



# Situation Report: 2025 Internet Shutdown - Iran

<https://ainita.net>

<https://infosec.exchange/@ProjectAinita>

# Project Ainita

- Established 2011
- Mission: To advance online anonymity, security, and freedom in high risk countries.
- How? Focus on connectivity!
- Threefold strategy: Conduct deep rigorous research, provide Internet intelligence and engineering capacity, developing and distributing circumvention and security tools.

# The Rise of NIN (National Information Network) and Shutdown Evolution

# 2009 – the “Green Movement”

- **Context:** Elections held June 12, 2009. Authorities announced just two hours after the polls closed that the incumbent president won receiving 62.63%. Protesters quickly took to the streets organizing, expanding, and documenting protests through social media platforms.
- **Response:** Facebook and Twitter were censored periodically in the weeks leading up to the elections. Authorities implemented first nationwide **full shutdown by “pulling the plug”** – lasting approximately 45 min – and restarting the Internet with extreme throttling and very low bandwidth. Subsequently major social media platforms and communication tools were filtered or limited.
- **Consequences:** Government realized detrimental effects of pulling plug method. Increased monitoring of social media → increased blocking and censorship → realignment of regime’s national security focus and resource shift to Internet governance, policies, and laws → prioritizes the development of NIN.

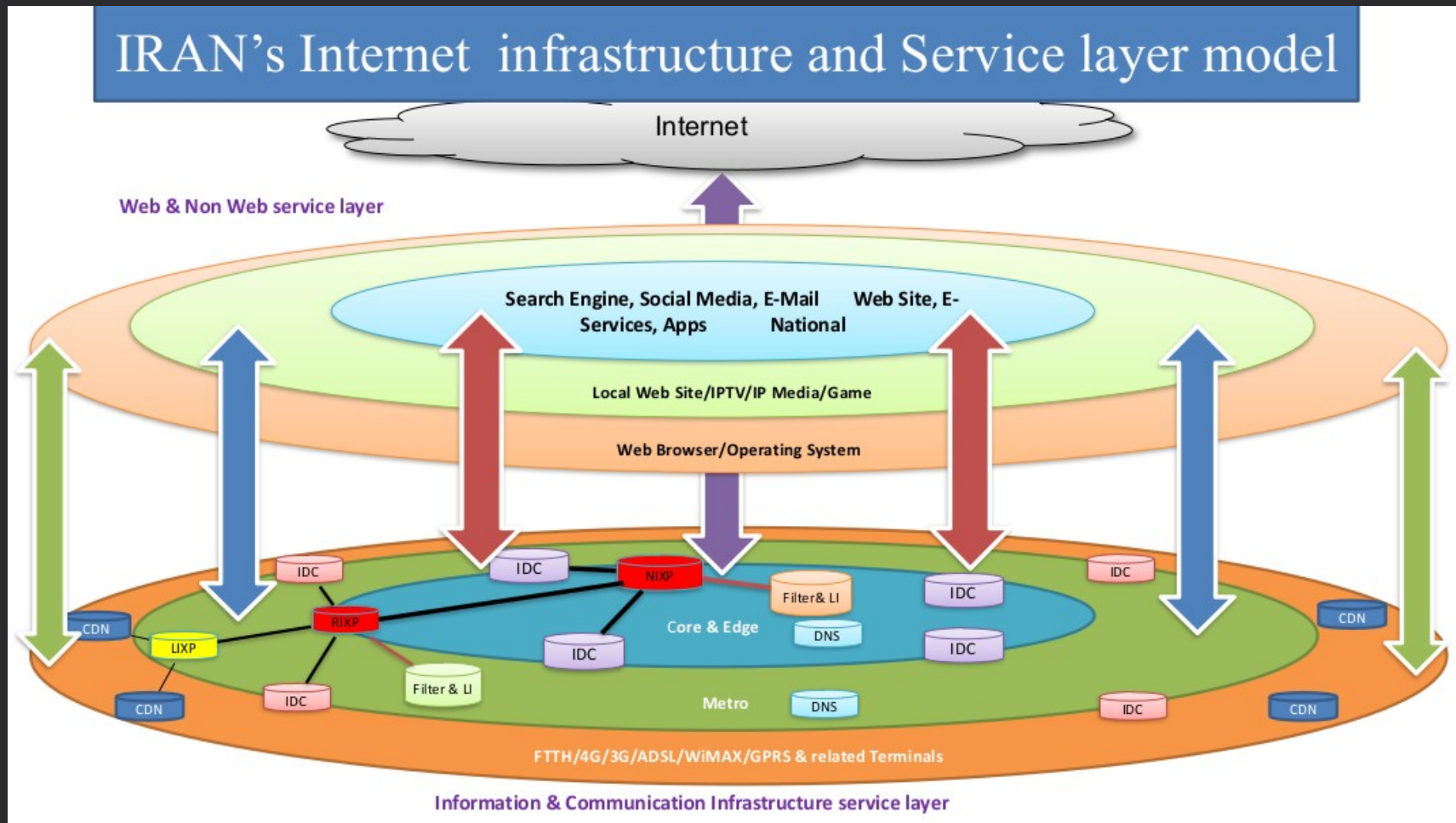


# 2012 – Preemptive Censorship Flex

- **Context:** February 7-13, 2012. First elections since 2009 to be held March 2, 2012. Domestic economic pressure and unrest mounting due to sanctions. On February 7, children of opposition leaders called for peaceful protests on February 14 to observe one-year mark for house arrest.
- **Response:** February 9, 2012, authorities implemented targeted blocking denying +30million users access to sites such as Facebook, Twitter, and Google including Gmail – “According to computer crime regulations, access to this website is denied.” February 13, the government restores email but flexes its censorship capabilities by cherrypicking foreign sites to remain blocked.
- **Consequences:** Government initiated the development of NIN → Supreme Council of Cyberspace established → Internet crackdown instills public fear of looming NIN and increased monitoring.

# National Information Network plan in 2013

with the aim to enforce control



# 2019 – “Bloody Aban” (Bloody November)

- **Context:** November 16-23, 2019. Stemming from a resurgence of public economic hardship due to existing and renewed sanctions, with this economic isolation incentivizing the government to fervently pursue strengthening and expanding NIN, and finally, the surprise new rations coupled with 50% hike in fuel prices on November 15 served as the inflection point for mass protests.
- **Response:** To regain control, the Supreme National Security Council ordered an Internet blackout – a near-total shutdown leaving only top government authorities with Internet access. Lasting for 7 days, global connectivity levels plummeted to 4-5% funneling netizens forcefully towards the now operational intranet – NIN. Internet on mobile carriers was not restored until November 27.
- **Consequences:** This shutdown provided the opportunity for authorities to conceal the scale of violence used against protesters with +300 estimated killed. Using these protests as a testing ground for NIN only revealed its clumsiness and faults as the **intranet-only** policy further degraded the economy with 7-day losses approximately at USD\$1.5 billion. Government’s biggest blunder: forgot that they needed international DNS and did not have internal search engine!

# 2025 – Conflict Induced Blackout

- **Context:** June 13-24, 2025 Israel initiated a large-scale attack against Iran targeting nuclear facilities and military installations, Iran retaliated, and US gets involved. Ceasefire declared on June 24 but tensions remain high.
- **Response:** Since 2019, the government imposed most severe shutdown dropping traffic levels by approximately 97% specifically between June 18-21 affecting major mobile networks, near-total disruption of international traffic. Government attributed shutdown to cybersecurity concerns.
- **Consequences:** Plunging the country into a digital blackout allowed the government to limit information flow both internally and externally and simultaneously prevent civilians from organizing and mobilizing during the conflict. Although connectivity is relatively restored to pre-shutdown levels, novel filtering patterns continue to emerge.



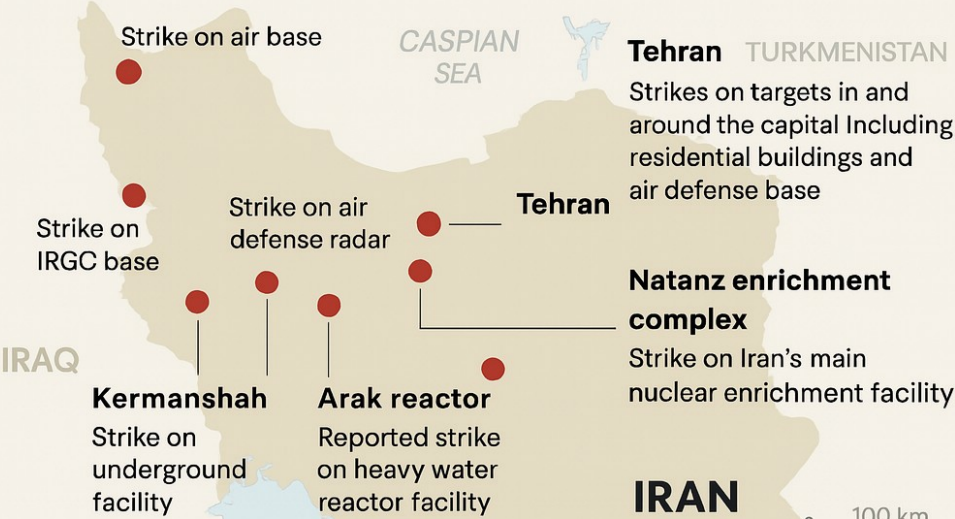
# Internet Shutdown Study: Iranian June 2025

# Surprise Attack on Iran

Israel large scale aerial attacks, triggers Internet disruption

## Where Israel attacked Iran on day one of strikes

Confirmed and reported air strikes on June 13 13, 2025, data as of June 13 at 8:00 AM ET



Note: Locations are approximate.  
Source: Institute for the Study of War and American Entrepreneurship

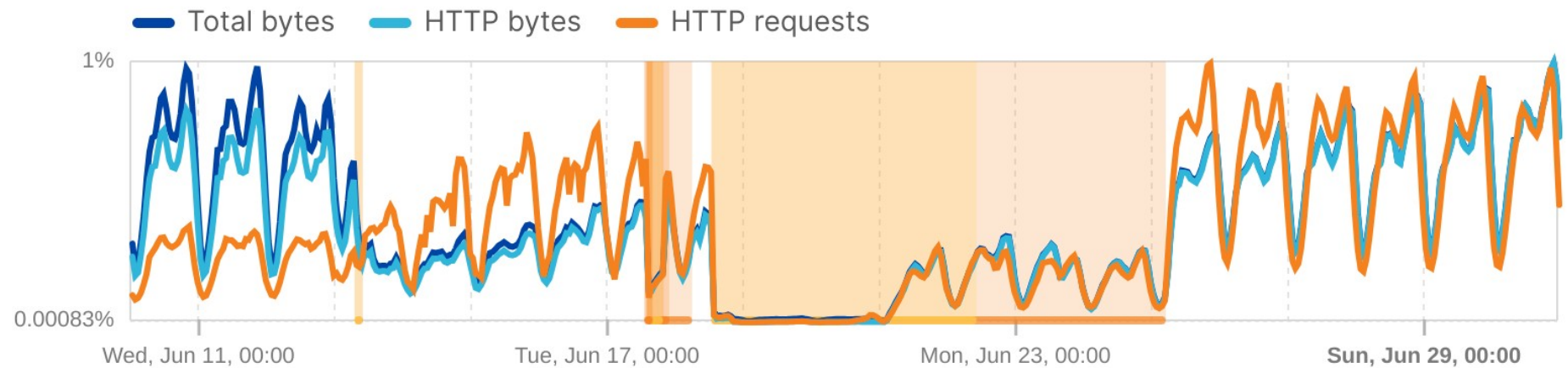


# Cloudflare Radar

June 10 - 30, 2025

## Traffic volume in Iran

Relative change from previous period



 **Cloudflare Radar**

Jun 10, 2025, 00:00 UTC → Jun 30, 2025, 23:45 UTC

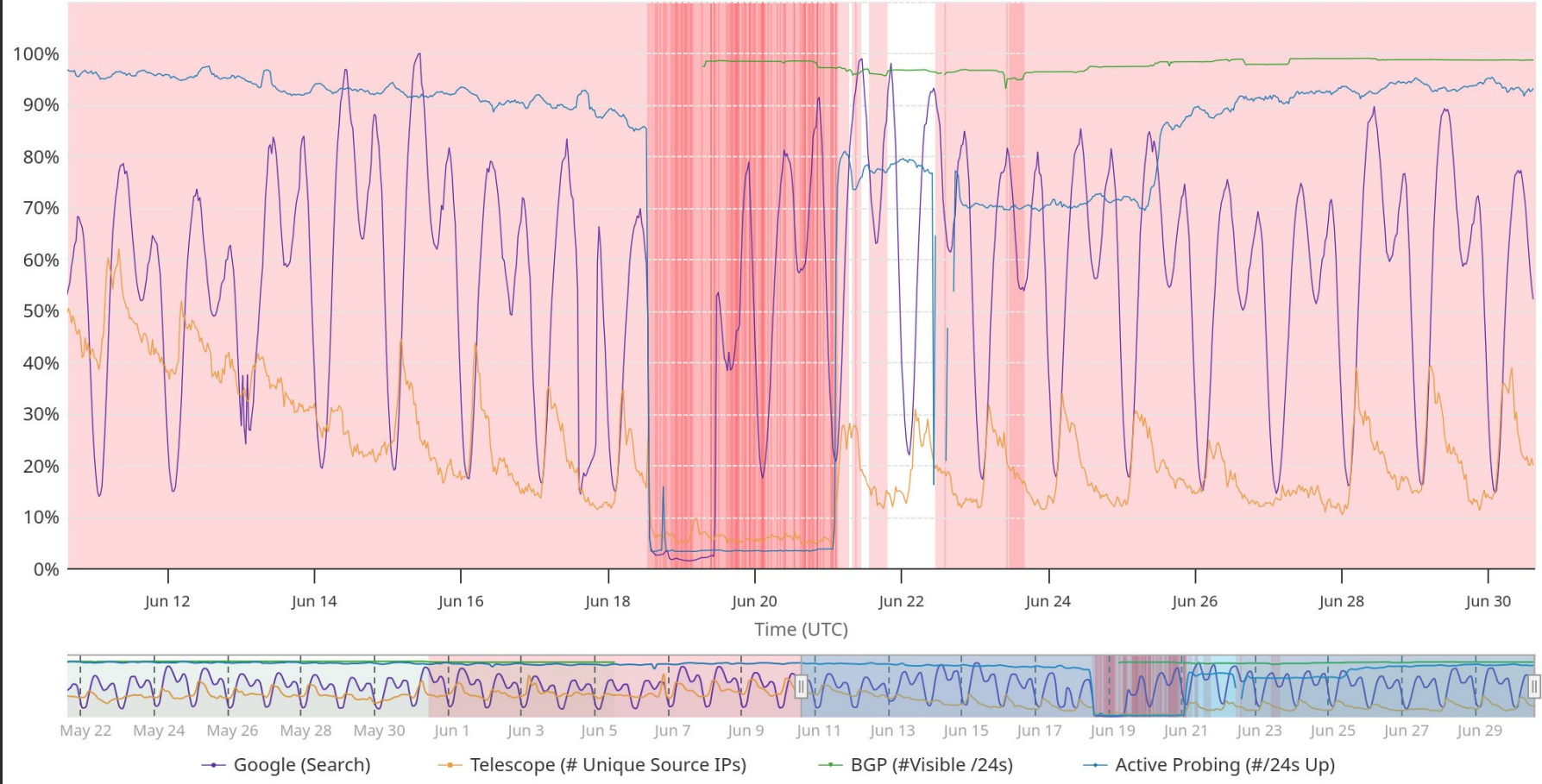


# IODA Portal

June 10 - 30, 2025

## Internet Connectivity for Iran (Islamic Republic Of)

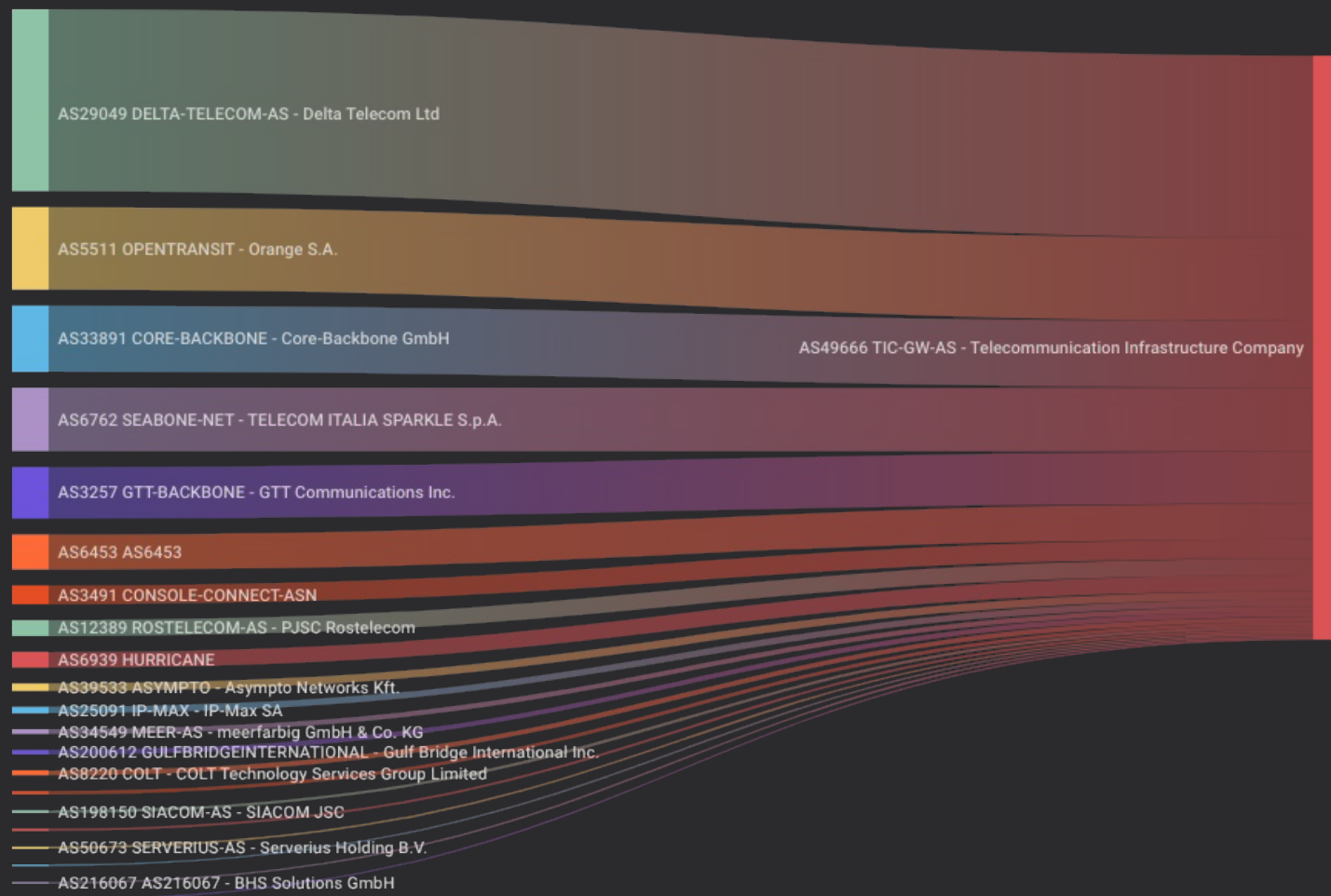
June 10, 2025 3:07pm - June 30, 2025 3:07pm UTC



# BGP Analysis of Shutdown Impact

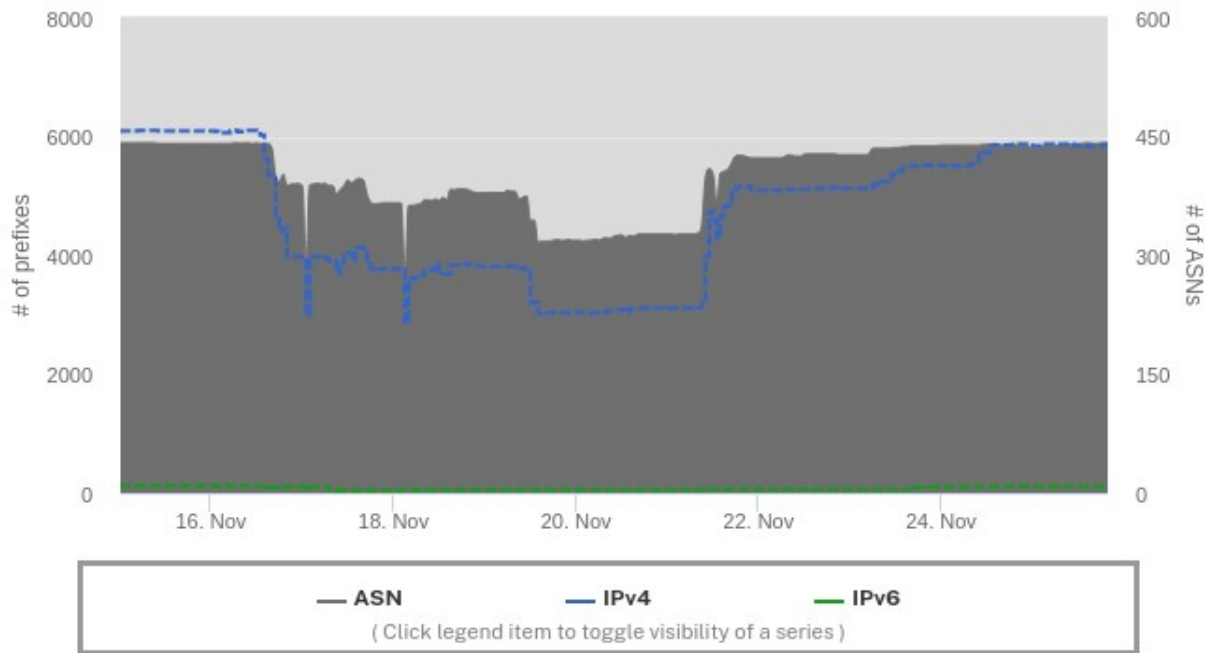
# Iran Internet Map

BGP Data on first day of Israel attacks, June 13, 2025

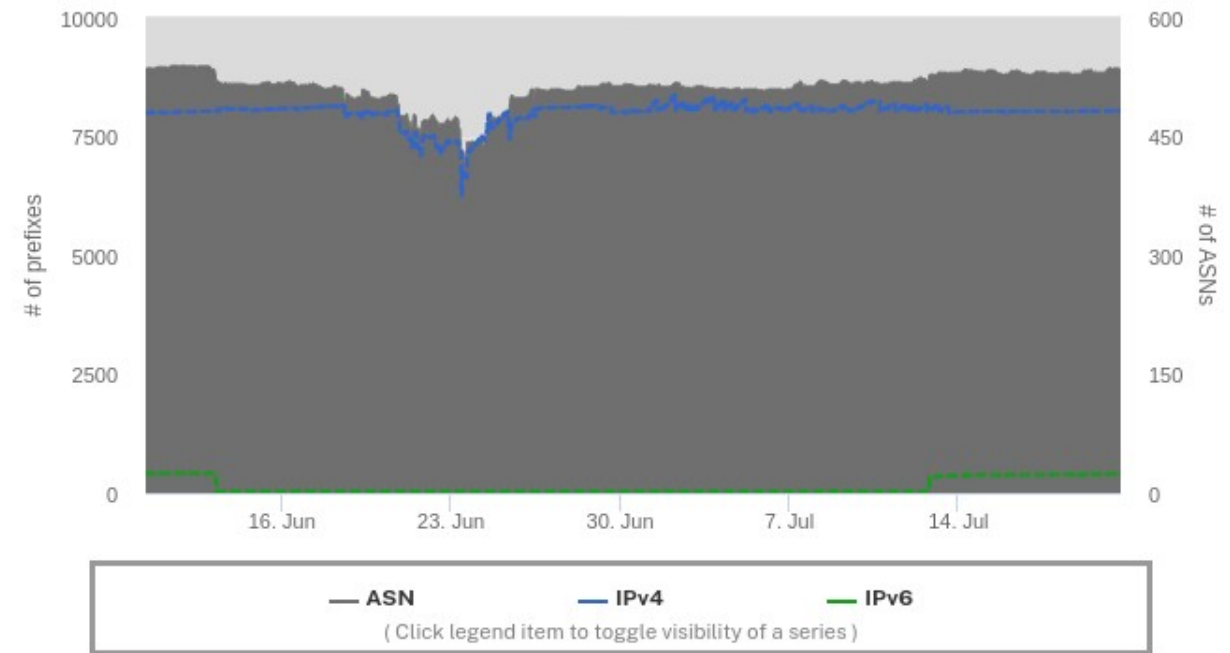


# Less impact on BGP

RIPE STAT comparison between 2019 and 2025 Internet shutdowns in Iran



IR IP prefixes announced Nov 15 to 25 2019

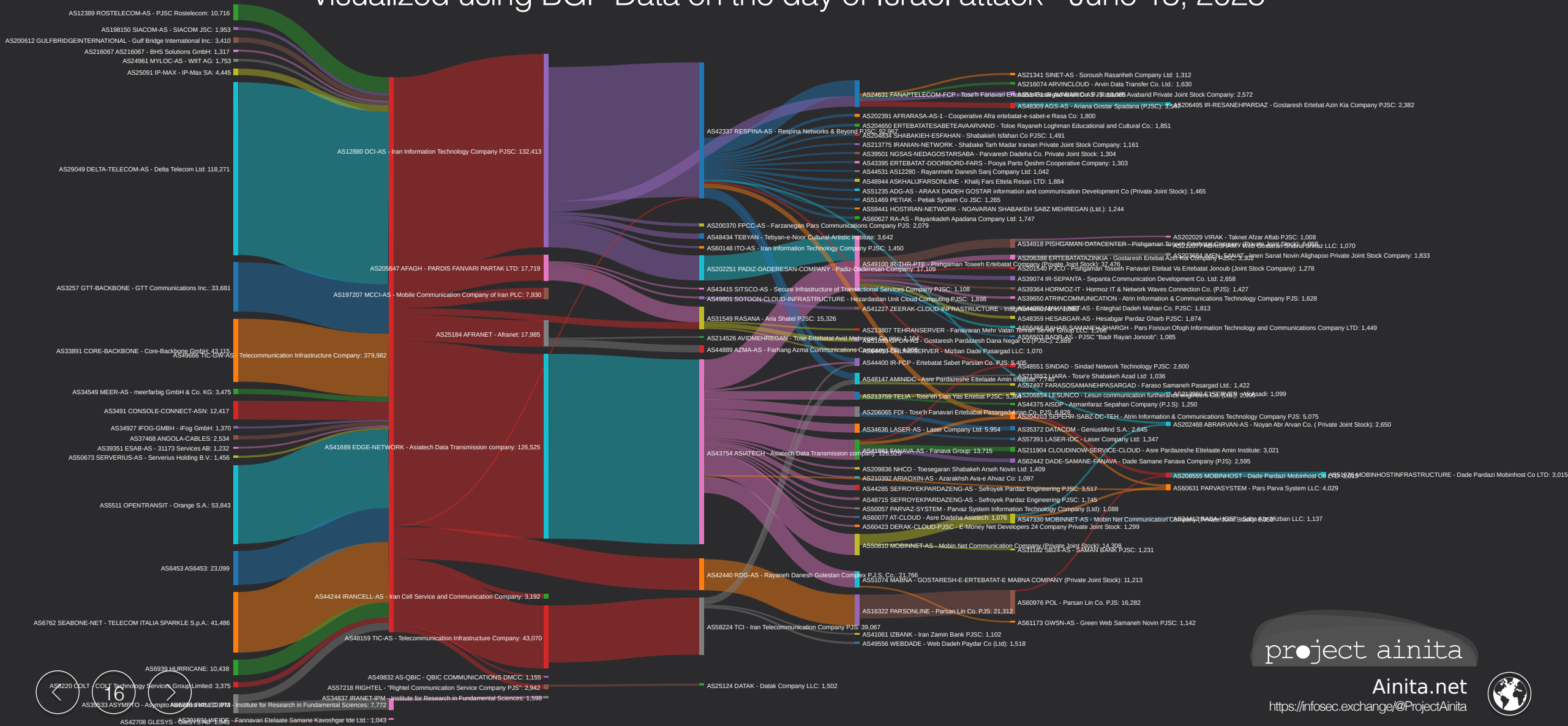


IR IP prefixes announced June 10 to 20 2025



# Iran Internet Map

Visualized using BGP Data on the day of Israel attack - June 13, 2025



# Shutdown Implementation, June 2025: Methodology

- Iranian National Information Network (NIN) is reaching maturity, meaning now shutdowns can be implemented with minimal collateral damage to domestic connectivity
- Not using BGP to “unplug” connectivity, instead using “censorship middle boxes” to drop connections
- The ease of implementing shutdowns could potentially increase frequency of these types events
- Loss of international connectivity could have severe impact on human rights in the country

The end