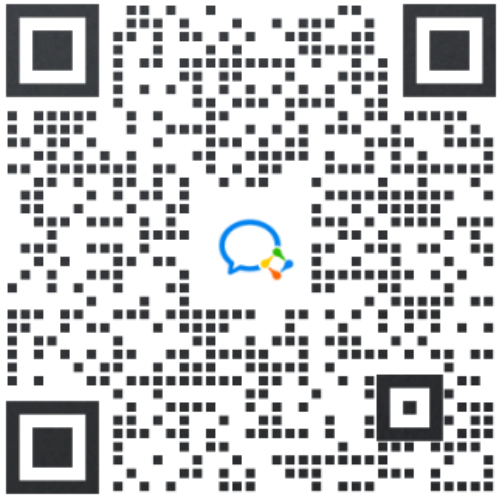
2023

网络空间
地图测绘理论体系白皮书

NSFOCUS

行业报告资源群



微信扫码 长期有效

1. 进群福利：进群即领万份行业研究、管理方案及其他学习资源，直接打包下载
2. 行研精选：每日分享6+份行业精选报告及3个行业主题研究资料
3. 查询报告：行研资料免费帮助查询下载
4. 严禁广告：本群仅限行业报告交流，禁止一切无关信息

NSFOCUS

CONTENTS

01

前言

随着互联网、移动通信、人工智能等技术的快速发展，网络空间已成为人们生活和工作中不可或缺的重要组成部分。网络空间测绘，通过对网络空间中的各种资源进行实时监测和分析，实现对网络空间的态势感知，可以帮助识别网络威胁、检测网络攻击，并及时采取相应的安全防护措施，提高网络安全防御和应急响应的能力，保护网络空间的安全稳定运行。

站在攻击者视角，攻击者往往需要通过网络空间测绘的各种手段搜集攻击目标的各种信息，以找出目标网络的突破口，其中最常用到的就是各种网络空间搜索引擎。它们普遍通过定期、持续地对全网 IP 地址和端口进行扫描，分析其硬件设备以及承载的协议、服务内容等信息，构建一个包含各种资源属性的网络资产数据库。攻击者利用这些数据库，从一个 IP、一个域名开始，逐步扩展深挖，发现攻击目标网络的突破口，完成攻击前置工作。

站在防守方视角，防守者希望对自身在网络空间中暴露给外部可访问的各类资源形成的攻击面进行防护，需要利用网络空间测绘各种手段对自身网络空间资产进行梳理，特别是其中对外的接口，往往需要做更多的防护和检查。攻击面管理被视为向主动安全转变的开始，可以实现尽早洞察安全威胁、采取适当措施来缓解威胁和降低风险的功能。

本文首先通过对传统地图测绘理论和相对主流的网空测绘理论体系进行梳理，介绍了网络空间测绘相关研究进展；其次提出了攻防对抗下的网络空间地图测绘理论体系框架，通过把地图、地志、对抗方针融入到多粒度、多层次、多视图、强动态的网络空间测绘全息地图中，以支撑网络安全攻防对抗场景需求；然后依次介绍基于此理论体系框架在地形图、地志图、战略图上的部分应用实践；最后总结并提出了后续研究展望，引导网络空间测绘未来研究发展方向。

02

网络空间测绘研究背景

本节主要介绍网络空间测绘中的已有相关工作。

2.1 网络空间的起源

网络空间的英文 Cyberspace 一词，最早出现于外国小说 [1][2]，主要表示通过计算机设备进入的信息聚合体空间。在 2001 年美国发布的《保护信息系统的国家计划》中首次提出了网络空间（Cyberspace）的表述 [5]。2008 年美国第 54 号国家安全总统令（NSPD）和第 23 号国土安全总统令（HSPD）中定义 Cyberspace 是信息环境中的一个整体域，由独立且互相依存的信息基础设施和网络组成，包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统 [1][3][4]。后续以色列、意大利、俄罗斯等国家也提出各自定义 [4]，强调网络空间的基础设施和数据内容。2016 年，方滨兴院士初步提出了构成网络空间的四要素定义 [4]，并在 2018 年对其进行了深化解释 [6]。

2.2 传统测绘理论

传统测绘是指研究测定描述地球自然地理要素（地貌）和地表人工设施（地物）形状、大小等属性的理论和技术。它为情报分析提供重要产品 [7]，情报分析产品从低到高可分为描述性（反映事物基本情况）、解释性（阐明事物间因果关系）、评估性（估量事物面临机遇风险）和预测性（预测未来某种 / 多种合乎逻辑的状况 [9]）分析产品四类 [8]。

地图是传统测绘产出的基础情报产品之一，往往具有客观介绍环境基础属性的描述性 [7]。地图可以分为普通地图和专题地图。普通地图主要表示地表自然地理要素和影响行动等人工障碍物设施，如地形图、海图、航空图等等。如图 2.1 左侧地形图，主要表示山地、平原等各种地貌、地物要素；海图主要表示海岸性质、海底地貌、地质等地理要素和航行障碍物、助航设施等航海要素；航空图主要表示与空中航行有关的居住地、道路、水系等地理要素和机场、垂直障碍物等航空要素。

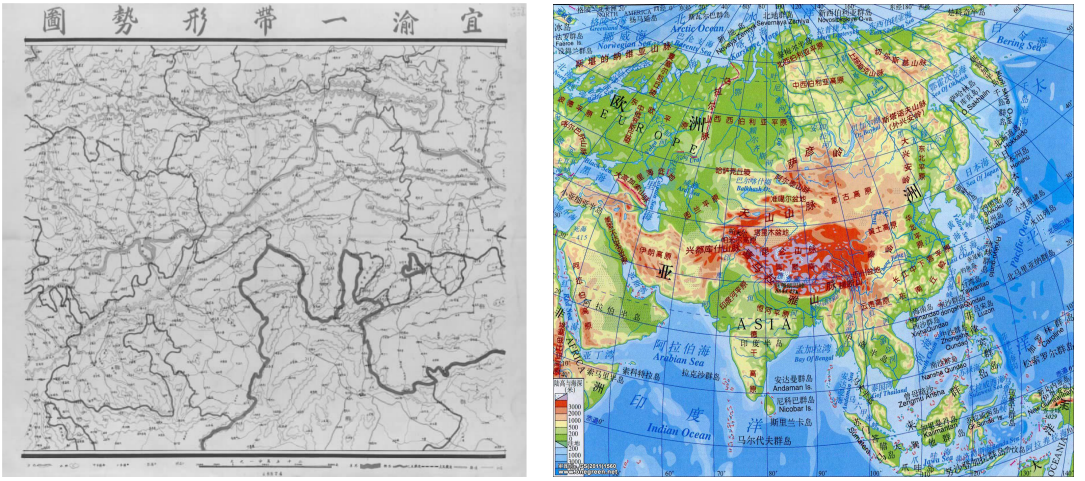


图 2.1　地形图示例 [11]（左）和地貌图示例 [12]（右）

专题地图则是以普通地图为底图，着重表示一个专题内容、用以满足某种特殊需要的地图，如地质图、地貌图、水文图、人口图、交通图、历史图等。如图 2.1 右侧的地貌图 [10]，强调各种不同地貌标志，如平原、丘陵；图 2.2 左侧水文图 [13]，强调降水、蒸发、径流、暴雨、洪水、泥沙、水质、冰情等水文要素特征值的地理分布情况；图 2.2 右侧的交通图 [14]，强调交通运输布局状况。

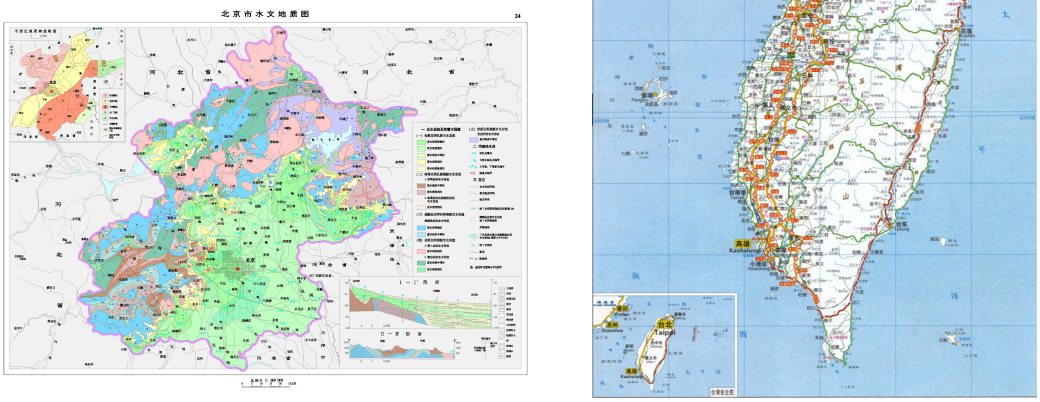


图 2.2　水文图示例：北京市水文图 [13]（左）和交通图示例：中国台湾交通图 [14]（右）

地志则是测绘产出的另一种情报产品。它是指根据需要，对某一地域的自然地理条件和社会因素及其对行动的影响，进行综合记述和评价的一种资料 [15][16]，同时具有描述性、解释性和评估性 [7]。普通地志一般包括环境的组成和价值，自然条件、交通运输、通信、社会情况、经济情况、战略要地及综合评价等 [18]。特种地志则主要表明影响特定行动的自然和人工地理要素，如气象志、江河志等 [18]，强调对特定兵行动的影响评价。

如图 2.3 所示，地志图中不仅包含传统地图，还包含各种注记，其内容范围比传统地图更广，也是制定对抗方针的重要前提 [17]，同时兼具阐述事物因果关系的解释性以及分析基本信息对行动影响的评估性。

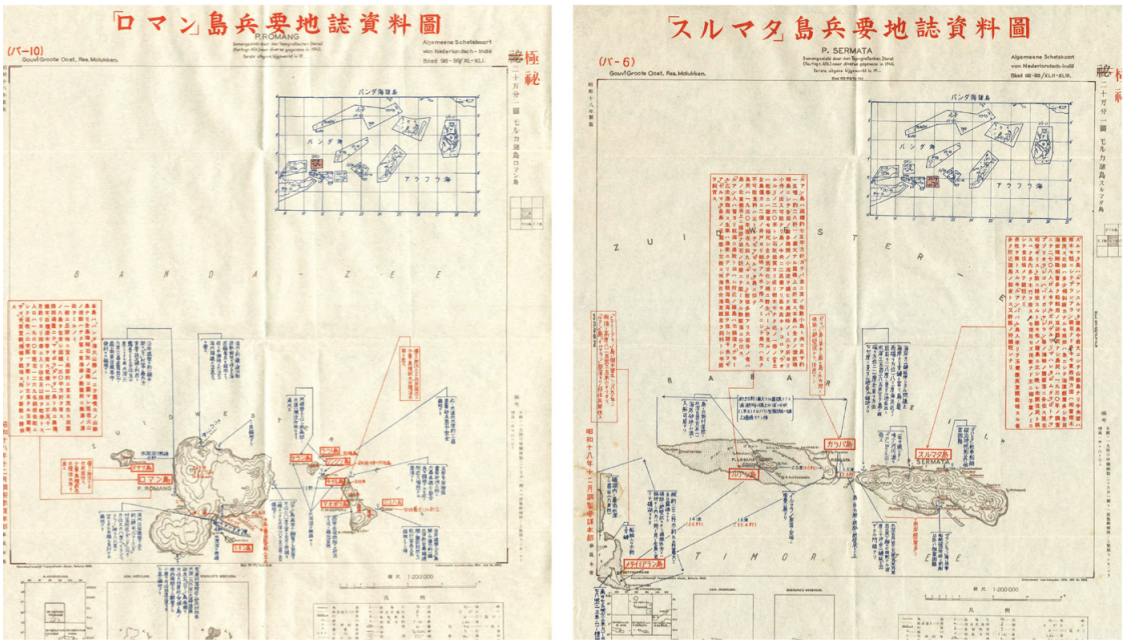


图 2.3　地志图示例：日军罗芒岛与瑟马塔岛屿地志图 [17]

进一步在地志的基础上，需要制定关于行动的基本企图，即对抗方针。它主要包括对抗战略、对抗目标的确定和关于引导对抗胜利发展的重大原则决定 [19]，结合战略战术，如孙子兵法、三十六计等，考虑进攻路线、进攻方式、备选方案等。如图 2.4 所示，展现对抗方针的战役态势图 [22] 具有一定程度预测性。

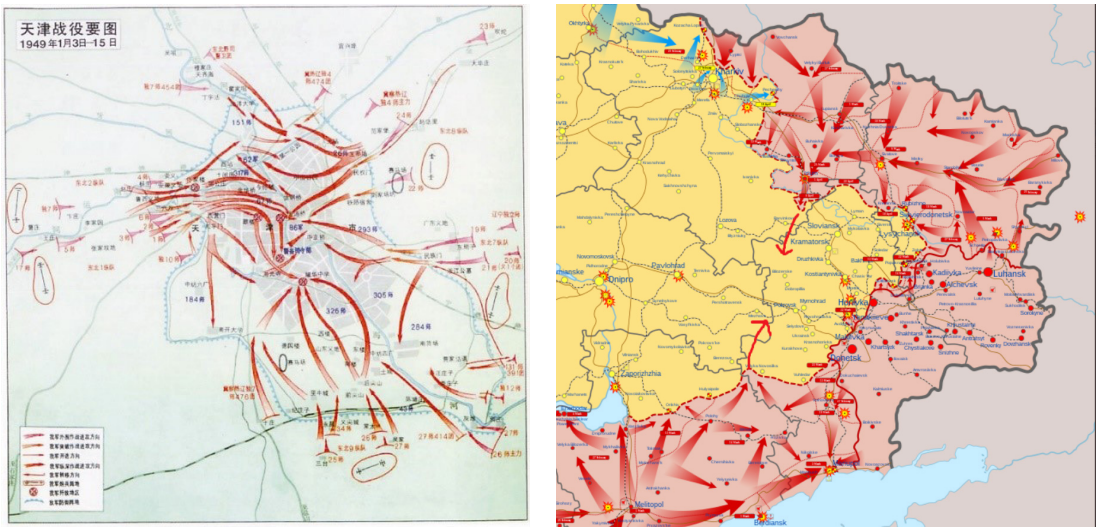


图 2.4　1949 年天津战役 [20] 和 2022 年俄乌战争的顿巴斯之战 [21]

总体而言，传统测绘可以产出地图、地志、对抗方针等递进式包含多种特性的情报分析产品，为对抗行动提供支撑。

2.3 网络空间测绘相关工作

测绘一词虽来源于地理测绘，但网络空间测绘的内涵很早就已出现。2006 年，美国国安局的藏宝图计划，以全网态势感知、侦察和攻击推演为目标，对网络空间进行多层次的信息探测和数据分析，形成大规模情报能力 [23][30]。2012 年，美国国防部国防高级研究计划局启动网络战发展项目“X 计划”，目的是生成网络空间作战态势图、制定作战方案、实施网络作战行动等 [25][26]。2014 年，俄罗斯卡巴斯基实验室发布网络威胁地图，致力于网络活动情况的实时表达 [28][29]。2015 年，美国国土局的 SHINE 计划，主要针对美国本土网络安全态势感知，建立美国本土网络空间关键基础设施信息数据库，监测关键行业网络可达性及安全态势，发现弱点设备和系统 [23][24]。

而国内首次相对系统性地提出“网络空间测绘”一词，是在 2016 年 [25]，解放军信息工程大学罗向阳等人认为构建网络空间地图的技术称为“网络空间测绘”。如图 2.5 左侧所示，他们提出的三层三空间映射的网空测绘理论体系框架，把网络空间测绘分为探测、映射、绘制层，强调把网络空间的实体资源向地理空间映射、虚拟资源向社会空间映射。进一步在 2018 年 [27]，如图 2.5 右侧所示，他们认为应该将网络空间与地理空间信息在一个统一的时空框架下进行无缝融合和数据挖掘与应用，提出了高度结合地理空间的网空测绘理论体系框

架。

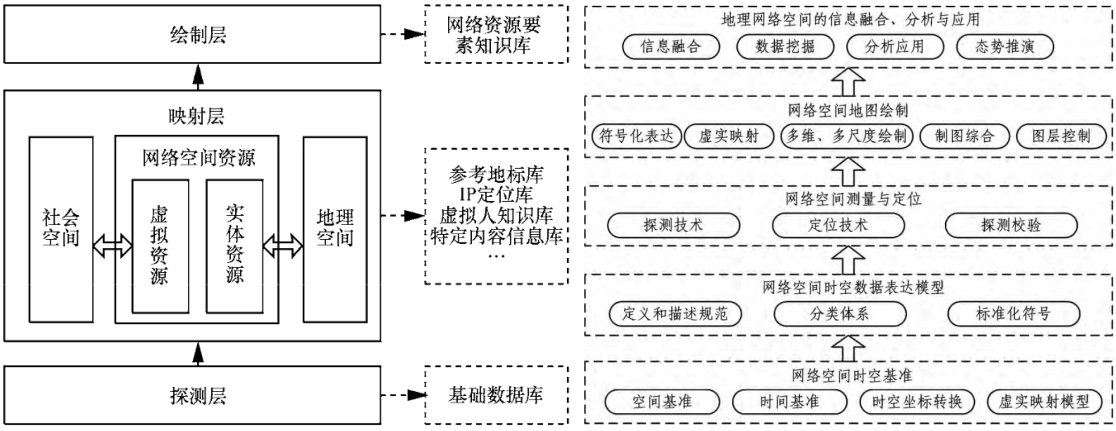


图 2.5　三层三空间映射的网空测绘理论体系框架 [25]（左）

和高度结合地理空间的网空测绘理论体系框架 [27]（右）

同年，信息工程研究所郭莉等人 [23] 将网络空间资源测绘定义为“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”，强调将网络空间、地理空间和社会空间进行相互映射，将虚拟、动态的网络空间资源绘制成一份动态、实时、可靠的网络空间地图。。如图 2.6 所示，他们提出的结合探测 (Detecting)、分析 (Analyzing)、绘制 (Visualizing)、应用 (Applying) 四个步骤循环过程 (DAVALoop) 的网络空间资源测绘体系：通过对各种网络空间实虚资源进行协同探测，获取探测数据；进一步对这些数据进行融合分析和时空映射，形成网络空间资源知识库；在此基础上，通过关联组织和可视表达来构建网络空间资源全息地图；最后，根据不同的场景目标按需应用这一全息地图，利用迭代演进使得测绘能力不断提升。

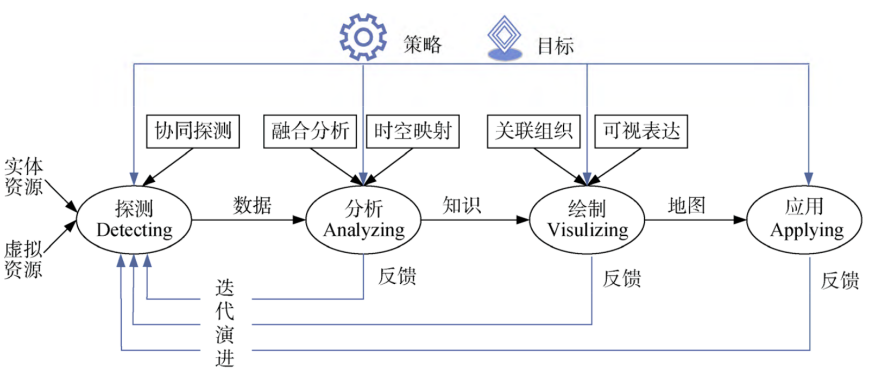


图 2.6　四步骤迭代演进的网空测绘理论体系框架 [23]

由上可知，网络空间测绘目标是绘制网络空间地图的观点被研究者普遍认可，而网络空间测绘的具体内容和相关技术，则根据不同研究者思路有所偏重。不过，大多数网络空间测绘理论体系，都离不开探测、分析、绘制这三个核心模块。下面分这三块进行简要介绍。

全量探测：针对某个具体对象进行探测，其目的是为了获取该对象的原始数据，用于描述该对象的相关属性值，解决该对象是什么的基础问题。而在网络空间测绘的全量探测研究中，主要面临的问题是探测对象的范围以及具体对象的探测技术深度。

映射分析：从更通用的角度上看，在网络空间探测获取到探测对象的基础数据之后，一方面需要针对探测对象作进一步分析处理，把基础探测数据，逐步抽象到类别标签代表的信息、知识，深入回答探测对象是什么、怎么样的问题；另一方面则需要在探测对象之间、各层次空间之间建立关联映射，从不同角度和视图描述探测对象，并基于其关联到的其他对象，刻画探测对象在网络空间的相对位置和作用。

展示绘制：已有网络空间地图制图方法相关研究，根据网络空间及其要素的地理空间相关性可分成地理空间强相关、弱相关、空间无关的三种类型 [33]。地理空间强相关（基于地理信息系统的网络空间可视化模型）表示网络空间中在地理上具有明确空间位置的要素，以地理坐标系为基础，侧重表达网络空间要素的地理属性特征；地理空间弱相关（基于网络拓扑的网络空间可视化模型）：表示网络空间中在地理空间上没有明确位置，或者地理空间位置并不重要，但是要素和要素之间有相对的空间关系；非空间相关（基于隐喻的网络空间可视化模型）：描述的对象主要有两类，一类是网络空间本身；另一类则是网络中与空间无关的要素。同时施群山等人 [34] 提出了基于图论 - 时空对象的网络空间测绘表达模型，将网络空间测绘表达对象概括为网络空间资源、关系、事件 3 类，并结合网络空间资源跨层、要素关联、事件多发、尺度多变的特点，遵循以图论为基础、结合多粒度时空对象模型、强化时间属性 3 个原则。

总而言之，本文提出的攻防对抗下的网络空间地图测绘理论体系，是在前述相关研究背景和工作的基础上，通过对传统测绘理论和相对主流的网空测绘理论体系进行融合扩展，把地图、地志、对抗方针融入到多粒度、多层次、多视图、强动态的网络空间测绘全息地图中，以支撑网络安全攻防对抗场景需求、指引网络空间测绘研究发展方向。

下面进行具体介绍。

03

测绘体系框架概念定义

本节主要介绍本文中定义的网络空间和网络空间测绘，及攻防对抗下的网络空间地图测绘理论体系框架总体思路。

3.1 网络空间

本文中所指的网络空间，基本沿用方滨兴院士的定义 [4][6]，即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与信息通信技术相关的活动。

如图 3.1 所示，组成网络空间运行体系的基本四要素包括载体、资源、主体和操作，即网络空间测绘的对象和范围。

载体是网络空间的软硬件设施，是提供信息通信的系统层面的集合，如互联网、物联网、工控网、移动网、内网、专网等等一系列网络环境。资源是在网络空间中流转的数据内容，包括人类用户及机器用户能够理解、识别和处理的信号状态，如 IP、域名、证书、网站、视频、音频等一系列数据资源。主体是网络用户，包括人类用户以及机器用户。操作是对网络资源的创造、存储、改变、使用、传输、展示等活动，由主体在载体之上对资源产生的一系列活动。

图 3.1　网络空间的基本四要素

3.2 网络空间地图测绘

攻防对抗下的网空地图测绘，是对抗的先行者和指引者。对抗前（常态化）：有助于争取对抗网空环境信息优势；是开展攻防对抗行动的重要依据；为攻防情报搜集提供侦察手段、重要产品。对抗时（特殊化）：提高网空环境态势感知、增加网空环境垂直和水平方向信息流透明度；为网空环境指挥、攻击手段使用以及对抗行动提供精确、实时的网络空间情报；保障指挥员了解对抗区域网空环境形势，掌握网空地形情况；保障执行员在对抗中正确利用网空环境；保障攻击工具准确定位，充分发挥进攻效能。

相对于已有面向通用场景的网络空间测绘研究，本文中攻防对抗下的网络空间地图测绘，结合了传统测绘理论，更注重围绕攻防目标执行对抗意图的测绘。通过网络探测、采集、处理、分析等方式，面向网络空间组成要素及其相关属性进行探测，通过分析标记、关联映射到多空间域（物理域、社会域、信息域、认知域），面向攻防对抗场景，挖掘重点目标和关键路径，

推荐模拟攻防策略和手段，绘制出一张多粒度、多视图、多层次、强动态的网络空间全息地图。它是包含，反映网空要素基本客观情况的描述性、阐明网空要素间影响关系的解释性、估量重点目标风险价值的评估性和模拟未来多种合乎逻辑状况的预测性，于一体的安全产品。

不过，考虑到网络空间全息地图是一个长期愿景，下面介绍的体系框架总体思路中先拆分出了三个步骤依次生成的网络空间地形图、网络空间地志图、网络空间战略图，来逐步逼近想象中的网络空间全息地图。

3.3 体系框架总体思路

攻防对抗下的网络空间地图测绘理论体系，其整体思路借鉴传统测绘理论基础，融合已有网络空间测绘体系，以网络空间全息地图为长期愿景，用于网络空间安全对抗、态势感知等应用场景。

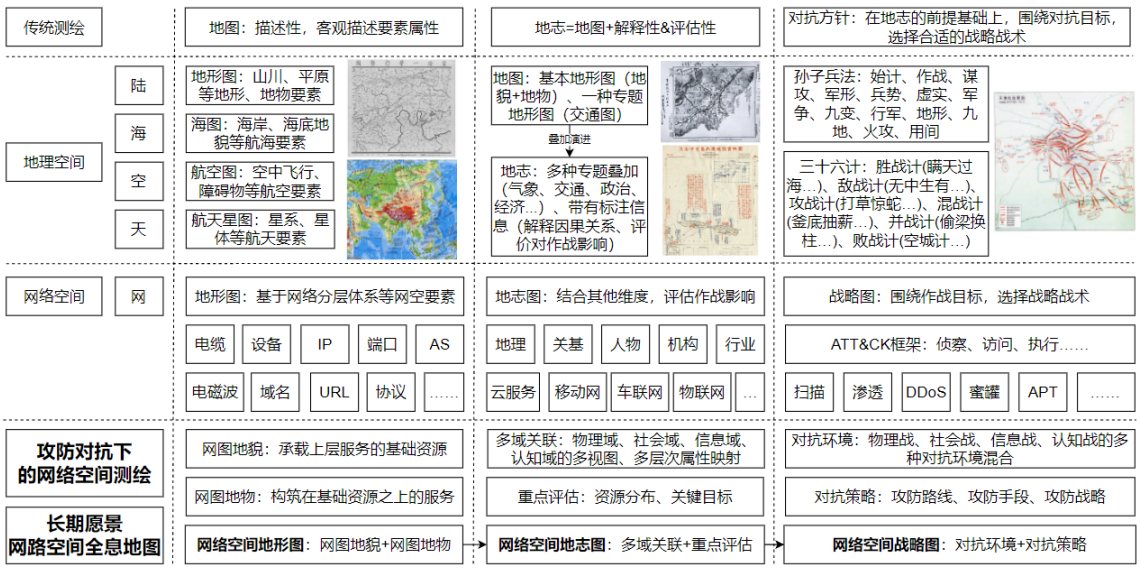


图 3.2　攻防对抗下的网络空间地图测绘理论体系

如图 3.2 上半部分所示，传统测绘主要面向物理空间的陆海空天，分别产出描述客观基本要素的地形图、海图、航空图和航天星图等；在地图基础上，通过叠加多种专题、在图上标注对行动影响的评价，产出地志图；最后在地志基础上，围绕目标选择合适的战略战术，绘制态势图。即通过传统测绘可以产出包括地图、地志、对抗方针等情报分析产品，为对抗提供支撑，保障对抗前常态化和对抗时特殊化的效果。

同理，如图 3.2 下半部分所示，攻防对抗下的网络空间地图测绘，面向网络空间基本要

素可产出网络空间地形图，结合多领域其他维度数据并评估对抗影响可产出网络空间地志图，围绕网络空间重点目标推荐战略战术可产出网络空间战略图，最终形成攻防对抗下的网络空间全息地图。下面分别进行简要介绍。

网络空间地形图的主要测绘对象是基于网络分层体系等基本网空要素，包括电缆、电磁波、设备、IP、AS、端口、协议、域名、URL 等等。具体而言，网络空间地形图等于网图地貌和网图地物的结合。网图地貌是指承载上层服务的网空基础设施和资源，如光缆、设备、IP、拓扑、域名、证书等；网图地物是指构筑在网空基础设施和资源之上的服务及内容，如 Web 网站、视频、CDN、邮件等。同时，面向特定应用场景，网图地貌和网图地物指代的具体对象不同，如分析虚拟机在服务器上的部署情况，则物理服务器是地貌、虚拟机为地物；若分析容器在虚拟机上的部署情况，则虚拟机是地貌、容器是地物。网络空间地形图强调单要素领域的基本客观描述。

网络空间地志图在基本网图地形的基础上，结合其他维度进行多域关联，评估资源分布、关键目标等对攻防对抗的影响。其他维度包括但不限于物理域、社会域、信息域、认知域。物理域主要指地理空间相关的地理定位，用于把网络空间中的对象映射到地理空间；社会域主要指社会空间相关的国家、组织机构、行业、人物等，用于发现网络空间资源的所属关系；信息域主要指带有一定特色的网络环境如云服务、移动网、车联网、物联网等，用于描绘网络空间中对象之间的拓扑关系；认知域主要指用户在网络空间中表现出来的态度、情感和倾向等，用于关联用户行为，为后续决策推荐做准备。而重点评估则是面向攻防对抗行动，挖掘在单个领域、多域映射关联下的重要资源和目标，分析和评估网络空间整体态势。网络空间地志图强调多要素领域关联的解释和评价。

网络空间战略图是在不同对抗环境下的网图地志基础上，围绕对抗目标，选择战略战术。从抽象、顶层的对抗战略上看，其实本质上差距不大，更多的是考虑不同对抗环境下的对抗策略推荐。网络空间对抗往往被称作信息战，但由于网络空间中涉及物理域、社会域、信息域、认知域等多域关联数据，网络空间对抗已不仅仅局限于网络空间，而是多种对抗环境的混合，网络空间测绘不仅直接作用于网络空间中的数据资源，也会作用于物理空间的真实设备、社会空间的组织机构、认知空间的用户倾向等等。而对抗策略则主要包括攻防路线、攻防手段、攻防战略，包括但不限于 ATT&CK 框架的侦查、访问、执行、扫描、渗透、APT 等等。未来的网络空间战略图是构建在知识图谱关联多领域数据之上，依赖智能推荐战略引擎，提供辅助攻防对抗决策推荐的工具。网络空间战略图强调带不同类型攻防手段箭头推荐。

总而言之，攻防对抗下的网络空间地图测绘的长期愿景，就是面向网络空间组成要素及其相关属性进行探测，通过分析标记、关联映射到多空间域，绘制出一张多粒度、多层次、多视图、强动态的网络空间全息地图。

多粒度是指对网空要素属性个数以及属性值精细程度进行基于数据安全角度的分级，做到有限度的公开，从少属性到多属性、粗粒度到细粒度、完全开放到严格保密。如果数据公开分级不合理，导致测绘敏感数据公开，易被攻击者使用，导致安全事件。

多层次是指设备、IP、域名、证书、网站、视频等多种要素图层叠加，对在网络空间中的每一种要素都可以切分出一个层次进行测绘，同时，可以根据基础设施资源和上层服务内容分为网图地貌和网图地物的两大类。

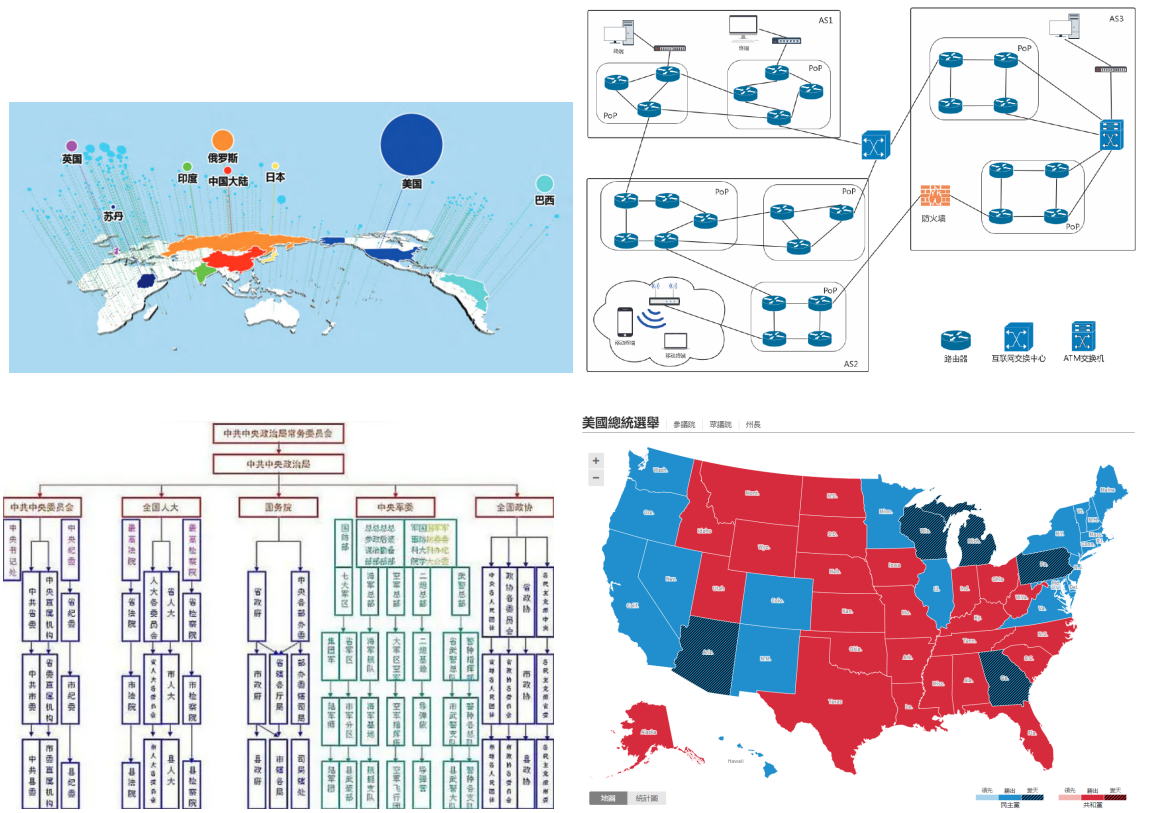


图 3.3　物理域视图示例 [32]（左上）、信息域视图示例 [35]（右上）、社会域视图示例 [36]（左下）和认知域视图示例 [37]（右下）

多视图是指物理域、信息域、社会域、认知域等四域映射多角度观测和展示，如图 3.3 左上，物理域往往是带有明确地理属性、以地理位置为底图的网络实虚资源分布图，这里物理域的

地理属性，是包含陆地、海洋、天空、太空等物理空间，而不仅仅只是图上狭义的陆地地理位置；如图 3.3 右上，信息域往往是与地理信息无关并带有连通属性、强调资源之间通联关系的网络实虚资源关联图；如图 3.3 左下，社会域往往是带有组织机构所属属性、以组织机构架构为底图的网络实虚资源分布 / 关联图；如图 3.3 右下，认知域往往是针对某个事件 / 观点、带有用户认知输出内容，强调特定人群认知倾向的网络实虚用户倾向分布图。

强动态是指实时测绘、动态更新，随时间跟踪地图变化情况。在探测、分析、绘制的过程中得到的任何要素及其相关属性，都带有时间参数；无论是后续的地形图、地志图、战略图，都具有强动态的时间特性，展示网络空间测绘地图的实时动态变化。

04

测绘体系框架应用实践

本节站在测绘最终愿景为构建网络空间全息地图的角度，依次介绍网络空间地形图、网络空间地志图和网络空间战略图的概念定义和设计实现。

4.1 网络空间地形图

如前所述，网络空间地形图的范围包含网图地貌和网图地物，更多地强调单要素领域的基本客观描述。如图 4.1 所示，网图地貌是指承载上层服务的网空基础设施和资源，如光缆、设备、IP、拓扑、域名、证书等；网图地物是指构筑在网空基础设施和资源之上的服务及内容，如 Web 网站、视频、CDN、邮件等。

这里主要是从服务提供的角度，把网络空间资源分为基础设施资源和具体服务内容，分别对应地貌和地物。通常来讲，网空基础设施资源主要指提供关键互联网服务的重要基础资源，包括数据包路由和转发 (IP/ 拓扑)、命名和编号系统 (域名)、安全和身份保护 (证书)、物理传输介质 (电缆) 等及其服务系统和支撑系统的底层基础设施等 [39]。而具体服务内容往往是指在其上运行、操作的各种各样的服务和应用。

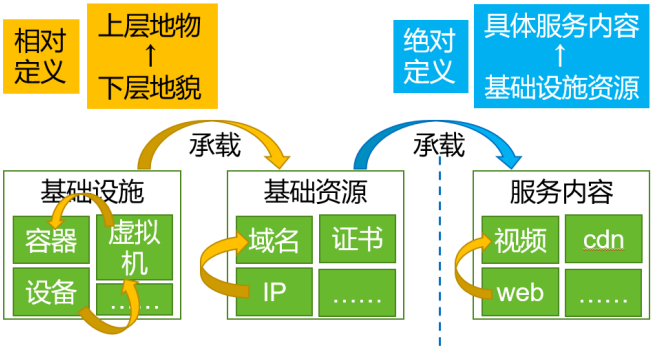


图 4.1　网络空间地形图之地物和地貌示例

同时，如图 4.1 所示，面向具体应用场景，网图地貌和网图地物指代的具体对象可能有所差别，比如在描述构建在硬件设备上的虚拟机时，设备是地貌，虚拟机是地物；而描述虚拟机上承载的容器时，虚拟机又变成地貌，容器成为地物。

网络空间地形图主要涉及到的技术是全量探测。针对某个具体对象进行探测，其目的是为了获取该对象的原始数据，用于描述该对象的相关属性值，解决该对象是什么的基础问题。而在网络空间测绘的全量探测研究中，主要面临的问题是探测对象的范围以及具体对象的探测技术深度。目前在网络测量等研究领域，针对某个具体对象的测量技术发展已经相对成熟。而根据探测方式的不同，可以把探测技术分为主动探测与被动探测两种，这里不过多赘述。

下面以绝对定义下的网络空间地形图基础资源为例，介绍本理论体系在设备资产、域名空间、网络拓扑、数字证书测绘中的应用效果。

设备资产作为网络空间的基础硬件设施，是网络空间基础地形之一。识别 IP 地址背后的设备类型和厂商版本信息，有助于组织机构进行资产管理，同时当发现设备版本漏洞时，及时了解漏洞影响范围，协助安全应急响应。

设备资产测绘系统的主要思路是：首先扫描全网或特定网络的可访问 IP 地址，构建设备资产指纹库，识别对应的设备类型、厂商、版本等信息；其次通过分析标记和运营迭代，持续发现已知、未知的设备资产；同时监测设备的生命周期，发现存活、新增、消亡的设备；最终构建一个面向全网或专网的设备资产动态变化数据库，为特定地域或组织机构提供设备资产地形图。

图 4.2　国内公网暴露摄像头（左）、WAF（中）、路由器（右）设备个数的地理位置分布

设备资产地形图的展示形式主要采用物理域分布视图，如图 4.2 所示，通过扫描并识别公网暴露 IP 地址背后的摄像头、WAF、路由器设备资产，利用 IP 地理定位，展示国内各个省市各类设备资产个数的分布情况，颜色越深表示暴露的设备个数越多。

域名空间标识网络空间资源，是网络空间基础地形之一。它把机器可读的 IP 地址转换成人类可读性高的字符串，在 IP 地址之上提供更多网络服务位置、标识网络服务入口。同时可以通过域名标记、识别资产所属责任主体，有助于映射关联到社会域，为组织机构进行资产风险提示预警。

域名空间测绘系统的主要思路是：首先利用公开的域名排名，获取重点关注的域名种子列表；其次通过获取域名注册信息、解析响应结果等属性，评估域名提供服务的重要性等指标；最后针对重点场景如关键基础设施组织机构、行业的域名进行分析绘制展示。

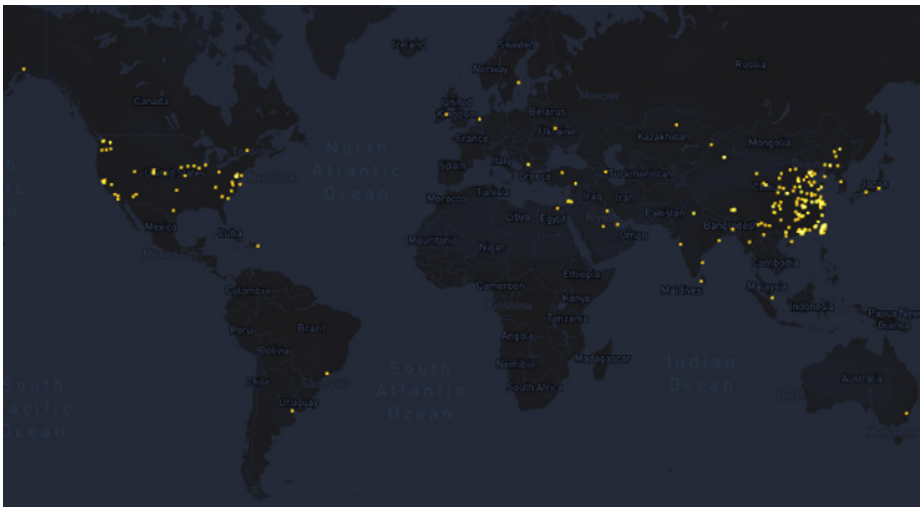


图 4.3　部分中国（含台湾等）政府域名解析 IP 地址的地理位置分布

域名空间地形图的展示形式主要采用物理域和社会域分布视图，如图 4.3 所示，抽取部分特定国家顶级域后缀域名并利用其解析 IP 进行地理位置定位，得到特定国家域名所提供服务在地理位置上的分布。通过对比域名国家顶级域后缀定位的地理位置和域名服务解析 IP 地址的地理位置定位，可发现地理位置定位上的不一致性，特别是在重点国家地区政府机构相关域名上，容易引入服务不可控风险。图 4.3 部分中国（含台湾等）政府域名解析 IP 地址的地理位置分布，基于第三方 IP 地理定位库，发现虽绝大多数域名解析 IP 地址集中在中国境内，但仍有少部分涉及美国等其他位置。一方面可能是 IP 地理定位库定位准确度有限，另一方面因为中国大陆与台湾、香港等域名服务实现特点不同，如部分地区域名解析的 IP 地址可能为云服务商遍布全球的 IP 地址，给各个地区用户提供更好的访问体验。

网络拓扑建立网络连通路径，是网络空间基础地形之一。其体现了网络空间资产本质关联，隐含社会域组织机构信息，通过获取 IP 地址间的网络连通关系，挖掘网络空间资源、乃至组织机构之间的网络连通依赖关系，有助于重点国家地区网络拓扑管理。

网络拓扑测绘系统的主要思路是：首先利用公开数据源和全球网络探针，获取 IP 级、路由器级、PoP 级和 AS 级等基本网络拓扑数据；然后通过构建网络连通图模型，推断各级拓扑相关属性如关键节点、关键路径；最后针对重点场景如特定国家地区、关键基础设施组织机构的网络拓扑进行分析绘制展示。

网络拓扑地形图的展示形式主要结合了物理域、社会域和信息域视图。如图 4.4 左侧所示，通过统计 AS 注册机构所属国家包含的 ASN 个数，展示了排名前 15 的国家地理位置分布。

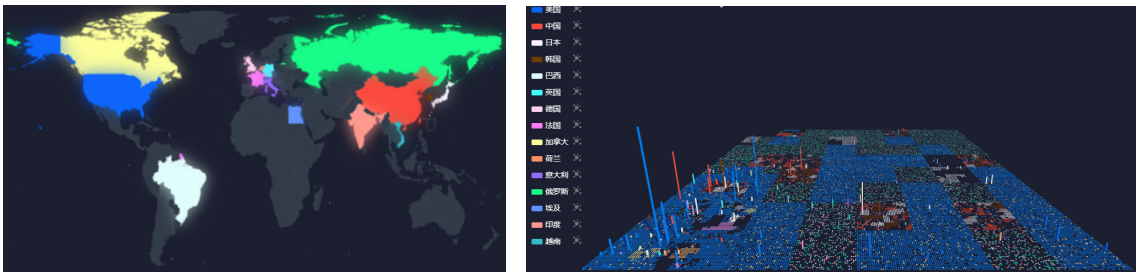


图 4.4　ASN 个数 Top15 国家的地理位置分布图（左）和 ASN/IPv4 网络空间分布图（右）

而图 4.4 右侧针对该 ASN 个数 Top15 国家，全面展示了 ASN 和 IPv4 个数的网络空间分布。参考 [28] 采用 Hilbert 曲线对 ASN 进行一维到二维变换，以三维空间 (x,y,z) 坐标系为基准，其中平面上每个 (x,y) 方块点表示 IPv4 空间的 65536 个 ASN 之一，z 轴表示该 AS 宣告的 IP 地址个数，不同颜色表示不同国家。由图可知，不同国家颜色方块平面面积越大，表示其包含 ASN 个数越多；z 轴直方柱越高，表示该 ASN 宣告的 IP 个数越多；可以清晰看出图中表示俄罗斯的绿色节点虽然 AS 个数多（分布面积广）但 IP 个数少（直方柱扁平）的特点。

如图 4.5 所示，根据不同 AS 商业角色建立 AS 之间的关联图，以宣告 IP 地址个数排序取 Top15 的国家，展示各个国家包含邻居个数 Top20 的 ASN 之间的商业关系。其中不同颜色点表示不同国家，不同颜色边表示商业角色类型；越中间、邻居越多的点表示其连通性越好，且对全球网络拓扑越重要。可以明显看出中间交错节点是对全球连通性影响较大的节点，越边缘的节点则越仅对自身的通联度影响较大，其中韩国、印度还存在完全游离在中心网络之外的 ASN 节点。

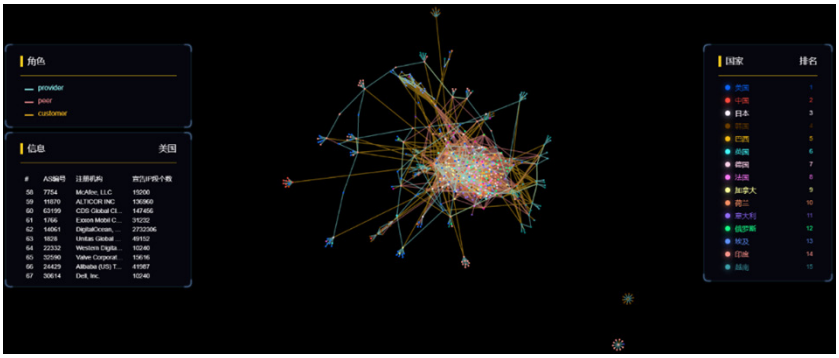


图 4.5　IPv4 个数 Top15 的国家之间 AS 拓扑商业关系图

同时分析图 4.4 右侧和图 4.5，发现图 4.4 右侧中宣告 IP 地址数最多的美国 ASN 749，其在图 4.5 中关联的邻居 ASN 只有 1 个。怀疑主要原因是 ASN 749 的注册机构为美国国防

部网络信息中心（DoD Network Information Center），该 AS 主要用于美国国防部，而图 4.5 中的邻居节点主要指商业关系概念上的邻居，所以虽然 ASN 749 宣告的 IP 地址数量极多，但商业关系邻居个数极少。

数字证书保障可信网络资源，是网络空间基础地形之一。它通过对数据进行加密和签名，以确保数据传输的安全性、完整性和真实性。数字证书广泛应用于互联网通信、电子商务、在线支付、身份认证等领域。基于证书透明度机制、证书授权依赖和共享证书使用，使得证书成为关联网络空间与社会空间的重要纽带。

数字证书测绘系统的主要思路是：首先通过基于 IP、域名和第三方等多源证书种子，迭代获取证书链上所有原始证书文件；然后对证书进行解析、处理、验证等操作，挖掘证书之间、证书颁发机构和颁发对象之间等关联依赖关系；最后针对特定区域和组织机构使用证书关联情况进行绘制展示。

数字证书的展示形式主要结合了社会域和信息域视图。如图 4.6 所示，通过分析数字证书中组织机构间的层级依赖关系，挖掘某地区各层级组织机构使用共享证书的情况，并采用逻辑上的关联关系进行表示，重点关注特定组织机构使用证书资源覆盖面。

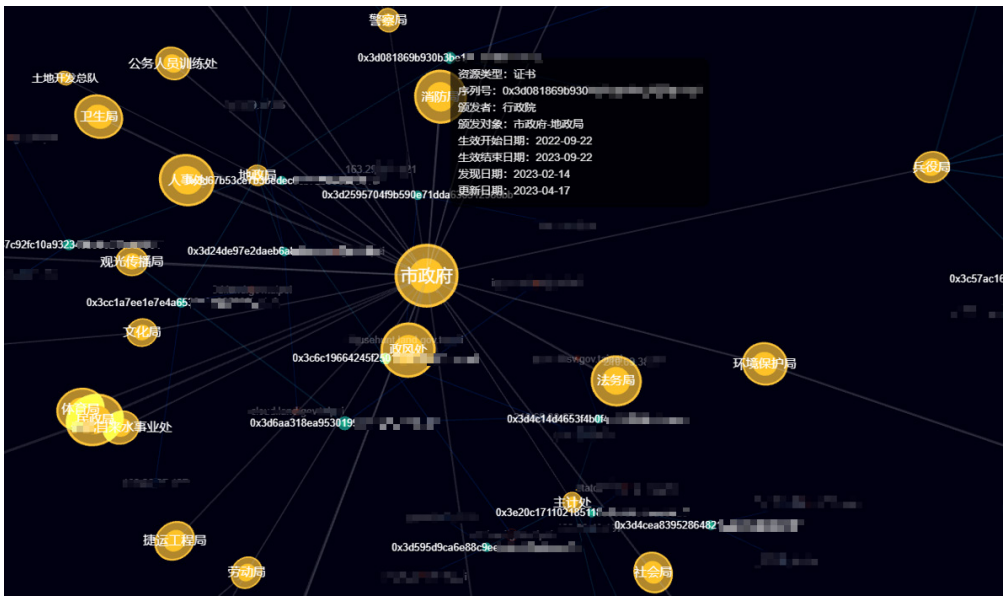


图 4.6　某地区各层级组织机构使用共享证书情况

综上所述，网络空间地形图往往强调单要素领域的基本客观描述，尽可能的展现其全量属性，同时考虑不同类别要素特点以及具体场景需求，选择物理域、社会域、信息域、认知

域等表现形式，为后续网络空间地志图的多域关联和重点评估提供更全量准确的基础数据维度。

4.2 网络空间地志图

网络空间地志图在基本网图地形的基础上，结合其他维度进行多层次和多域关联，评估资源分布、关键目标等对攻防对抗的影响。其他维度包括但不限于物理域、社会域、信息域、认知域。物理域主要指地理空间相关的地理定位，用于把网络空间中的对象映射到地理空间；社会域主要指社会空间相关的国家、组织机构、行业、人物等，用于发现网络空间资源的所属关系；信息域主要指带有一定特色的网络环境如云服务、移动网、车联网、物联网等，用于描绘网络空间中对象之间的拓扑关系；认知域主要指用户在网络空间中表现出来的态度、情感和倾向等，用于关联用户行为，为后续决策推荐做准备。而重点评估则是面向攻防对抗行动，挖掘在单个或多个层次、多域映射关联下的重要资源和目标，分析和评估网络空间整体态势。

网络空间地志图主要涉及到的技术是映射分析。网络空间测绘的探测对象范围，会对后续分析、绘制的思路产生较大的影响。而从更通用的角度上看，在网络空间探测获取到探测对象的基础数据之后，一方面需要针对探测对象作进一步分析处理，把基础探测数据，逐步抽象到类别标签代表的信息、知识，深入回答探测对象是什么、怎么样的问题；另一方面则需要在探测对象之间、各层次空间之间建立关联映射，从不同角度和视图描述探测对象，并基于其关联到的其他对象，刻画探测对象在网络空间的相对位置和作用。

目前通过构建网络空间测绘知识图谱，建立多层次和多域关联，同时基于漏洞风险关联挖掘重点脆弱目标，评估其对攻防对抗的影响。

网络空间测绘的知识图谱本体涉及 IP、域名、证书、设备、软件等 10 多个信息域实体，同时关联物理域的各粒度地理位置、社会域的各层级组织行业、认知域的多源安全事件等等。可以支撑对某个地区、组织机构较为全面的网空资产暴露面概览；同时关联到的漏洞实体，可以支持对其暴露面的风险进行挖掘分析，能够针对性的对某个组织机构进行提示预警。

如图 4.7 所示，表示安全事件关联设备资产、某个地区关联漏洞 IP、相似设备资产共享相同基础设施资源、某地区隐藏漏洞风险资产等知识图谱实体间关联案例。

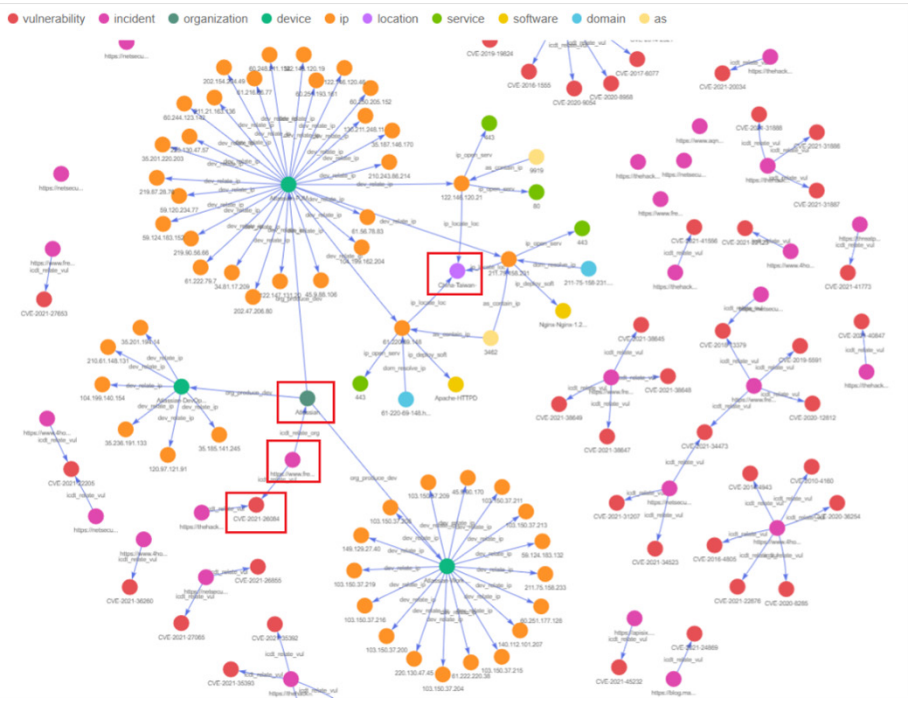


图 4.7　测绘知识图谱多实体之间的多域关联示例

具体而言，下面以挖掘某个地区暴露资产风险为例，介绍网络空间测绘知识图谱的关联分析思路，主要涉及信息域、物理域、社会域的相关实体及关系。

思路一从漏洞出发，考虑已知漏洞是否影响某个地区的某些用户资产。首先通过 198 个已知 CVE 漏洞关联到 17646 个 IP 地址，然后基于 IP 地理定位到该地区的 335 个 IP，之后利用解析到这些 IP 上的 266 个域名数据，识别出使用该域名服务的 27 个组织机构（用户）。思路二从已关联漏洞该地区 IP 出发，利用相似算法推荐后进行验证的方式，挖掘该地区具有已知漏洞的隐藏 IP 地址。首先从思路一该地区关联的 335 个 IP 地址中，基于服务相似性算法推荐出 1135 个可疑 IP 地址，然后利用动态 POC 和第三方知识库验证，发现其中疑似关联已知漏洞的 257 个隐藏 IP 地址。

如图 4.8 所示，表示设备资产识别时的相似资产推荐扩展示例。目前存在大量未知、新兴资产，难以通过已有的资产识别算法进行直接标记识别。为了能够快速为大量未标记设备打上标签，通过基于设备共享基础设施等特征，在待识别设备和已识别标签设备之间建立相似边，实现设备资产识别的相似资产推荐扩展，同时具有可解释性强和展示性强的特点。

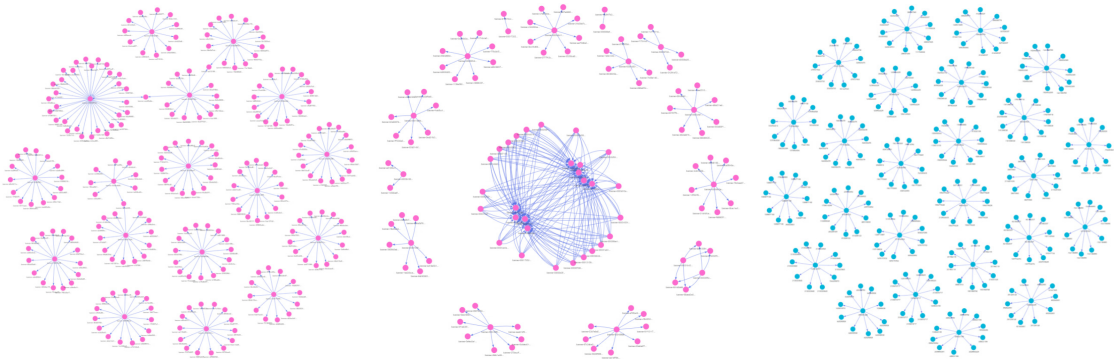


图 4.8　测绘知识图谱内容（左）、结构（中）、图标（右）相似资产推荐示例

网络空间地志图除了需要包含多层次多域关联映射外，还需要包含对网络空间地形图得到的基本描述信息进一步加工分析，评估其中的重点目标，为攻防对抗行动做准备。

下面以重点域名评估为例。面向攻防对抗的应用场景，所谓的重点评估，可以拆解为高重要性和高脆弱性。重要性是指地位高、有价值，如在 Alexa 等排名列表中存在且有较高名次、域名及其服务存活性和活跃性高、域名包含的子域名及其价值重要性高、域名的使用者是关键基础设施涉及的组织机构和行业等。脆弱性是指失效高、有漏洞、易攻击，如域名解析 IP 开放特殊端口可能被攻击、域名解析的 IP 地址关联 CVE 高危漏洞、域名提供的服务存在数据泄露等危险、域名解析依赖高风险域名或 IP 地址等。

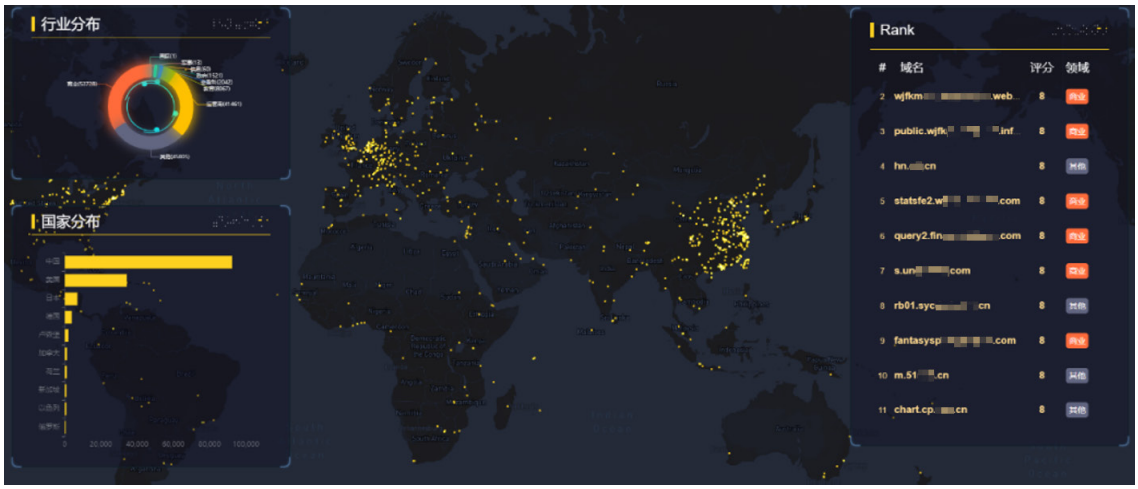


图 4.9　重要国家、行业使用域名风险排名推荐图

如图 4.9 所示，通过提取的 20+ 重要性和安全性评估指标，对 15w+ 域名进行风险评分

计算，并结合物理域、社会域进行展示；左侧考虑域名对应的社会域属性使用者行业、域名注册国家分布统计，右侧对域名按自定义风险评分进行排序。

4.3 网络空间战略图

网络空间战略图是在不同对抗环境下的网图地志基础上，围绕对抗目标，推荐战略战术，展示形式强调带不同攻防手段箭头推荐。网络空间对抗往往涉及物理域、社会域、信息域、认知域等多域关联数据，已不仅仅局限于网络空间，而是多种对抗环境的混合。网络空间测绘不仅直接作用于网络空间中的数据资源，也会作用于物理空间的真实设备、社会空间的组织机构、认知空间的用户倾向等等。而对抗策略则主要包括攻防路线、攻防手段、攻防战略，如 ATT&CK 框架的侦查、访问、执行、扫描、渗透、APT 等等。未来的网络空间战略图是构建在知识图谱关联多领域数据之上，依赖智能推荐战略引擎，提供辅助攻防对抗决策推荐的工具。

网络空间战略图主要涉及的技术是认知推荐，通过结合人工智能等技术，战略图本身需要具有一定程度的认知智能。同时，在地志图映射分析的基础上，需要更进一步面向对抗行动指挥官和执行者，提供辅助对抗行动决策推荐。结合如图 4.10 所示网络杀伤链、ATT&CK 框架 [40] 等攻击手段，推荐具体的攻击路径和步骤，同时能够预测整个战场环境随攻击手段执行的变化情况。考虑到使用战略图的主体不同，战略图作为认知工具也需要设计不同的表达形式。

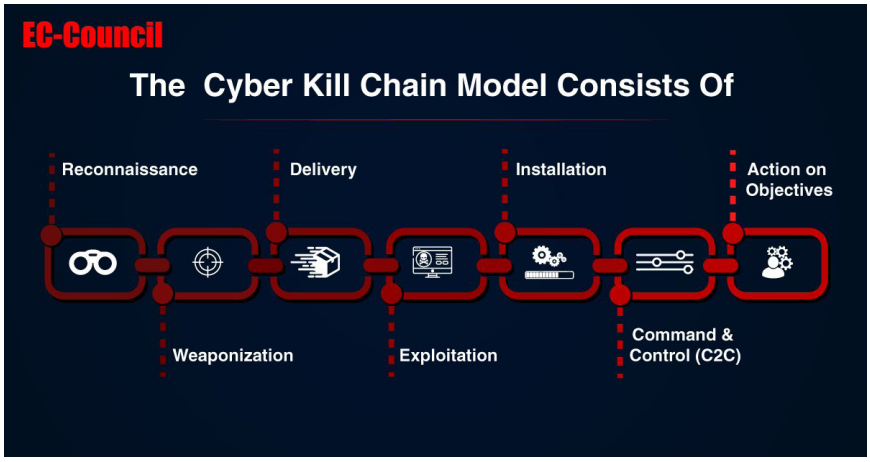


图 4.10　Cyber Kill Chain 模型框架 [38]

05

总结与展望

为了能够引导网络空间测绘相关领域重点研究方向及技术进展，本文通过对传统测绘理论和已有网络空间测绘相关文献的梳理，站在安全的本质——攻防对抗的角度，提出了攻防对抗下的网络空间地图测绘理论体系。通过把地图、地志、对抗方针融入到多粒度、多层次、多视图、强动态的网络空间测绘全息地图中，扩展已有地理空间、社会空间、网络空间的三空间到物理域、社会域、信息域、认知域的四域视图，逐步构建支撑网络安全攻防对抗场景需求的网络空间地形图、地志图和战略图，以逼近网络空间全息地图的长期愿景，同时介绍了在设备资产、域名空间、网络拓扑、数字证书等基础地形测绘和知识图谱多域关联、重点评估上的部分研究进展。后续我们会继续完善本理论体系框架总体思路和具体测绘方向实践案例，支撑网络安全攻防对抗场景需求。

未来，网络空间测绘将面临越来越丰富和复杂的数据源，需要研究多源异构的多模态数据融合，如何将不同源的多模态数据进行整合，实现更全面、更准确的测绘结果；同样，随着机器学习、深度学习、大语言模型等人工智能技术的发展，需要研究对大规模数据的自动处理、分析和挖掘，提高测绘效率和精度，支持更智能化的测绘应用需求；并且，网络空间测绘涉及大量的数据采集、处理和传输，对网络安全和隐私保护也提出了新的挑战，需要在安全和隐私保护方面加强技术研究和应用实践，确保测绘过程中和测绘结果的数据安全和隐私保护得到有效的保障；同时，网络空间是一个动态、复杂的生态系统，网络拓扑结构、网络流量特征等可能随时发生变化，需要实时获取、处理和分析大量的网络数据，并对网络动态性和复杂性做出应对，这对技术算法、数据处理和实时性也提出了更高要求；此外，网络空间测绘不仅要站在测绘制图的视角，也要站在使用网络空间地图的不同用户视角，考虑网络空间地图的表达形式，加强用户认知。

最后，站在网络空间安全的角度，攻防双方是一体两面，攻防博弈也永不停歇。防守方占据先验知识的透明优势，而攻击方占据以点破面的隐蔽优势。网络空间测绘的相关技术，就是在与网络空间反测绘的较量中逐步提升，进一步形成攻防对抗的循环局面。

攻防不止，测绘不休。

参考资料

[1] 张焕国 , 韩文报 , 来学嘉 , 林东岱 , 马建峰 , 李建华 . 网络空间安全综述 [J]. 中国科学 : 信息科学 ,2016,46(02):125-164.

[2] G. William, “Neuromancer,” Translated by Limin Lei and Chu’ an Wen (in Chinese), Shanghai: Shanghai Scientific & Technological Education Publishing House, pp. 7-9, 1999.

[3] 方滨兴 . 从层次角度看网络空间安全技术的覆盖领域 [J]. 网络与信息安全学报 ,2015,1(01):2-7.

[4] 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.

[5] 罗军舟 , 杨明 , 凌振 , 吴文甲 , 顾晓丹 . 网络空间安全体系与关键技术 [J]. 中国科学 : 信息科学 ,2016,46(08):939-968.

[6] 方滨兴 . 定义网络空间安全 [J]. 网络与信息安全学报 ,2018,4(01):1-5.

[7] 袁关伟 , 杨延军 . 论军事测绘在军事情报中的作用 [J]. 情报探索 ,2021(02):129-134.

[8] 高金虎 . 军事情报学 [M]. 江苏人民出版社 : 解放军国际关系学院情报研究丛书 , 201612.285.

[9] 王唯西 . 情报产品概念辨析及基本类型研究 [J]. 竞争情报 ,2021,17(02):11-19.DOI:10.19442/j.cnki.ci.2021.02.004.

[10] https://baike.baidu.com/item/%E5%9C%B0%E8%B2%8C%E5%9B%BE/783242

[11] 李鹏 . 清代民国重庆军事地图叙录 [J]. 军事历史研究 ,2014,28(02):179-188.

[12] http://m.onegreen.net/maps/HTML/23861.html

[13] http://www.geoscience.cn/UploadFiles/2016_10_28/hgm24.JPG

[14] http://m.cgzdl.com/zhongguo/taiwan/3064.html

[15] 赵振南 , 张宏军 . 兵要地志信息系统的关键技术分析 [J]. 计算机工程 ,2004(17):65-67.

[16] 沈克尼． 近代以来日本对中国的地图盗测［J］． 地图，2017(6) : 84 一 93

[17] 沈克尼 . 再说近百年来日本军队对我国兵要地志的研究（下）[J]. 军事史林 ,2021,58(01):70-78.

[18] 邵自升 . 兵要地志的历史发展和军事价值 [J]. 国防 ,1988(07):4-5.

[19] 熊武一、周家法主编．《军事大辞海·上》：长城出版社，2000 年 5 月：第 1578 页

[20] https://www.sgss8.com/tpdq/7424198/2.htm

[21] http://www.xinhuanet.com/mil/2022-04/29/c_1211642262.htm

[22] [11]https://www.zhihu.com/question/50501018

[23] 郭莉 , 曹亚男 , 苏马婧 , 尚燕敏 , 朱宇佳 , 张鹏 , 周川 . 网络空间资源测绘 : 概念与技术 [J]. 信息安全学报 ,2018,3(04):1-14.DOI:10.19363/J.cnki.cn10-1380/tn.2018.07.01.

[24] Grant Tim, On the military geography of cyberspace, Leading Issues in Cyber Warfare and Security: Cyber Warfare and Security, 2:119, 2015

[25] 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.

[26] https://en.wikipedia.org/wiki/Plan_X.

[27] 周杨 , 徐青 , 罗向阳 , 等 . 网络空间测绘的概念及其技术体系的研究 [J]. 计算机科学 , 2018, 45(5): 1-4.

[28] 王继龙 , 庄姝颖 , 缪葱葱 , 安常青 . 网络空间信息系统模型与应用 [J]. 通信学报 ,2020,41(02):74-83.

[29] KSHETRI N. Kaspersky lab: from Russia with anti-virus[J]. Emerald Emerging Markets Case Studies, 2011, 1(3): 1-10.

[30] O. Rashid, I. Mullins, P. Coulton and R. Edwards, “Extending cyberspace: location based games using cellular phones,” Computers in Entertainment, vol. 4, no. 1, 2006.

[31] http://internet-map.net/

[32] 王永 , 李翔 , 任国明 , 等 . 全球网络空间测绘地图研究综述 [J]. 收藏 , 2019, 5.

[33] 李响 , 杨飞 , 王丽娜 , 俞鑫楷 , 费腾 , 江南 . 网络空间地图制图方法研究综述 [J]. 测绘科学技术学报 ,2019,36(06):620-626+631.

[34] 施群山 , 周杨 , 蓝朝桢 , 吕亮 , 胡校飞 , 徐青 . 面向网络空间测绘的图论 - 时空对象表达模型 [J]. 测绘科学 ,2023,48(01):258-268.DOI:10.16251/j.cnki.1009-2307.2023.01.027.

[35] 李雄略 . 互联网 AS 级路径推测技术研究 [D]. 国防科技大学 ,2019.DOI:10.27052/d.cnki.gzjgu.2019.000494.

[36] http://mms2.baidu.com/it/u=940369791,273681518&fm=253&app=138&f=JPEG&fmt=auto&q=75?w=667&h=500

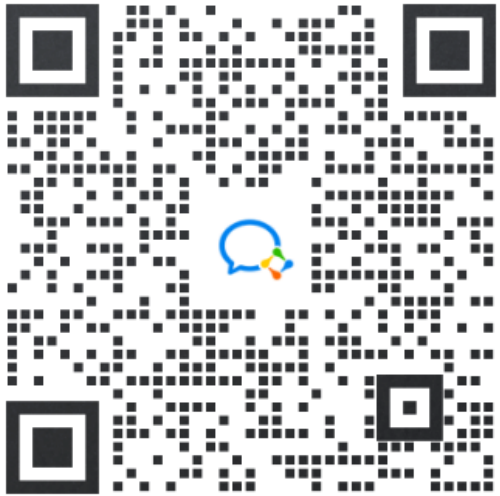
[37] https://graphics.reuters.com/USA-ELECTION/RESULTS-LIVE-US/oakvenxampr/

[38] https://twitter.com/ECCOUNCIL/status/1356464906892107777/photo/1

[39] https://en.wikipedia.org/wiki/Critical_Internet_infrastructure

[40] https://attack.mitre.org/#

行业报告资源群



微信扫码 长期有效

1. 进群福利：进群即领万份行业研究、管理方案及其他学习资源，直接打包下载
2. 行研精选：每日分享6+份行业精选报告及3个行业主题研究资料
3. 查询报告：行研资料免费帮助查询下载
4. 严禁广告：本群仅限行业报告交流，禁止一切无关信息

NSFOCUS

THE EXPERT BEHIND GIANTS

巨人背后的专家

扫描绿盟科技官微二维码
可在手机端直接观看报告电子书