网络空间视角下的哈萨克斯坦动乱

知道创宇 404 实验室

版本	时间	描述
第一版	2022 年 3 月 17 日	完成《网络空间视角下的哈萨克斯坦动乱》第一版

目录

一．背景介绍

2022 年伊始，哈萨克斯坦西部石油重镇扎瑙津爆发抗议活动，随后迅速蔓延到包括阿拉木图在内的其他城市。抗议从抵制液化石油气价格飙升逐渐发展为暴力骚乱。部分示威者甚至闯进前首都阿拉木图政府，阿拉木图市政府和检察院遭纵火。但随着集体安全条约组织成员国向哈萨克斯坦派遣军队提供援助，哈萨克斯坦的局势逐渐得到控制。

在整个动乱事件的背景中，哈萨克斯坦政府切断全国网络成为了控制局势稳定的重要一环。哈萨克斯坦数字发展与航空工业部代理部长穆兴表示：网络的关闭是由于恐怖分子利用网络来进行协调和沟通。

根据新闻报道，2022 年 1 月 5 日晚，哈萨克斯坦政府切断了全国的网络。2022 年 1 月 7 日，哈萨克斯坦总统托卡叶夫表示政府已决定恢复部分地区的网络服务。2022 年 1 月 10 日，阿拉木图市和其它部分地区的移动网络与有线网络恢复、即时通信软件和社交网站也恢复运行。

在切断网络和网络恢复的这几天时间内，哈萨克斯坦的局势得以控制，全国各地的宪法秩序已大体恢复。在此，我们也将从网络空间的视角入手，看一看在动乱发生前后，哈萨克斯坦的网络有哪些变化。

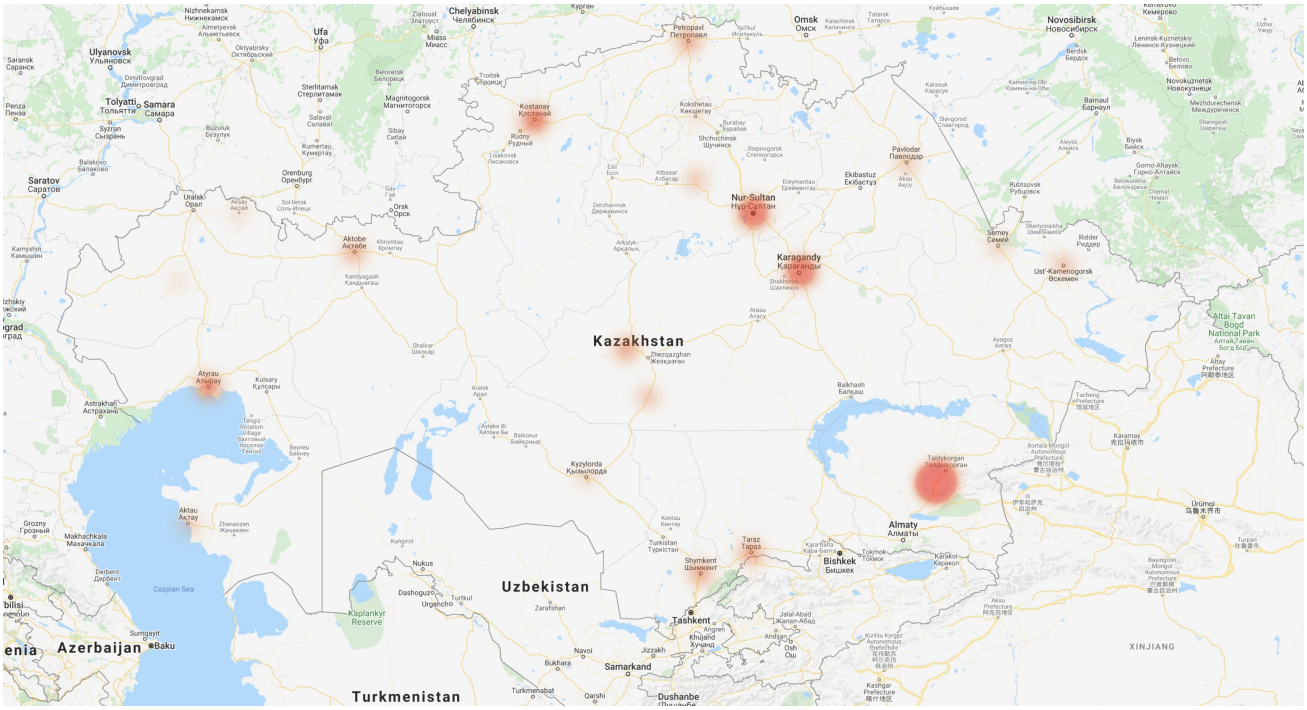
注：本文部分引用的部分数据可能因各种原因导致判断不准确、本文关于 IP 地址的位置解析主要依赖于 IP 库的数据，在部分地区的位置可能存在误差，故本报告所含信息仅供参考。

二．动乱前的哈萨克斯坦网络空间

2.1 哈萨克斯坦网络设备分布情况

截止 2022 年 1 月 5 日 24 时，ZoomEye 网络空间搜索引擎一共收录哈萨克斯坦 1712153 个 ip 和 356427 个域名的 4786464 条历史数据，其中 4786341 条数据可以定

位到具体的地理位置。根据地理位置信息进行统计，前首都阿拉木图北部、现首都努尔苏丹、卡拉干达都是网络设备大量聚集的地区。



2.2 哈萨克斯坦的互联网发展情况以及 GPON 路由的占比情况

2017 年，哈萨克斯坦政府通过“数字哈萨克斯坦”国家规划，旨在依靠数字技术加快国家经济发展，提高居民生活质量。从哈萨克斯坦的整体数据来看，哈萨克斯坦已经达到较高的互联网普及率，但互联网相关产业仍在发展中：

1. 互联网已经走进了哈萨克斯坦的千家万户。根据网络设备类型进行统计，哈萨克斯坦端口数据中 GPON Home Gateway 占比超过 22.04%,实际数量超过 1055345 条。GPON Home Gateway 是一款常见的 GPON 设备，也就是所谓的光猫。GPON Home Gateway 所属的网络自制域多是 AS9198（哈萨克斯坦电信公司）
2. 互联网相关行业仍有很大发展空间。根据 AS 自治域的统计结果，排名前列的也多是网络运营商、VPS 提供商，其中甚至出现了俄罗斯的抗 DDoS 自治域。整体来说，互联网接入、互联网服务提供商居多，利用互联网进行各类商务活动的企业占比较少。这类企业仍有很大的发展空间。

哈萨克斯坦的自治系统分布如下：大致和上述的互联网提供商一致，但也出现了俄罗斯的抗 DDoS 网段。

AS 自治域	数量	备注（公司名称/运营公司信息等）
9198	2981143	哈萨克斯坦电信
21288	714765	Beeline 是哈萨克斯坦的蜂窝、移动和有线互联网运营商
48716	186017	ps.kz 提供网站托管服务
29355	149114	Kcell 提供移动语音电信服务、消息服务、多媒体和移动内容服务等增值服务，以及包括互联网接入在内的数据传输服务
207333	71256	Hoster.KZ 是哈萨克斯坦最大的托管服务提供商之一，是第一个获得认可的 .KZ 域名注册商
35104	54490	电信运营商
202958	48256	Hoster.KZ 是哈萨克斯坦最大的托管服务提供商之一，是第一个获得认可的 .KZ 域名注册商
57724	44352	俄罗斯的 DDOS-GUARD
41798	41796	电信运营商
35566	39755	Beeline 是哈萨克斯坦的蜂窝、移动和有线互联网运营商

在本次分析中，我们结合以下两条外部数据，决定通过额外关注 GPON Home Gateway 的数量变化来了解哈萨克斯坦的网络恢复情况：

1. 根据世界银行的统计数据，哈萨克斯坦 2019 年总人口为 18513673。
2. 根据联合国关于哈萨克斯坦《消除对妇女一切形式歧视公约》中的内容可知，2009 年哈萨克斯坦每个家庭由 3.5 个成员组成。

(GPON 设备数量 * 家庭成员数量) /(哈萨克斯坦人口总数 * 哈萨克斯坦电信公司份额占比) = 32.03%

这说明接近三分之一的哈萨克斯坦家庭使用哈萨克斯坦电信公司网络和互联网紧密相连。GPON Home Gateway 在网络上恢复也就意味着对应地区的秩序已经恢复。

2.3 哈萨克斯坦外交政策和 SSL 证书信息/域名的关联

哈萨克斯坦在大国之间奉行政治上“多元平衡”与经济上积极合作的政策，尤其是在中、美、俄三国关系上，进行“等边三角形”外交。

从哈萨克斯坦的 SSL 证书的国家分布也可以看到，中国、美国、德国等国家的证书占比要远高于其本国的证书比例。一方面是因为其国民用来上网的光猫是中国生产的 GPON

Home Gateway，该光猫使用的 SSL 证书地区是中国，另一方面其 https 网站的 SSL 证书签名来自国外，例如 Let's Encrypt 等。同样也可以看出来，哈萨克斯坦本土网络发展进度较慢。仅有 4349 个 SSL 证书的国家为 KZ。

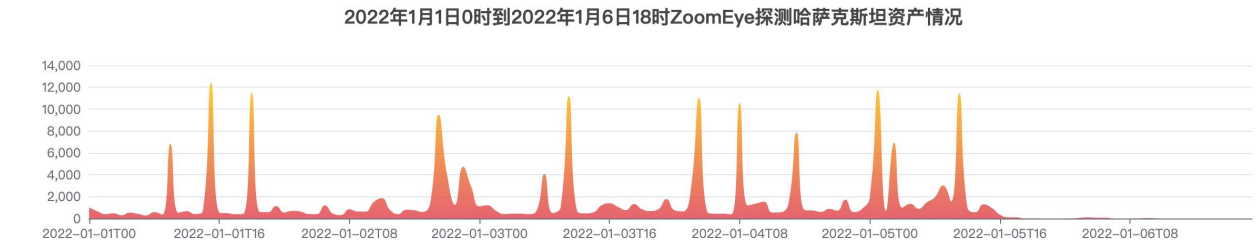
从解析后 IP 地址位于哈萨克斯坦境内的域名所属顶级域入手（为了防止泛解析影响最终的统计结果，所以子域名都归类到对应的二级域名下，计数为 1），哈萨克斯坦本地的.kz 顶级域占据了绝对的多数，其次是.com 域和.ru 域，而.cn 顶级域的数量仅为三条。这也从侧面说明了多国在哈萨克斯坦投资的侧重点不尽相同。

SSL 证书的国家/地区信息	数量
CN	591577
US	189981
无	33131
GB	16370
CH	10308
AT	4590
KZ	4340
RU	3465
XX	2609

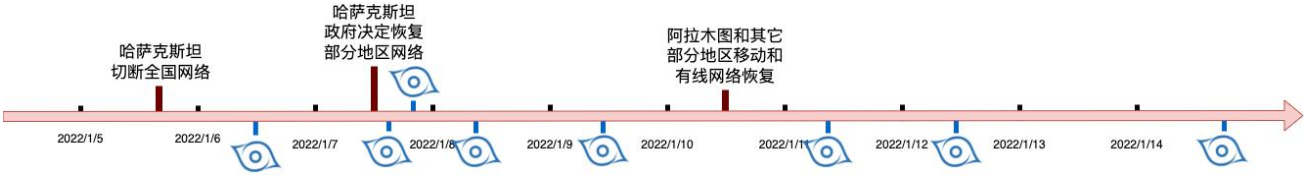
顶级域	数量
.kz	88733
.com	6257
.ru	4148
.org	629
.net	612
.info	537
.online	448
……	……
.cn	3

三．断网前后哈萨克斯坦网络空间设备的变化情况

根据 ZoomEye 网络空间搜索引擎的探测结果，2022 年 1 月 5 日 16 时开始，仅能探测到极少量哈萨克斯坦主机。该时间略早于新闻报道的中所述的 2022 年 1 月 5 日晚。

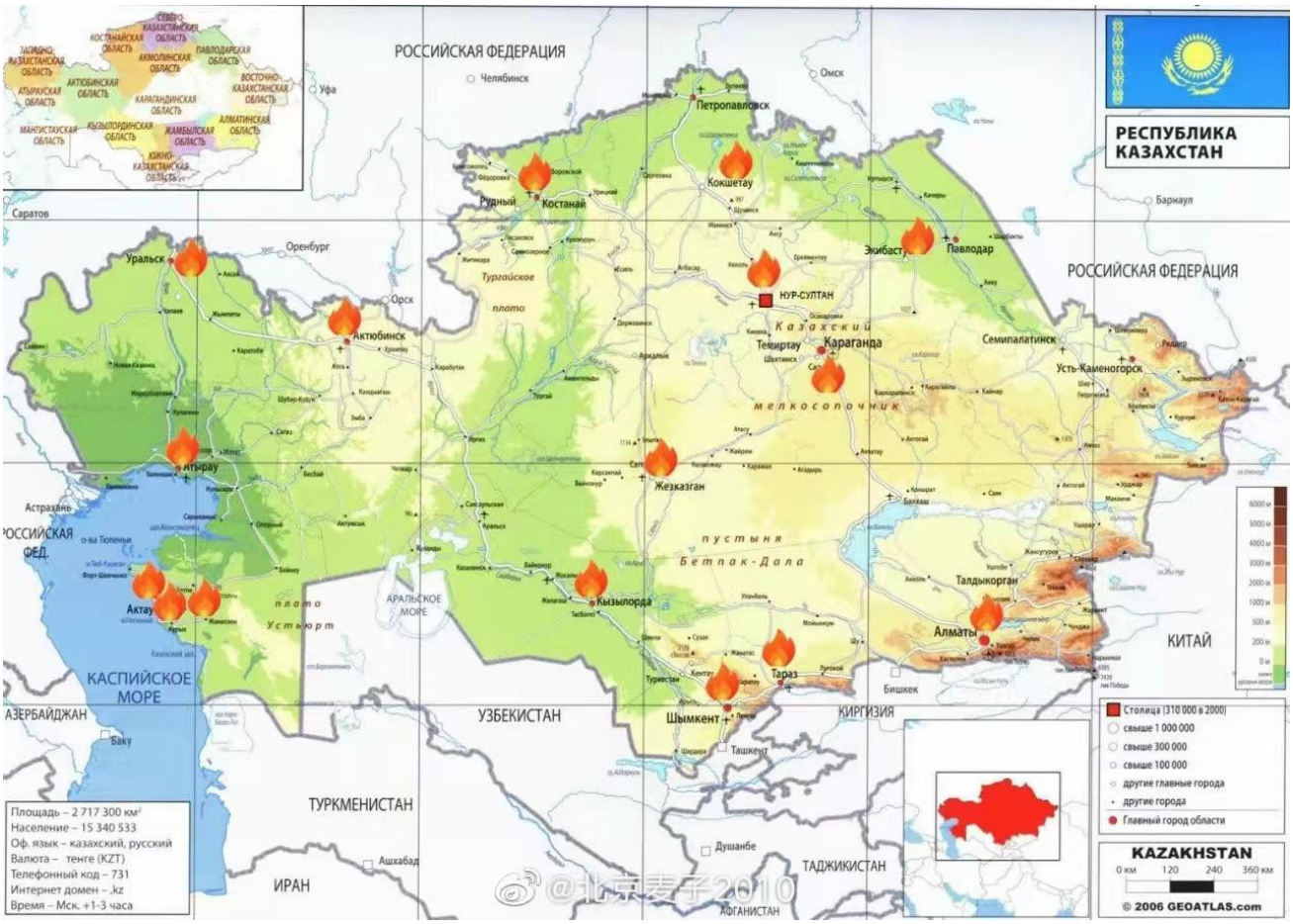


在意识到哈萨克斯坦切断网络这一事件爆发后，ZoomEye 网络空间搜索引擎在 2022 年 1 月 6 日 12 时、2022 年 1 月 7 日 15 时、2022 年 1 月 7 日 20 时、2022 年 1 月 8 日 9 时、2022 年 1 月 9 日 11 时、2022 年 1 月 11 日 9 时、2022 年 1 月 12 日 11 时、2022 年 1 月 14 日 18 时进行了多轮探测。



3.1 动乱爆发地点特点

在动乱初期，网上流传有一张哈萨克斯坦发生大规模游行抗议的城市图，和 2.1 节中的分布图相比较不难发现，大部分爆发游行抗议的城市互联网都较为发达。



图源自网络（https://share.api.weibo.cn/share/280817239.html）

但仔细对比之下也出现了一些细节上的差异：

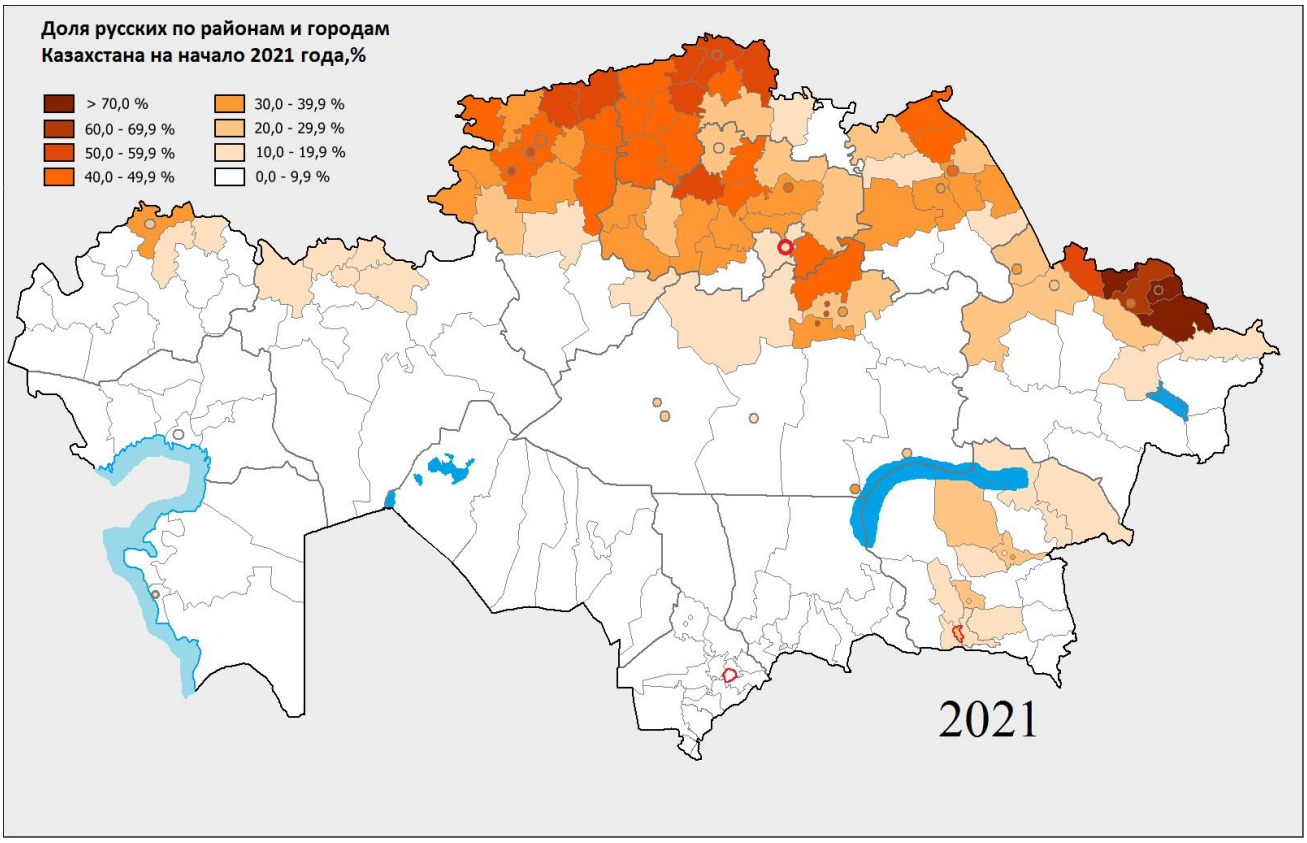
1. 哈萨克斯坦西部的曼格斯套州仅有极少的网络设备，但却包含抗议活动的发起地区扎瑙津，以及另外两个抗议爆发地点。

2. 哈萨克斯坦北部靠近俄罗斯边界的彼得罗巴甫尔、东部塞米伊、东部厄斯克门(俄语旧语：乌斯季卡缅诺戈尔斯克)虽然也存在网络设备聚集，但没有发生抗议游行等活动。

对于哈萨克斯坦西部的曼格斯套州，存在丰富的石油气资源，但是现代化发展有限，网络设备较少。从地理位置和经济发展上来看，哈萨克斯坦西部距离政治/经济中心较远、贫富差距不断拉大、油气收入分配不均都是引发抗议活动的原因。丰富资源产出分配不均和现代化的缓慢发展之间的冲突在这些城市蔓延发酵。

哈萨克斯坦同样是一个多民族的国家，根据外交部的数据，截止 2021 年 7 月，哈萨克斯坦约有 140 个民族，其中哈萨克族占 68%，俄罗斯族占 20%

（https://www.fmprc.gov.cn/web/gjhdq_676201/gj_676203/yz_676205/1206_676500/1206x0_676502/）。由于多方面的历史原因，哈萨克斯坦的俄罗斯族人主要聚集在哈萨克斯坦北部地区。从 2021 年哈萨克斯坦俄罗斯族人各城市的占比图中可以看到，哈萨克斯坦北部彼得罗巴甫尔、东部塞米伊、东部厄斯克门(俄语旧语：乌斯季卡缅诺戈尔斯克)均是俄罗斯族占比极高的地区。这也许是这些地区没有发生抗议游行活动的原因之一。

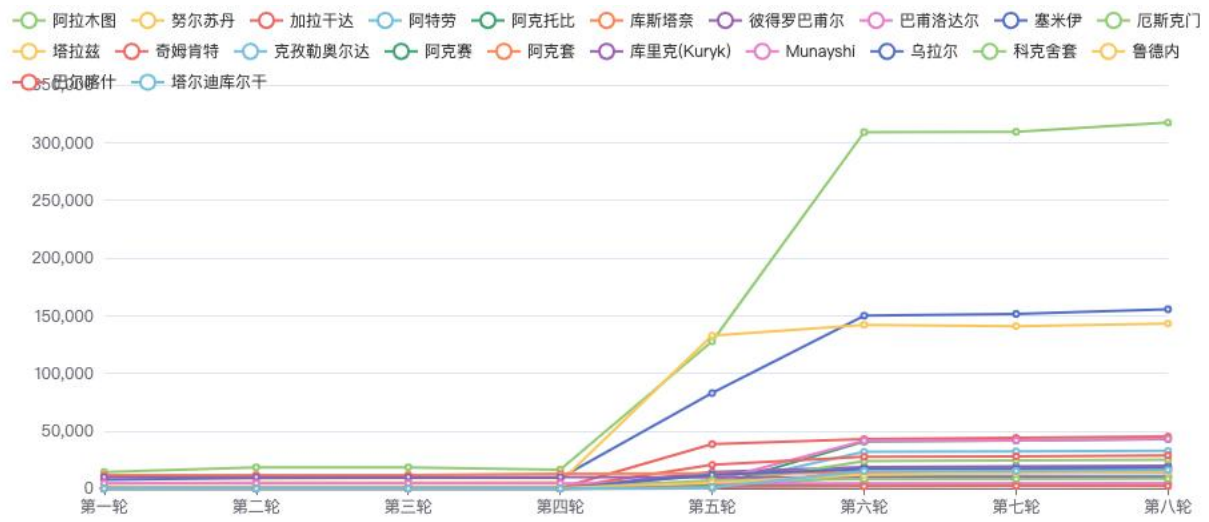


图来源于网络（https://tr.wikipedia.org/wiki/Kazakistan%27%C4%B1n_Etnik_Demografisi#/media/Dosya:Russians_in_Kazakhstan_Rus.png）

结合事后的哈萨克斯坦总统托卡耶夫给这场动荡定性为未遂政变来看，本次动乱可能主要集中发生在哈萨克族人自身，作为哈萨克斯坦境内第二大名族俄罗斯族则牵涉较少。

3.2 断网恢复期间的差异性

在对多轮探测的数据进行分析后，哈萨克斯坦境内各城市的网络恢复大致呈现出三种状态：

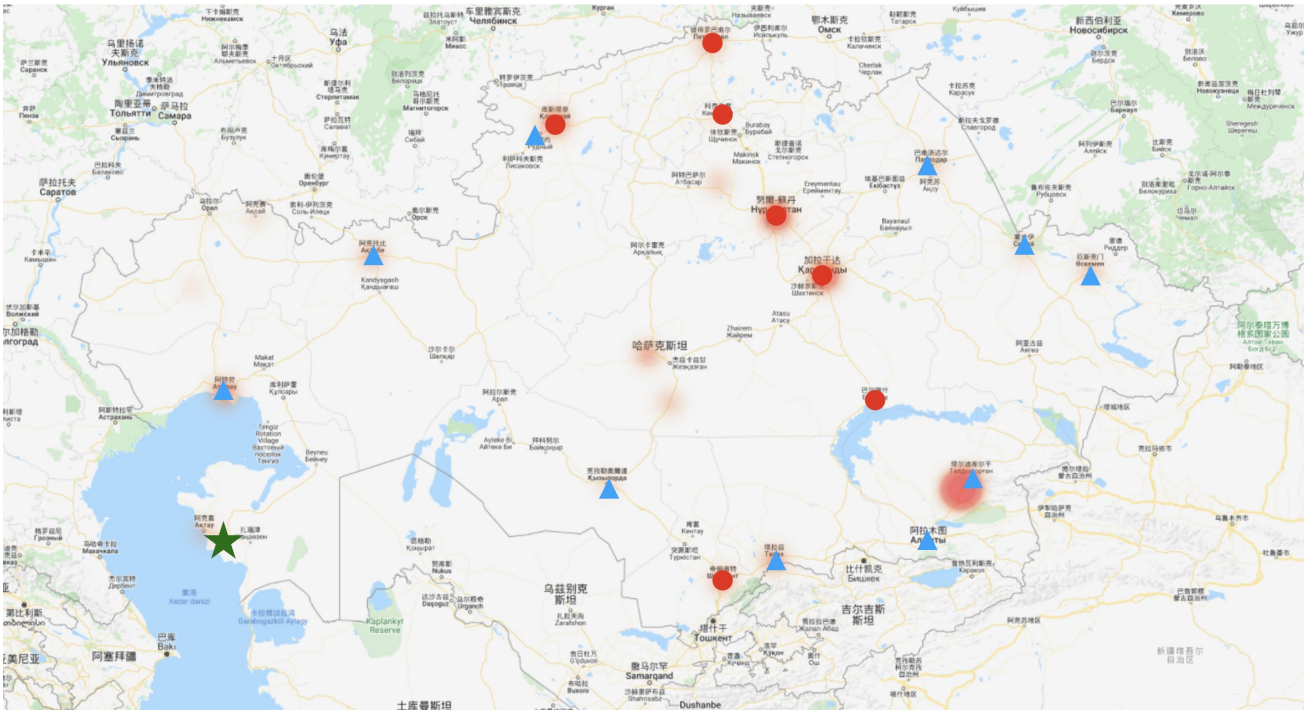


1. 以哈萨克斯坦现首都努尔苏丹为代表，在第五轮扫描时就已经恢复了大部分网络设备。下图中红色圆圈表示。

2. 以哈萨克斯坦前首都阿拉木图为代表，在第四轮到第六轮扫描期间网络在持续恢复。下图中蓝色三角表示。

3. 以动乱爆发地附近阿克套地区为代表，在多轮扫描的过程中，网络设备没有明显变化。下图中绿色五角星表示。

在 2.1 节中的分布图基础上，分别标记出上述三类城市的地理分布：



可以看到，哈萨克斯坦中部偏北、以现首都为中心的主要城市网络最快恢复，哈萨克斯坦东边（包括前首都阿拉木图）和西边的城市恢复的较慢，而动乱最先爆发的石油重镇扎瑙津附近，网络设备并没有明显变化。

这似乎也能说明这场动乱最先在哈萨克斯坦首都为中心的主要城市被平息，然后在哈萨克斯坦全国范围内平息。而动乱最开始爆发的扎瑙津附近地区，也仅仅只是引信被点燃的地区，而不是动乱爆发最激烈的地区。

3.3 断网及恢复期间 CIDR 段变化情况

根据 2.2 节的结论，我们将对比整个哈萨克斯坦以及 GPON Home Gateway 所涉及网段在恢复期间的变化情况。

根据后缀为 24 的 CIDR 段去分割哈萨克斯坦的网络空间（注：下文所述 CIDR 段均指后缀为 24 的 CIDR 段），对比多轮探测中出现和消失的 IP 段，可以得出两个结论：

1. 在第六轮扫描（2022 年 1 月 11 日 9 时）时，哈萨克斯坦的大部分网络已经重新和互联网连接，回到动乱前的状态。在第一轮扫描的数据中，也就意味着相较于历史记录，断网时有 8592 个的 CIDR 段消失，但在第五轮和第六轮一共有 6961 个（81.01%）CIDR 段重新出现。

2. 在第七轮扫描（2022 年 1 月 12 日 11 时）之前，哈萨克斯坦人民的日常网络连接也恢复正常。。GPON 相关的 CIDR 段在第七轮（2022 年 1 月 12 日 11 时）出现 292 个，

消失 206 个，在第八轮（2022 年 1 月 14 日 18 时）出现 234 个消失 200 个，说明 GPON 相关的 CIDR 段已经开始动态变化，符合 GPON 使用的正常规律，出现 GPON 设备频繁上下线网段变化的情况。

在第二轮的数据中，出现了 282 个 CIDR 段，但只出现了 4 个和 GPON 有关的 CIDR 段，这部分 CIDR 段还需要继续关注。

四．思考和总结

根据已知的报道，哈萨克斯坦动乱被定性为未遂政变，但在整个事件中，能找到多方势力闻风而动的影子。断网可能是切断恐怖分子进行沟通协调途径的办法之一，但也要警惕可能产生的应对方案：破坏者依旧可以使用蓝牙、无线电的方式在断网的情况下快速传递信息，实现破坏最大化。

对于我们的邻国哈萨克斯坦，我们了解的资料的确有限。消息也存在一定的滞后性。希望能从这篇文章中拓展出一种动态测绘某个地区的思路，通过网络空间和现实空间事件的结合，从而开启另一个角度的思考。

文中部分结论可能受时间、地区、IP 库的精准度等多个条件影响，如有错误，欢迎指正。