网络空间测绘技术的实践与思考

陈庆　李晗　杜跃进　张义荣

(360 集团,北京 100015)

摘要: 作为支撑数字化转型的基础,网络安全自身的数字化升级和转型也面临急迫的要求。网络空间测绘技术作为网络空间安全和网络空间地理学的交集中的重要组成部分,也是网络安全自身数字化转变的重要技术支撑,因此受到业界越来越多的关注。该技术在网络安全领域的实践已经包括了资产管理、攻击面发现、自动化渗透测试、漏洞事件应急、挂图作战、态势感知等一系列应用方向,并显示出一些问题。通过对这些问题进行分析,提出网络空间测绘技术应用方向的具体建议。

关键词: 网络空间测绘; 网络安全; 测绘定义网络

中图分类号: TP393.2　　文献标识码: A

引用格式: 陈庆, 李晗, 杜跃进, 等. 网络空间测绘技术的实践与思考[J]. 信息通信技术与政策, 2021,47(8):30-38.

doi: 10.12267/j.issn.2096-5931.2021.08.005

0　引言

近年来,网络空间测绘已成为网络通信技术、网络空间安全、地理学等多学科交叉融合的前沿领域[1]。该领域关注网络空间信息的“全息地图”,构建能面向全球网络实时观测进行准确采样、映射和预测的强大基础设施,通过采用网络探测、采集、汇聚、分析、可视化等方式,将网络空间资源属性以及网络资源间的关联关系进行建模和表达,实现全球网络空间全要素全息数字化映射和可视化地图展现[2],以反映网络空间资源状态变化、网络行为和上层人类意图。网络空间测绘将作为数字化时代实现数字化生产生活和数字化治理的基础设施,同时还与网络空间自身发展演进相互作用、相互影响,为构建全球网络空间命运共同体提供新视角和新技术。

1　网络空间测绘的主要应用领域展望

结合目前的网络技术和数字化发展愿景,网络空间测绘的应用场景主要包括网络安全应用领域、数字化管理应用领域以及测绘定义网络领域。随着技术进步、时间发展和应用的不断深化,这三个方向是层层递进的(见图1)。

图1　网络空间测绘的三大主要应用领域

网络安全应用是测绘应用的起步; 数字化管理应用是指面向城市、产业以及社会个人的全面数字化变革背景下,为它们提供基于测绘的丰富管理场景; 测绘定义网络则是基于“端”与“网”测绘的融合,以实现丰富的联网资源调度和自组织网络业务场景。从第二个方向开始,测绘将立足安全,超越安全,深入融合到数字化经济的场景中。

1.1　网络安全应用

网络空间测绘对网络安全应用的进步有重大支撑作用,网络攻击与现实世界有着密切的关联[3],在这个

方向上将网络空间挂图和网络空间作战任务耦合是需求强烈的发展方向。从最早开展的资产发现和漏洞检测,到近年来大热的威胁情报分析和态势感知,再到面向未来的网络空间作战地图,网络空间攻防对抗需求激增带动了网络空间测绘技术不断发展进步。目前,典型的场景包括数字资产识别与脆弱性侦测业务,面向特定区域的网络情报分析挖掘业务、关基监管、挂图作战和态势感知业务、实战攻防演练和靶场业务,以及对网络空间新风险的定义和分析等。

1.2 数字化管理应用

随着相关数字化产业的全面崛起,网络空间测绘的应用需求将更广泛地应用于数字化及数字孪生的各类产业场景中,从数字化城市、数字化产业到数字化社会。面对海量数字资产,无论是城市、工厂,还是个人,将愈发依靠测绘技术来支撑其所属、租用、关联的资产管理和业务。典型的业务应用领域包括数字城市建模与运营、物联网和工业互联网资产监控管理、制造业数字孪生车间管理、面向个人的数字化生产生活全生命周期管理、数字化转型的成效实时科学度量等。

1.3 测绘定义网络

目前的测绘应用领域主要还局限于“端”的探测,而未来网络空间测绘将更多地实现网的测绘、端网的融合以及基于测绘的网络优化。基于多云环境、云边协同计算和 SDN 应用进程的加快和普及的背景,从网络空间资源调度方向上,如果将端网测绘融合作为基础,突破现有的网络“硬架构”,即可实现灵活实时的联网资源调度和网络路径选择,以及弹性的可任意复制或折叠的自组织网络及其资源,将其称为测绘定义网络(Surveying & Mapping Defined Network,SMDN)。

SMDN 将带来丰富的应用场景,例如对一个组织或城市拥有的在线算力,以及根据业务需求和治理需求进行整体度量和调度优化;由于上层业务的变化构造与之相适应的网络传输和自组织网络安全防护结构;或者对某个区域的网络进行即时测量和仿真复制引流;通过多层映射反映人类因素的网络空间行为测度和影响分析等。

2 网络空间测绘在网络安全领域的应用

2.1 网络空间测绘在网络安全领域应用的回顾

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。美国作为网络空间资源测绘最早和最成熟的国家,在国家安全和商业应用领域都取得了体系化的进展[4]。

(1) 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。

(2) 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。

(3) 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。

此外,在商用领域国内外陆续推出了一系列面向公众开放的互联网网络空间测绘和资源检索系统及服务。早期主要有国外的 shodan.io、censys.io,中国的 zoomeye.org、fofa.so 等。这些系统和服务面向全球联网设备和服务进行探测,并结合用户社区收集和公开漏洞数据等形成集社区运营、网络空间测绘、资产数据搜索和漏洞风险关联于一体的互联网商业服务体系,同时输出部分能力到其他领域。

2.2 主要网络空间测绘技术领域

在当前网络安全领域中,比较活跃的网络空间测绘商用系统的设计思想和初期理念,基本参考了互联网上 2012 年发布的一篇匿名黑客的报告《Internet Census 2012(互联网普查 2012)》[5]。

该报告描述了其首先使用 Nmap 脚本引擎(NSE)在互联网上探测到数量惊人的无认证或默认认证的嵌入式设备,并侵入这些设备,构建了约 42 万台探测用的僵尸网络 Carna Botnet。接下来利用 Carna Botnet 对全网所有 IPv4 地址进行扫描,包括常用端口、ICMP Ping、反向 DNS 和 SYN。在此基础上,进行数据分析并估算了 IP 地址的使用情况,最终在报告中展示了多维度数据统计分析结果,绘制了全球网络空间 IP 使用情况的动态图。这篇早期的匿名报告充分体现了当前网络安全领域网络空间测绘系统所遵循的主要技术思路和工作步骤(见图 2)。

图2　Carna Botnet 测绘互联网的主要步骤

2.2.1　基础探测

基础探测部分的理念及技术主要来自于 Nmap (Network Mapper) 和 Zmap 开源项目[6]。Nmap 是 Gordon Lyon 在 1997 年开发的网络扫描引擎，通过发包和回包分析实现对网络中主机和设备的探测分析，广泛应用于网络管理与网络安全领域。Zmap 于 2013 年诞生于密歇根大学，当时 Zakir Durumeric、Eric Wustrow 和 J. Alex Halderman 构建了单包的 Zmap 扫描引擎，主要用于网络安全研究。Zmap 相比 Nmap，最大的特点是实现了发包和回包分析的分离，采用了无状态的扫描技术，没有进行完整的 TCP 三次握手，从而实现了大规模的单向发包探测能力。图 3 为 Zmap 架构图。

此外，在 Zmap 的基础上，Masscan 开源项目也采用了类 Zmap 的无状态扫描技术，通过使用 PF_RING，最快可以达到 6 min 内扫完全互联网的速度[7]。当然，一个网络空间测绘系统除了底层的扫描引擎之外，探测节点的资源数量、质量和分布也是探测能力的决定性因素。

2.2.2　产品识别

在扫描探测基础上，真正为网络空间测绘赋予现实意义的，就是对探测数据进行的产品设备级的分析识别。测绘资产的识别是通过 IP 属性、产品信息等数据关联分析的，图 4 列举了一些典型的关联逻辑。

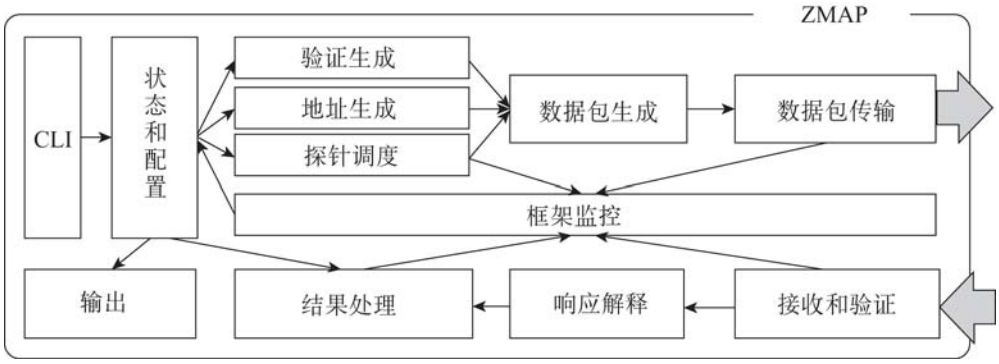

图3　Zmap 架构图

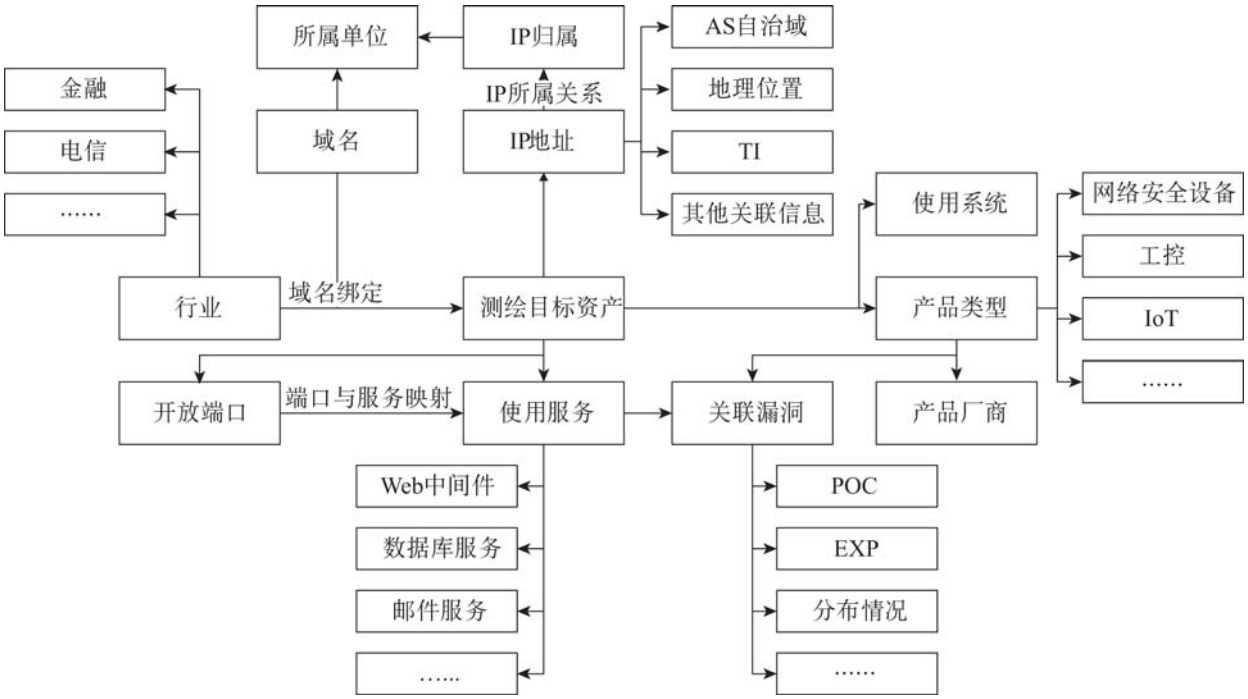

图4　资产属性关联图

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。

2.2.3 漏洞感知

漏洞感知能力其实是数据分析方向上的一种方式，这里单独提出来论述，是因为在现有的技术应用中，对漏洞的感知不单单依靠数据的关联，还为用户提供了进一步验证自身资产有关的漏洞的能力。因此，漏洞验证技术的应用，也自然成为了此类系统的核心技术之一。

漏洞数据关联的方式是基于漏洞信息与产品版本的对应关系而实现的。漏洞是数字化时代的网络攻防战略资源，现在的行业共识是人编写出来的程序就一定有漏洞存在。Synopsys 公司发布的《2020 年开源软件风险分析报告》指出，在审计范围内，75%的开源代码库有漏洞，49%的开源代码库含有高危漏洞。漏洞是依附于产品版本而存在的，伴随着不断公布的新漏洞，通过产品识别进行关联，是漏洞应急响应的重要环节。

然而，仅依靠漏洞跟产品数据层面上的简单关联，会为漏洞感知带来很多误报。其原因一方面在于无状态扫描探测技术的数据误报率比较高，另一方面也在于产品指纹库匹配不够精准。因此，仅依靠数据关联获取漏洞感知，会带来巨大的数据噪声，从而影响正常的判断工作效率。比较成熟的测绘系统往往通过提供漏洞验证技术，让用户对自身具体资产的漏洞影响情况进行实际验证测试，从规避或减少这种漏洞误报噪声对业务结果的影响。

2.2.4 数据分析

当前主流系统的数据分析技术主要侧重于网络安全攻防领域方面的应用，以下从两个方面来进行说明。

(1) 不同数据维度：主流系统的数据层次更多的是局限在网络设备层和网络应用层进行关联分析，在某些用户场景下，也结合了地域属性、管理属性和组织属性。

(2) 数据时间维度：数据时间维度分析的重点在于实时分析的快速要求，和历史分析的全量要求。由于在攻防对抗环境下，漏洞的利用时间差有可能影响攻防竞争的成败，因此在漏洞相关的实时性分析上，需要网络空间测绘系统提供更及时和精准的能力。而在历史数据的整理分析方向上，对全时间、全量数据的要求就被提升上来。

2.2.5 地图绘制

地图绘制技术的实质是网络空间可视化表达和可视化分析技术的业务场景应用；也是当前网络安全领域主流网络空间测绘系统较弱的技术部分，主流活跃的大部分系统仅实现了对资产数据的简单可视化展现，缺乏网络空间地理学测绘技术和业务管理的有效支撑，更无法实现可视化分析。网络空间地图应用的前提是必须具备对全球网络空间的测绘能力，只有内网探测能力，缺乏全球互联网(即大网)探测经验和测绘数据，是无法实现真正的网络空间地图的绘制的。

2.3 当前商用系统在网络安全领域的主要应用场景

2.3.1 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。

2.3.2 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。

2.3.3 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。

例如,利用常见漏洞库与资产库的关联,对区域内漏洞影响资产的分布、数量等进行统计分析和展示; 对新爆发出来的漏洞事件进行快速评估、定位和通报处置。这是一种利用测绘数据来支持态势感知能力的应用模式。

2.3.4 企业内外网暴露面评估服务

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。

2.3.5 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。

2.3.6 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。

2.3.7 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。

3 当前网络安全领域测绘应用的一些问题

3.1 用户使用简易度不足的问题

由于网络空间测绘系统的开发厂商大多具有安全攻防背景,目前主流的网络空间测绘系统是以类似百度的搜索框形式作为其第一用户交互界面。在使用中,用户通过登录访问交互搜索首页,在搜索框中需要按照系统约束的语法格式输入查询语句,以获得期望的资产搜索结果。

由于不同的系统有不同的语法设计,导致用户在使用不同的系统搜索资产的时候,有比较高的使用门槛。

(1) 搜索框的输入方式更类似于攻防研究人员习惯的 cli 方式,缺乏更人性化的图形化交互,普遍以 XX: "YY"、或 XX = "YY"这类格式作为常用的搜索输入语法基础,有的高级语法还需要在语句中加入如"&&"、"||"类的管道符连接,这些输入语法对于普通的新用户难以学习、记忆和使用。

(2) 不同厂商设计的搜索框查询语法有较大的区别,甚至在赋值符号是冒号还是等号这些细节都有所不同,从而给使用者造成了很多认知障碍。

(3) 在搜索的首页设计上,有些系统一味追求界面设计简洁,而没有给不熟悉的用户更多提示,导致大部分新用户因为无法看懂界面而无法使用,严重影响到新用户的接受度。

总之,当前网络空间测绘系统这类搜索框方式的使用交互设计,本质上是基于攻防研究者这些高阶用户的思维模式和习惯而制作的,缺乏从防护方的普通用户或者安全监督管理人员角度思考设计的用户交互。从设计风格上来说,更多地在于追求简洁、高冷、科技的设计风格,而将许多小白用户拒之门外。

这种带有自身意识的设计并没有从更广泛的用户角度考虑,可能不是恰当的产品规划思路,也影响了系统在更大领域内的推广。具体表现在国内的网络空间测绘始终是在小圈子用户范围内比较火热,而在广大的网络安全用户范围内缺少使用。

虽然通过设计 favicon 图标关联搜索,对近期关注热点搜索词界面上推荐直接点击等功能,可以降低系统的使用门槛。然而 favicon 只适用于 Web 应用,热点搜索和关联热词都有很大的局限性,还不能做到用户只需要鼠标点击,无需键盘输入语法就能任意使用系统,搜索到自己需要的查询结果这样的效果。

如何在现有 favicon 等方式的基础上增加更多的点击交互性,或者考虑不以搜索框,而以更友好的图形

化界面作为缺省的系统交互方式，都是需要从业者深入思考的问题。

3.2 与当前安全管理体系兼容度不足的问题

从广大的政企用户角度出发，网络安全工作不仅只是技术范畴，而是结合了安全治理、安全管理、安全运营、安全技术架构和安全业务的综合体系。新的理念的出现，要么需要与现有的安全管理体系相适应，要么需要改进安全管理体系以融合新的技术产品。当前网络空间测绘系统的应用，主要局限在网络安全攻防技术领域，除了部分攻防演习管理体系中，将网络攻击暴露面管理作为必须的环节，很少有防护方的管理体系将其纳入到日常的固定流程之中，也缺乏有效的安全运营。例如，很多企业用户的演练方案中，往往只把测绘暴露面放在准备阶段，将其作为一年一度演练的一次性任务，即使演练成功，也没有在后续的日常安全运营工作中将其作为一个持续性的工作环节，导致仍然有安全事件在演练结束后出现。网络空间测绘系统对现有安全管理体系的意义，主要体现在以下两个方面。

(1) 加强了现有安全管理体系中响应和分析环节的能力。传统的网络安全体系仅仅局限于单台设备或局部网络的风险评估和分析；网络空间测绘提供了一种全局的视角和数据，大大加强了现有网络安全管理体系这方面的能力。但这样也就代表着网络安全测绘系统在规划、设计、开发和实施中必须考虑和现有安全管理体系兼容的问题。在当前的应用环境中，往往空间测绘系统只能作为资产数据的可视化展示工程，无法真正对安全管理体系中重要环节的能力进行加强，也很难融入其中。

(2) 扩展了现有安全管理体系的事前预警能力。也就意味着在应用这类系统中，首先需要对现有的安全管理体系进行更新。需要从治理、管理方面进行新的规划，加强组织、岗位、人员、流程、考核、标准等方面的设计，来构建全新的安全管理体系。但现有厂商无法帮助用户做到这一点，而用户由于缺乏足够的了解也无法自行开发更新安全管理体系，导致无法实现预期效果。

3.3 数据深入分析不足的问题

在当前的网络空间测绘应用模式中，主流系统对于数据分析主要从 4 个维度展开，一是结合用户社区和公开收集到的漏洞数据进行风险感知；二是结合厂商和产品数据进行专题发掘；三是对漏洞感知数据可以进行周期性的挖掘，进而关联其他网络安全事件或威胁情报数据，可以做部分动态的数据分析；四是对用户的搜索数据进行关联分析，以获得更多热点分析数据。图 5 为网络安全领域测绘数据分析应用思路。

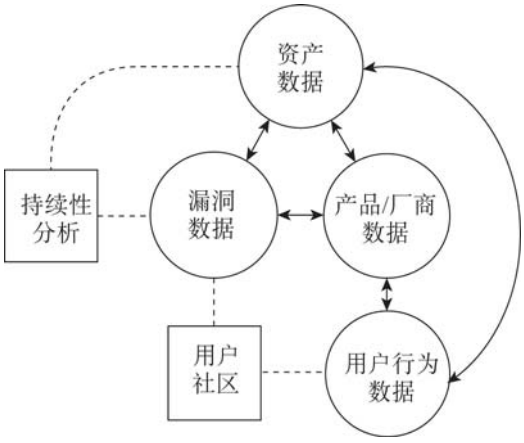

图 5 网络安全领域测绘数据分析应用思路

当前的数据分析应用仅仅局限在网络安全领域的攻防信息搜集领域，对测绘数据的分析和关联，则局限在以资产设备为核心，关联相关的漏洞信息，以及部分 IP 地理经纬度信息。这样的数据分析方向无法充分发挥网络空间测绘在构建网络空间地图，全面展示网络空间信息要素的价值。

网络空间由多个不同的但相互关联的层组成，每个层都捕获了该域上的重要特征和行为。例如，物理层由地理特征和物理网络组件组成，逻辑网络层主要描述静止、运动或物理层内使用的数据，社会角色层包括相互交互的实体以及其他两个层的数字表示。每层实体都分别映射，并具有不同程度的有效性。物理层的表示得益于数十年来在其他的战争领域使用的地理空间信息系统(GIS)的成熟。其他层具有零散的解决方案，可以映射网络、社交互动和其他有限的数据集。然而，当前没有覆盖多层网络空间并充分捕获层内和层间相互作用的整体映射。

网络安全应用上的一个问题表现在：在网络空间测绘数据分析中，攻防背景的技术人员往往关注于资产的属性和关联，缺乏对网的认识和研究，以及对网络的刻画和建模能力，也很难实现端网关联映射技术的

跟踪和研究。

如何能够将网络空间多层多源数据汇入,实现大数据融合分析; 如何能够实现对安全事件信息和动态数据流向的建模和表达,进而构建多层面知识图谱,实现人—网—地的多层建模和关联; 这些都是从业者需要认真思考的问题。

3.4 测绘数据面向可视及可视分析能力不足的问题

网络空间测绘的可视化表达和数据可视化分析是当前应用模式中最为薄弱的一个环节。

系统厂商应用的方向,一方面偏重于攻防对抗的漏洞分析需求,另一方面缺乏对可视化表达和分析的理论研究和数据积累。因此,导致有数据的不懂安全,懂安全的不懂展示,懂展示的没有数据,这样的现象也就导致了测绘展现无法实现理想的效果。

由于上述原因,现有的主流网络空间测绘系统或者网络资源搜索引擎只能对资产数据和漏洞影响做简单的地理关联展示,这些关联展示基本上都是基于公网 IP 的经纬度坐标数据,甚至有些系统由于缺乏地理坐标数据,只能依靠 IP 归属信息做一些国家或省市级别上宏观统计的关联展示。

这些展示基本上都是以“地图+炮”的形式来提供给用户观看,而无法做更多的业务应用。这一现状导致了大部分的网络安全态势系统实际上存在着业务和展示两张皮、无法融合使用,甚至统计数据下钻也没有的情况,不能在可视化地图上实现指挥管理,更没有在地图上可视化分析的能力。

网络空间是不同于地理空间的一个新的独立空间,因此对网络空间的建模和展示需要考虑三个步骤: 一是对社会层、应用层、网络层、设备层、地理层等多层次的信息要素进行建模和定义; 二是建立这些层面信息的复杂关联关系和坐标映射系统; 三是通过业务场景驱动,实现多维信息的全息展示和可视化分析和交互。这些都是需要从业者重视并思考的。

多层映射将突出显示网络空间内在的复杂交互,并允许用户可视化其良性或其他影响。映射不仅考虑到地理特征、网络节点和数据,还考虑到在地理特征、网络节点和数据上操作的角色,从而实现对更加复杂的网络空间运营的规划和执行。图 6 为多层信息可视化思路。

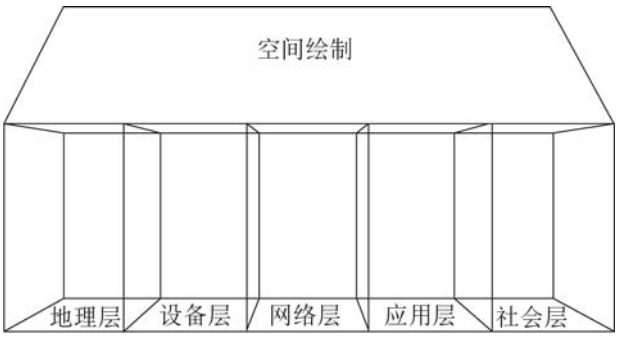

图 6 多层信息可视化思路

4 测绘在网络安全领域应用的改进建议

通过以上分析不难看出,网络空间测绘在网络安全领域的应用,虽然可能已经走在别的领域的前列,但整体上来说,还是处于起步阶段,甚至是起步阶段的初级阶段。

网络空间测绘是数字孪生时代的一项基础技术,也是未来网络安全体系的基础设施之一。所以作为基础设施的定位来看待网络安全领域的应用模式,实际上现有主流测绘系统或引擎的应用是有一些局限性和思路偏差的。主要表现在: 重于强调攻防对抗中的资产和弱点发现,忽视了数据分析和可视化的复杂应用; 重于服务高阶技术能力的用户,无形中拉高了普通用户的使用门槛; 重于强调技术解决问题,忽视了用户的管理需求; 重于将网络空间测绘系统视为一个“菜刀”式的工具,而忽略了很多用户需要真正有业务价值的结果。这些应用上表现出来的问题,导致了目前网络空间测绘应用仅仅局限在小部分网络安全行业的用户群体,而无法在更大规模的网络安全领域内普及应用。对于这些问题,给出了以下建议。

4.1 关注“北向”需求: 扩展网络空间测绘能力的应用边界

既要关注网络安全“南向”需求,也要关注“北向”需求。南向主要指技术和攻防方向,北向主要指治理和管理方向。从用户群体上看,要在攻防技术人员之外更多地考虑安全管理人员的工作需要; 从产品业务逻辑上看,要摆脱工具化思维,将业务需要的结果通过系统使用交付出来; 从产品交互设计上看,要增加点击,降低语句输入操作门槛,甚至重新设计整体用户图形化交付方式,摆脱搜索框模式,而以真正的地图形式与用户交互。

4.2 建设面向典型业务的网络空间全息测绘地图

全息测绘的理念是数据分析×(叠加绘制 + 时空建模) = 全息测绘。在数据分析部分,要重点考虑人、网、地多层数据的融合分析;在叠加绘制部分,不但要考虑 IP 与地理地图的坐标映射,还要考虑社会层、应用层、网络层、设备层、地理层等多个层面的复杂交互映射,并且以地理坐标、IP 坐标、AS 坐标、DNS 坐标等多种坐标体系展示网络空间的多维全息地图,展示方式除了最为接受的地图形式,还可以考虑希尔伯特曲线(Hilbert Curve)构造的二维 IP 坐标系空间展示、社会组织关系图展示以及基于 DNS 关系图展示等多种方式;在时空建模部分,要引入地理信息方向时空建模的理论研究,广泛考虑面向时空变化特征的逻辑时空建模和基于事件的时空建模等方法[8],从而更准确地表达安全事件,进而推动业务和可视化分析能力的加强。图 7 为希尔伯特曲线。

4.3 加强网络空间测绘应用的速度和测绘维度

未来网络空间安全的焦点在于对资源的争夺,网络空间资源的重要组成因素包括网络空间基础资源和其中的人类活动,因此只要人类活动存在,网络空间攻防对抗就不会摧毁网络空间,而只会导致资源控制权的变化。随着网络空间测绘的应用普及,对于网络空间测绘自身的要求也会越来越高。网络空间测绘自身的对抗,测绘能力与其否定层面的反测绘,以及否定之否定层面的对反测绘的对抗,都对测绘技术的实现效率和数据维度提出了更高的要求。

在这种网络空间资源争夺构成的网络安全场景中,对于网络空间测绘的快速反应能力和数据维度需求越来越高:不但要能够看见、看清,还要能够及时看清。只要够快,就找不到破解克制它的方法。这种思路要求规划者在考虑应用方向的时候,要站在人工智能代入、提高自动化和易用性等方面考虑产品功能和可视交互设计等,以减少时间成本的无谓损耗。另一方面要求系统提供更多维度,更准确地关联数据和知识,便于用户迅速理解、分析以及做出决断和动作,提升整体反应速度,及时争夺和掌握资源控制权。

5 结束语

相信随着从业者的不断努力,特别是网络空间测绘应用的不断研究和实践,网络空间测绘技术应用将

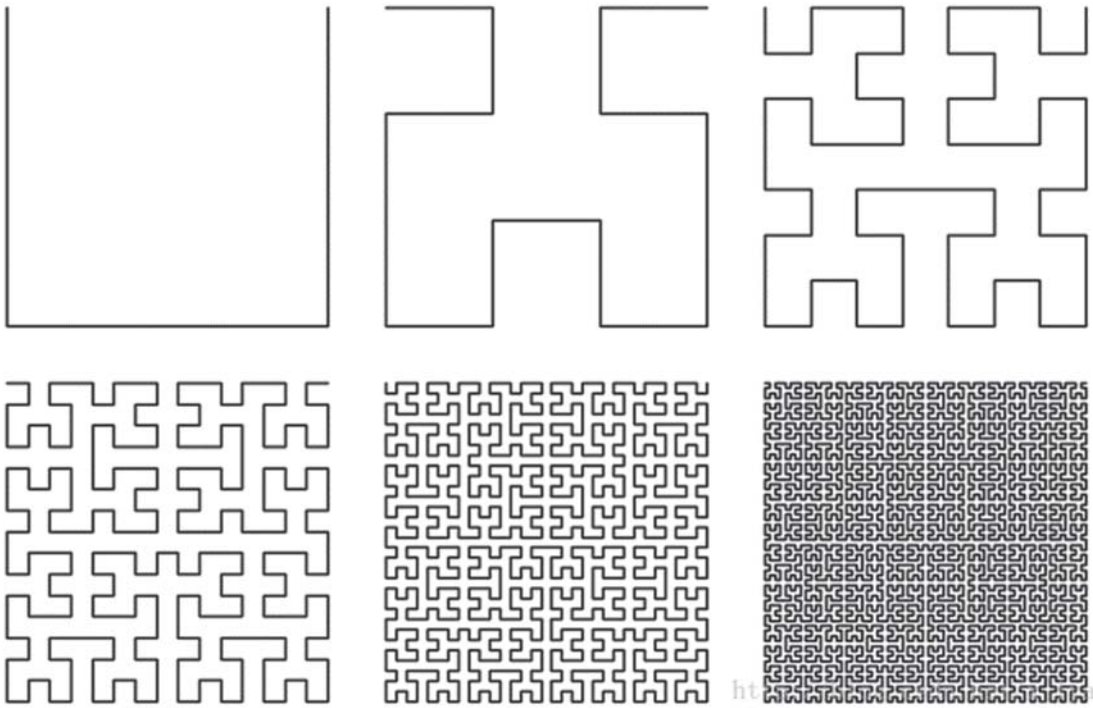

图 7 希尔伯特曲线

成为未来连接虚拟网络空间和现实物理世界的桥梁，为国家安全保障、社会健康发展、数字经济建设和人民幸福生活作出全面的贡献。

参考文献

[1] 高春东，郭启全，江东，等. 网络空间地理学的理论基础与技术路径[J]. 地理学报，2019，74(9)：5-18.

[2] 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.

[3] 沈逸，江天骄. 网络空间的攻防平衡与网络威慑的构建[J]. 世界经济与政治，2018(2)：49-70+157.

[4] DustinW. 网络空间测绘在网络国防中的重大意义和作用[EB/OL]. (2019-01-03)[2021-05-20]. https://www.secrss.com/articles/7551.

[5] CarnaBotnet. Internet census 2012[EB/OL]. 2012[2021-05-17]. https://internetcensus2012.github.io/InternetCensus2012/paper.html.

[6] admin. 基于无状态的极速扫描技术[EB/OL]. 2014[2021-05-17]. http://www.91ri.org/10800.html.

[7] w7ay@知道创宇404实验室. 从Masscan，Zmap源码分析到开发实践[EB/OL]. (2019-10-12)[2021-05-17]. https://paper.seebug.org/1052/.

[8] 李旭晖，刘洋. 时空数据建模方法研究综述[J]. 现代图书情报技术，2019，3(3)：1-13.

作者简介:

陈庆　360集团网络空间测绘产品高级经理，长期从事网络安全、网络空间测绘等方面的研究及产品研发工作

李晗　360集团未来安全研究院资深专家，正高级工程师，清华大学博士，多次获得省部级科技进步奖，长期从事网络空间测绘、网络大数据分析、网络安全等方面的业务及研发工作

杜跃进　通信作者。360集团副总裁，首席安全官，未来安全研究院负责人，曾两次获得国家科技进步一等奖，新世纪百千万人才工程国家级人才，全国青年岗位能手，长期从事网络安全战略和技术研究等方面的工作

张义荣　360集团未来安全研究院智库负责人，国防科技大学博士，多次获省部级科技进步奖，长期从事网络安全战略和技术研究等方面的工作

Practice and thinking of cyberspace surveying and mapping technology

CHEN Qing, LI Han, DU Yuejin, ZHANG Yirong

(360 Group, Beijing 100015, China)

Abstract: As the foundation for supporting digital transformation, the digital upgrade and transformation of network security itself is also facing urgent requirements. As an important part of the intersection of cyberspace security and cyberspace geography, cyberspace surveying & mapping technology is also a fundamental technical support for the digital transformation of cybersecurity. Therefore, it has received more and more attention from related industries. The practice of related technologies in the field of network security has included a series of application directions such as asset management, attack surface discovery, automated penetration testing, vulnerability incident response, map-supported operations, situational awareness, and some other related applications, as well as some problems revealed. This article briefly analyzes these typical problems, and finally puts forward some specific suggestions for application directions.

Keywords: cyberspace surveying & mapping; cybersecurity; surveying & mapping defined network

(收稿日期: 2021-06-22)