Understand the ***status***

Evaluate the ***threats***

One step closer to ***future***

Global CyberSpace Surveying and Mapping Report 2022

Tsinghua University-Qihoo Technology Joint Research Center

CONTENTS

Background

About us

Tsinghua University-Qihoo Technology Joint Research Center for Cyberspace Surveying and Mapping was established on January 13, 2022

What we do

- Cooperated research in global cyberspace surveying and mapping technology
- Implement global cyberspace surveying and mapping

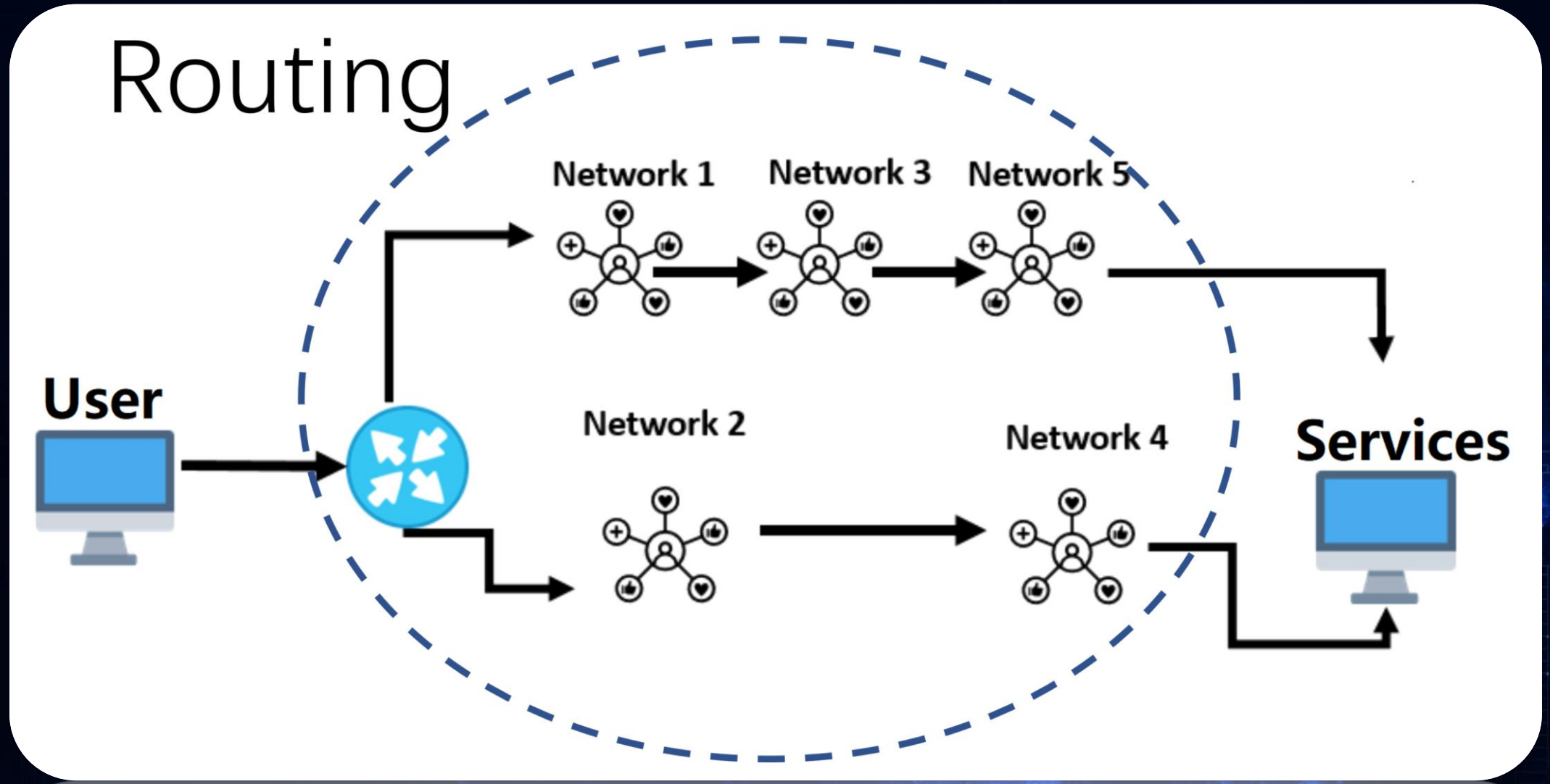
Surveying and Mapping

- **Surveying**: the process of collecting, analyzing, calculating, valuing, integrating, and managing for a land with its geographic information that have the character of spatial layout.
- **Mapping**: the process of displaying specifically the terrain features, surface features, and varieties of natural and human materials according to the result of surveying.


Cyberspace

What we want to survey
What we want to know
How we do

What we want to survey



What we want to know

Availability

- Distribution and robustness
- **Understand the status**

Risks

- Related possible weakness
- **Evaluate possible threats**

Insights

- Further cross-disciplinary analysis
- **One step closer to future**

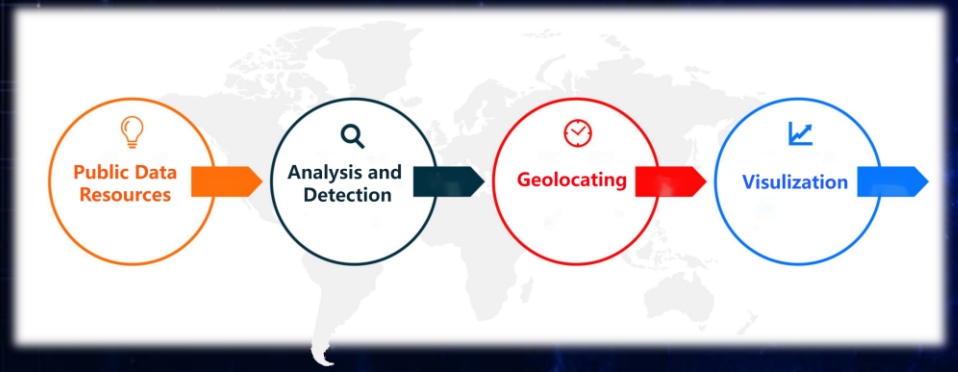
How we do

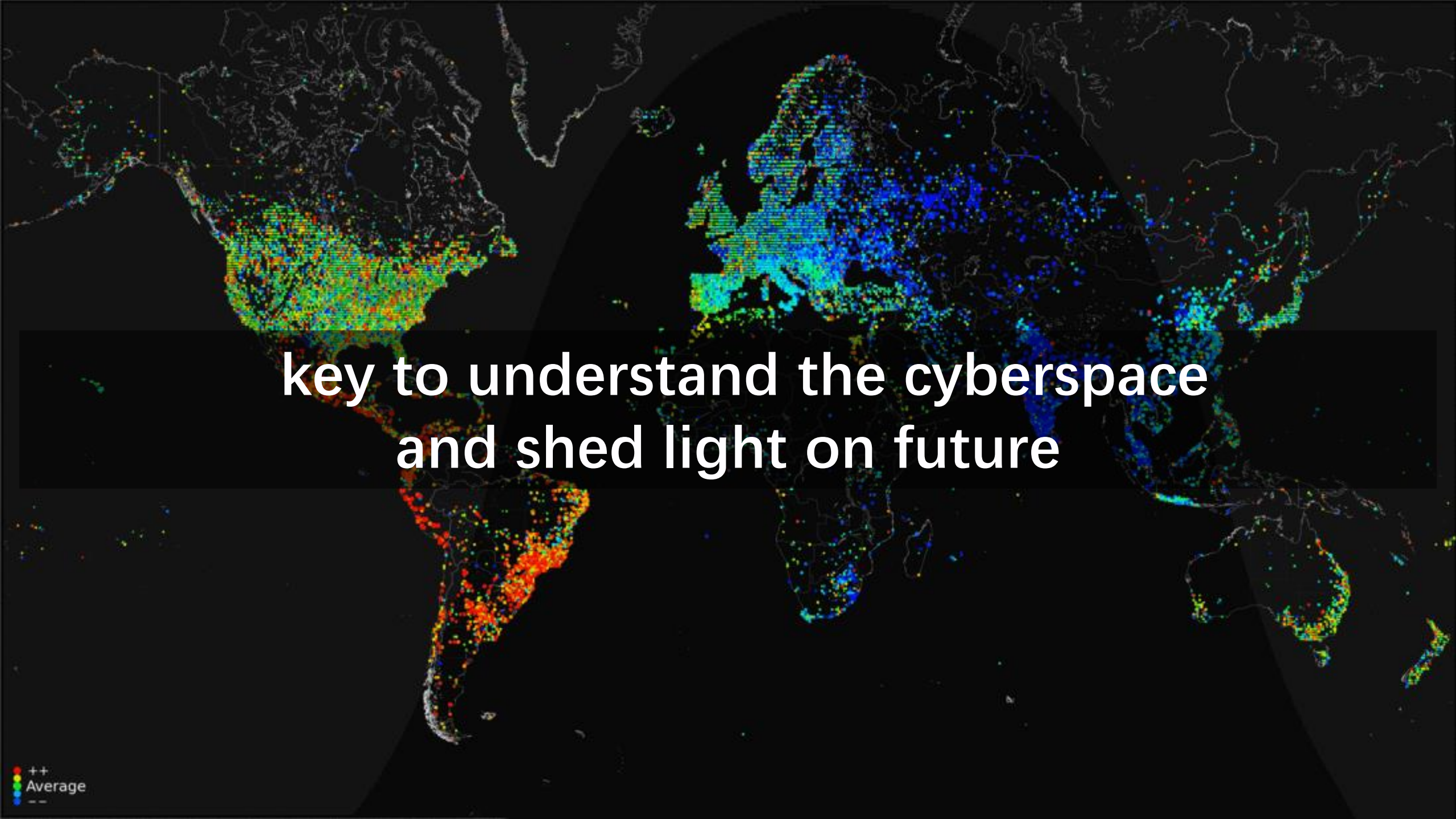
ROUTING

- Availability → Robustness
- Risks → BGP hijacking

SERVICES

- Availability → Distribution
- Risks → Known security issues

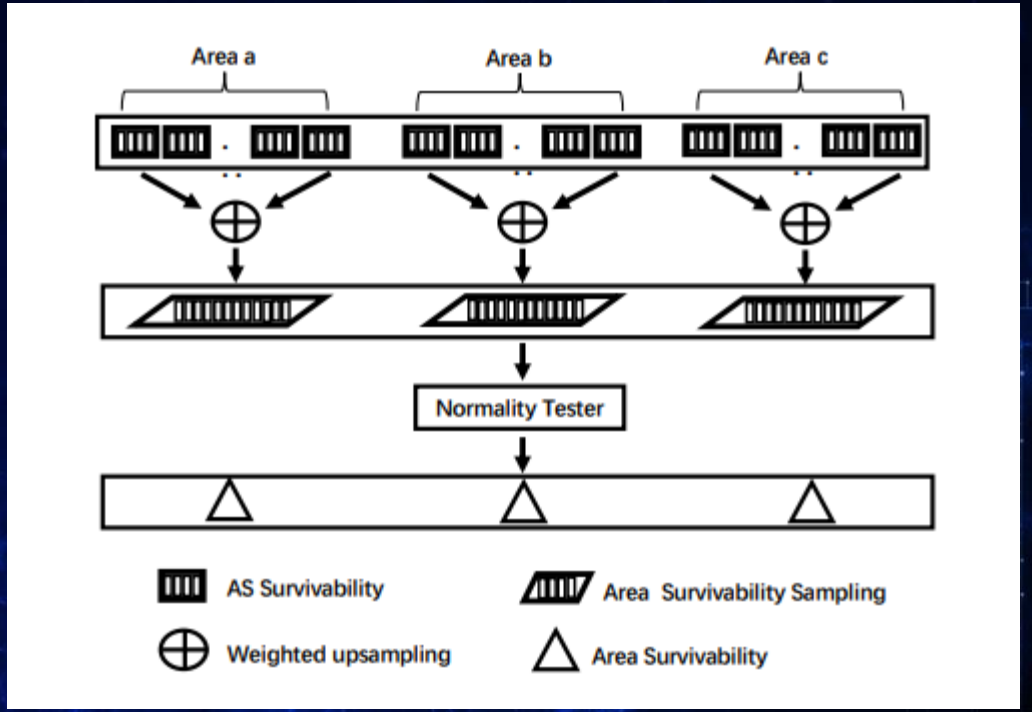



key to understand the cyberspace
and shed light on future
++
Average
--

Routing robustness

- **Data source**: public BGP data
- **Purpose**: analyze the availability when the communication of regions is broken
- **Method**: Based on hierarchical sampling, the destruction is simulated to approximate the damage situation of the real-world area.

$$e_{ix} = \frac{\sum_{b \in \boldsymbol{B}} r_b}{\sum_{o \in \boldsymbol{O}} r_o}$$



Results

Compared with **2020**,

the robustness of **2022** in **most regions**

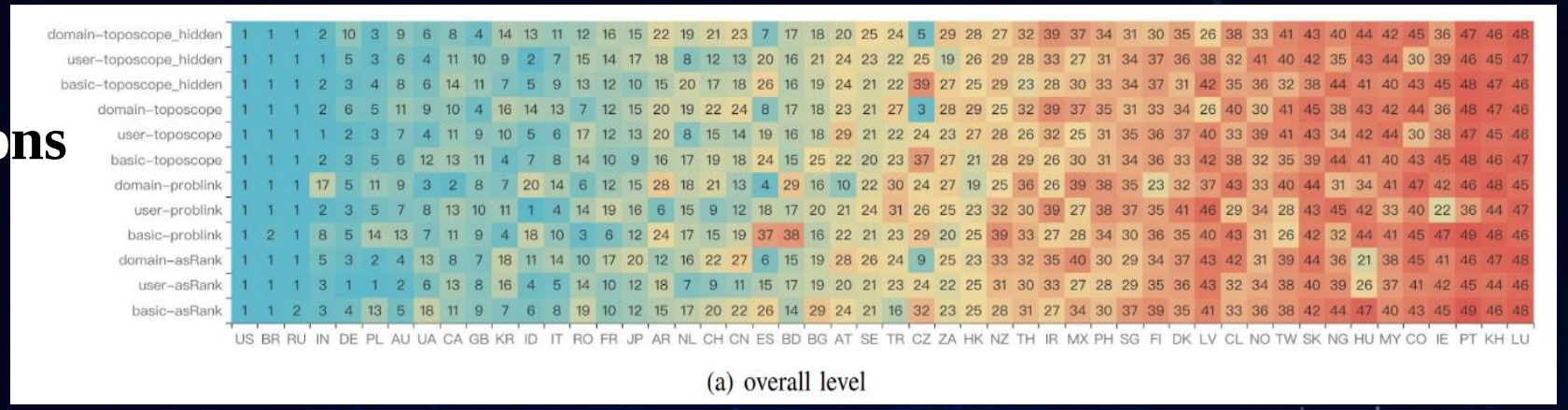
has been **greatly improved**,

Argentina,

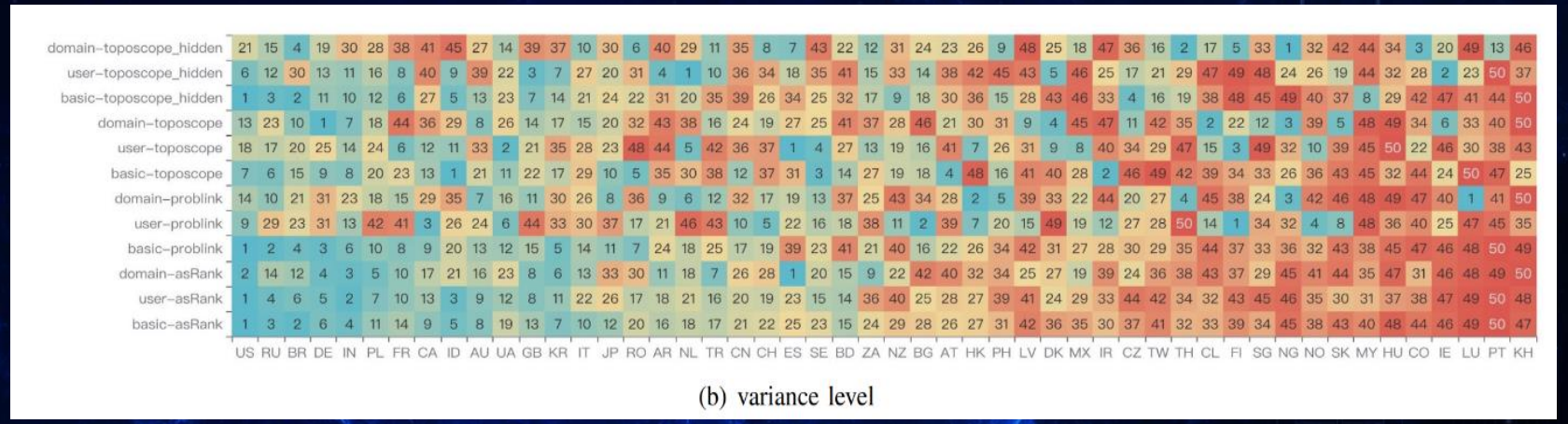
Bulgaria,

Chile, and **Colombia**

having the **largest improvements**



(a) overall level

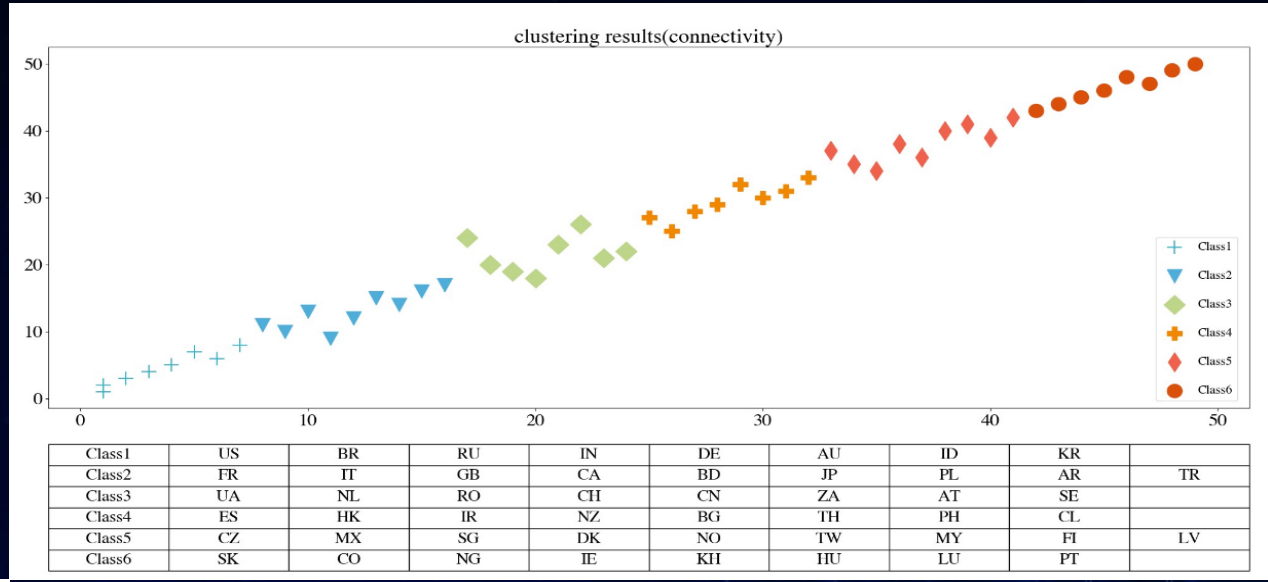


(b) variance level

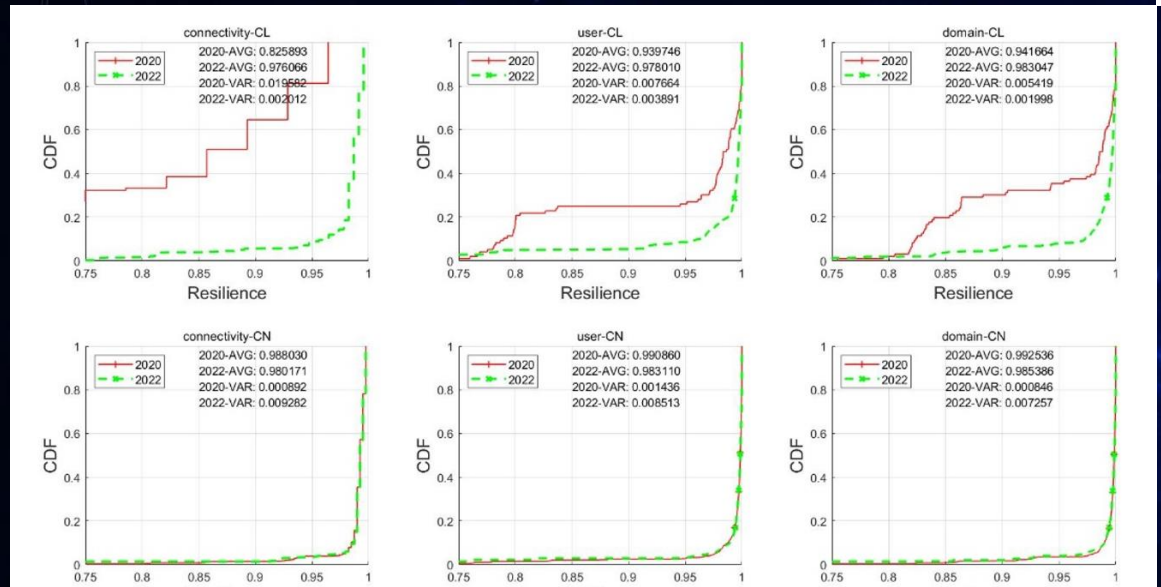
Results

United States, **Russia**, **Brazil**, **Germany**, **India**

have **better robustness**



Class1	US	BR	RU	IN	DE	AU	ID	KR	
Class2	FR	IT	GB	CA	BD	JP	PL	AR	TR
Class3	UA	NL	RO	CH	CN	ZA	AT	SE	
Class4	ES	HK	IR	NZ	BG	TH	PH	CL	
Class5	CZ	MX	SG	DK	NO	TW	MY	FI	LV
Class6	SK	CO	NG	IE	KH	HU	LU	PT	



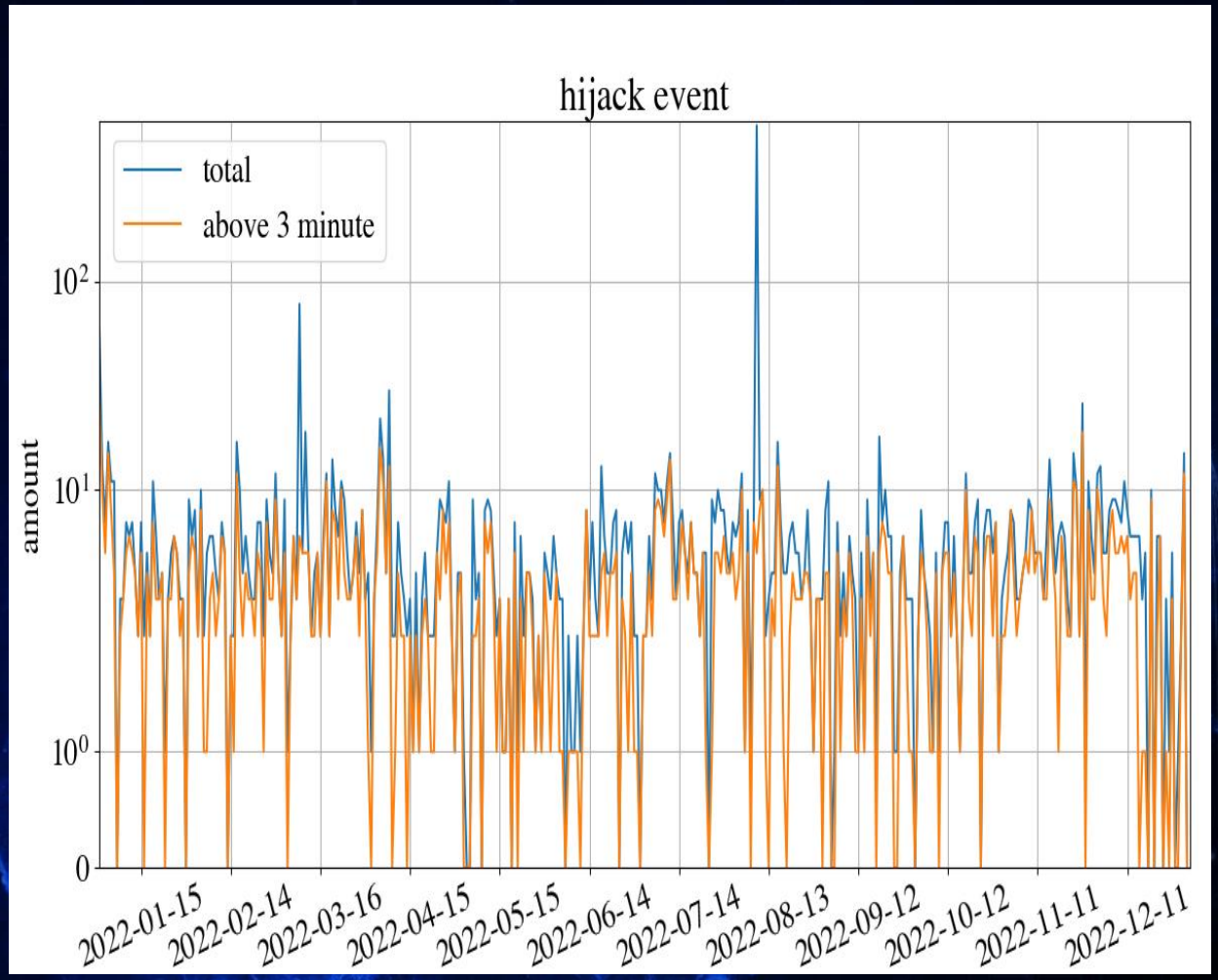
In **Asia**,

South Korea, **Japan**, **Indonesia**

have **a high ranking**

Possible BGP hijacking

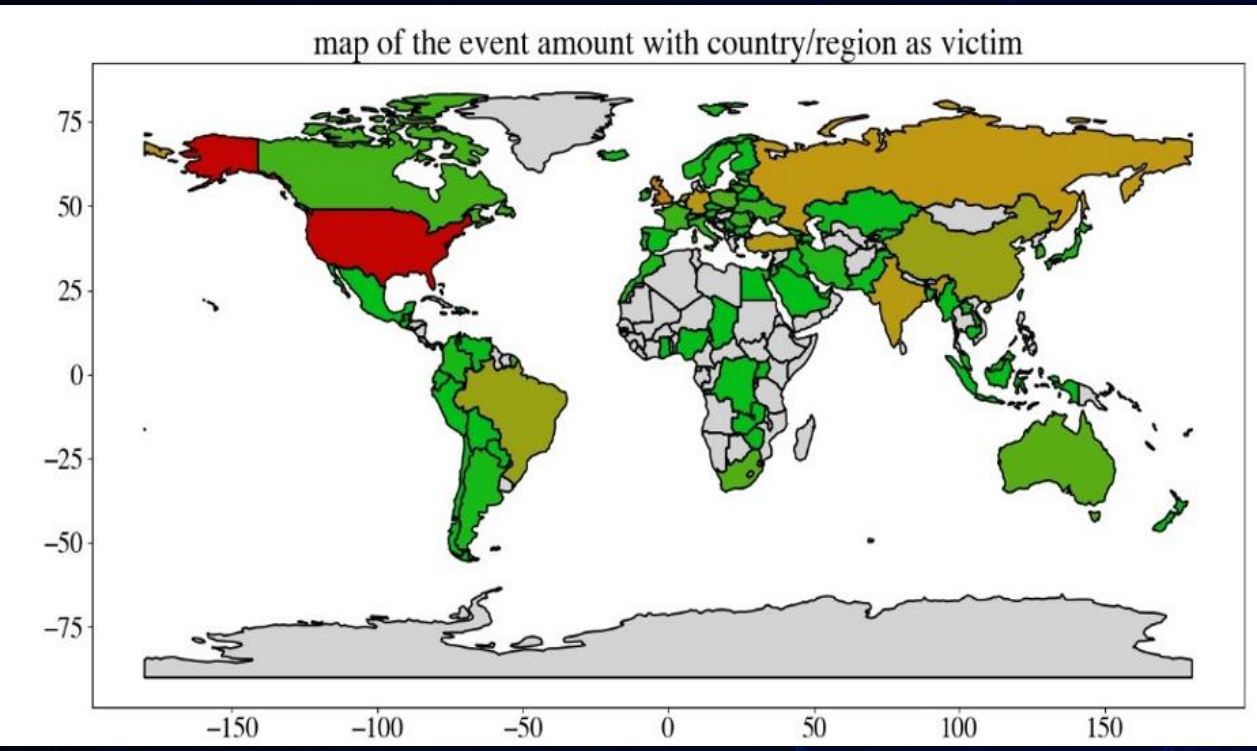
- **Detection**:
  - multiple origin AS (MOAS) events
- **Reporting**:
  - rates events based on the importance of the hijacked prefix and the victim's AS
  - the number of websites contained in the hijacked prefix
    - >5, the event level is high level,
    - Between 1 and 5, or the victim AS is IDC/CDN or top-level ICP, the event level is middle level,
    - otherwise the event level is low level

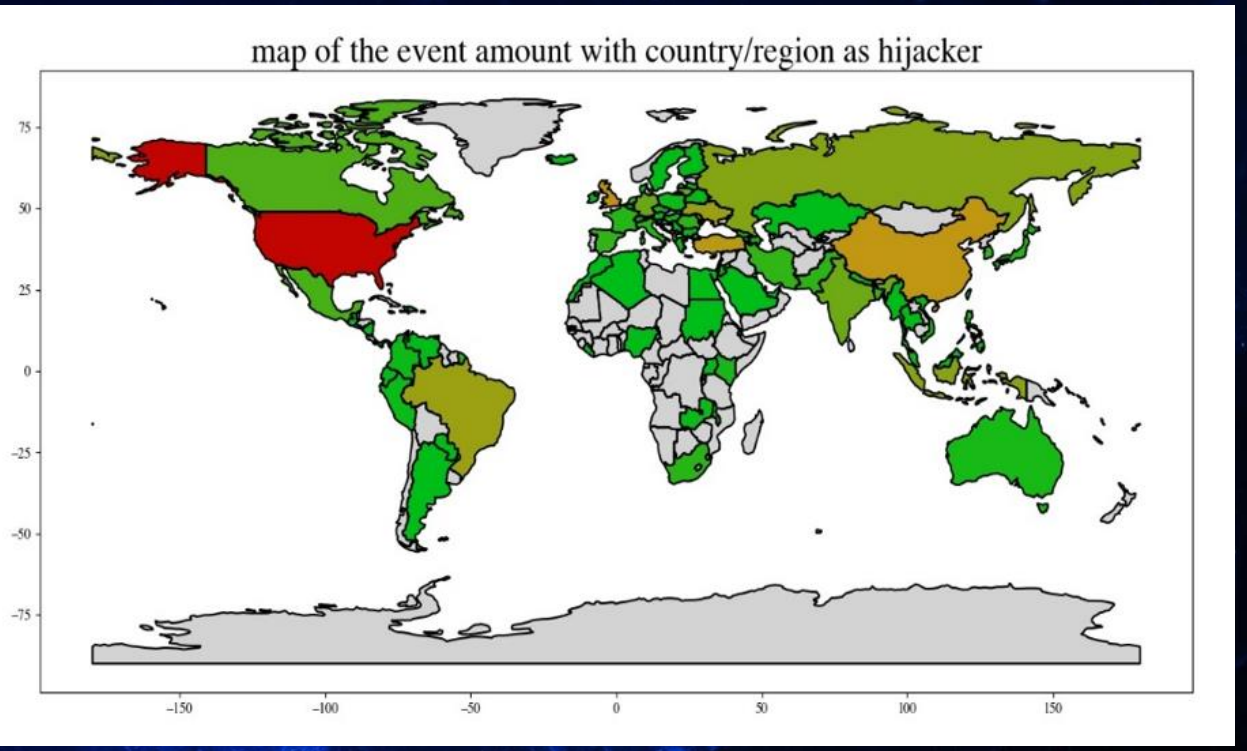


Results

Most routing prefix hijacking events have little impact,

with about **60**% of events observed by only **1**%-**20**% of watchpoints.





Results

Some of them are **notorious**.

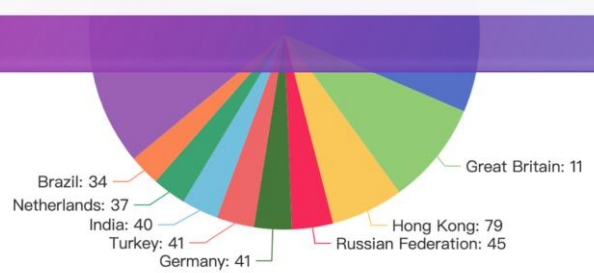
AS13414 hijacked by **AS8342**

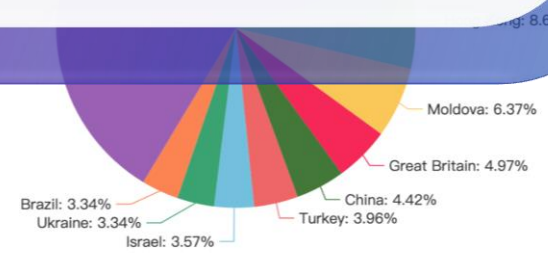
TWITTER RTCOMM-AS, RU

Crypto Exchange KLAYswap lost **$1.9 million** after BGP hijacking

length distribution of hijacked IPv4 prefix

length distribution of hijacked IPv6 prefix

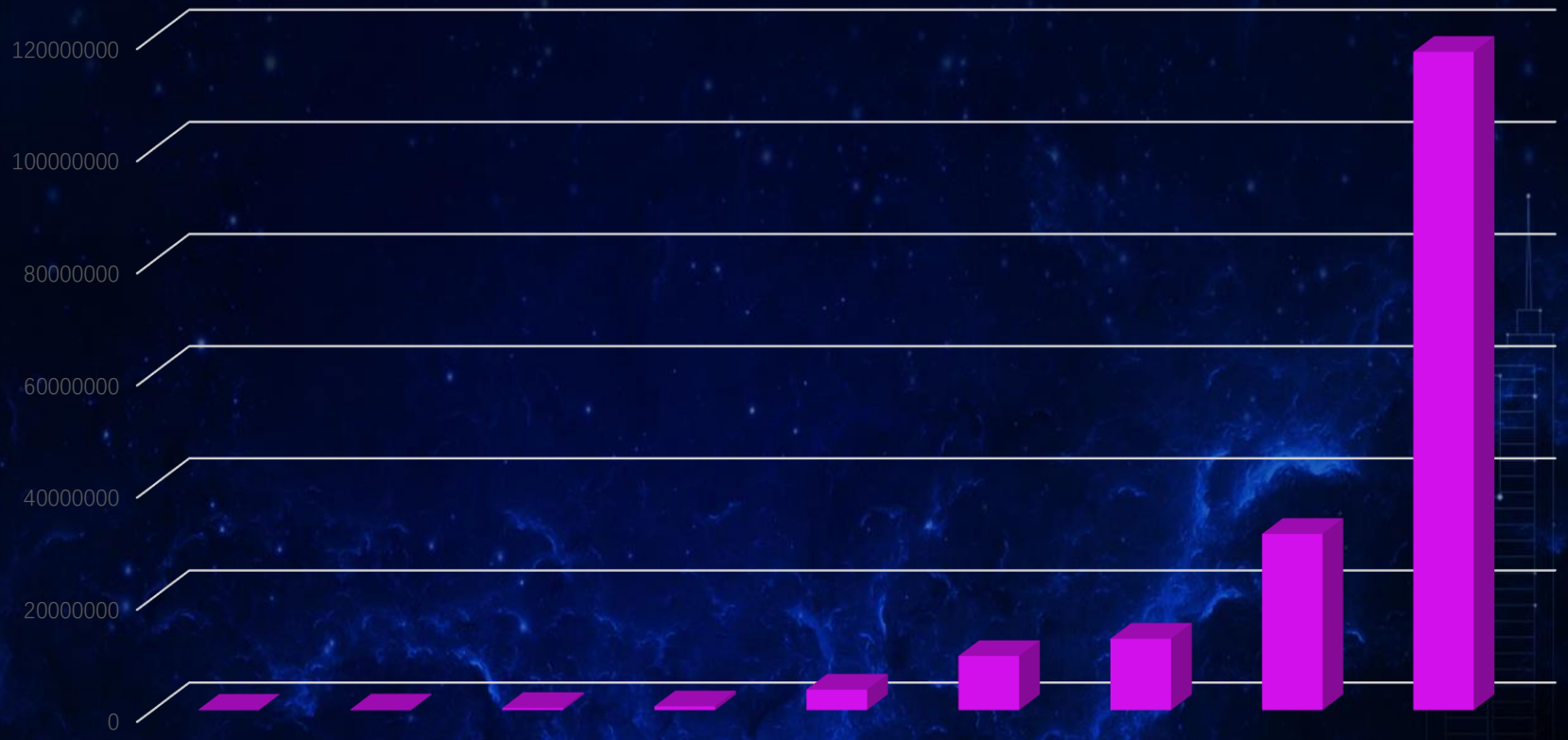




high-risk events medium-risk events low-risk events

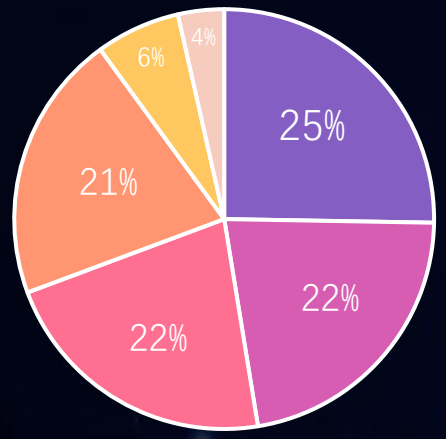
Internet services

- **Network services**: the combination of IP address and port, is the service access entrance.
- **Method**: port scanning, intelligent service protocol detection, software banner identification
- **Classification**:
  - Infrastructure
  - Video IOT
  - Database
  - VPN
  - Industrial Internet
  - Blockchain
  - Honeypot
  - OA system
  - Satellite Internet

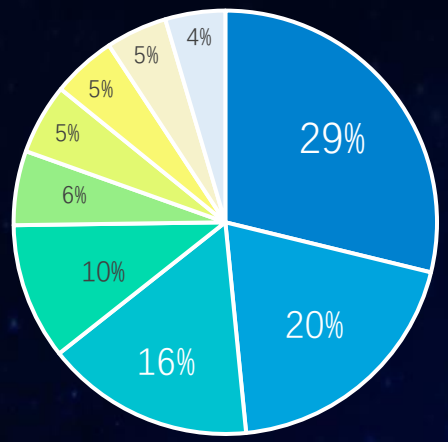


Internet services and city population

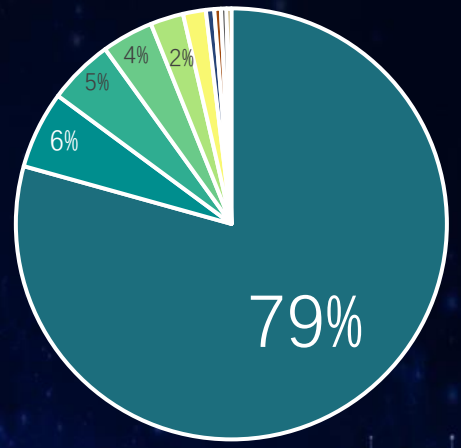
Infrastructure, industrial, video, vpn, honeypot



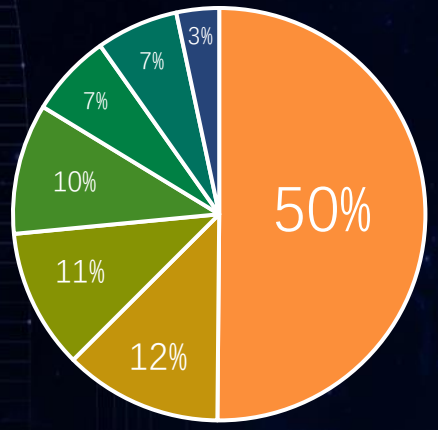
- Amazon CloudFront httpd
- CloudFront
- Incapsula CDN
- Cloudflare
- AkamaiGHost
- Akamai CDN



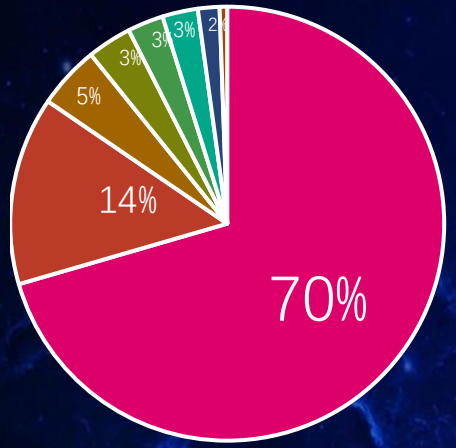
- SOMFY
- Tridium Inc.
- TAC-Xenta-Controller
- Siemens AG.
- The jQuery Foundation.
- moxa
- Lantronix, Inc.
- SoftPLC Corporation
- Gentoo Foundation, Inc.



- Hikvision杭州海康威视数字技术股份有限公司（Hikvision海康威视网络摄像头/海康威视Hikvision Web服务器）
- D-Link友讯科技股份有限公司（D-Link DCS-932L摄像头/D-Link DCS-5020L摄像头等）
- Dahua浙江大华技术股份有限公司（大华摄像头）
- 浩云科技股份有限公司（浩云安防）
- 深圳市同为数码科技股份有限公司（TVT同为视频监控）
- intelbras Inc.（Intelbras监控摄像头）
- Samsung三星集团（三星摄像头SamsungDVR）
- lorex_technology（Lorex视频监控）
- netwavesystems（Netwave-网络摄像机）
- 杭州雄迈信息技术有限公司（雄迈视频监控设备）



- IKE VPN
- MikroTik-PPTP-VPN
- Fortios
- Fortigate-sslvpn下一代VPN防火墙
- DrayTek-Vigor路由器PPTP-VPN入口
- Fortinet security device httpd



- kippo蜜罐
- Kojoney SSH 蜜罐
- glastopf蜜罐
- elasticsearch蜜罐
- amun http蜜罐
- imap 蜜罐
- HFish蜜罐
- Honeypy ES蜜罐

Findings

- Network services can be an indicator of real world society,
  - **Parallel development**: **Hanoi City** and **Ho Chi Minh City**
  - **Large capital**: **South Korea** and **Japan**,
    most network services are in their capital city.
  - **Small capital**: **United States**, **Brazil**, **India**, **Turkey**,
    the number of network services in the capital
    is much smaller than that of the largest cities.
- **Top 3 cities by network services number**:

  Hong Kong, **Los Angeles**, and **Seoul**.

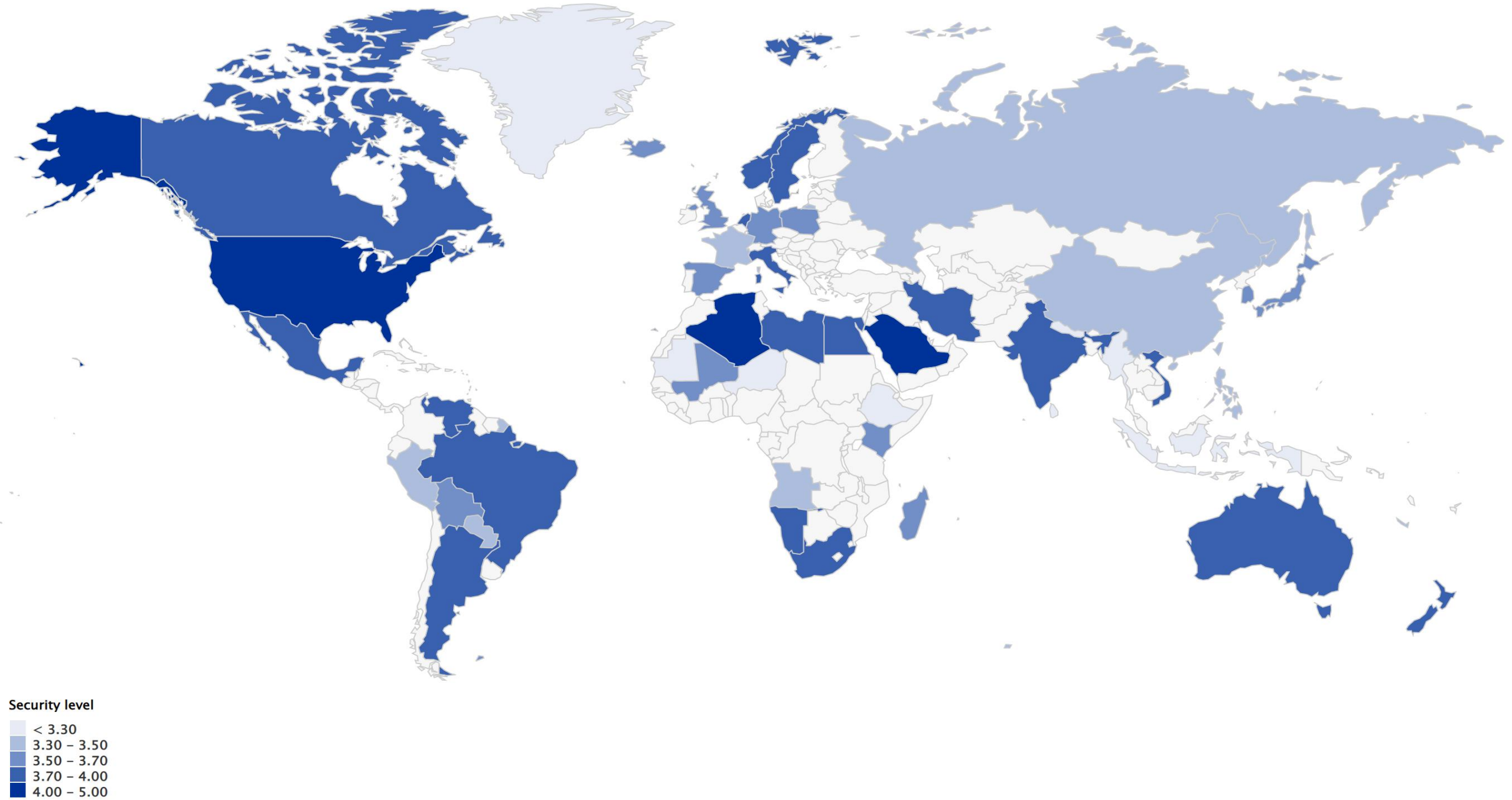
Internet services security

- **Method**: vulnerabilities are inferred from the identified protocol and servers' banners, and compare with the public CVE database

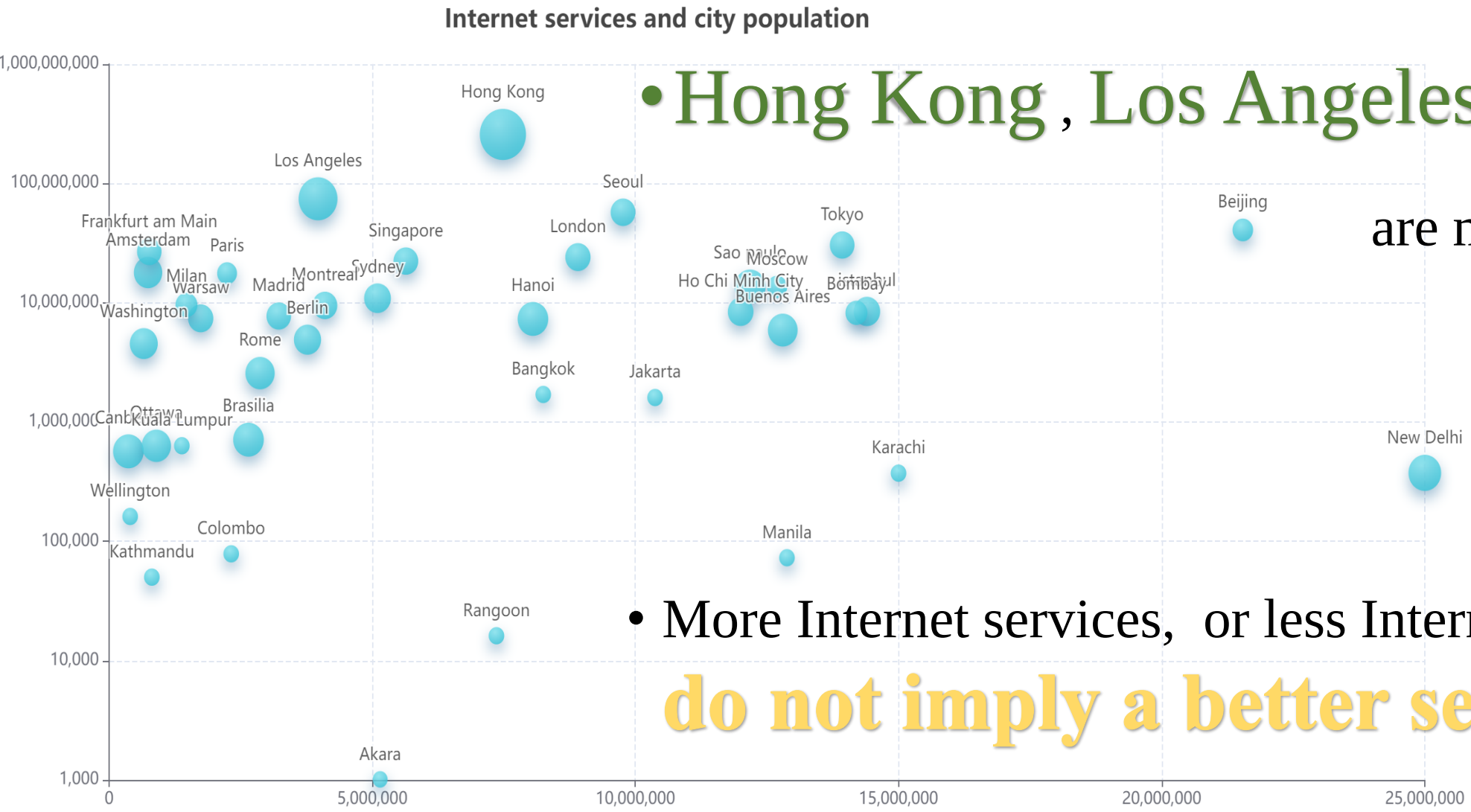
- **Security index**: measure the ratio of the number of network services to the number of possible vulnerabilities, to be more intuitive, we use a logarithmic treatment similar to decibels

  ex=Log(n/x)

  - N is the number of network services
  - X is the number of possible vulnerabilities


Security level
< 3.30
3.30 – 3.50
3.50 – 3.70
3.70 – 4.00
4.00 – 5.00

Findings



- Hong Kong , Los Angeles , New Delhi are more **secure**

- More Internet services, or less Internet services, **do not imply a better security level**

Conclusions: Cyberspace surveying and mapping (CSM)

- Current approach: measure, analyze, discover and visualize the cyberspace resources and their relationships, network service and routing system are important building blocks
- Further efforts: as a complex combination of physical domain, logical domain and social domain, it can provide many aspects of information, thus a cross-disciplinary view may be helpful to understand the cyberspace.
- Limitations: data may not be perfect, analysis may be preliminary, however, the statistics in this report may provide insights for future surveying and mapping practice.

Tsinghua University-Qihoo Technology Joint Research Center