WebRAY 盛邦安全

网络空间的博弈：网络空间反测绘

技术实践

目录

案例：关键目标测绘

100个C段

发现：**7401个IP存活（主动：5600个）**，包含了258个端口，69个服务

4个金融集团

30万IP地址范围，3.09万有效IP地址；8.56万IP+端口

IP地址识别对比	主动识别结果	被动识别结果
IP地址总量	8196	7063
重叠IP地址	5385	5385
特有IP地址	2811	1678

IP+Port识别对比	主动识别结果	被动识别结果
IP+Port总量	15907	48108
重叠IP+Port地址	8316	8316
特有IP+Port地址	7591	39791

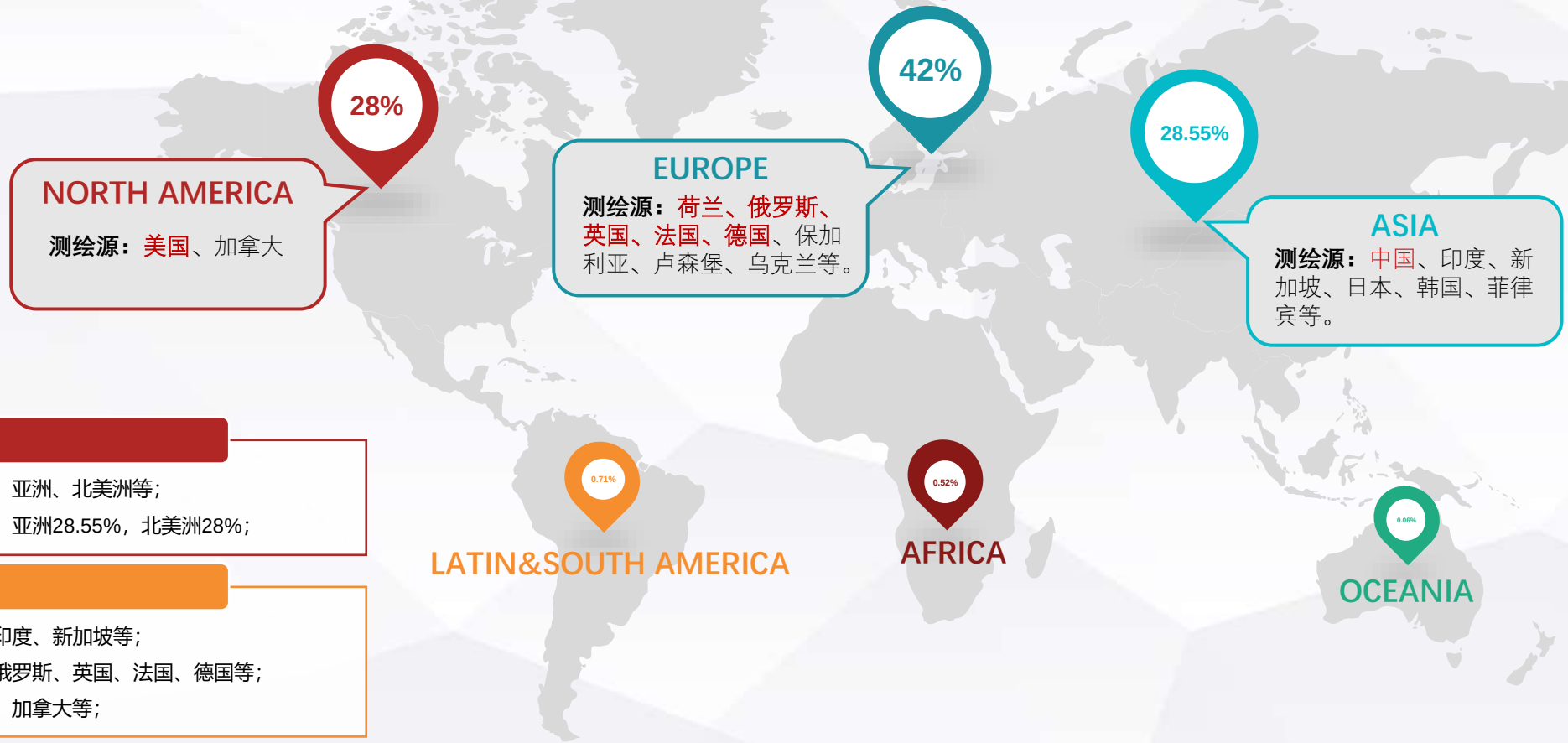
网络空间测绘的现状

全球主流测绘平台76个（2~21天全球测一遍）

单位	类别	描述
美国政府	国外	美国国家安全局的宝藏地图项目，“宝藏地图”倡议旨在提高该国的情报能力。收集数层网络空间(地理、物理、逻辑和社会)的数据并进行快速分析由此产生了建立情报的大规模能力。它还向其“五眼联盟”(包括美国、英国、加拿大、澳大利亚和新西兰)提供情报支助。（美国国安局）
	国外	X项目打算提高美国军方的网络能力，现场地图了辅助生成作战计划，它还鼓励有效完成网络业务活动。在美，DRARAPA说:为了提供视觉视角和总体用户经验,如果网络战在未来变得非常普遍因此，网络战必须像iPhone(iPhone)那样简单。（美国军方）
	国外	SHINE倡议利用网络空间扫描引擎检查美国重要基础设施网络资源的安全情况。 这是该国历史上首次使用互联网为土著网络空间地址清单提供安全意识。此外,根据工业控制系统网络应急茶，ICSCERT定期向其所有人提供安全通知。保护重要基础设施网络。由密歇根大学与Rapid7合作创建的Cansys搜索引擎平台更广为人知。它不仅扫描了IPv4的地址。还审查了域名和证书。（来源美国国土安全部）
国外厂商	国外	Censys、Shodan、BinaryEdge、Arbor、Bitsight、AdScore以及各研究机构测绘平台，旨在对网络空间暴露面进行测绘和分析。
国内机构	国内	中国科学技术科学院、中国电子技术网络信息安全有限公司、中国电子大学和青华大学等，已经完成了对网络特有资源探测和网路探测等技术的重大技术批准。
国内厂商	国内	国内商用平台数量众多
开源工具		测绘主流工具：Nmap、 Masscan、 Zmap、Zgrab、 Nuclei。

测绘来源主要区域

全球网络空间测绘源区域分布



全球测绘

- 主要来源欧洲、亚洲、北美洲等；
- 欧洲占比42%，亚洲28.55%，北美洲28%；

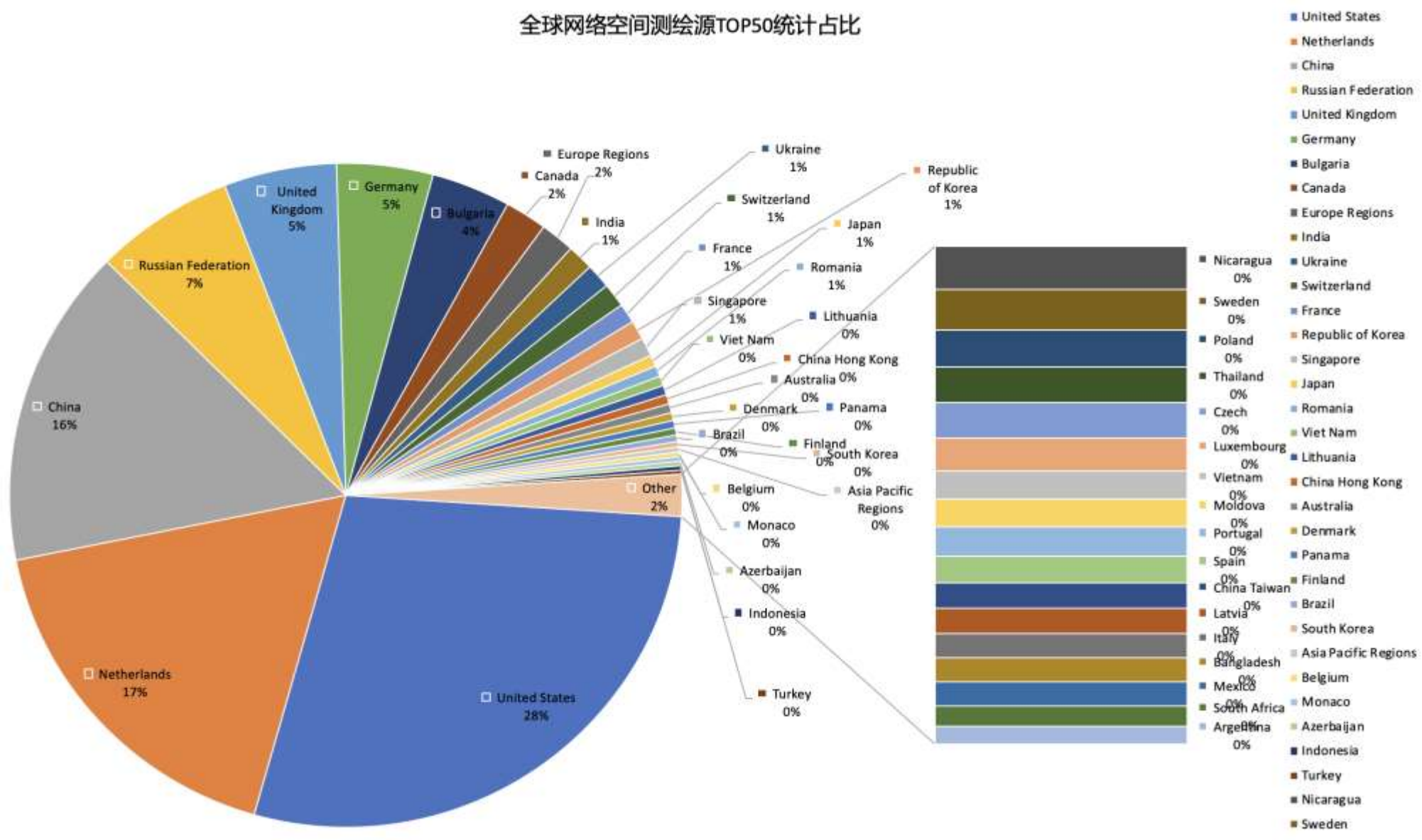
区域TOP

- 亚洲：中国、印度、新加坡等；
- 欧洲：荷兰、俄罗斯、英国、法国、德国等；
- 北美洲：美国、加拿大等；

国家TOP

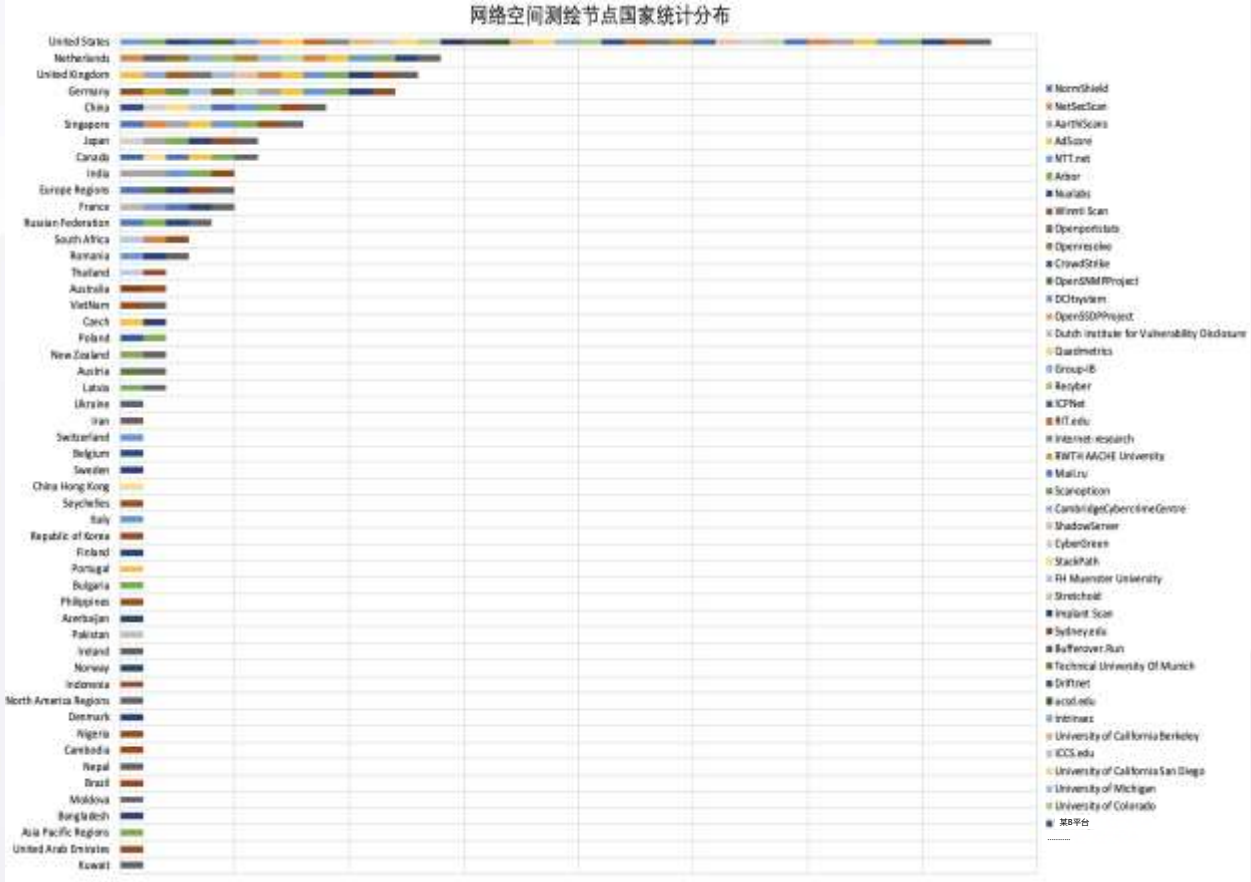
- 美国、荷兰、中国、俄罗斯等；

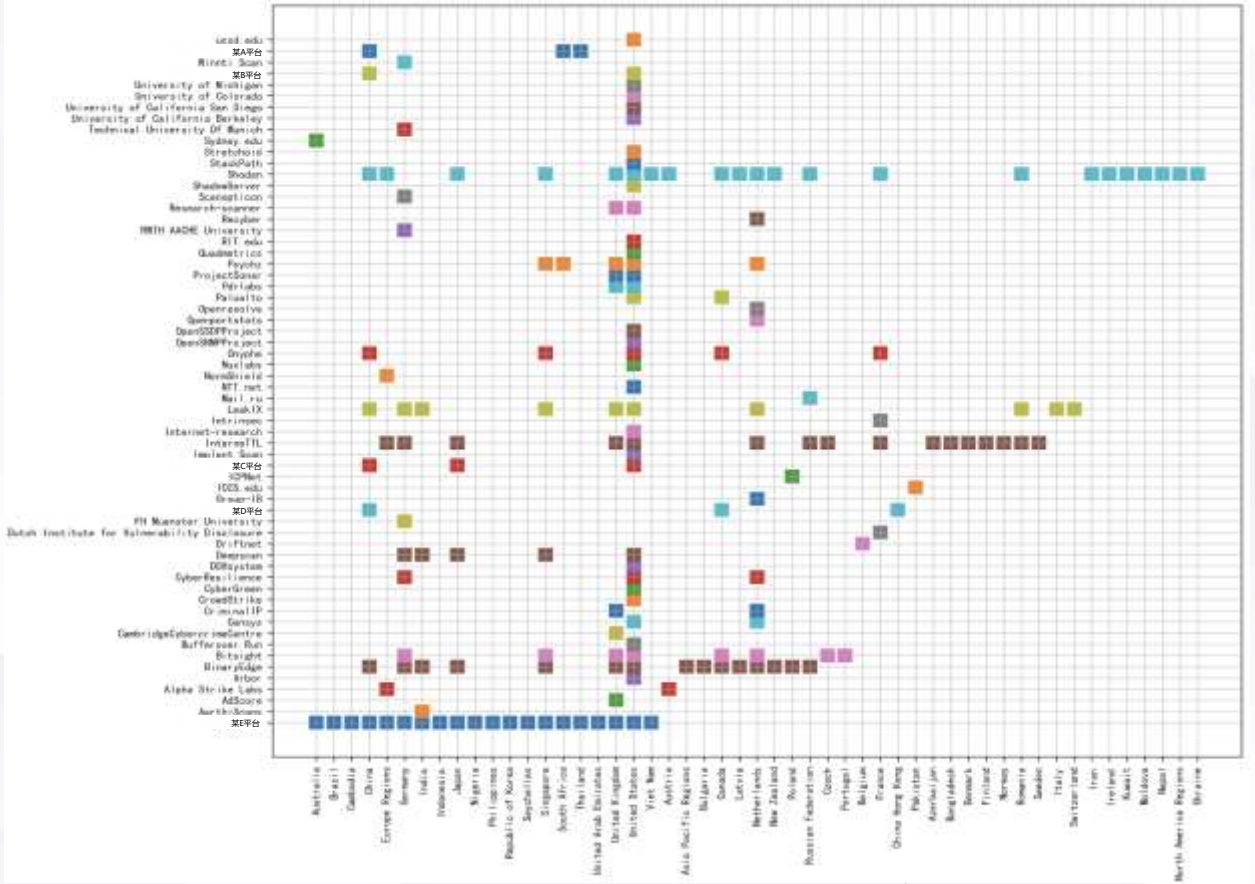
测绘来源重点国家



国家	Sum of 数量
United States	2665074
Netherlands	1640601
China	1461223
Russian Federation	630674
United Kingdom	509243
Germany	434564
Bulgaria	357076
Canada	190447
Europe Regions	154516
India	118527
Ukraine	112417
Switzerland	109484
France	89743
Republic of Korea	86671
Singapore	85457
Japan	52597
Romania	49114
Viet Nam	44497
Lithuania	43893
China Hong Kong	42823
Australia	40797
Denmark	35875
Panama	34845
Finland	32560
Brazil	29898
South Korea	23507
Asia Pacific Regions	23202
Belgium	21294
Monaco	21281
Azerbaijan	20528
Indonesia	19762
Turkey	17734
Nicaragua	16780
Sweden	15278
Poland	14261
Thailand	13957
Czech	13415
Luxembourg	12850
Vietnam	10917
Moldova	10805
Portugal	10788
Spain	10554
China Taiwan	9928
Latvia	9693
Italy	9350
Bangladesh	9195
Mexico	9131
South Africa	7687
Argentina	7110

全球测绘源分布





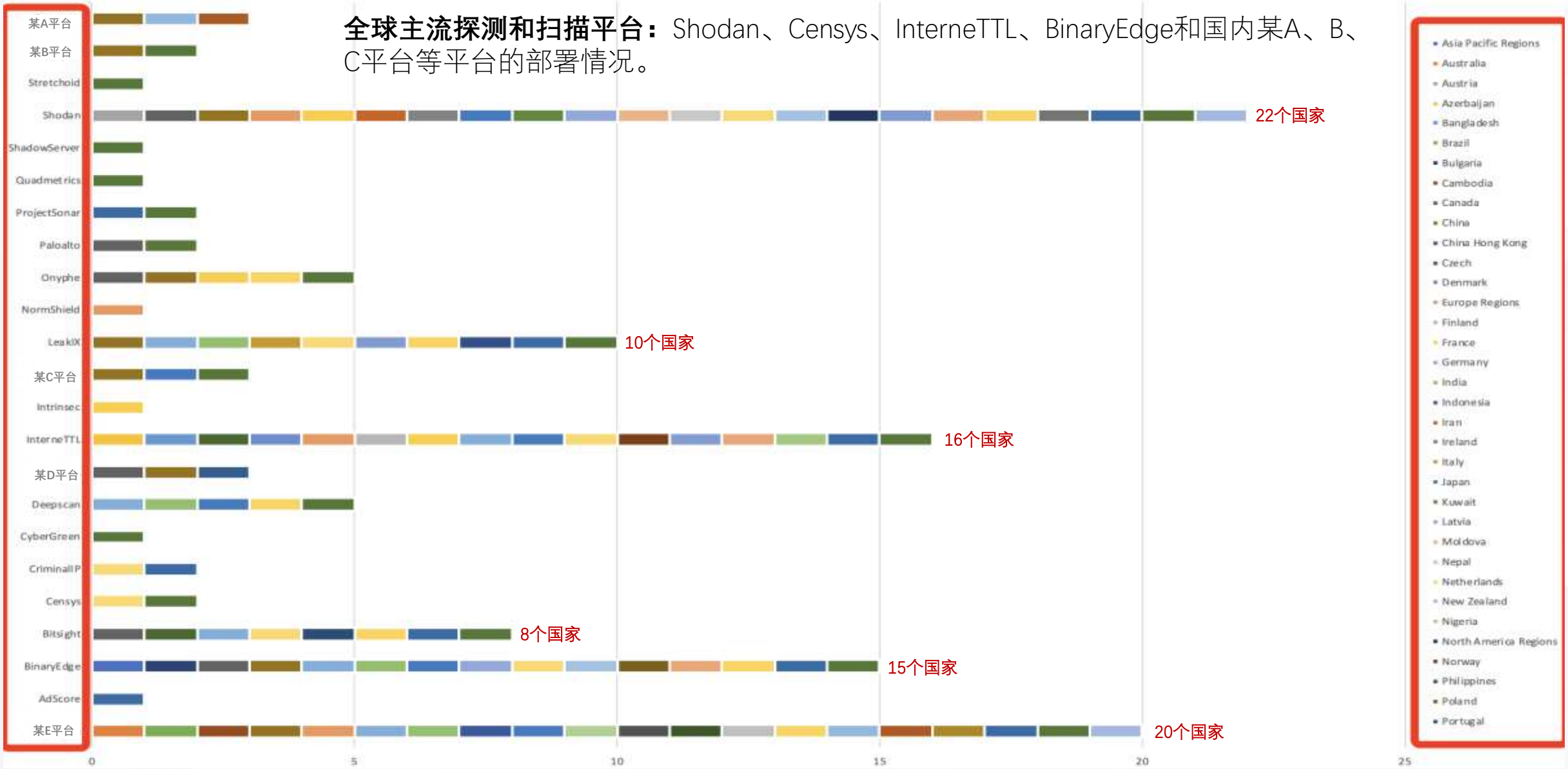
全球测绘源平台在51+个国家存在部署探测和扫描节点

全球测绘源平台当前部署最多的已有22个国家

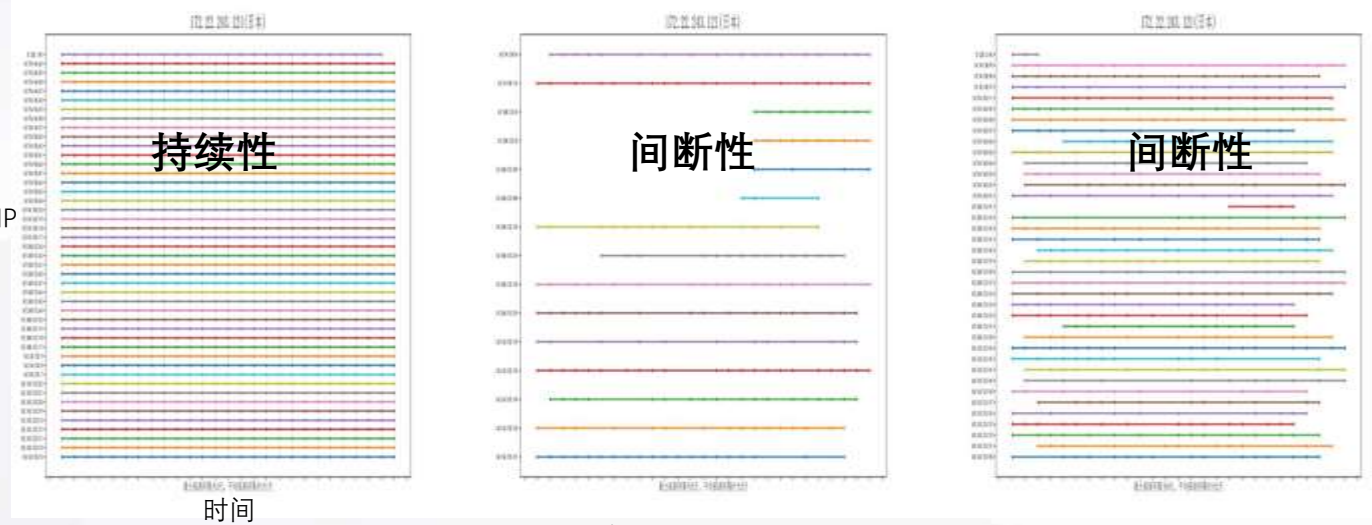
共79+个探测和扫描平台持续不断地对互联网进行扫描和探测

测绘来源主流平台

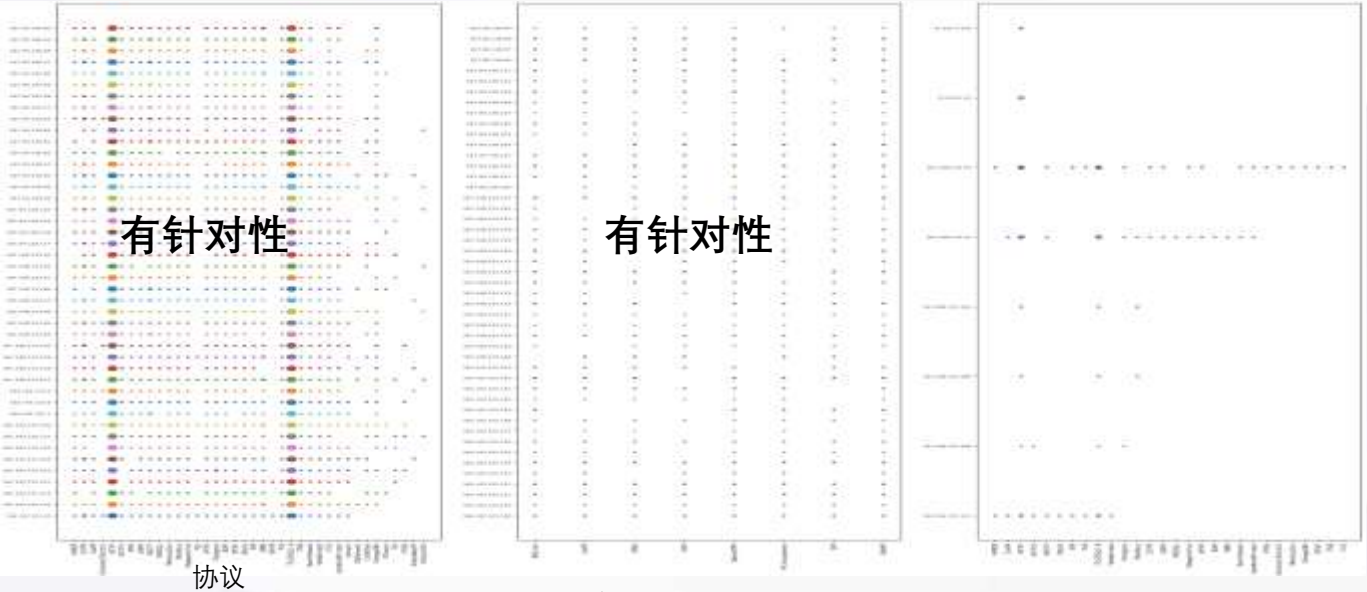
全球主流探测和扫描平台：Shodan、Censys、InterneTTL、BinaryEdge和国内某A、B、C平台等平台的部署情况。



目标测绘的方式方法



如图1



如图2

如图1和2，以Censys为例，不同的IP职能不同，网络化探测和扫描的方式也不同。具体表现为：探测扫描更具有针对性；更多样化和离散化；方式方法更趋于精细化。

探测扫描更具有针对性

- 将目标划分为不同集合，有针对性扫描；
- 时间上趋于持续性、间断性和偶发性。

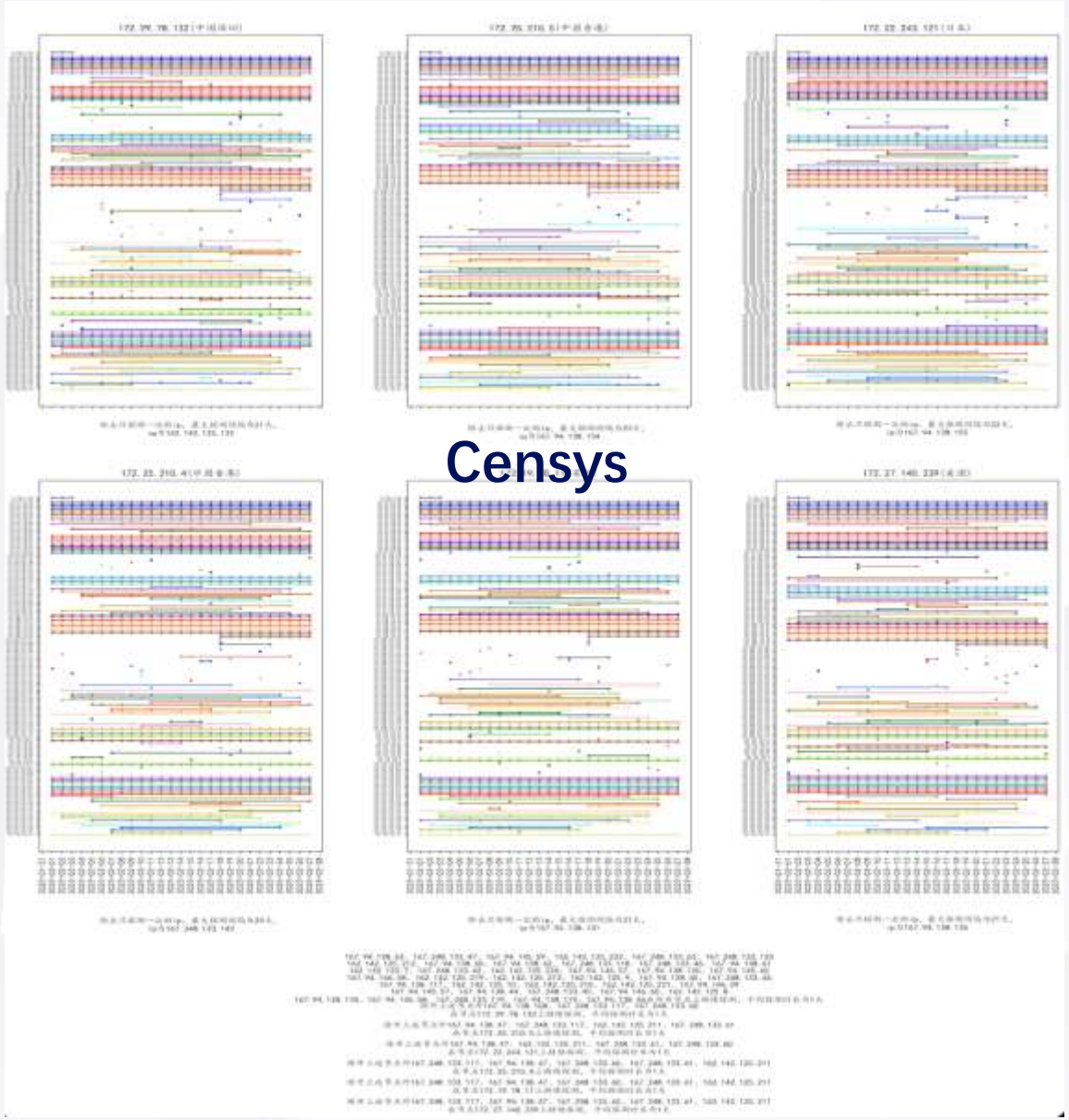
更多样化和更离散化

- 具有不同的探测扫描策略，更多样化；
- 短时间内针对同网段或同网络目标更离散化。

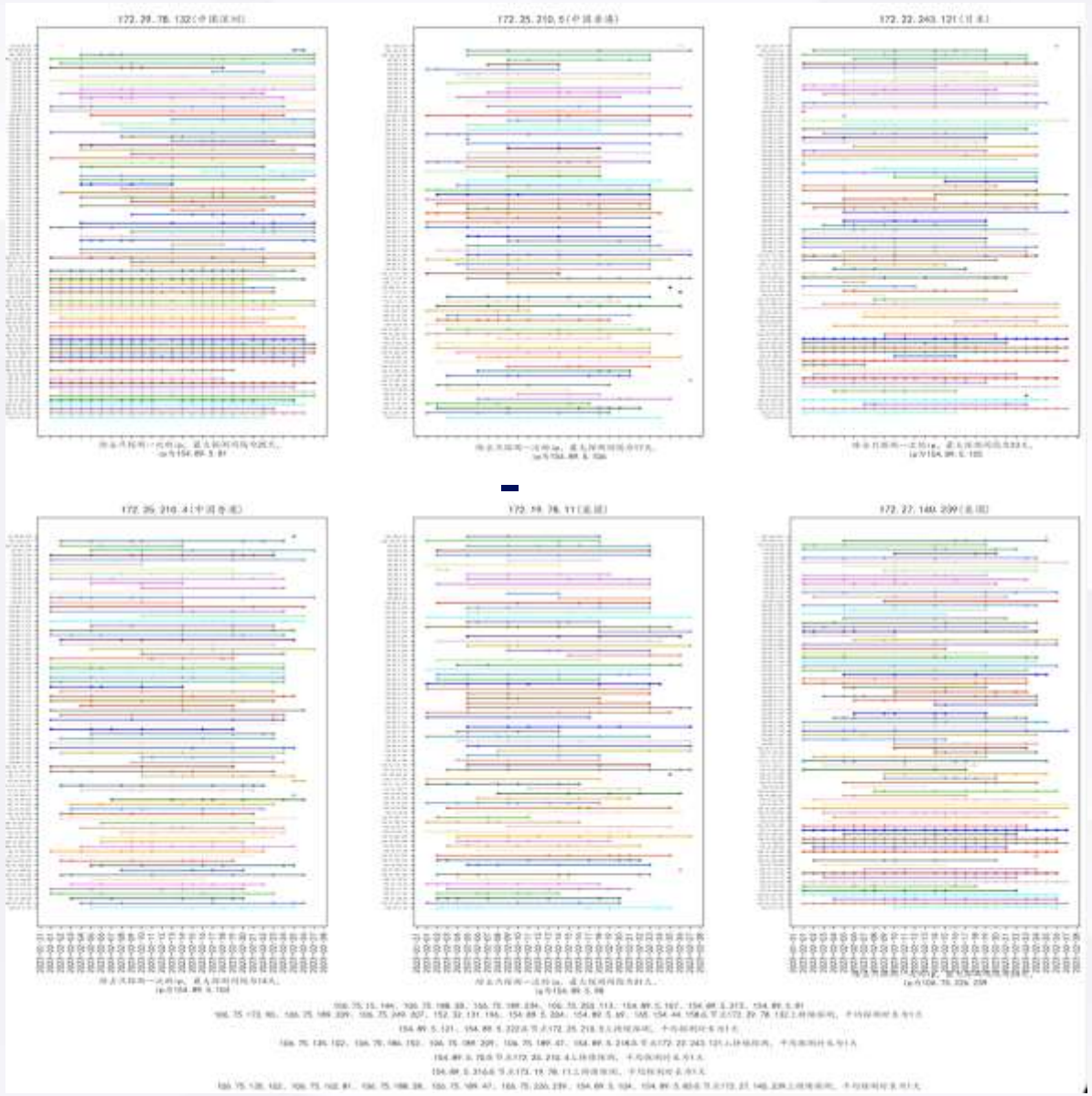
方式方法更趋于精细化

- 探测内容去特征化；
- 探测方法更精细。

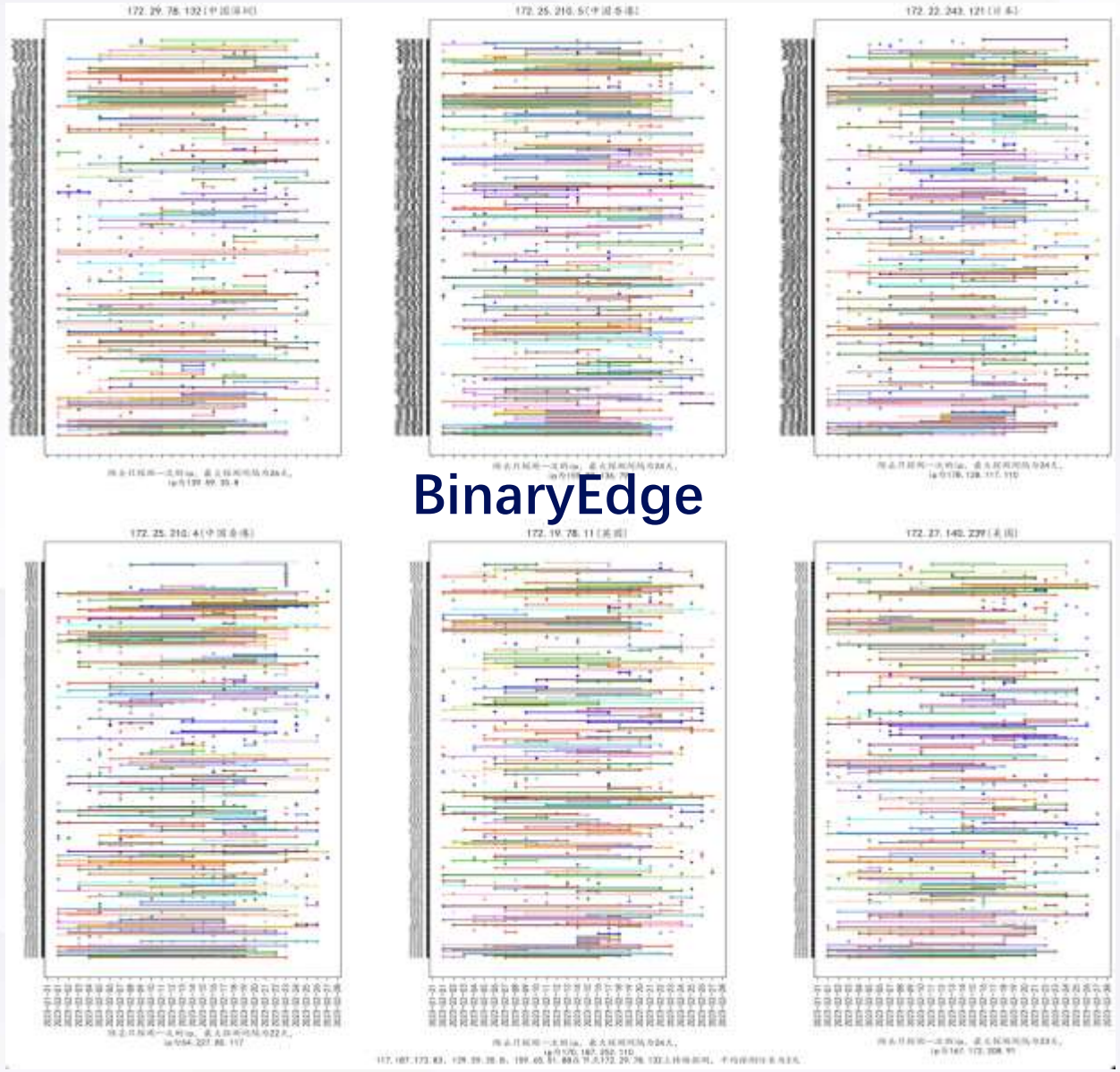
主流测绘平台的测绘行为



主流测绘平台的测绘行为



BinaryEdge

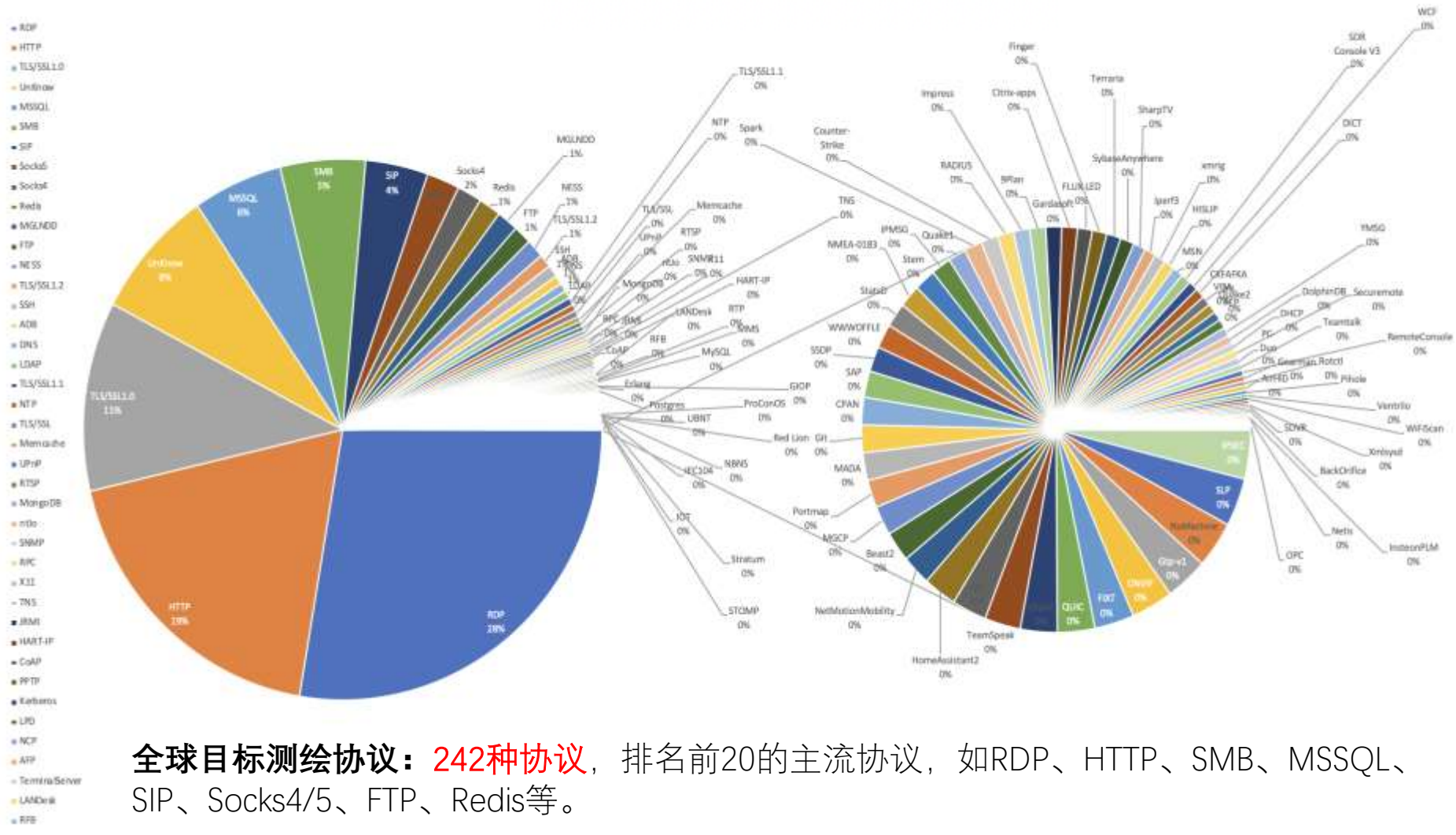


测绘热点城市

路由交换设备			网络摄像头			网络存储设备			工控		
中国	台湾	772110	美国	california	268675	中国	台湾	240657	美国	florida	100648
	香港	704255		florida	219173		广东	182571		minnesota	25290
	江苏	358806		texas	189660		江苏	159778		texas	24857
	广东	344701		new york	171063		浙江	126825		california	21021
	浙江	256717		pennsylvania	78557		香港	121097		maryland	5821
美国	california	273643	越南	ho chi minh	457865	德国	northrhine-westphalia	78000	卡塔尔国	baladiyat ad dawhah	58077
	texas	182578		hanoi	334240		bavaria	67018		baladiyat al khawr wa adh dhakhirah	2
	new york	117138		haiphong	57722		baden-wurttemberg region	46804			
	florida	109971		tinh quang nam	46377		lower saxony	30659			
	minnesota	103249		tinh ha tinh	40991		hesse	29487			
英国	england	1395199	中国	台湾	469415	美国	california	41097	日本	tokyo	27704
	scotland	82865		广东	168061		new york	16849		kanagawa	3180
	wales	45708		江苏	155946		texas	16623		nagasaki	2352
	northern ireland	29858		浙江	136629		florida	15035		yamaguchi	1849
	united kingdom	1378		香港	119703		washington	11081		aichi	1752
意大利	lombardy	236671	英国	england	603232	法国	ile-de-france	63440	法国	provence-alpes-cote dazur	10136
	latium	168440		scotland	41441		auvergne-rhone-alpes	26824		occitanie	8400
	campania	145173		wales	28731		occitanie	16942		ile-de-france	4831
	emilia-romagna	144050		northern ireland	20618		provence-alpes-cote dazur	15843		nouvelle-aquitaine	4069
	tuscany	112298		united kingdom	66		nouvelle-aquitaine	15343		auvergne-rhone-alpes	1013
巴西	minas gerais	339656	韩国	gyeonggi-do	114893	韩国	seoul	60116	德国	north rhine-westphalia	9726
	sao paulo	225649		seoul	89210		gyeonggi-do	51947		bavaria	7148
	santa catarina	61455		gyeongsangbuk-do	32146		incheon	8483		hamburg	4012
	parana	60326		gyeongsangnam-do	31943		busan	7260		baden-wurttemberg region	4007
	rio grande do sul	55151		jeollabuk-do	26200		gyeongsangbuk-do	6954		hesse	1804

目标测绘的主要协议

全球网络空间测绘协议统计分布



全球目标测绘协议：242种协议，排名前20的主流协议，如RDP、HTTP、SMB、MSSQL、SIP、Socks4/5、FTP、Redis等。

Protocol	Sum of Num
RDP	2004433
HTTP	1354217
TLS/SSL1.0	822187
UnKnow	570003
MSSQL	404889
SMB	385095
SIP	282886
Socks5	148915
Socks4	110888
Redis	101604
MGLNDD	96460
FTP	81679
NESS	80392
TLS/SSL1.2	58167
SSH	52484
ADB	39200
DNS	37347
LDAP	33071
TLS/SSL1.1	32319
NTP	28384
TLS/SSL	28207
Memcache	23234
UPnP	20889
RTSP	20135
MongoDB	19782
ntJo	17533
SNMP	16529
RPC	15438
X11	13326
TNS	12286
JRMI	11872
HART-IP	10758
CoAP	10465
PPTP	10360
Kerberos	10334
LPD	10270
NCP	9999
AFP	9844
TerminalServer	9761
LANDesk	9407
RFB	9351
RTP	9322
MMS	8986
MySQL	8870
DominoConsole	8867
GIOP	8809
Erlang	8315

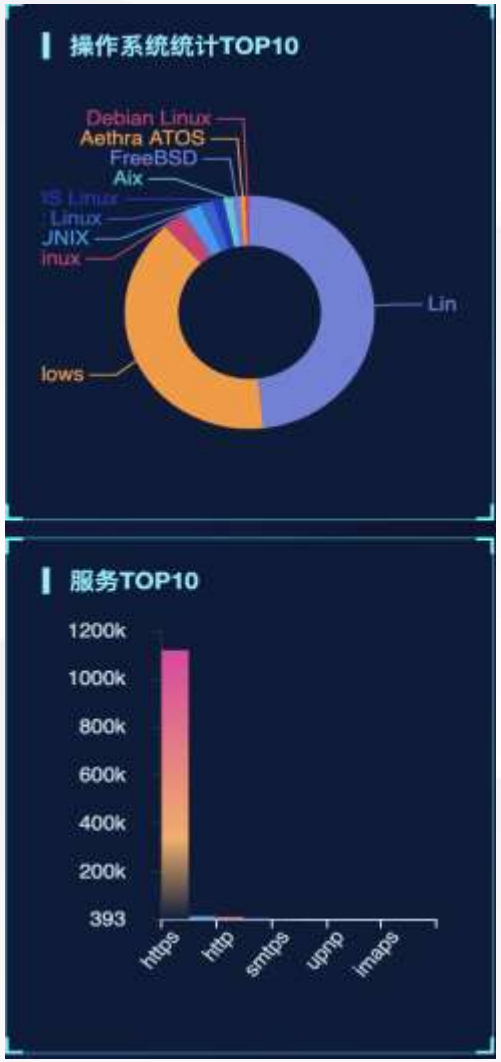
主流测绘平台的服务测绘特征

网络空间测绘引发的思考

目录

反测绘的重要性

5G、云计算技术发展带来的“网络空间泛化”使企业数字资产数量和类型激增，另一方面，随着物联网（IoT）的逐步普及、工控系统的广泛互联，直接**暴露在网络空间的联网设备数量大幅增加，随之可能面对更多的风险。**



反测绘的重要性

IPv4资产

- 2023年3月底存活目标数：**1,939,070,692**个

IPv6资产

- 2023年3月底存活目标数：**1,383,323,319**个

存在脆弱性目标

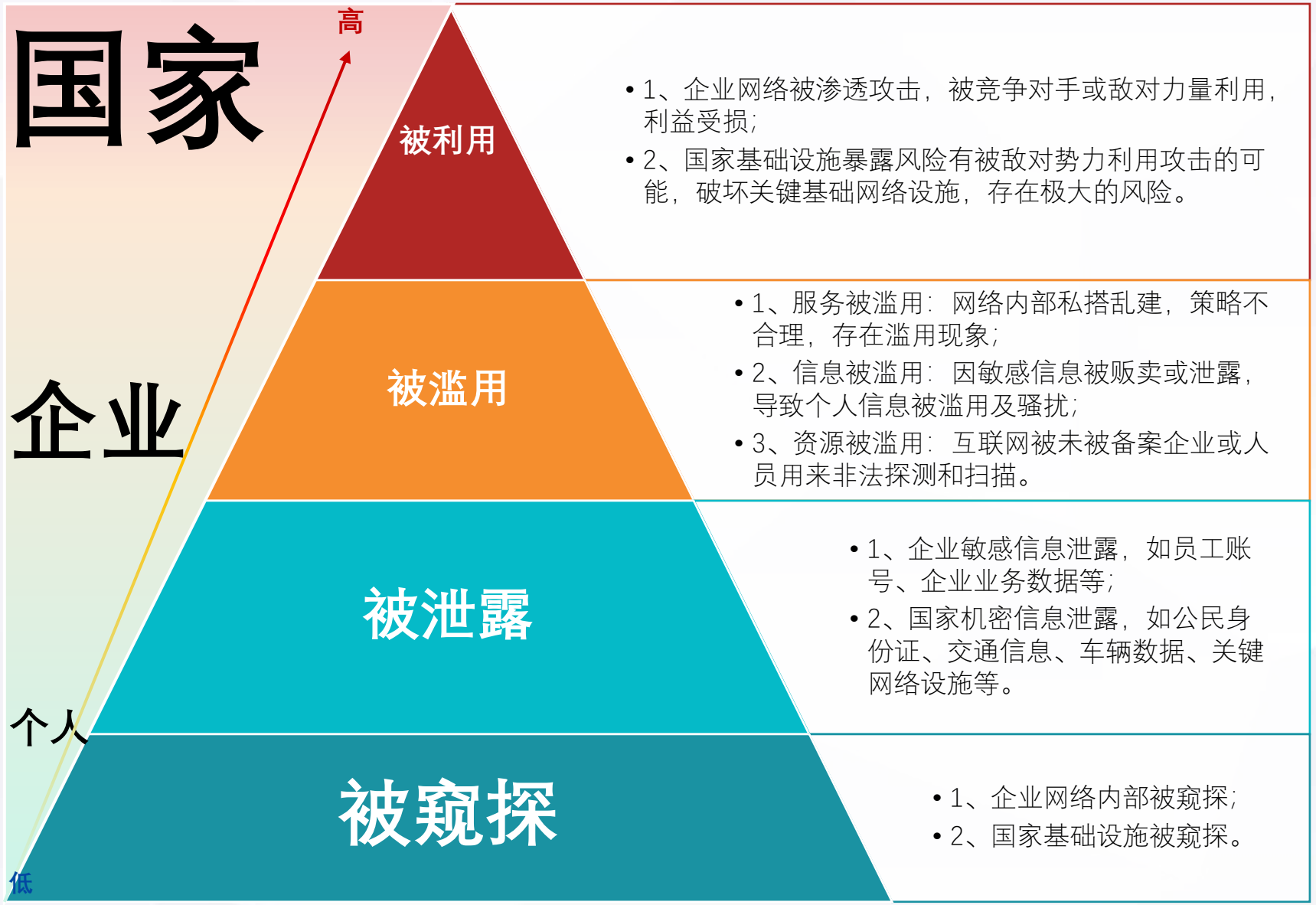
- 2023年3月底存在脆弱性目标数：**116,362,680**个

可渗透利用目标

- 2023年3月底可渗透利用目标数：**891,810**个

2023年底，暴露面资产（IPv4+IPv6）总数为：**3,322,394,011**个，其中脆弱性目标占比**3.5%**，可渗透利用目标占比**0.027%**左右，且呈上升趋势，暴露面的激增对我国互联网和关基建设的影响危害及大，**急需构建针对互联网及关键信息基础设施的反测绘技术应用**，对保护我国互联网和关基设施十分重要。

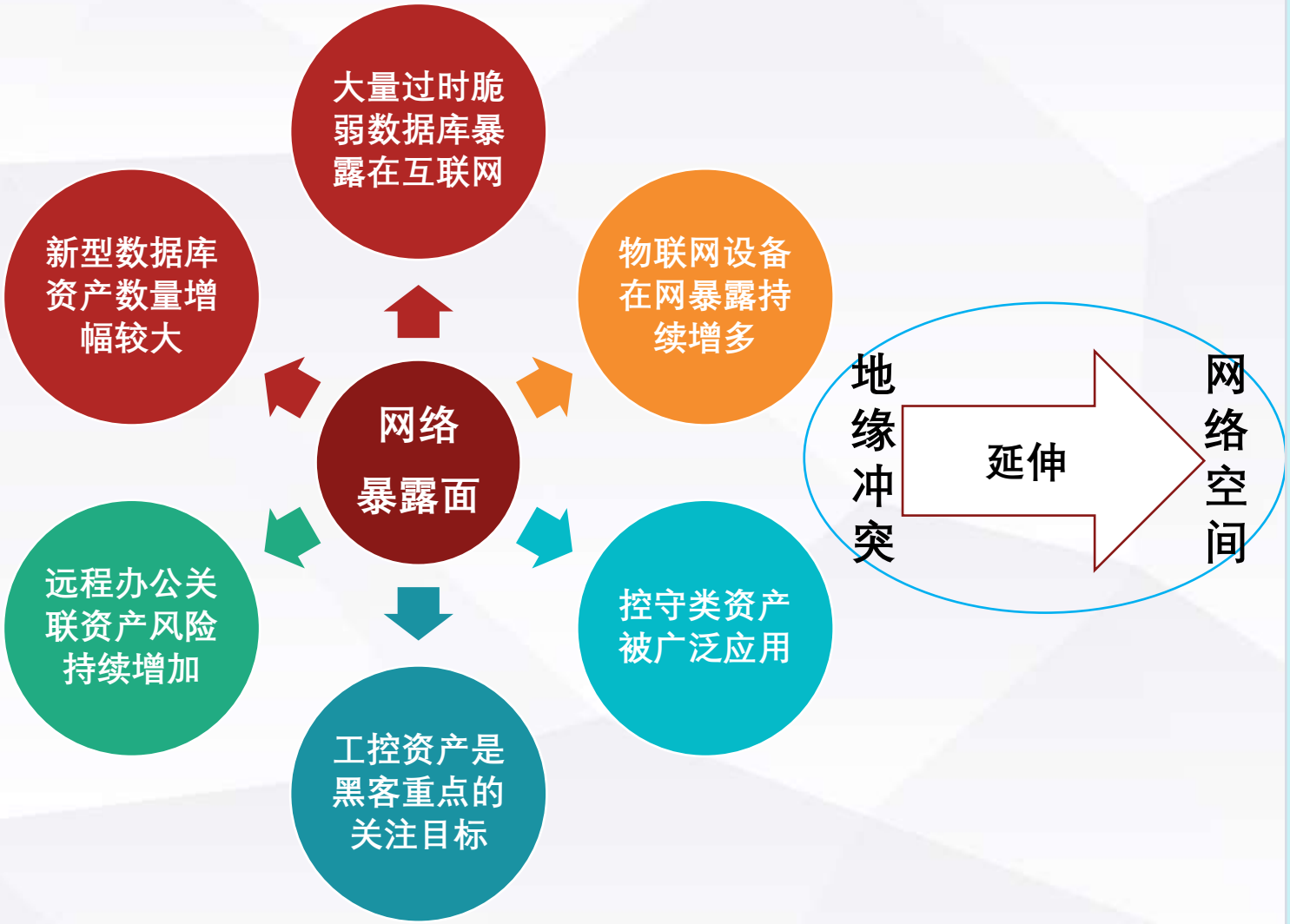
反测绘的必要性



当前网络空间测绘被用来管理和监控资产的同时，也极有可能被攻击者当作“窥探”网络内部的工具，并被泄露、滥用以及利用，从而对个人、企业、国家造成巨大的内外损失。

因此，有必要优化网络结构、减少设施资产对外的暴露点和暴露面，**推进关键信息基础设施反测绘技术**的研究和应用，提升关键信息基础设施自身的防御能力。

反测绘才能反扫描



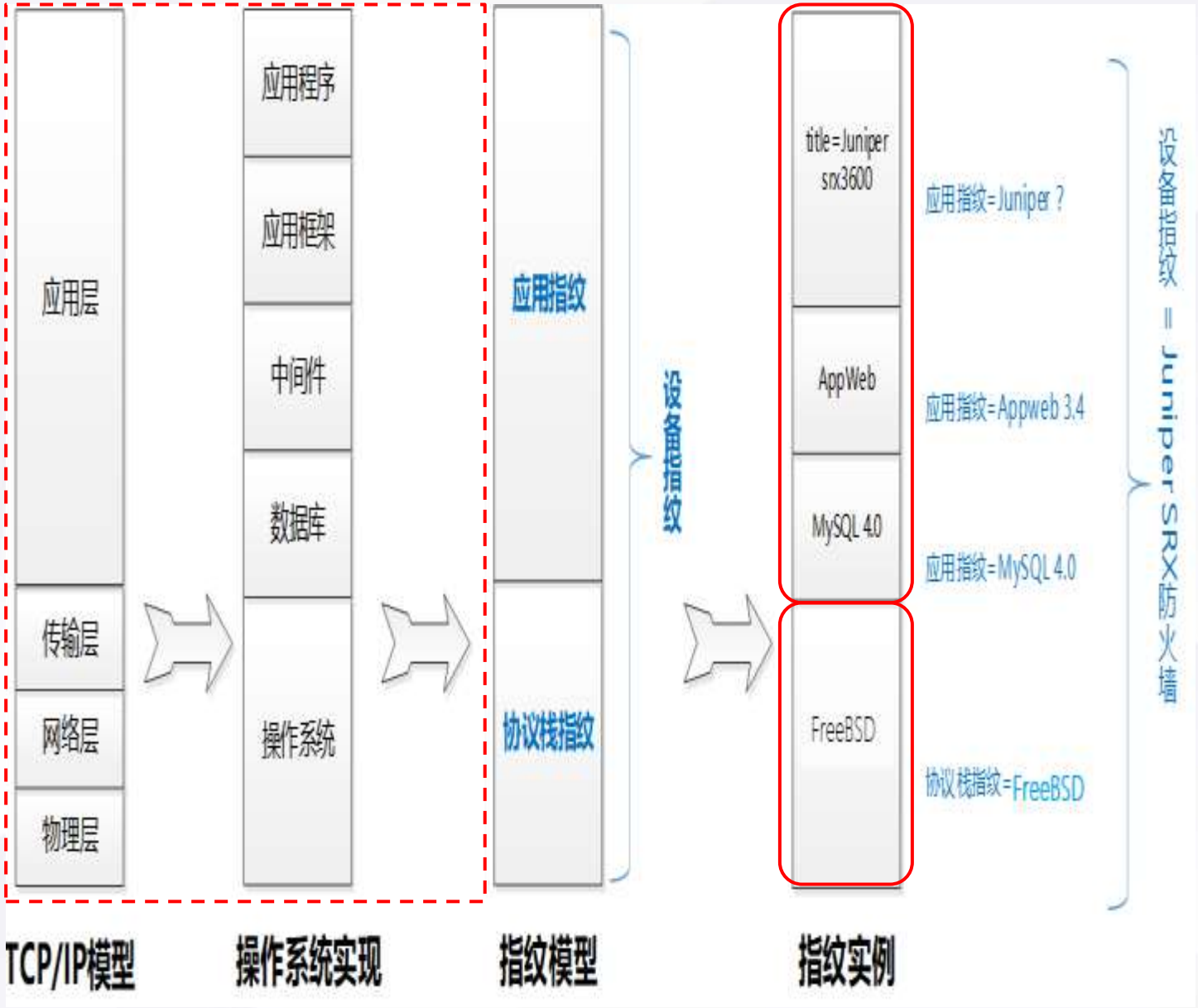
2022年地缘冲突，短时间激增的暴露面资产，对网络空间安全产生了深远影响。

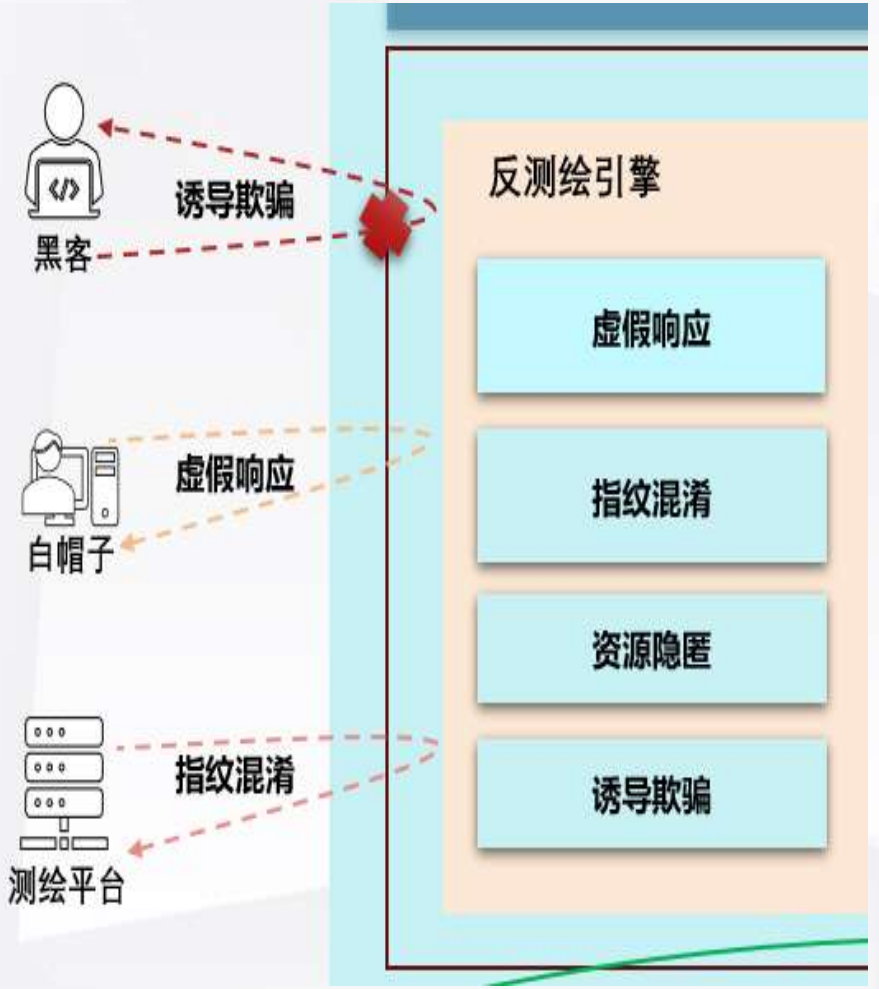
在新兴与制造业加速融合下，软硬件更新、设计匮乏以及建设周期长等问题驱动下，网络空间安全风险急剧增加，对国家关键基础设施建设以及企业产生巨大的安全挑战。

在此背景下，**反测绘技术产生和应用**有助于在地缘冲突时，**极大的减小国家关键基础设施和企业网络暴露面所带来的损失，**保护国计民生，意义深远。

目录

反测绘原理机制

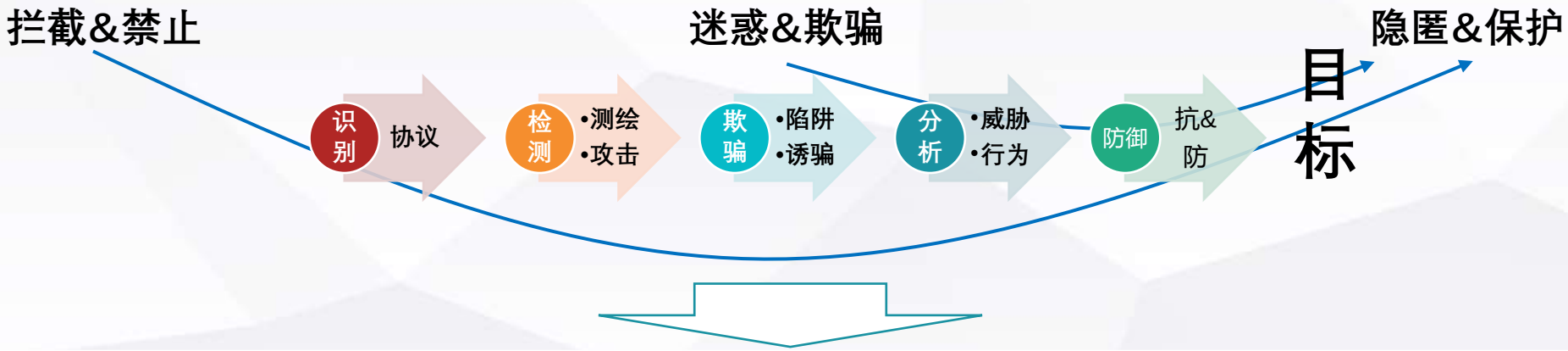




反测绘关键能力

WebRAY 盛邦安全

地址隐藏	指纹模型	伪造服务	伪造资源	伪造网络
禁Ping	禁探测	混淆指纹	诱骗扰乱	伪装隐匿	网络隐遁

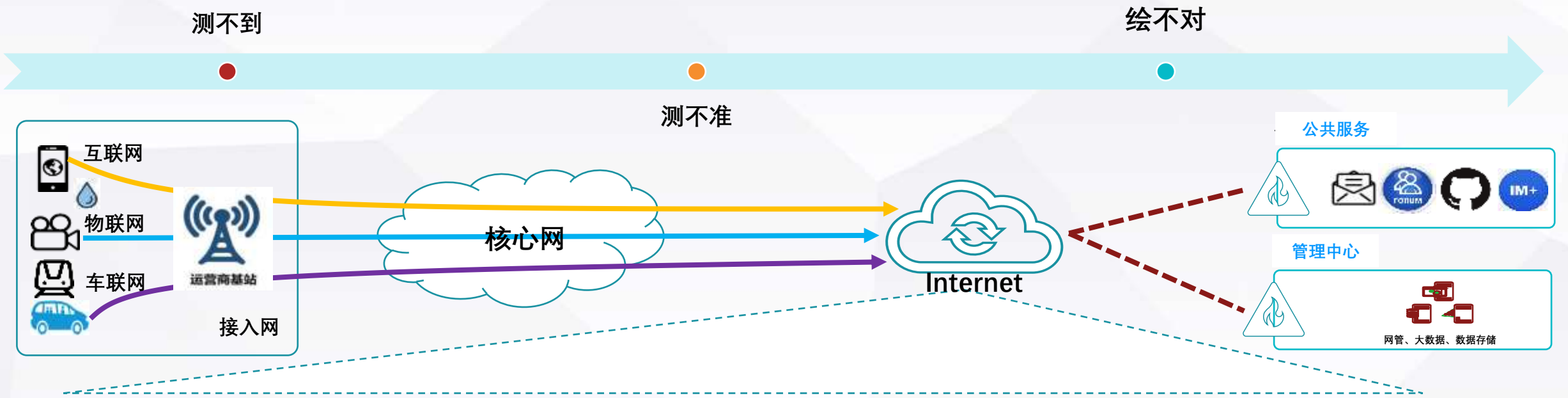


网络空间反测绘分析模型

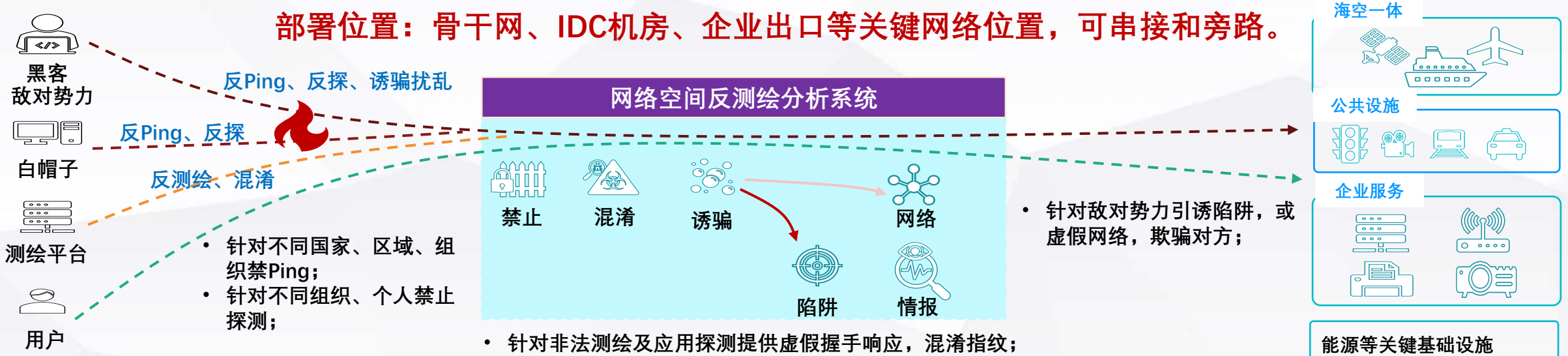
浅 网络空间反测绘关键能力 深

反测绘原理机制

核心：反探测；关键服务去指纹；关键设施隐藏



部署位置：骨干网、IDC机房、企业出口等关键网络位置，可串接和旁路。



- 针对不同国家、区域、组织禁Ping；
- 针对不同组织、个人禁止探测；

- 针对敌对势力引诱陷阱，或虚假网络，欺骗对方；

- 针对非法测绘及应用探测提供虚假握手响应，混淆指纹；
- 威胁情报分析，针对反测绘数据分析能力分析威胁情报。

反测绘关键措施-反探测

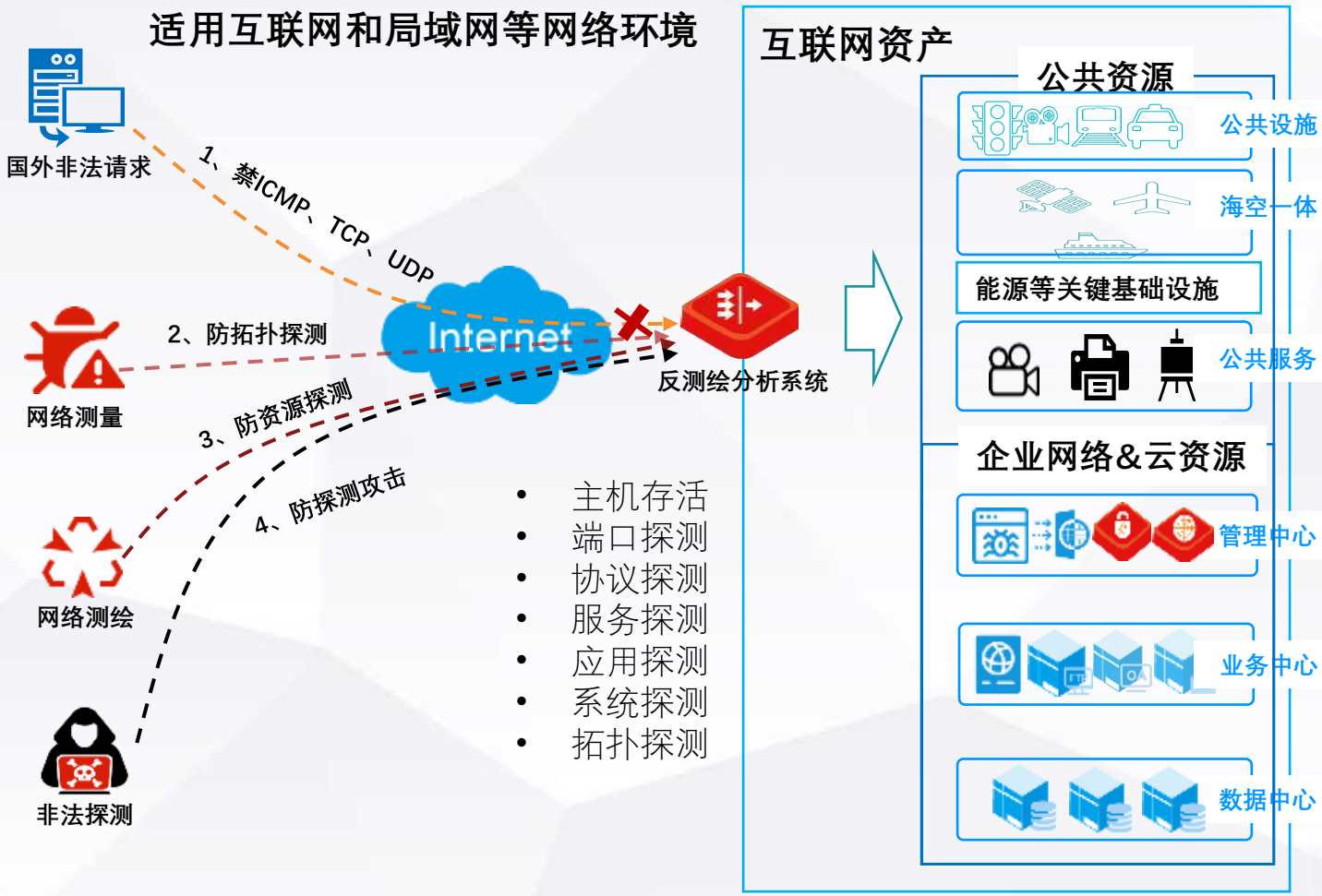
禁止ICMP探测
- IP地理位置库

禁TCP、UDP探测
- 网络行为分析

防拓扑探测
- 网络行为分析

防资源探测
- 扫描器指纹库
- 探测工具指纹库
- 爬虫指纹库

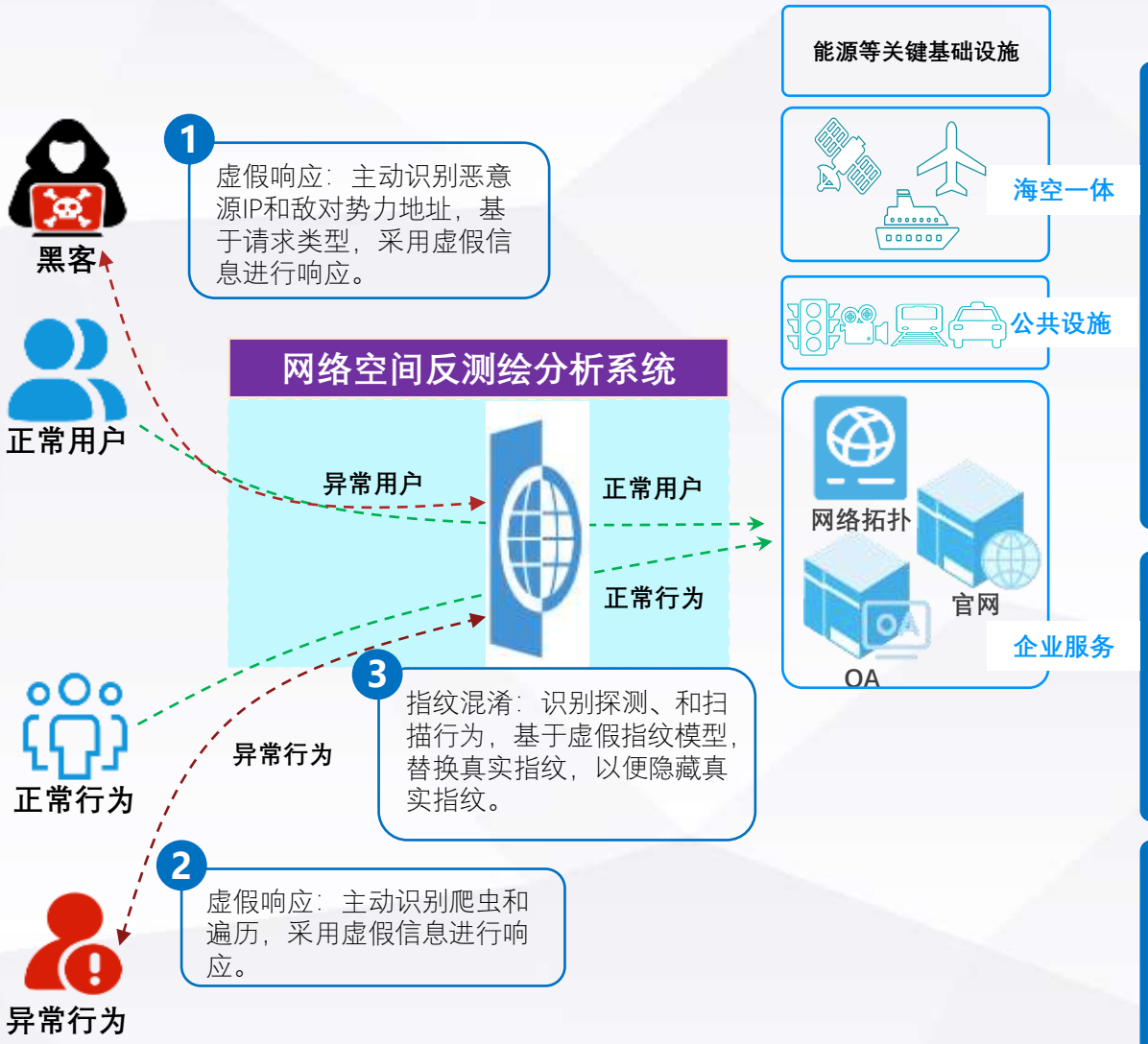
支持虚拟化、云原生等场景，
适用互联网和局域网等网络环境



- 主机存活
- 端口探测
- 协议探测
- 服务探测
- 应用探测
- 系统探测
- 拓扑探测

基于**IP地理位置库、扫描器指纹库、探测指纹库、爬虫指纹库、流量行为分析（+自学习建模）**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。

反测绘关键措施-虚假响应



2个模型

1、**虚假指纹模型**：梳理设备、系统、服务及应用等指纹结构和关系，构建虚假的指纹层次结构和关联关系，以便识别到探测及扫描行为时，能够高效的替换和混淆指纹；

2、**虚假响应模型**：梳理不同协议的响应内容，保留静态资源，剥掉动态数据，当发现恶意IP和敌对势力地址、爬虫及遍历异常行为时，则会采用协议的静态资源+动态生成数据响应对方,或将代码植入响应中进行响应。

虚假响应

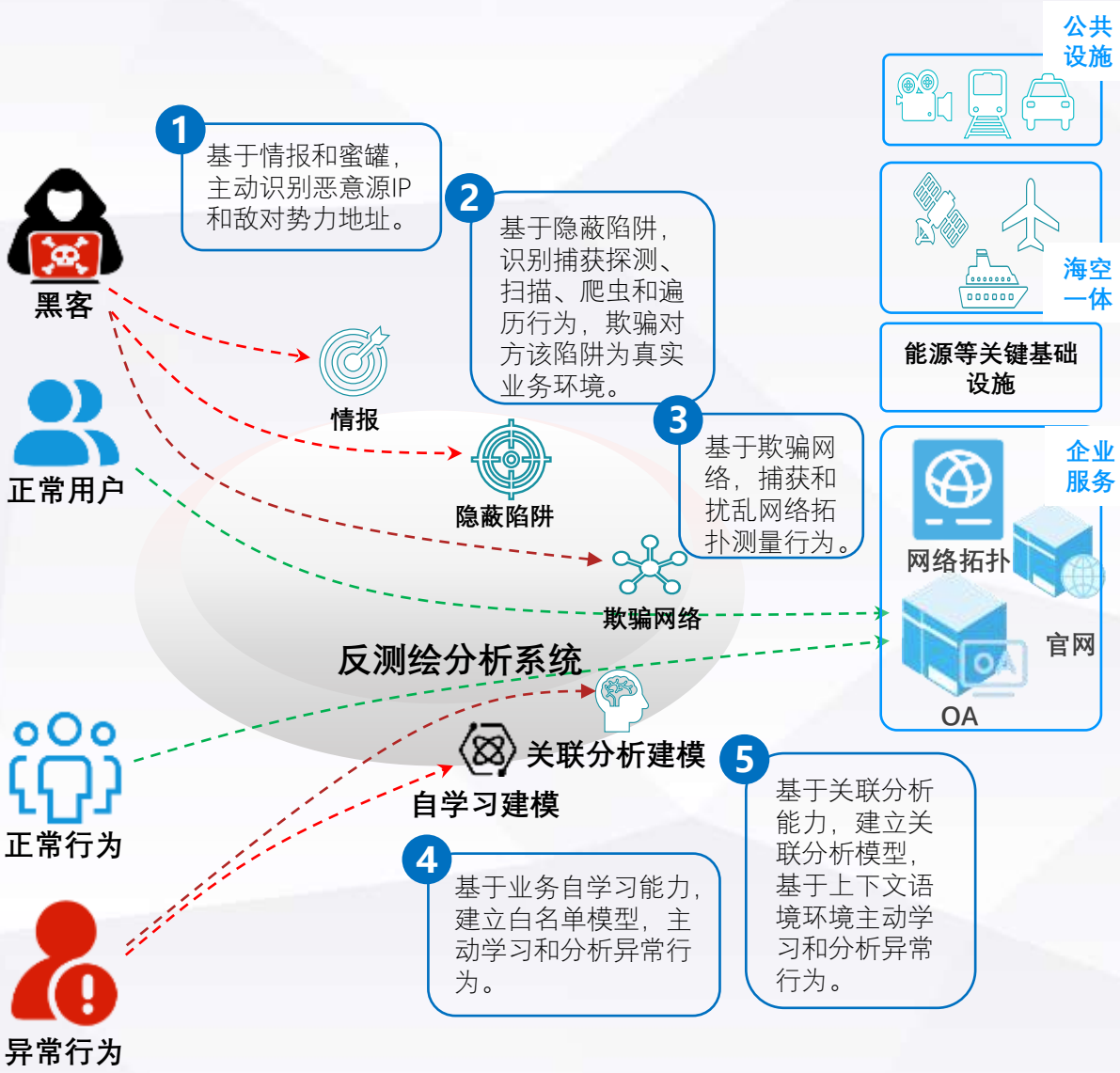
1、主动识别恶意源IP和敌对势力地址，根据访问请求协议类型和内容，基于虚假响应模型进行响应。

2、主动识别爬虫和遍历异常动作行为，根据访问请求协议类型和内容，基于虚假响应模型进行响应。

混淆指纹

主动识别网络探测、和扫描行为，基于虚假指纹模型，替换真实指纹，隐藏真实指纹，减小业务暴露风险。

反测绘关键措施-诱骗扰乱（草船借箭）



2个模型

1、**自学习模型**：自动梳理业务结构，识别业务保护对象；基于学习结果建立白名单模型，建立非白即黑策略；

2、**关联分析模型**：基于关联分析能力，建立关联分析模型，基于上下文语境环境主动学习和分析异常行为。

诱骗扰乱

1、基于情报和蜜罐，主动识别恶意源IP和敌对势力地址，诱骗并诱使其访问隐蔽陷阱等进行联动防御。

2、基于隐蔽陷阱，识别和捕获探测、扫描、爬虫和遍历行为，欺骗异常访问者该隐蔽陷阱为真实业务环境。

3、基于欺骗网络，捕获和扰乱网络拓扑测量行为，提供虚假的拓扑响应。

采用**虚假**的设备、服务应用、资源数据及网络**陷阱**欺骗非法访问者；**扰乱**其探测和扫描等**行为**，使其得到**错误的结果**。

反测绘关键措施-对抗大数据

大数据分析

时间 特权帐号 会话 角色 异常 资产 地点 事务 行为 IP地址

海空一体
基础设施
公共设施
企业服务
公共服务

对抗分析

非法请求：
1、恶意IP和敌对势力地址；
2、网络探测、爬虫等；
3、网络扫描和渗透。

恶意服务器

拟态响应
静态模板+动态数据
地址隐藏

正常的业务请求

反测绘分析系统

正常的业务请求

正常用户

能源等关键基础设施
公共设施
海空一体
公司服务
网络拓扑
官网
OA

拟态响应-》大数据分析

1、根据用户业务，构造和模拟真实的用户响应；
2、去除单一化，应多样化交互；
3、避免被识别为虚假业务或蜜罐。

静态模板+动态数据-》对抗大数据分析

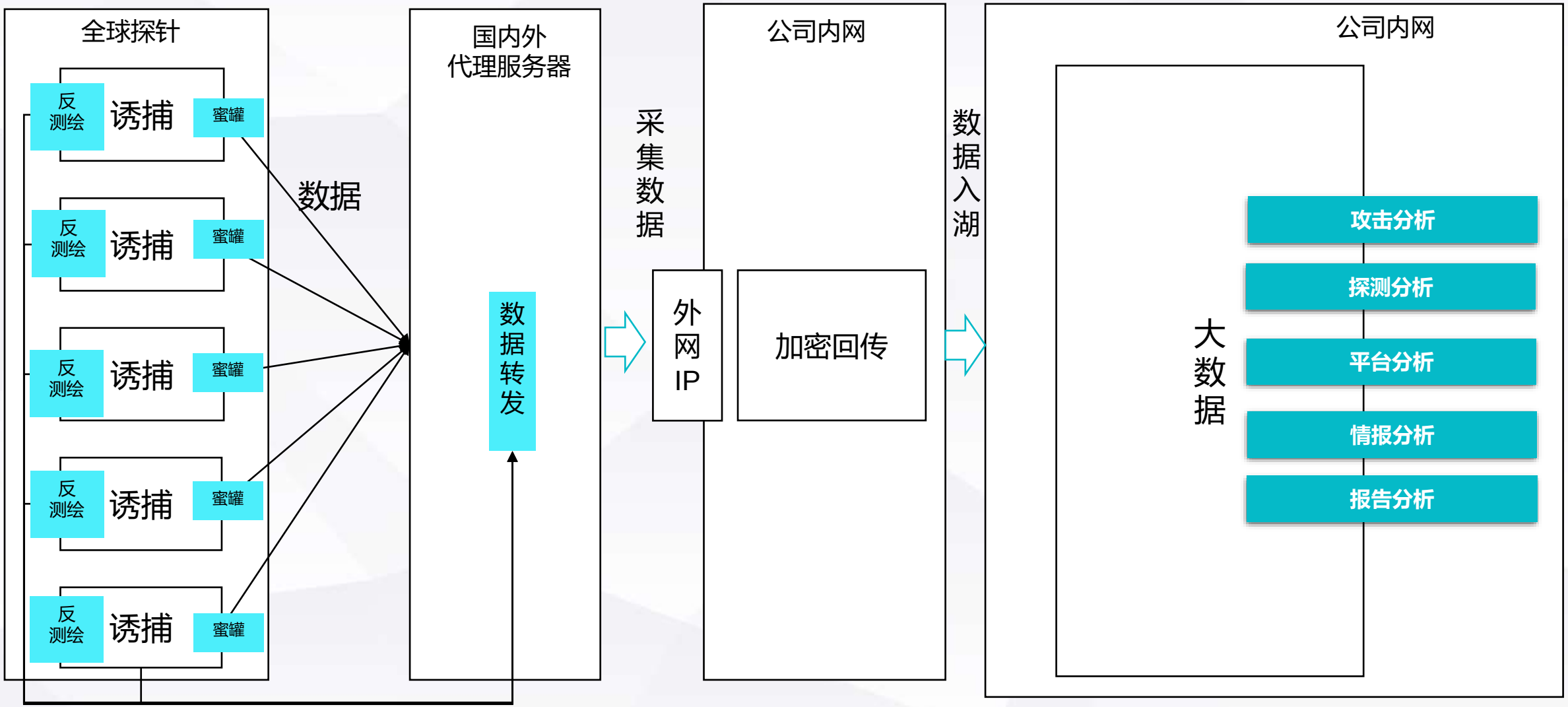
1、构造静态响应模板，预留动态数据插入点；
2、根据动态数据插入点，适时构造动态响应数据，插入响应数据中，进行响应。
3、基于静态模板+动态数据，保持响应的动态性和数据的无关性。

地址隐藏-》对抗大数据分析

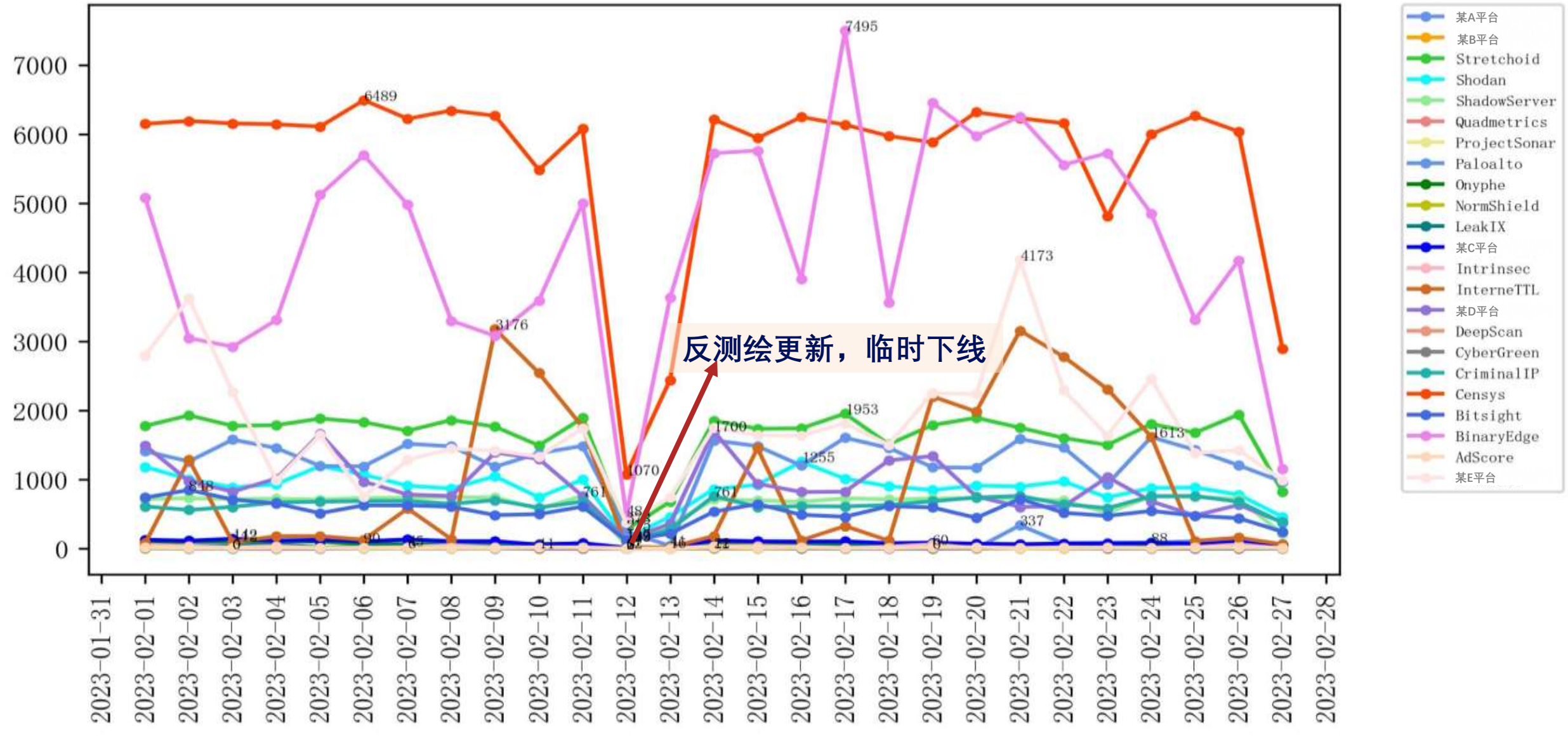
1、构建地址隐藏服务，将真实的业务地址隐藏起来；
2、基于地址漂移能力，使大数据无法关联分析，减小真实业务的暴露信息。

目录

反测绘成功应用

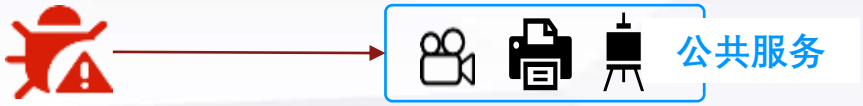


反测绘成功应用



反测绘成功应用

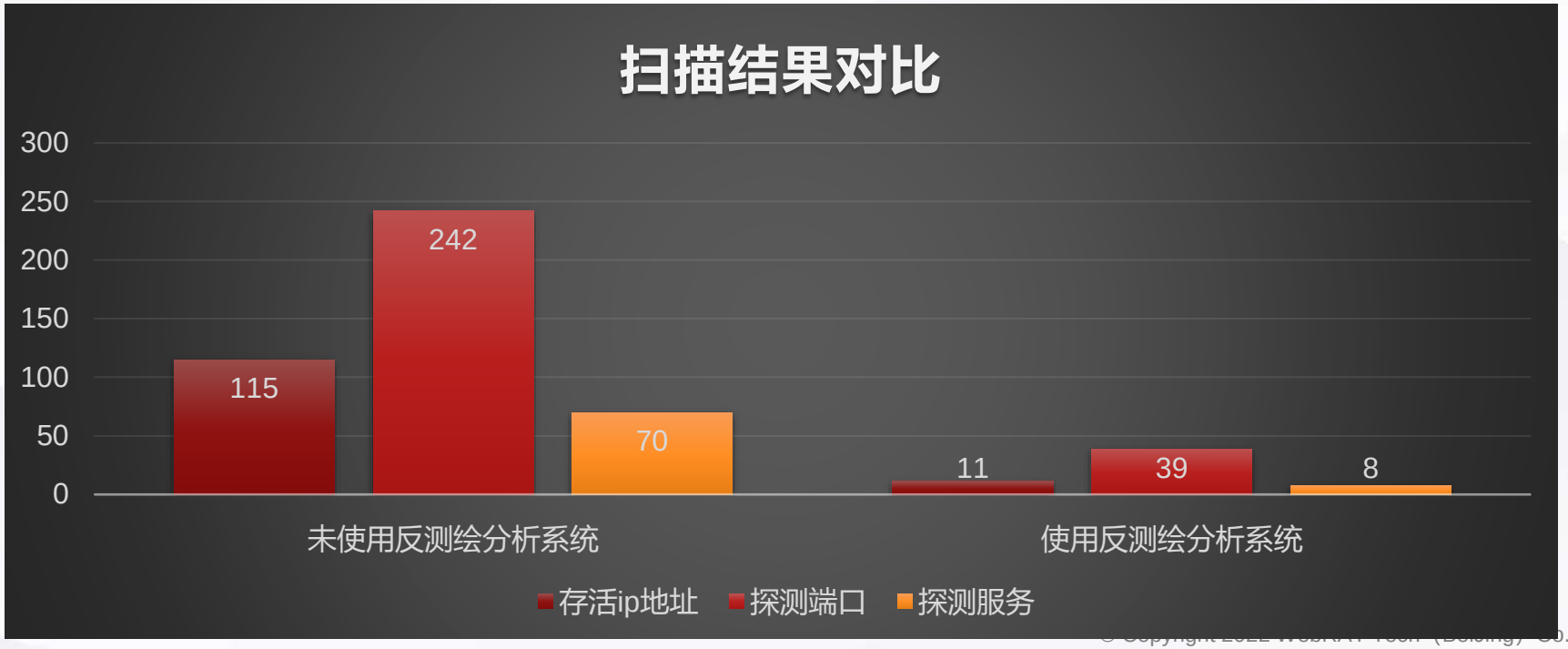
使用NMAP工具，扫描C端公共服务地址，比较未使用和使用反测绘系统情况



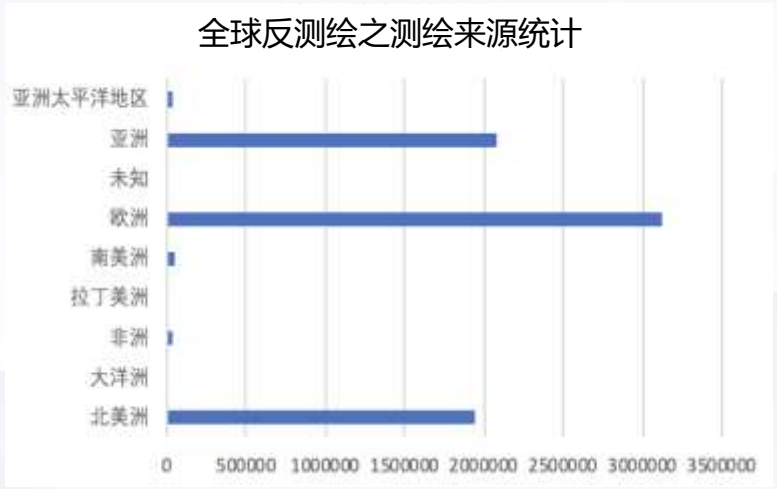
存活IP地址	端口	服务
115	242	70

反测绘分析系统

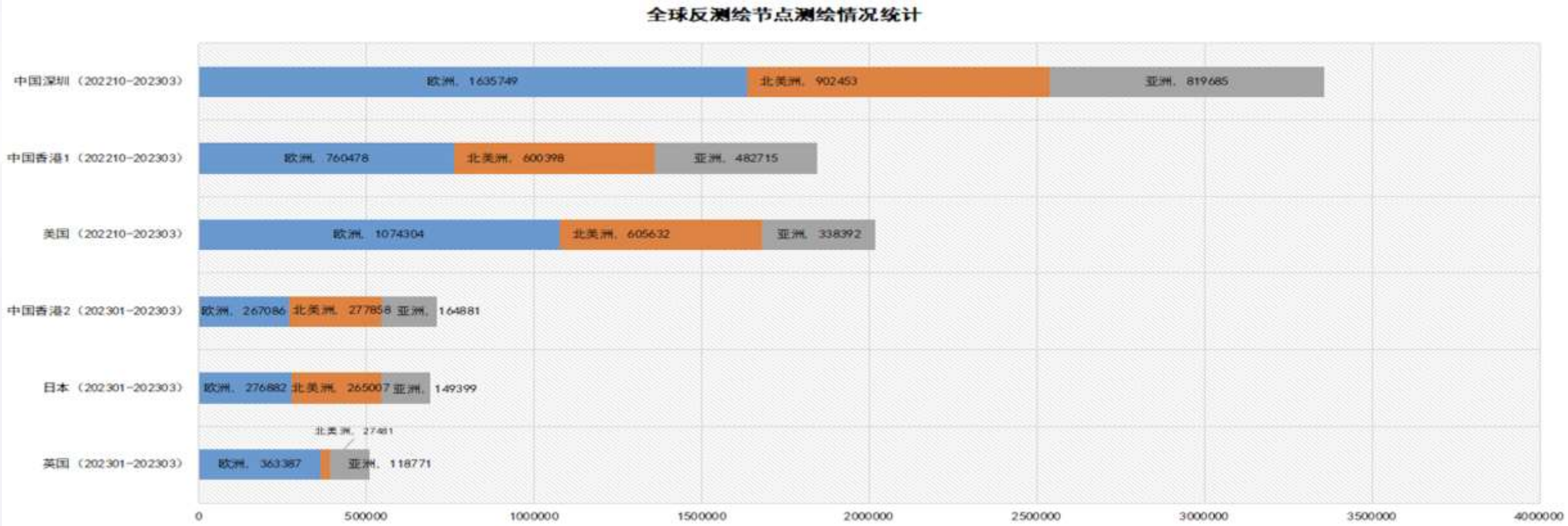
存活IP地址	端口	服务
11	39	8



反测绘成功应用



反测绘成功应用



英国节点（202301-202303）		日本节点（202301-202303）		中国香港2节点（202301-202303）		中国香港1节点（202210-202303）		美国节点（202210-202303）		中国深圳节点（202210-202303）	
数量	国家	数量	国家	数量	国家	数量	国家	数量	国家	数量	国家
239617	United States	239931	United States	254453	United States	542324	United States	536772	United States	853403	Netherlands
124942	Netherlands	108826	Netherlands	105326	China	334209	China	285747	Netherlands	851977	United States
87064	Russian Federation	80042	China	69371	Netherlands	198312	Netherlands	237164	China	636844	China
67638	China	42727	Russian Federation	45652	United Kingdom	136886	Russian Federation	183344	Russian Federation	235387	Germany
30376	United Kingdom	28719	United Kingdom	45524	Russian Federation	103110	Bulgaria	164575	Bulgaria	201244	United Kingdom
27399	Bulgaria	23608	Germany	24079	Bulgaria	65829	United Kingdom	137423	United Kingdom	135129	Russian Federation
21790	Germany	17644	Canada	17653	Germany	64859	Germany	71267	Germany	48635	India
16692	Canada	17503	Bulgaria	16921	Canada	46117	Canada	45606	Ukraine	47591	Canada
15960	Europe Regions	14716	Europe Regions	13070	Europe Regions	43379	Europe Regions	45482	Canada	44121	Singapore
11425	Switzerland	12414	Republic of Korea	12194	Republic of Korea	38150	Switzerland	40939	Europe Regions	39323	Ukraine

WebRAY 盛邦安全

THANKS

www.webray.com.cn