1] 张宏莉, 方滨兴, 胡铭曾, 等. Internet 测量与分析综述[J]. 软件学报, 2003, 14(1): 110-116.

[2] 赵帆, 罗向阳, 刘粉林. 网络空间测绘技术研究[J]. 网络与信息安全学报, 2016, 2(9): 1-11.

[3] 陈涛, 程丽君, 李明桂, 等. 网络空间测绘系统及应用研究[J]. 通信技术, 2020, 53(11): 2832-2837.

[4] 叶晓贞, 宁焕生, 夏博明, 等. 广义网络空间研究综述[J]. 计算机科学与应用, 2020, 10(5): 893-905.

[5] 方滨兴. 定义网络空间安全[J]. 网络与信息安全学报, 2018, 4(1): 1-5.

[6] 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, 2018, 3(4): 1-14.

[7] 齐云菲, 白利芳, 唐刚, 等. 网络空间测绘概念理解与分析[J]. 网络空间安全, 2018, 9(10): 45-49.

[8] 张江, 孙治, 徐锐, 等. 一种网络空间资源的测度方法研究[J]. 信息技术与网络安全, 2019, 38(5): 7-11.

[9] 覃岩岩, 张铁刚, 王宁. 浅谈网络空间测绘技术及其应用前景[J]. 网络安全技术与应用, 2018(8): 119-120.

[10] 王宸东, 郭渊博, 甄帅辉, 等. 网络资产探测技术研究[J]. 计算机科学, 2018, 45(12): 24-31.

[11] 邓美林. 基于主被动探测的安全态势指标体系研究[D]. 成都: 电子科技大学, 2020.

[12] 黄子豪, 张舒. 网络爬虫对互联网安全的影响及“反爬”策略的研究[J]. 科学技术创新, 2021(10): 120-121.

[13] 刘翔元. 基于网络流量分析的网络设备类型识别关键技术研究[D]. 南京: 南京邮电大学, 2019.

[14] LI R G, SHEN M, YU H, et al. A survey on cyber-space search engines[C]//China Cyber Security Annual Conference, 2020: 206-214.

[15] DURUMERIC Z, ADRIAN D, MIRIAN A, et al. A search engine backed by internet-wide scanning[C]//Computer and Communications Security, 2015: 542-553.

(收稿日期: 2021-06-02)

作者简介:

刘红(1986-), 女, 硕士, 工程师, 主要研究方向: 工控系统及安全、网络安全。

姚旺君(1983-), 男, 硕士, 高级工程师, 主要研究方向: 工控系统及安全。

孙彻(1993-), 男, 硕士, 助理工程师, 主要研究方向: 网络拓扑测量。