奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

美国查封伊朗媒体域名事件技术分析

刘保君 清华大学-奇安信联合研究中心

2021-07-07

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

1

事件回顾
Event Timeline

6月22日，美国司法部查封36个伊朗媒体域名

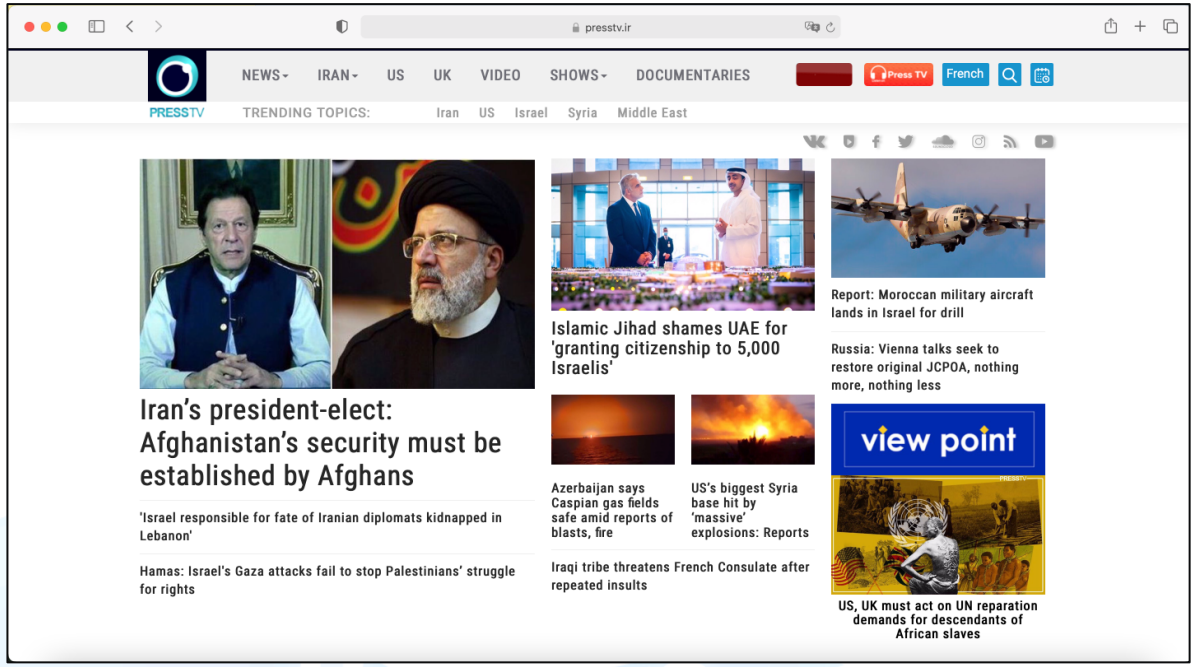
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

- **部分查封的域名**
  - 伊朗英文电视台 presstv.com
  - 伊朗世界新闻卫视 alalamtv.net
- **查封的理由**
  - “违反美国的制裁措施”
  - “传播针对美国的虚假消息”

被查封的域名 presstv.com 主页

6月22日，美国司法部查封36个伊朗媒体域名

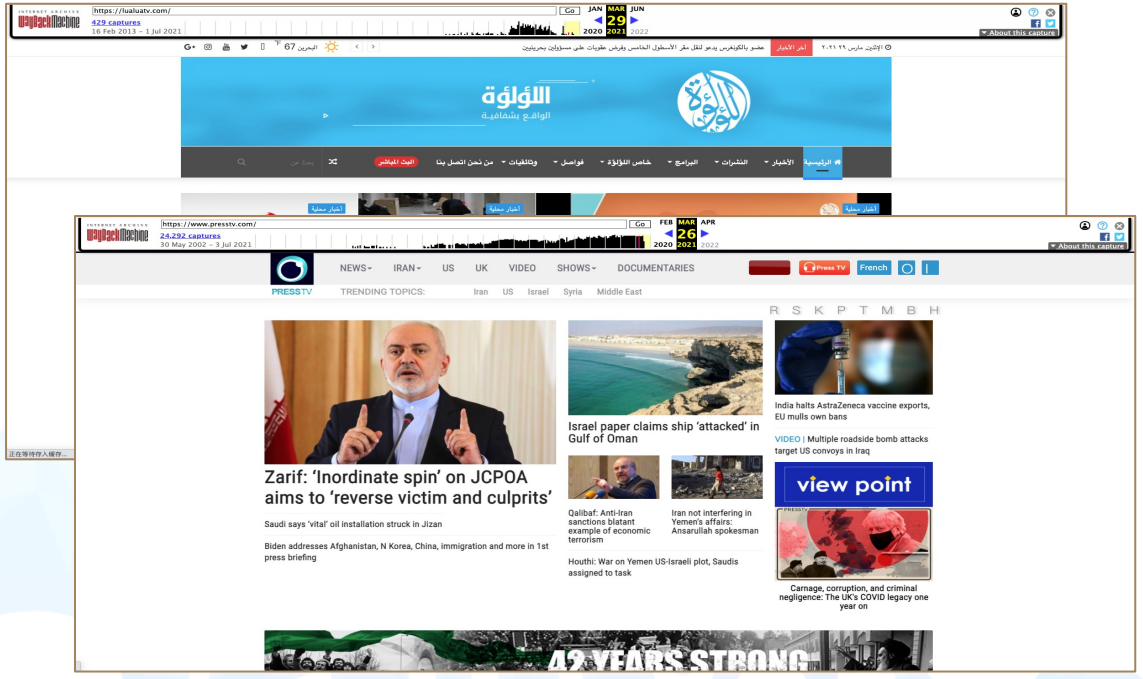
- 部分查封的域名
  - 伊朗英文电视台 presstv.com
  - 伊朗世界新闻卫视 alalamtv.net
- 查封的理由
  - “违反美国的制裁措施”
  - “传播针对美国的虚假消息”
- **伊朗媒体更换域名，恢复服务**
  - presstv.com → presstv.ir



presstv.ir 网站主页

伊朗媒体域名的网页内容 – Internet Archive

- 绝大部分网站内容为阿拉伯语，仅有少量网站为英文

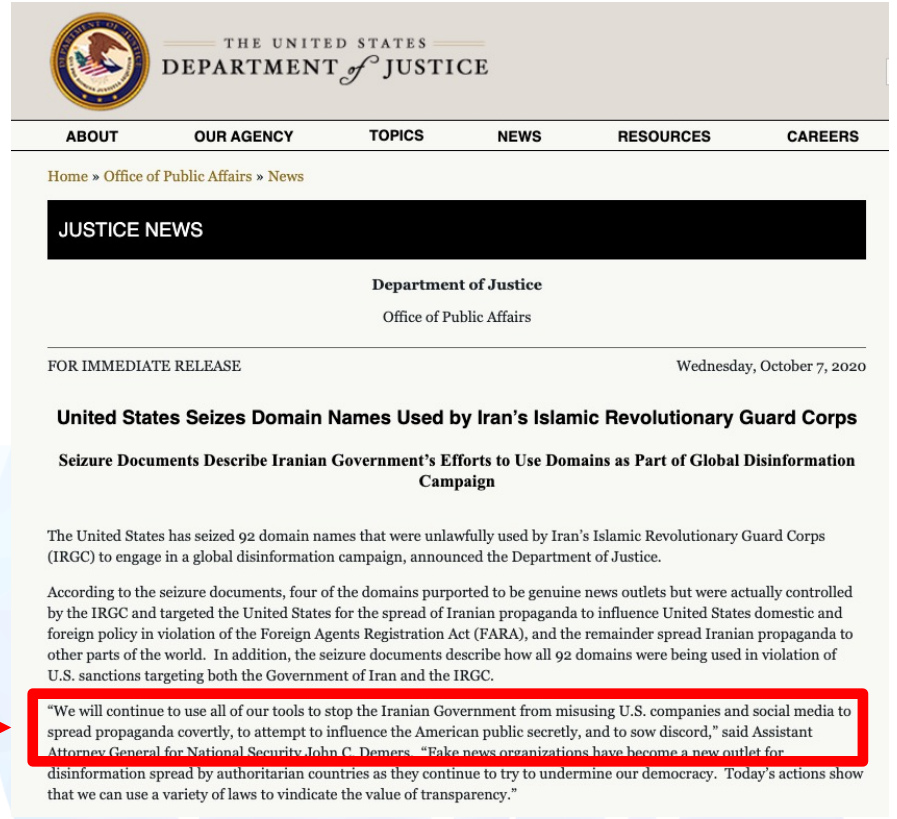


2020年10月，美国查封92个伊朗革命卫队域名

- **查封的理由**
  - “从事虚假宣传活动”
  - “影响美国国内和外交政策”

我们将继续使用一切工具，阻止伊朗政府滥用美国公司和社交媒体进行政治宣传活动，试图秘密影响美国公众并挑拨离间。

--国家安全助理司法部长



THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | TOPICS | NEWS | RESOURCES | CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Wednesday, October 7, 2020

United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps

Seizure Documents Describe Iranian Government's Efforts to Use Domains as Part of Global Disinformation Campaign

The United States has seized 92 domain names that were unlawfully used by Iran's Islamic Revolutionary Guard Corps (IRGC) to engage in a global disinformation campaign, announced the Department of Justice.

According to the seizure documents, four of the domains purported to be genuine news outlets but were actually controlled by the IRGC and targeted the United States for the spread of Iranian propaganda to influence United States domestic and foreign policy in violation of the Foreign Agents Registration Act (FARA), and the remainder spread Iranian propaganda to other parts of the world. In addition, the seizure documents describe how all 92 domains were being used in violation of U.S. sanctions targeting both the Government of Iran and the IRGC.

"We will continue to use all of our tools to stop the Iranian Government from misusing U.S. companies and social media to spread propaganda covertly, to attempt to influence the American public secretly, and to sow discord," said Assistant Attorney General for National Security John C. Demers. "Fake news organizations have become a new outlet for disinformation spread by authoritarian countries as they continue to try to undermine our democracy. Today's actions show that we can use a variety of laws to vindicate the value of transparency."

美国司法部公共事务部新闻

国内新闻媒体对该事件的报道与解读

环球网 ☰

警惕！美国如何能“封杀”伊朗网站？中国专家说出真相

环球时报 刘洋 2021-06-24 06:18 TT 小字

【环球时报综合报道】美国对伊朗网站的“封杀”举动引起全球网络安全专家的警惕。俄罗斯卫星网22日称，美国司法部查封了超过30个伊朗网站。报道称，此次查封目前仅针对美国管辖范围内的.com和.net网站域名，暂未涉及伊朗网站域名，因此部分网站通过更换伊朗域名.ir已重新上线。

天津大学法学院互联网政策与法律研究中心主任秦安23日接受《环球时报》记者采访时表示，这只是美国网络霸权的牛刀小试。美国不光能查封网站，它甚至能让整个国家从全球互联网版图中消失，核心在于美国控制着绝大部分根服

国内新闻媒体对该事件的报道与解读

环球网

警惕！美国如何能“封杀”伊朗网站？中国专家说出真相

环球时报 刘洋 2021-06-24 06:18 Tт 小字

【环球时报综合报道】美国对伊朗网站的“封杀”举动引起全球网络安全专家的警惕。俄罗斯卫星网22日称，美国司法部查封了超过30个伊朗网站。报道称，此次查封目前仅针对美国管辖范围内的.com和.net网站域名，暂未涉及伊朗网站域名，因此部分网站通过更换伊朗域名.ir已重新上线。

天津大学法学院互联网政策与法律研究中心主任秦安23日接受《环球时报》记者采访时表示，这只是美国网络霸权的牛刀小试。美国不光能查封网站，它甚至能让整个国家从全球互联网版图中消失，核心在于美国控制着绝大部分根服

这只是美国网络霸权的牛刀小试。美国不光能查封网站，它甚至能让整个国家从全球互联网版图中消失，核心在于美国控制着绝大部分根服务器和域名管理服务器。

天津大学法学院

互联网政策与法律研究中心

国内新闻媒体对该事件的报道与解读

环球网

警惕！美国如何能“封杀”伊朗网站？中国专家说出真相

环球时报 刘洋 2021-06-24 06:18 TT 小字

【环球时报综合报道】美国对伊朗网站的“封杀”举动引起全球网络安全专家的警惕。俄罗斯卫星网22日称，美国司法部查封了超过30个伊朗网站。报道称，此次查封目前仅针对美国管辖范围内的.com和.net网站域名，暂未涉及伊朗网站域名，因此部分网站通过更换伊朗域名.ir已重新上线。

天津大学法学院互联网政策与法律研究中心主任秦安23日接受《环球时报》记者采访时表示，这只是美国网络霸权的牛刀小试。美国不光能查封网站，它甚至能让整个国家从全球互联网版图中消失，核心在于美国控制着绝大部分根服

头条 今日头条 打开

互联网霸权真挺猛！美国忽然没收伊朗媒体域名 哈梅内伊没辙

木春山谈天下 原创 关注
06月23日 · 公共外交中心研究员 外交...

木叔这篇国际评论，来分析美国和伊朗关系。

伊朗人选出强硬派新总统莱西之后，美国和伊朗关系如何走向？不仅木叔在关注，很多朋友也在分析。

虽然莱西没有否认要继续和美国讨论伊核协议，并且要求美国撤销全部对伊朗的制裁，但这并不意味着美国和伊朗之间长达40多年的隔阂能一朝化解。

互联网基本就是西方人的底层设计，美国人对此有很大的安全掌控权。

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

2

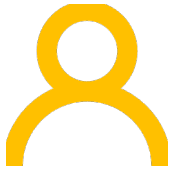
技术分析
Technical Analysis

互联网域名注册与管理机制

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022



域名注册人

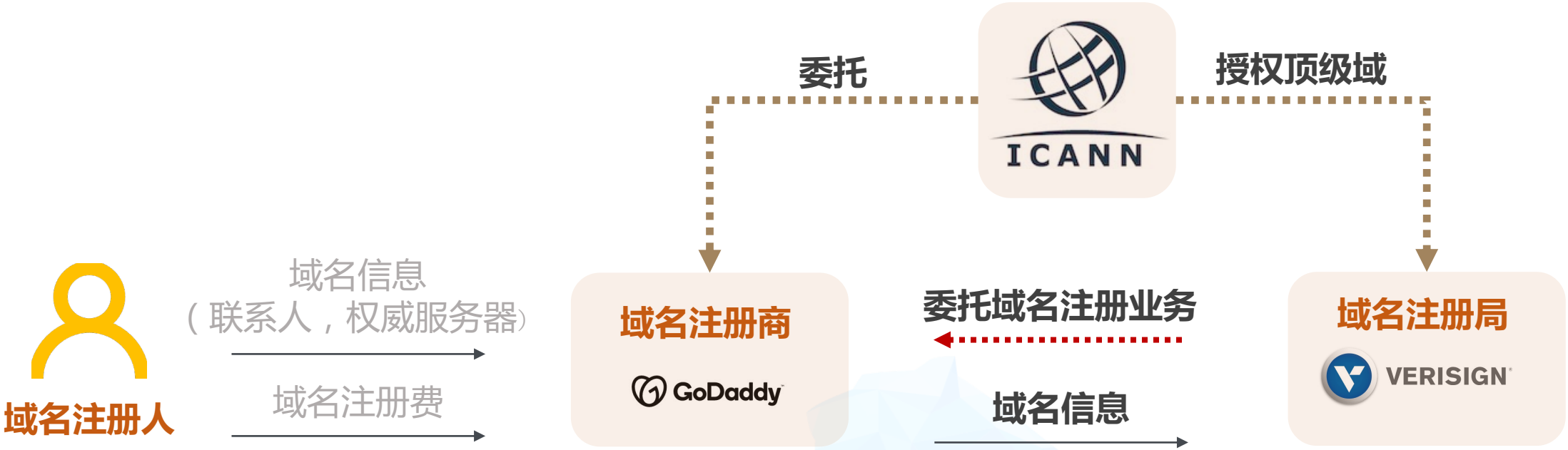
域名信息
（联系人，权威服务器）

域名注册费

域名注册商

GoDaddy

互联网域名注册与管理机制



域名注册数据分析

- **32个域名，从属于2个域名注册局，20余个域名注册商**
  - 涉及4个顶级域：.com .net .org 以及 .tv
  - 涉及20个域名注册商，7家为非美国注册商

  - Verisign 公司管理 .com .net .tv顶级域， PIR公司管理 .org 顶级域
  - 注：Verisign 与 PIR 公司均位于美国

本次域名查封，是域名注册局行为，还是域名注册商行为？

域名注册WHOIS数据变更分析

- **本次域名查封事件，是美国执法部门要求域名注册局执行的，与注册商不存在直接关系。**

```
Domain Name: PRESSTV.COM
Registry Domain ID: 85275201_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.instra.net
Registrar URL: http://www.instra.com
Updated Date: 2021-06-22T14:31:55Z
Creation Date: 2002-04-05T03:55:48Z
Name Server: NS-1088.AWSDNS-08.ORG
Name Server: NS-1900.AWSDNS-45.CO.UK
Name Server: NS-388.AWSDNS-48.COM
Name Server: NS-977.AWSDNS-58.NET
```

更新日期：2021年6月22日

权威服务器被更改为AWSDNS

注册局视角：

域名权威服务器信息发生变更

注册商视角：

域名权威服务器信息未变更

```
Domain Name: presstv.com
Registry Domain ID: 85275201_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.instra.net
Registrar URL: http://www.instra.com
Updated Date: 2021-04-03T15:04:08Z
Creation Date: 2002-04-05T03:55:48Z
Name Server: ns1.presstv.ir
Name Server: ns2.presstv.ir
```

更新日期：2021年4月3日

权威服务器未被更改

3 域名接管的现有实践

Security Practices

域名接管是技术社区常用的安全管控手段

- 当域名被滥用时，需要权威机构介入，强行接管控制域名解析

僵尸网络

处方药

儿童色情

盗版侵权

究竟由谁来发起域名接管的流程？

域名接管流程的现有实践（一）

- **用户或安全厂商，发起域名滥用（DNS Abuse）投诉**
  - 一般共识性的域名滥用情况
    - 恶意软件、僵尸网络
    - 钓鱼攻击、垃圾邮件
- **用户申请域名仲裁，启动快速中止程序**
  - 域名争议问题
    - 域名商标
    - 域名抢注
  - 域名在仲裁期间将被锁定

域名滥用投诉在线表单

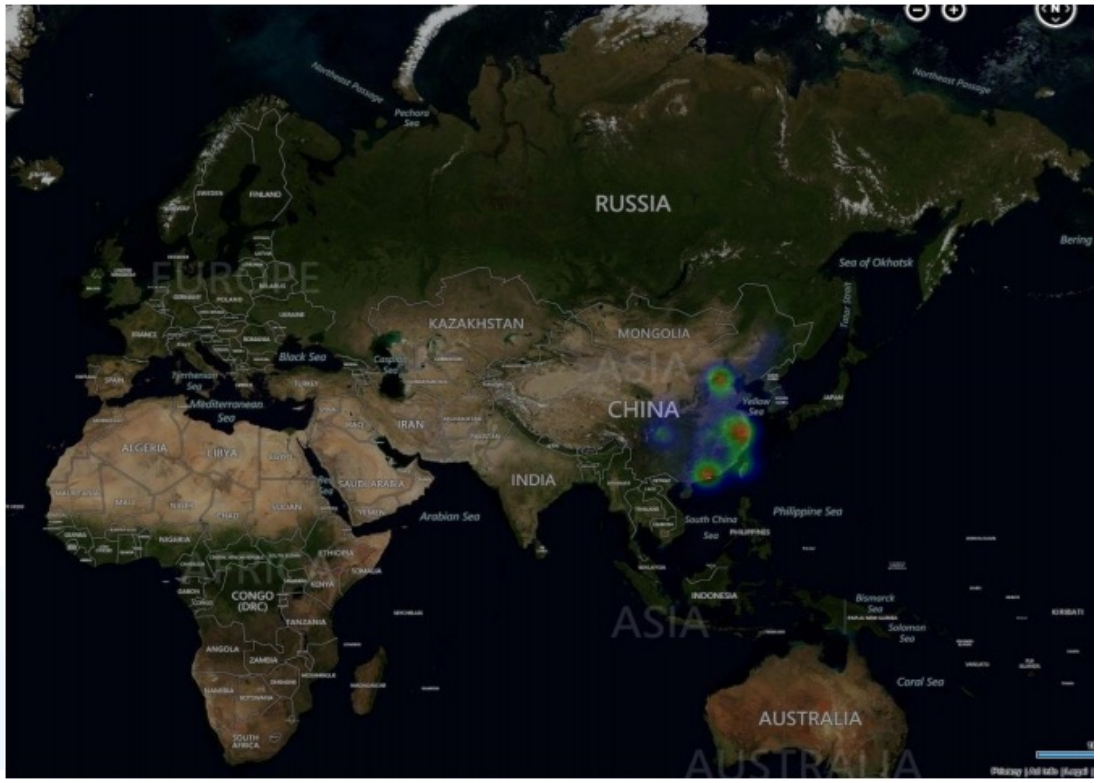
域名接管流程的现有实践（二）

- **执法机构申请法院命令，进行域名接管**
  - “扣押令”（Seizure warrant）
  - “限制令”（Restraining order）

- 域名可被视为一种资产。通过法院命令接管本国域名注册管理的域名，似乎已经成为一种常见的司法实践。

历史上知名的域名接管事件（一）

- **3322.org**
  - 3322.org是中国某公司运维的动态域名，曾经被用作Nitol僵尸网络的域名
  - 为打击Nitol僵尸网络，微软公司获得法院许可，接管动态DNS服务提供商 3322.org 域名



僵尸网络受感染主机地理位置分布

历史上知名的域名接管事件（二）

- **dajaz1.com**
  - 美国知名嘻哈音乐网站
  - 因四首音乐未获得版权，被美国唱片业协会举报
  - 美国联邦当局将域名临时查封，一年之后将域名归还

4

讨论
Discussion

域名接管流程缺乏最佳实践（Best Practices）

- 域名滥用的适用范畴，仍然缺乏清晰明确的判定标准？
- 域名注册机构如何处理跨境法院发起的域名接管请求？
- 域名被查封后，未来能否被恢复？

互联网域名资产的安全风险评估

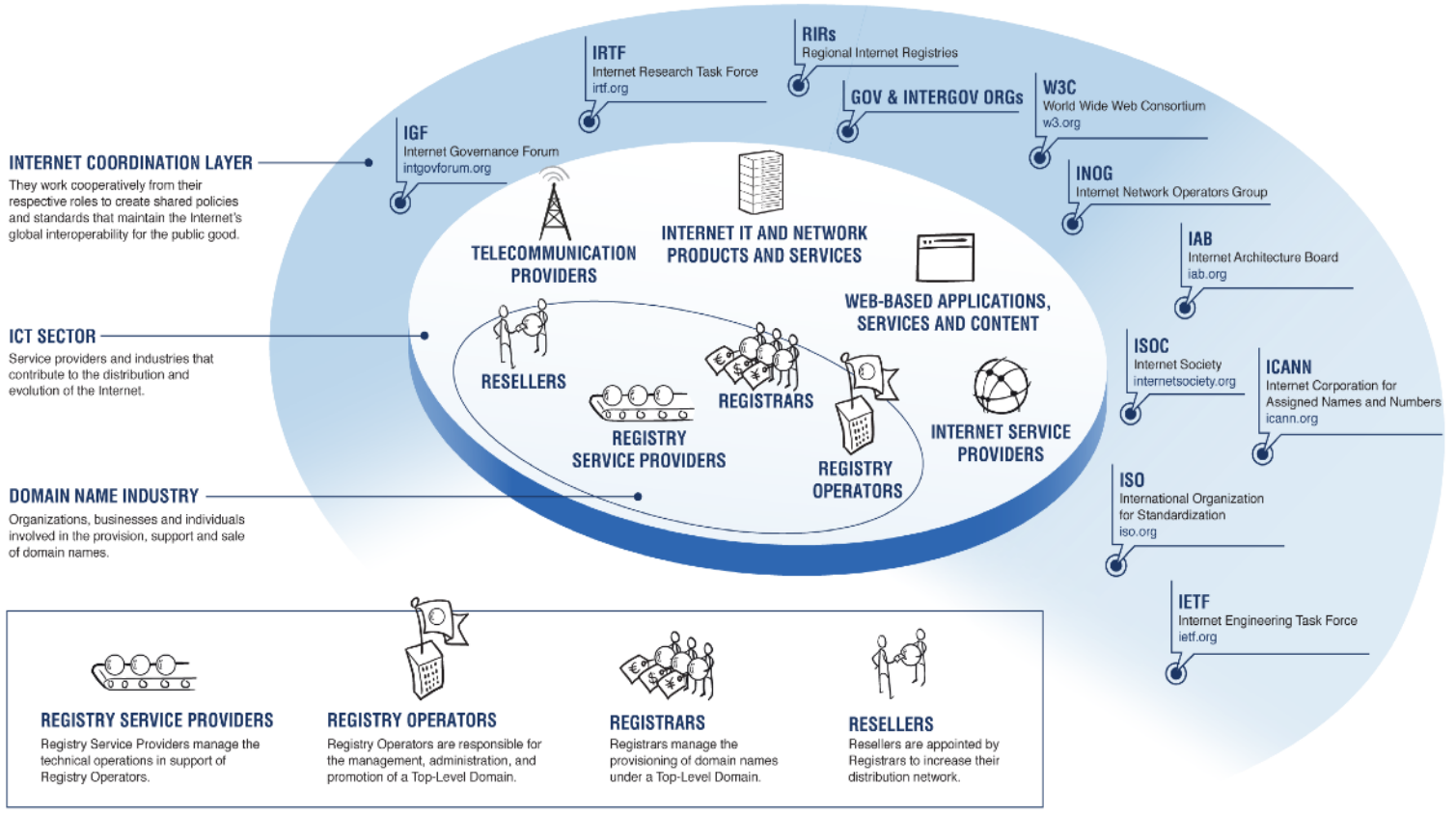
- 美国执法部门能否通过类似途径查封互联网上所有域名？
- 美国真的能够完全控制互联网或者域名系统吗？
- .com 域名被美国法院强行查封的风险是否永久存在？

域名生态中每个机构的作用都是独特且有限的

对域名系统不矮化，不神话，不泛化。以理性客观之精神，多研究具体问题，寻找解决之道。

ICANN北京合作中心

张建川博士



奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

谢谢！