Insights into an Iranian Internet Shutdown

Anonymous, Niklas Niere, Felix Graf Lange, Juraj Somorovsky

Paderborn University

20 July 2026

Motivation

- Iran known for sophisticated censorship system

Motivation

- Iran known for sophisticated censorship system

- Hard to gather insights into shutdown events

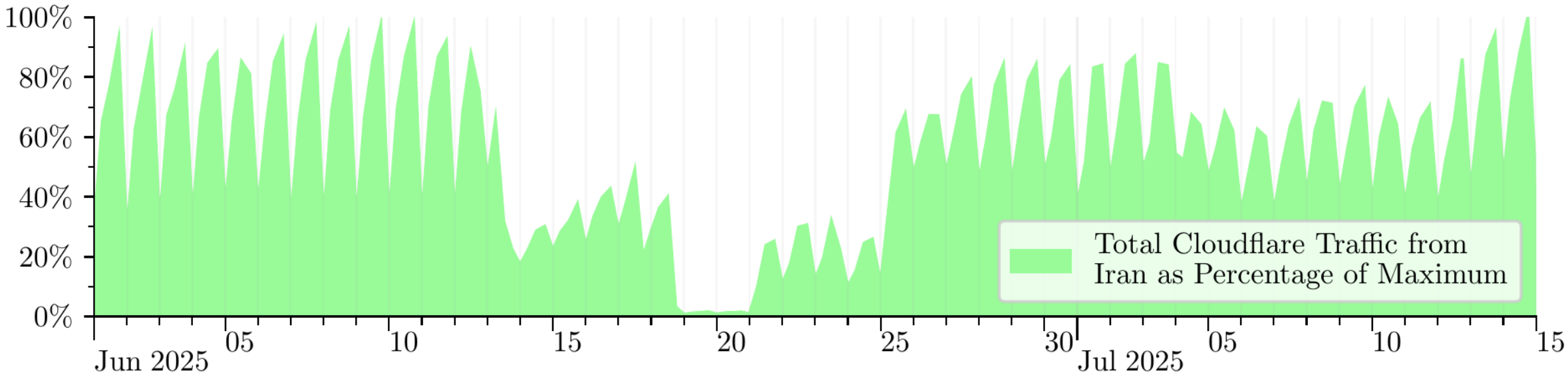
Motivation

- Iran known for sophisticated censorship system

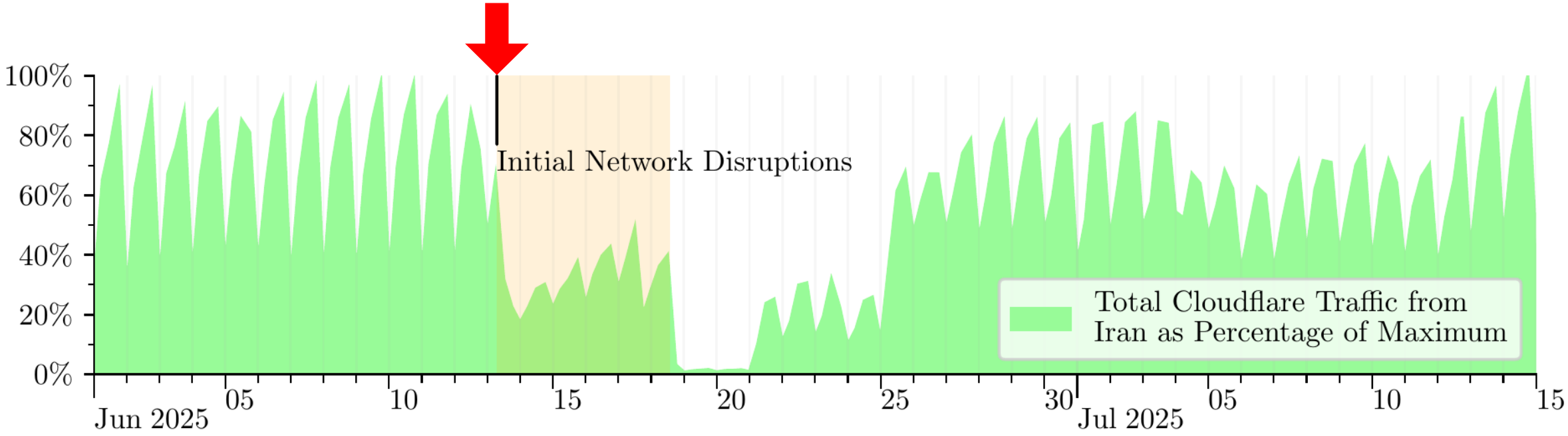
- Hard to gather insights into shutdown events

Contribution: Unique measurements surrounding June 2025 shutdown

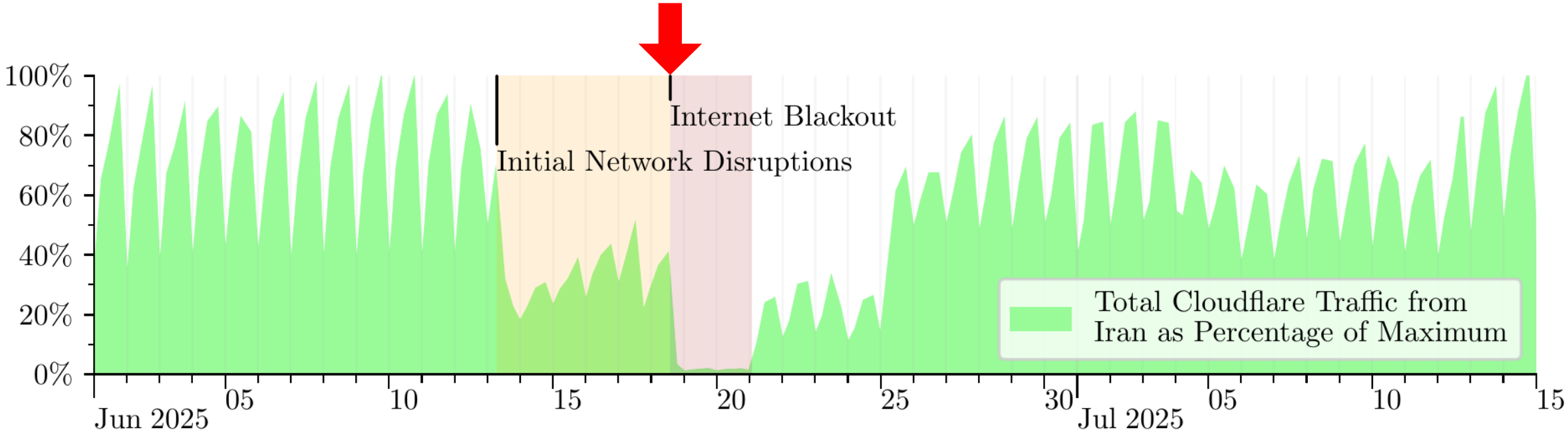
June 2025 Shutdown



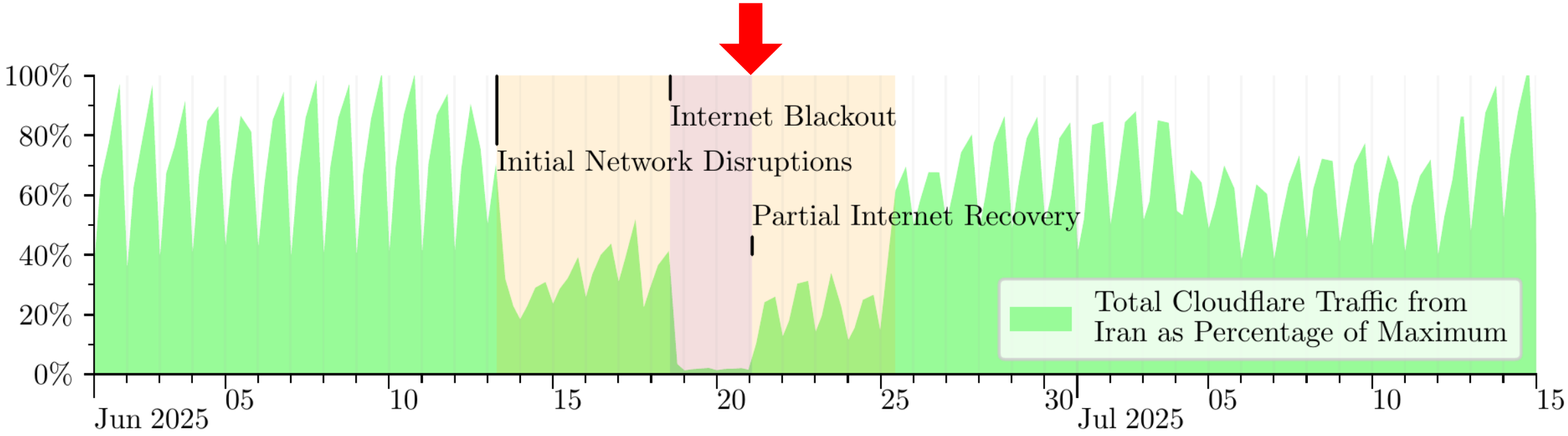
June 2025 Shutdown



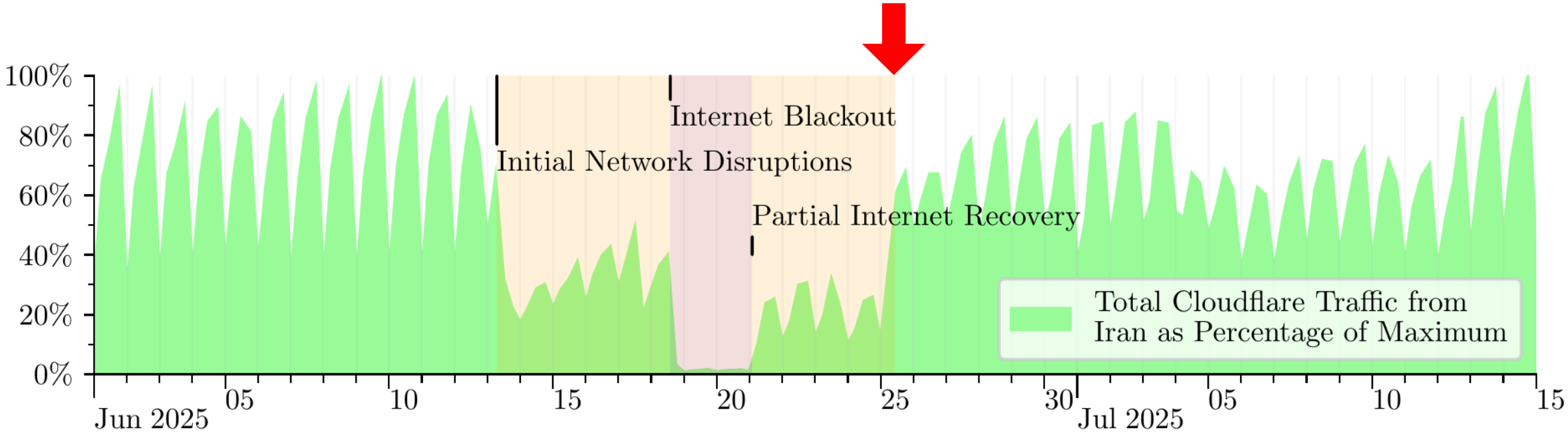
June 2025 Shutdown



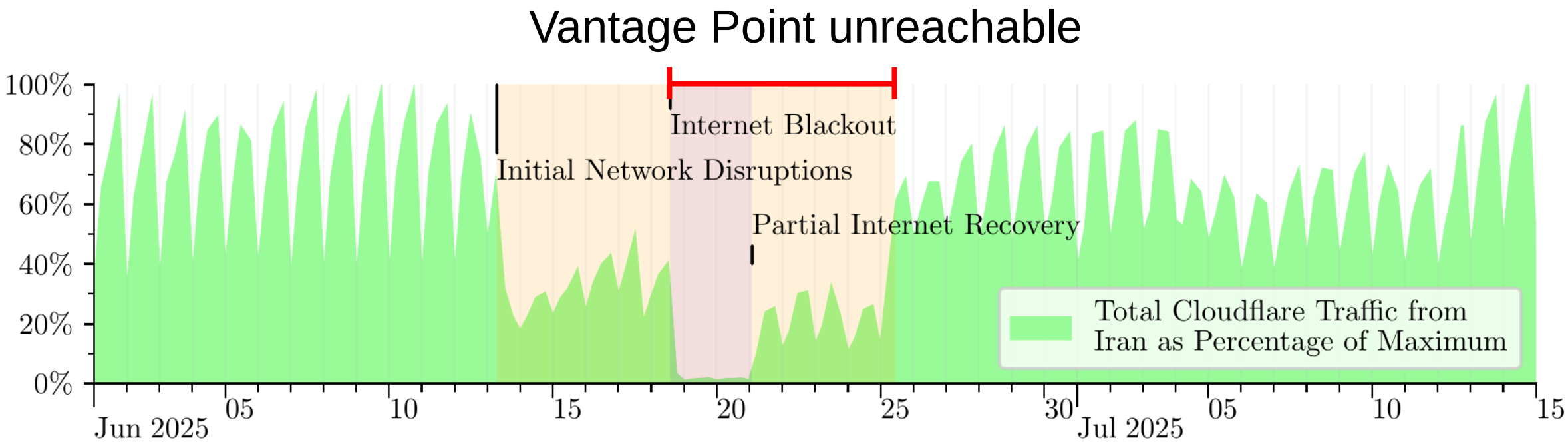
June 2025 Shutdown



June 2025 Shutdown



June 2025 Shutdown



Methodology

- Unrelated DPI scans of Tranco top 100k domains

Methodology

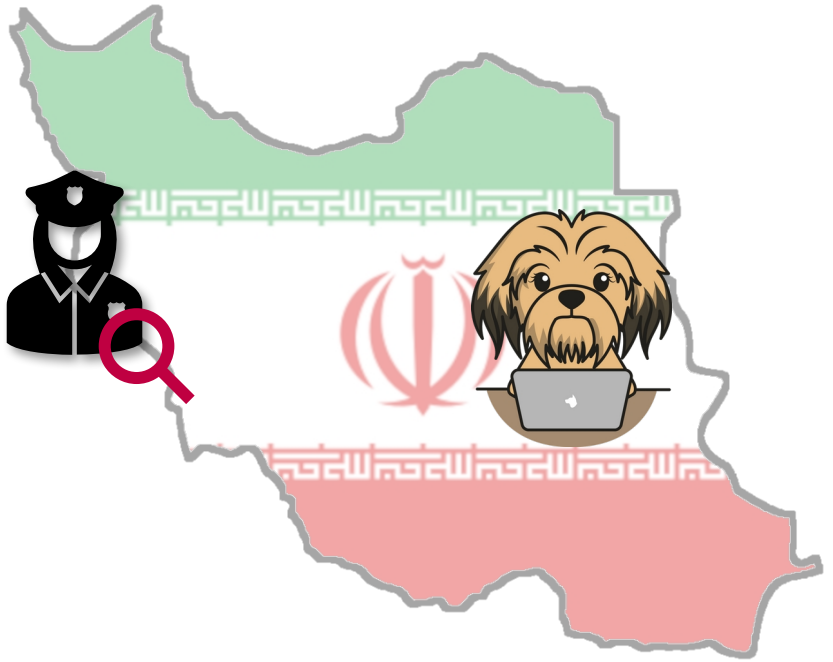
- Unrelated DPI scans of Tranco top 100k domains
  - DNS
  - HTTP
  - TLS
  - QUIC

Methodology

- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP **`GET`** request
  - TLS **`ClientHello`**
  - QUIC **`Initial (ClientHello)`**

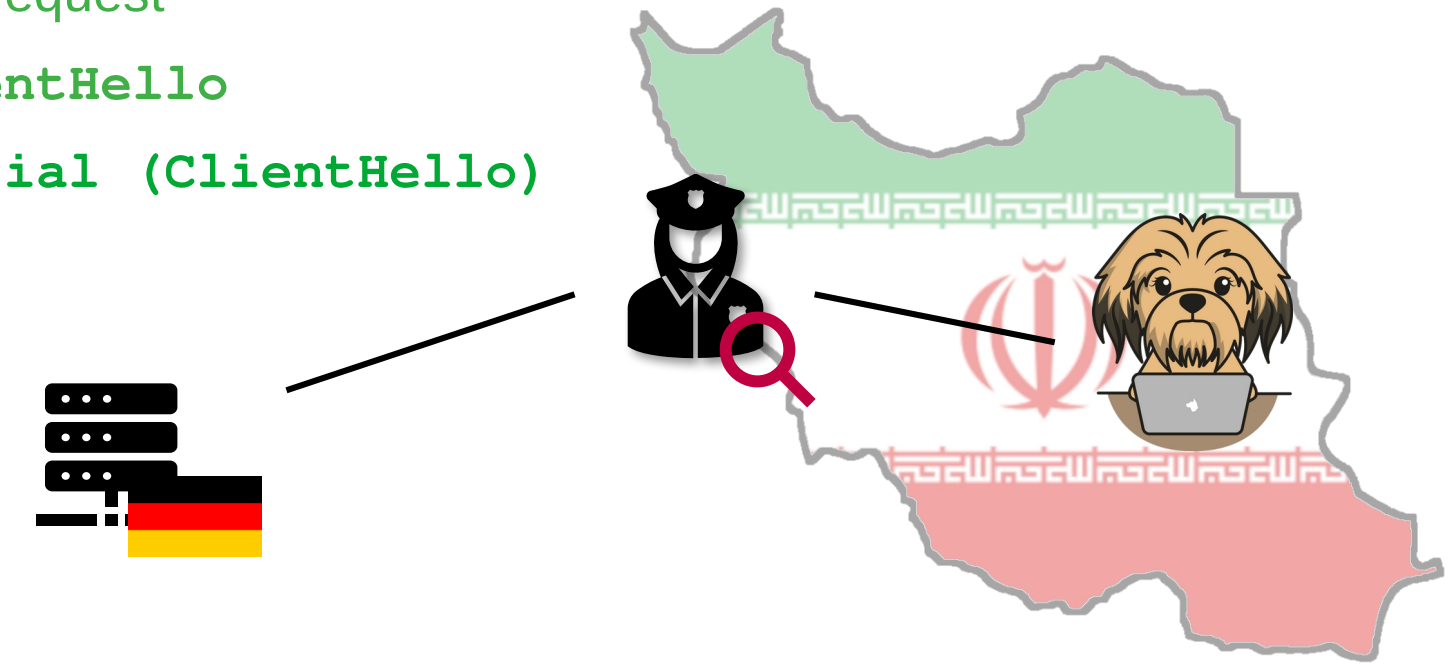
Methodology

- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP `GET` request
  - TLS `ClientHello`
  - QUIC `Initial (ClientHello)`



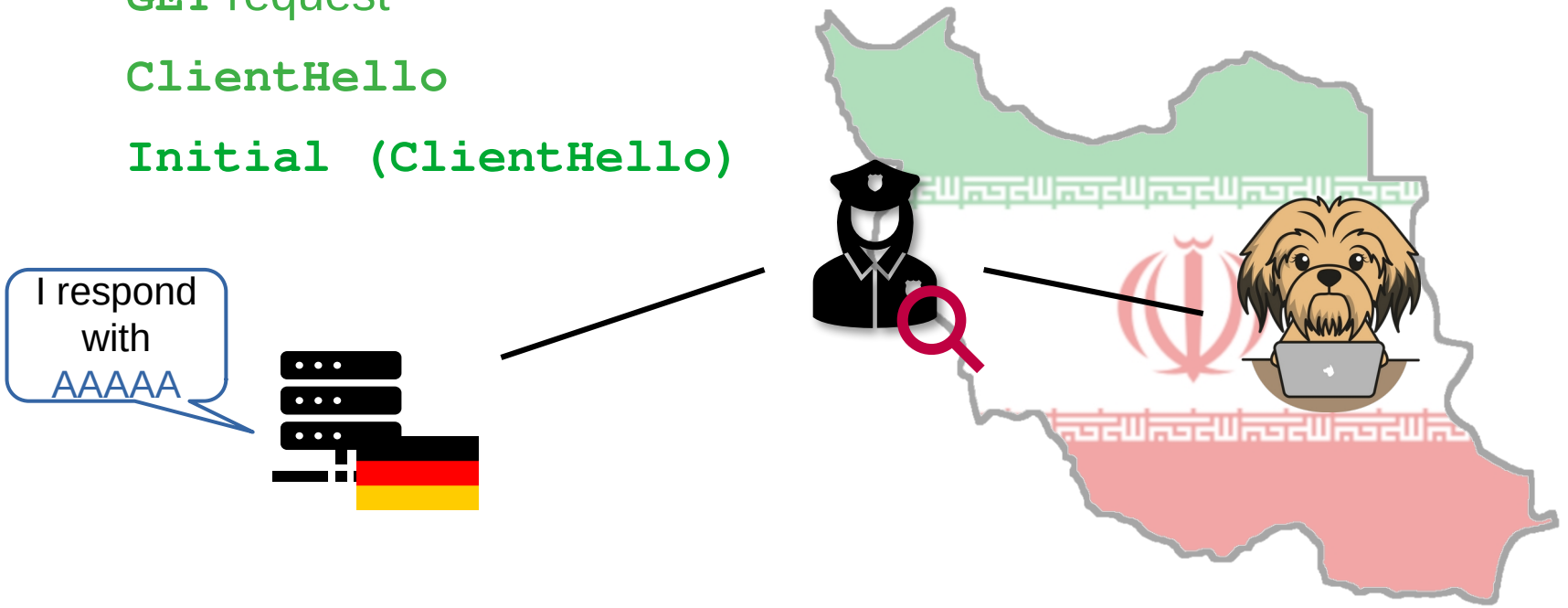
Methodology

- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP `GET` request
  - TLS `ClientHello`
  - QUIC `Initial (ClientHello)`



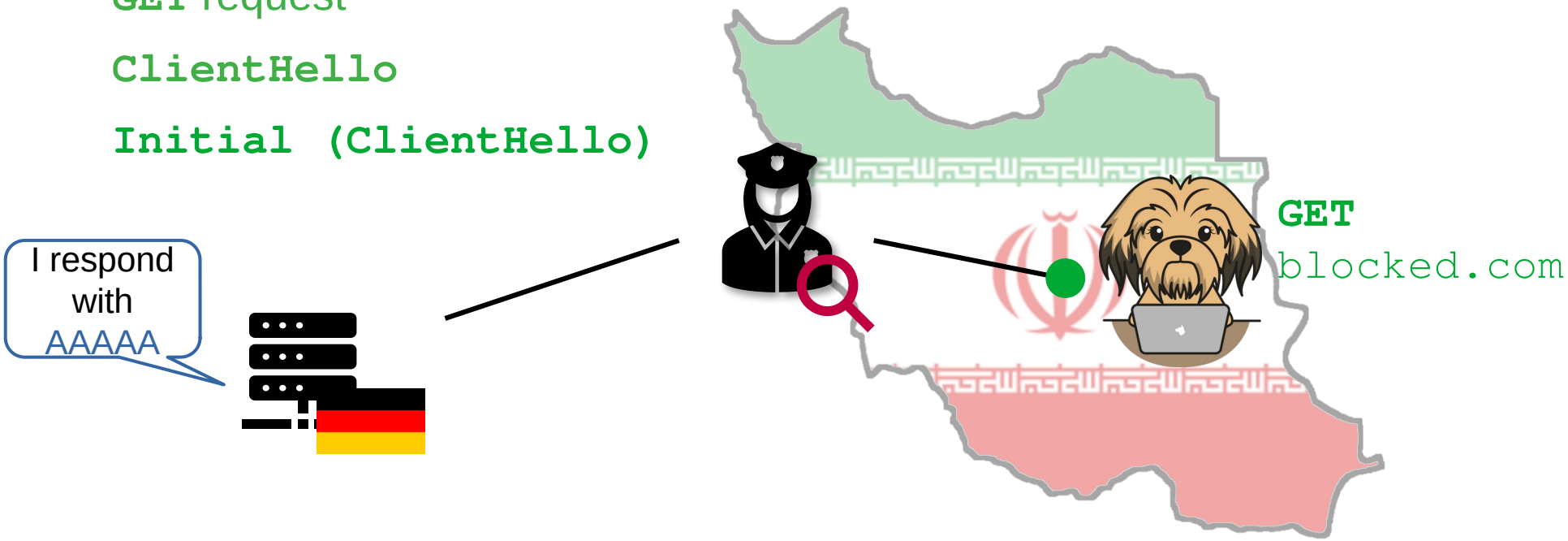
Methodology

- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP `GET` request
  - TLS `ClientHello`
  - QUIC `Initial (ClientHello)`



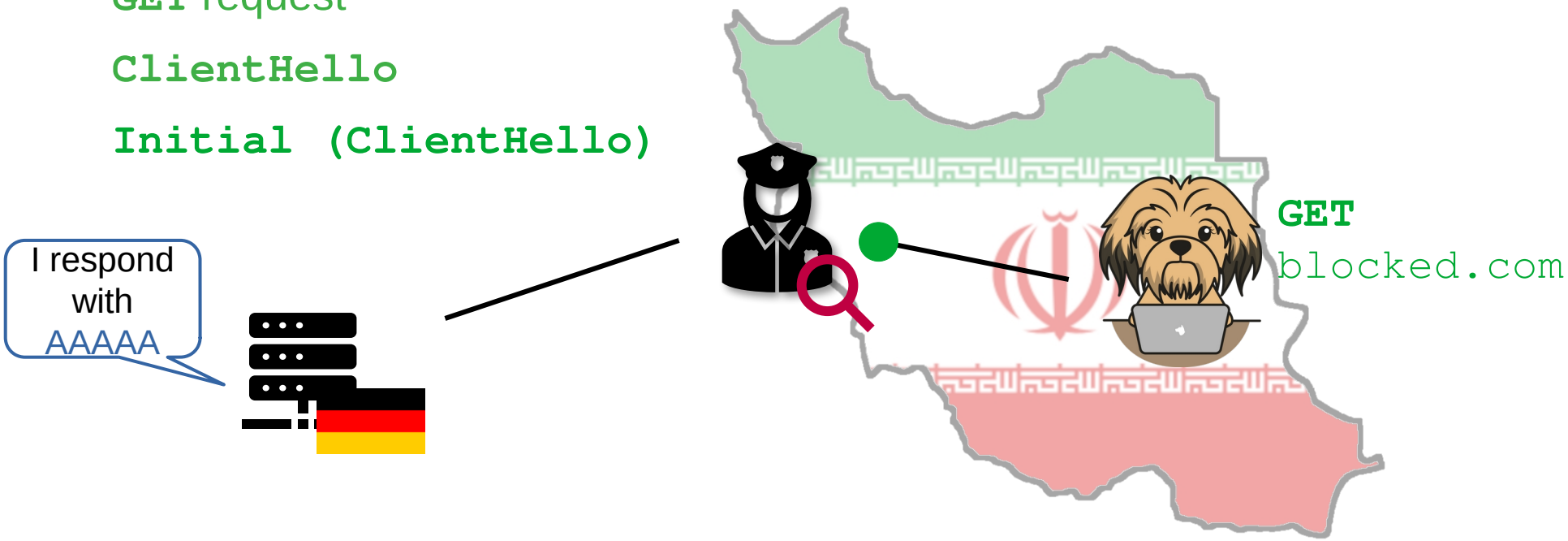
Methodology

- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP **`GET`** request
  - TLS **`ClientHello`**
  - QUIC **`Initial (ClientHello)`**



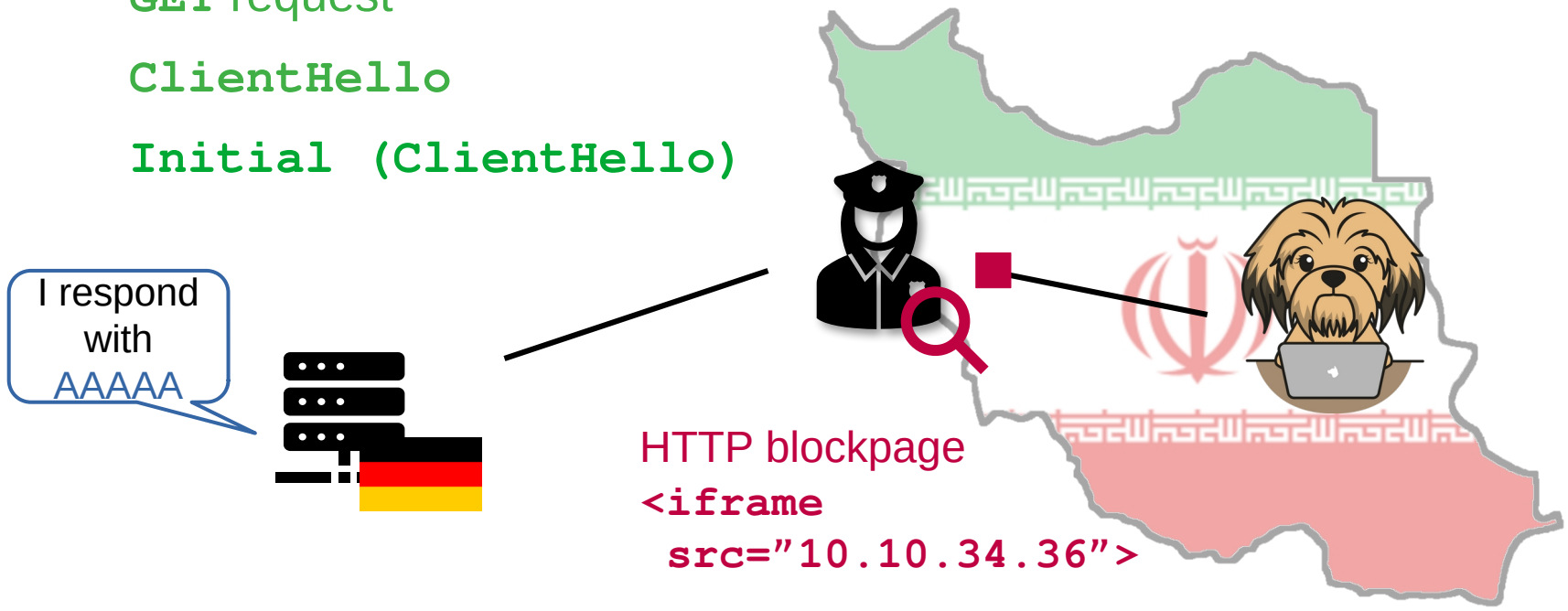
Methodology

- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP **`GET`** request
  - TLS **`ClientHello`**
  - QUIC **`Initial (ClientHello)`**



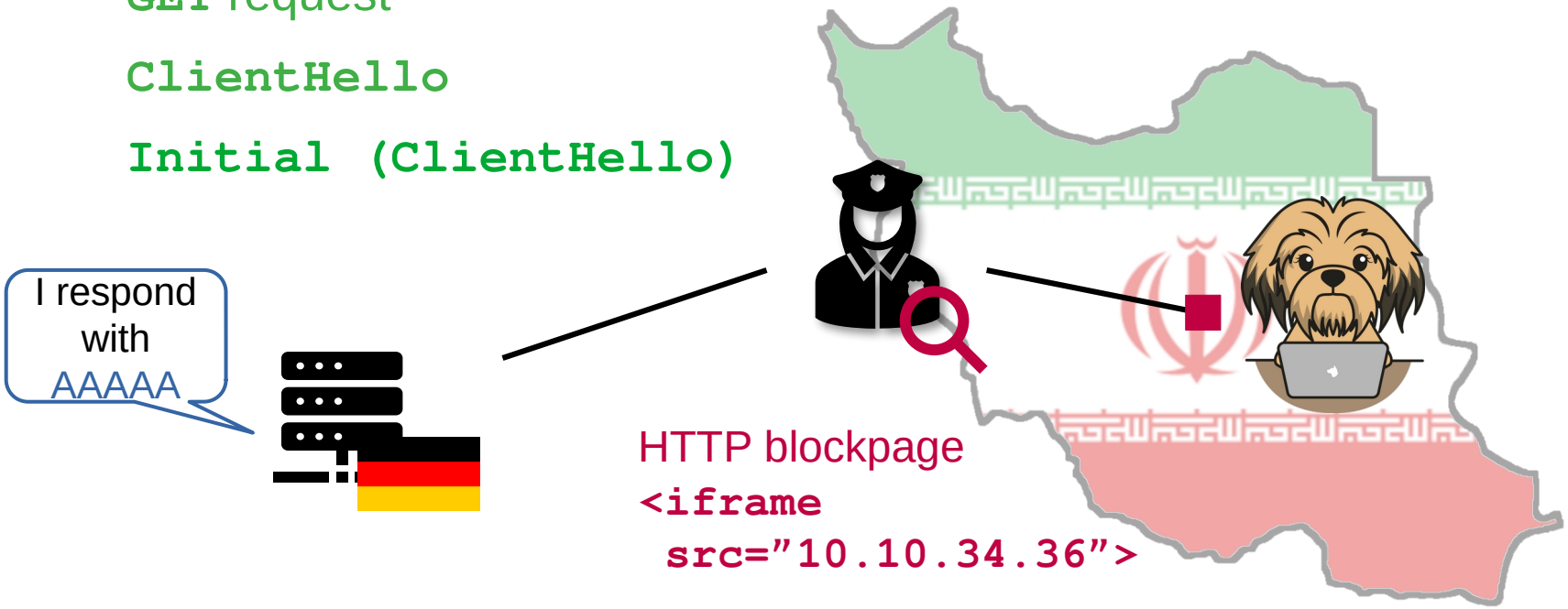
Methodology

- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP `GET` request
  - TLS `ClientHello`
  - QUIC `Initial (ClientHello)`

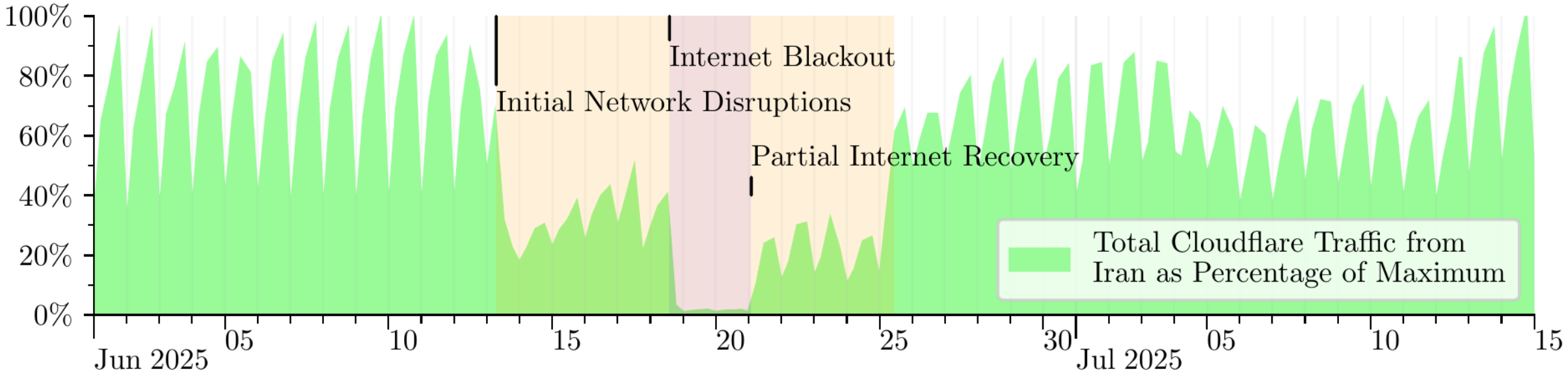


Methodology

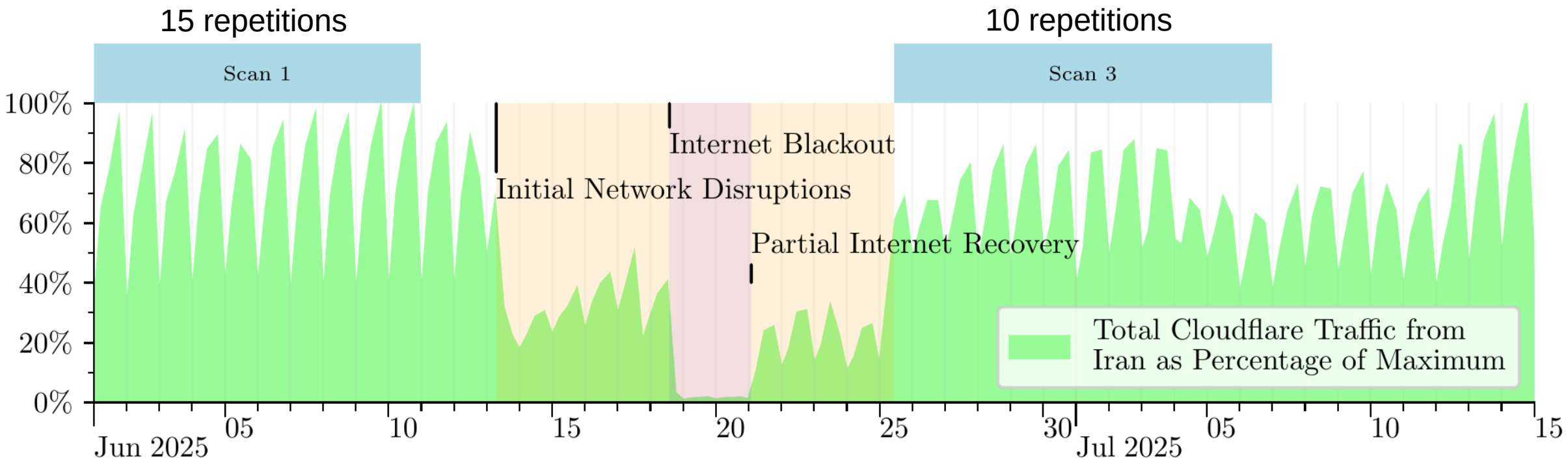
- Unrelated DPI scans of Tranco top 100k domains
  - DNS query over UDP/TCP
  - HTTP `GET` request
  - TLS `ClientHello`
  - QUIC `Initial (ClientHello)`



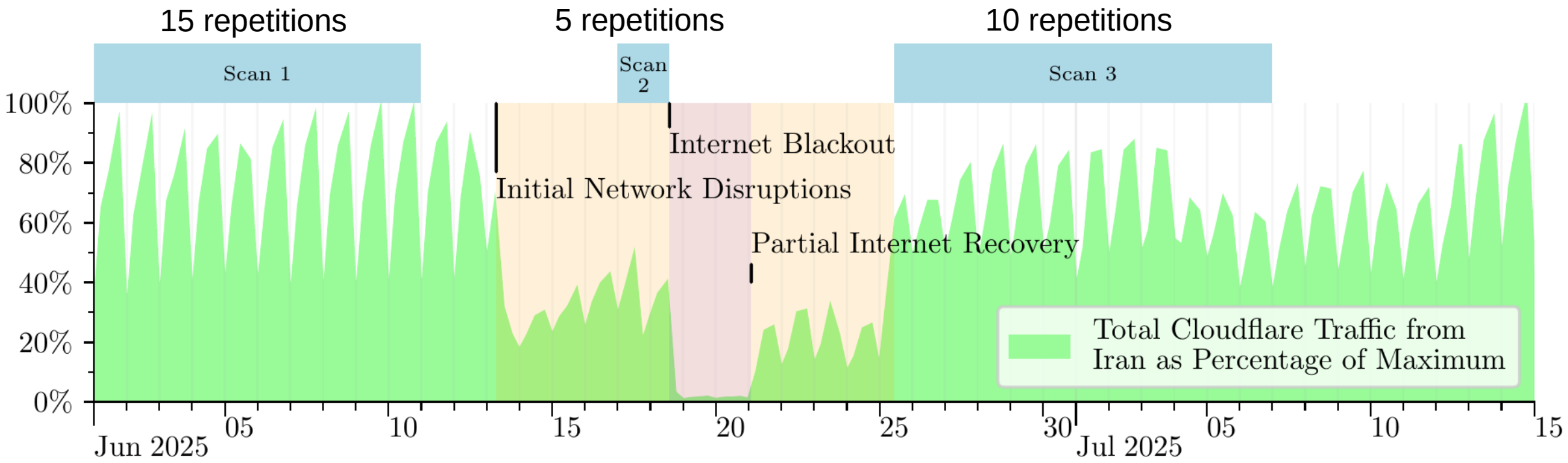
Scan Timeline



Scan Timeline



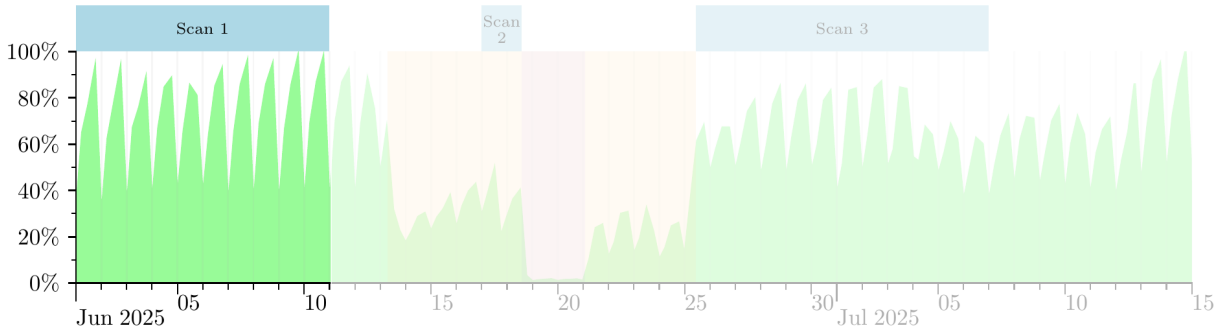
Scan Timeline



Scan 2: only 9,000 domains

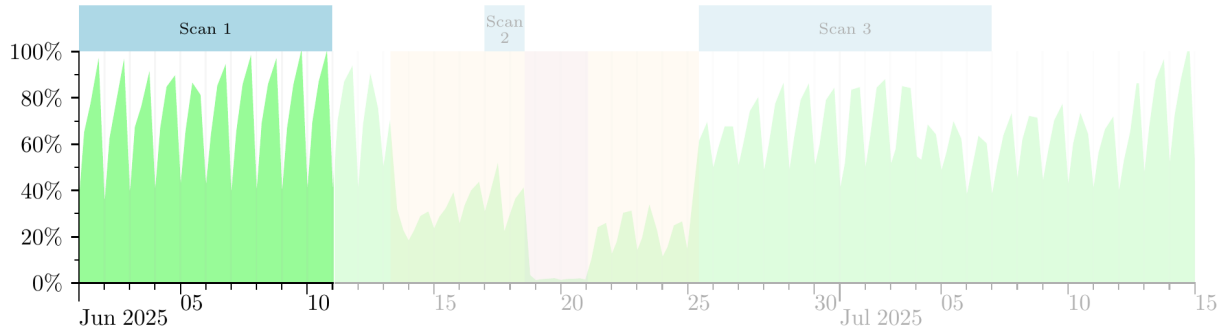
Scan Results

Censorship before Shutdown



Scan Results

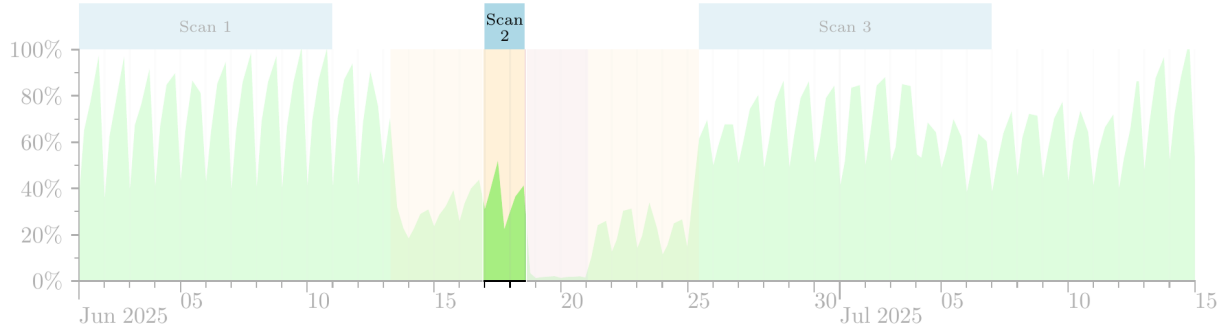
Censorship before Shutdown



- **Scan 1**:
  - Domain-dependent censorship behavior
    - DNS/UDP 1,361 (15,12%)
    - DNS/TCP 1,361 (15,12%)
    - HTTP 1,375 (15.28%)
    - TLS 1,351 (15.01%)
    - No QUIC censorship
  - 1,216 (13.51%) censored across protocols

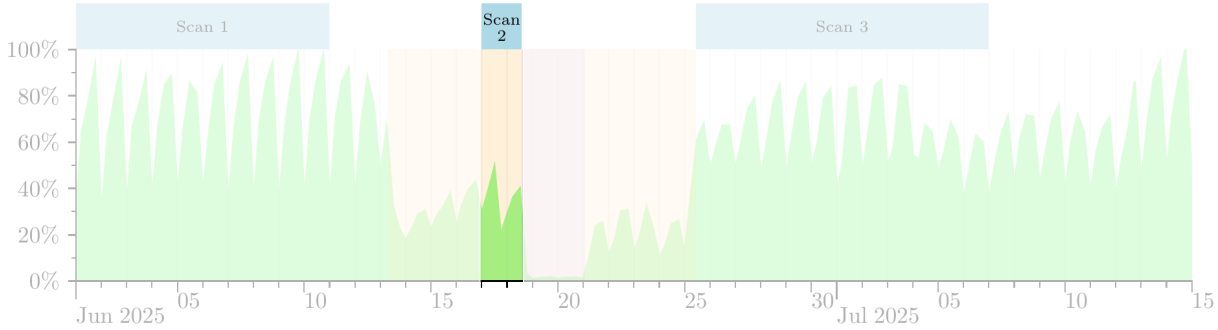
Scan Results

Initial Disruptions



Scan Results

Initial Disruptions



- **Scan 2**:
  - Censorship changes
    - Complete QUIC blockage
    - DNS/TCP:
      96.68% unresolvable
    - temporary blockings of other protocols

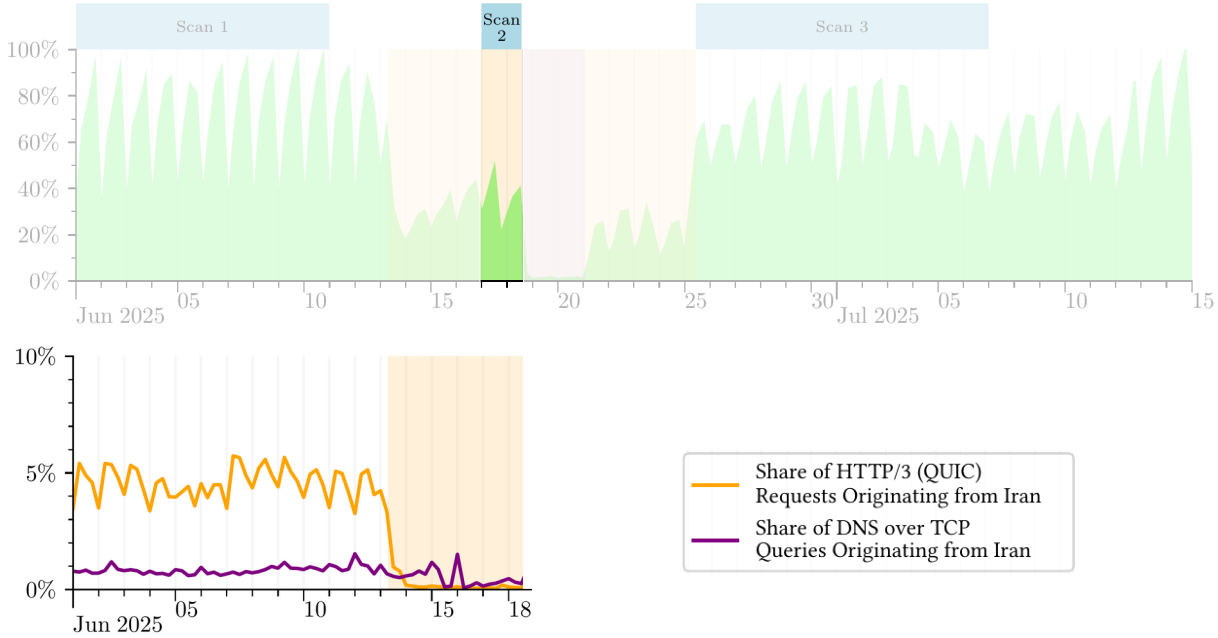
Protocol	Scan 1	Scan 2
DNS/UDP	1,361 (15.12%)	1,509 (16.77%)
DNS/TCP	1,361 (15.12%)	**8,701 (96.68%)***
HTTP	1,375 (15.28%)	1,730 (19.22%)
TLS	1,351 (15.01%)	1,555 (17.28%)
QUIC	1 (0.01%)	**9,000 (100%)**‡
Total	9,000	9,000

* No server response after successful TCP handshake
‡ Complete QUIC blocking

Scan Results

Initial Disruptions

- **Scan 2**:
  - Censorship changes
    - Complete QUIC blockage
    - DNS/TCP:
      96.68% unresolvable
    - temporary blockings of other protocols



Protocol	Scan 1	Scan 2
DNS/UDP	1,361 (15.12%)	1,509 (16.77%)
DNS/TCP	1,361 (15.12%)	**8,701 (96.68%)***
HTTP	1,375 (15.28%)	1,730 (19.22%)
TLS	1,351 (15.01%)	1,555 (17.28%)
QUIC	1 (0.01%)	**9,000 (100%)‡**
Total	9,000	9,000

* No server response after successful TCP handshake
‡ Complete QUIC blocking

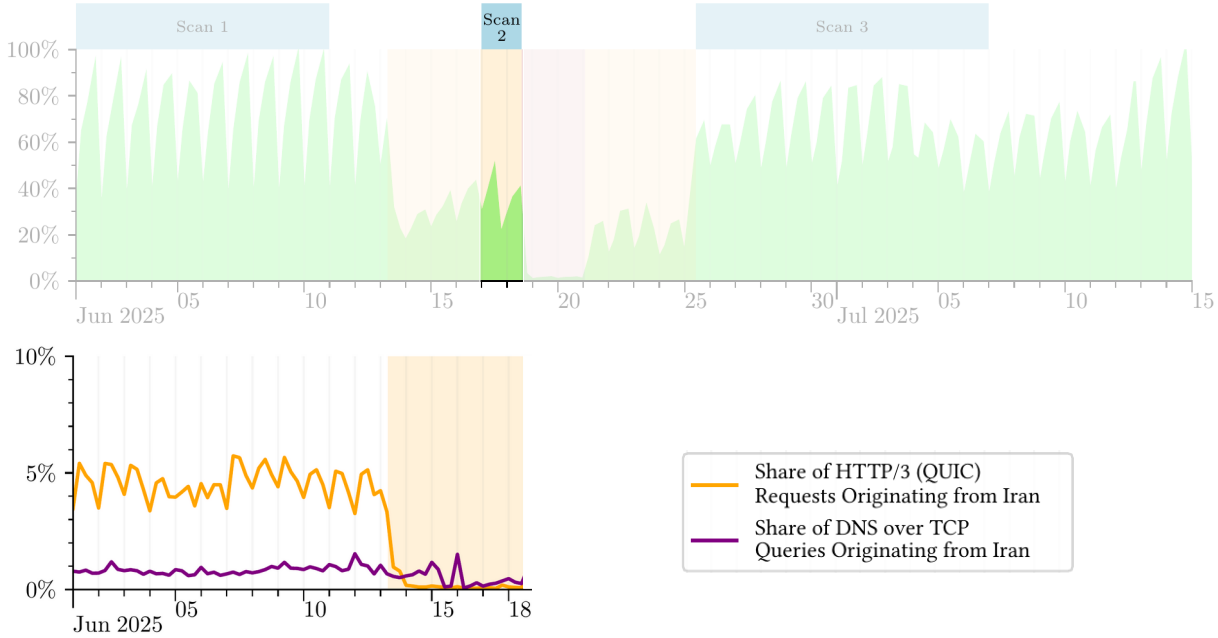
Scan Results

Initial Disruptions

- **Scan 2**:
  - Censorship changes
    - Complete QUIC blockage
    - DNS/TCP:
      96.68% unresolvable
    - temporary blockings of other protocols

➡ Preliminary steps towards shutdown

Cui et al. [2]: localized shutdown drills

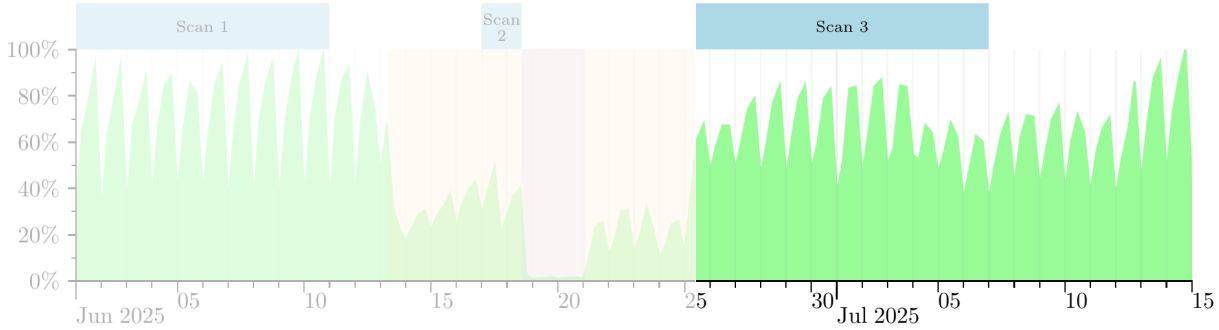


Protocol	Scan 1	Scan 2
DNS/UDP	1,361 (15.12%)	1,509 (16.77%)
DNS/TCP	1,361 (15.12%)	**8,701 (96.68%)***
HTTP	1,375 (15.28%)	1,730 (19.22%)
TLS	1,351 (15.01%)	1,555 (17.28%)
QUIC	1 (0.01%)	**9,000 (100%)‡**
Total	9,000	9,000

* No server response after successful TCP handshake
‡ Complete QUIC blocking

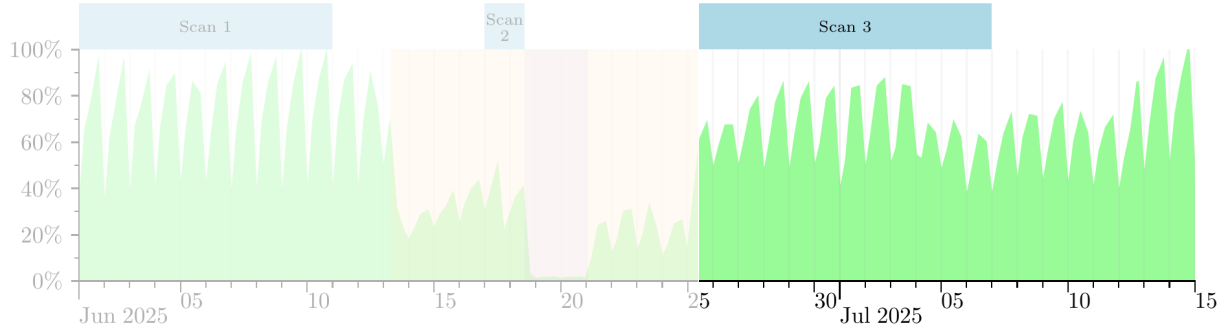
Scan Results

Censorship after Shutdown



Scan Results

Censorship after Shutdown



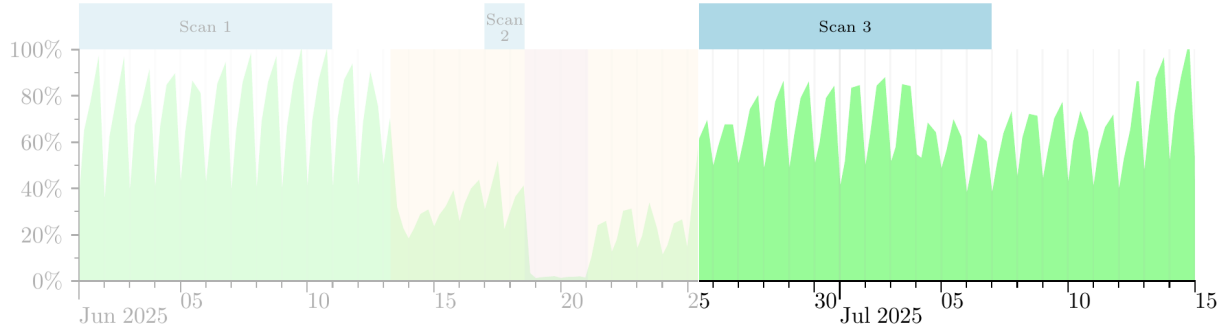
- **Scan 3**:
  - QUIC blockage remained
  - TCP based protocols mostly unaffected
  - DNS/UDP: increased packet drops

Protocol	Scan 2	Scan 3
DNS/UDP	1,509 (16.77%)	**8,026 (89.18%)**†
DNS/TCP	**8,701 (96.68%)***	1,384 (15.38%)
HTTP	1,730 (19.22%)	1,412 (15.69%)
TLS	1,555 (17.28%)	1,369 (15.21%)
QUIC	**9,000 (100%)**‡	**9,000 (100%)**‡
Total	9,000	9,000

* No server response after successful TCP handshake
† Not domain-specific, caused by general UDP transport instabilities
‡ Complete QUIC blocking

Scan Results

Censorship after Shutdown



- **Scan 3**:
  - QUIC blockage remained
  - TCP based protocols mostly unaffected
  - DNS/UDP: increased packet drops

Protocol	Scan 2	Scan 3
DNS/UDP	1,509 (16.77%)	**8,026 (89.18%)**†
DNS/TCP	**8,701 (96.68%)***	1,384 (15.38%)
HTTP	1,730 (19.22%)	1,412 (15.69%)
TLS	1,555 (17.28%)	1,369 (15.21%)
QUIC	**9,000 (100%)**‡	**9,000 (100%)**‡
Total	9,000	9,000

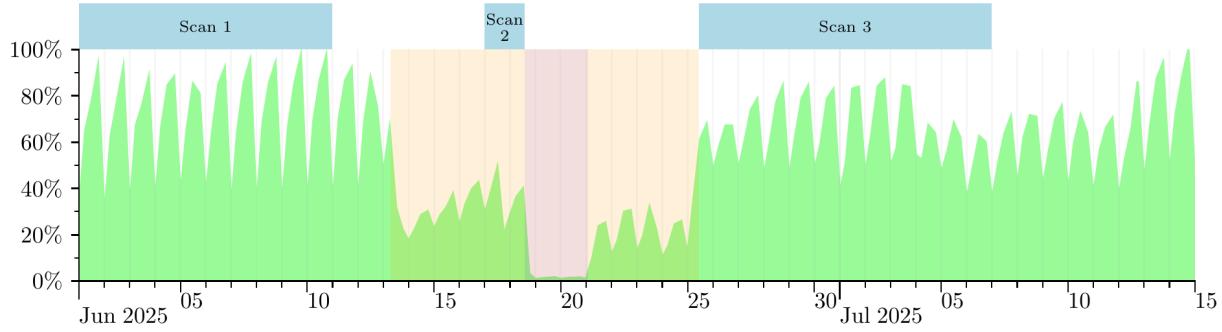
* No server response after successful TCP handshake
† Not domain-specific, caused by general UDP transport instabilities
‡ Complete QUIC blocking

Observed behavior coherent with user reports [3, 4]

Scan Results

Summary

- Censorship policy changes before shutdown
- UDP instabilities after shutdown



Protocol	Scan 1	Scan 2	Scan 3
DNS/UDP	1,361 (15.12%)	1,509 (16.77%)	**8,026 (89.18%)**†
DNS/TCP	1,361 (15.12%)	**8,701 (96.68%)***	1,384 (15.38%)
HTTP	1,375 (15.28%)	1,730 (19.22%)	1,412 (15.69%)
TLS	1,351 (15.01%)	1,555 (17.28%)	1,369 (15.21%)
QUIC	1 (0.01%)	**9,000 (100%)**‡	**9,000 (100%)**‡
Total	9,000	9,000	9,000

* No server response after successful TCP handshake
† Not domain-specific, caused by general UDP transport instabilities
‡ Complete QUIC blocking

Injection Patterns

```
<title>NTL1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

Injection Patterns

```
<title>NTL1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

```
<title>NTE1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

Injection Patterns

```
<title>NTL1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

(a) Observed TTL values: 53–55

```
<title>NTE1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

(b) Observed TTL values: 186–188

Injection Patterns

```
<title>NTL1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

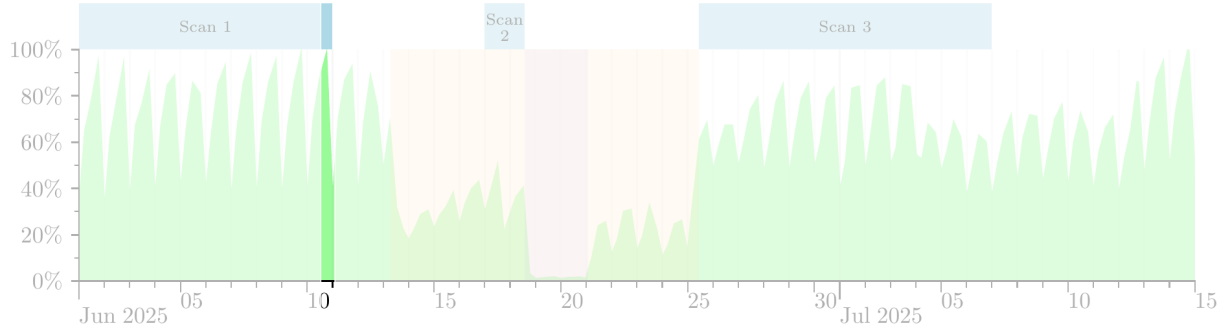
(a) Observed TTL values: 53–55

```
<title>NTE1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

(b) Observed TTL values: 186–188

➡ Distinct injectors

Injection Patterns




```
<title>NTL1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

(a) Observed TTL values: 53–55

```
<title>NTE1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

(b) Observed TTL values: 186–188

➡ Distinct injectors

Further Shutdowns and Predictability

- Fine-grained shutdown: preparation and recovery
- January 2026 shutdown: early signs of disruptions [1]

Further Shutdowns and Predictability

- Fine-grained shutdown: preparation and recovery
- January 2026 shutdown: early signs of disruptions [1]

Early detection possible, but:

- Long-term measurements
- Vantage point limitation

Bibliography

[1] Giuseppe Aceto, V. Persico, and Antonio Pescapé. 2026. Iran's January 2026 Internet Shutdown: Public Data, Censorship Methods, and Circumvention Techniques. https://www.semanticscholar.org/paper/289dff849784c17d4729d914ae8ba941ccb55795

[2] Shibo Cui, Mingxuan Liu, Baojun Liu, Haixin Duan, Ruixuan Li, Chaoyi Lu, Jin Zhang, Zhicheng Wang, and Jinghua Bai. 2026. Characterizing Iran's Phased National Internet Shutdown in 2025: A Progressive and Distributed Action. In Proceedings of the ACM Web Conference 2026 (United Arab Emirates) (WWW '26). Association for Computing Machinery, New York, NY, USA, 1830–1840. doi:10.1145/3774904.3792699

[3] Phoenix-999. 2025. Iran networks after the shutdowns (since 2025-06-25) · Issue #489 · net4people/bbs. https://github.com/net4people/bbs/issues/489#issuecomment-3067006744 Accessed: 2026-03-09.

[4] ranthe21. 2025. Internet is completely blocked in Iran (2025-06-17 to 2025-06-26) · Issue #484 · net4people/bbs. https://github.com/net4people/bbs/issues/484#issuecomment-3011967607 Accessed: 2026-03-09.