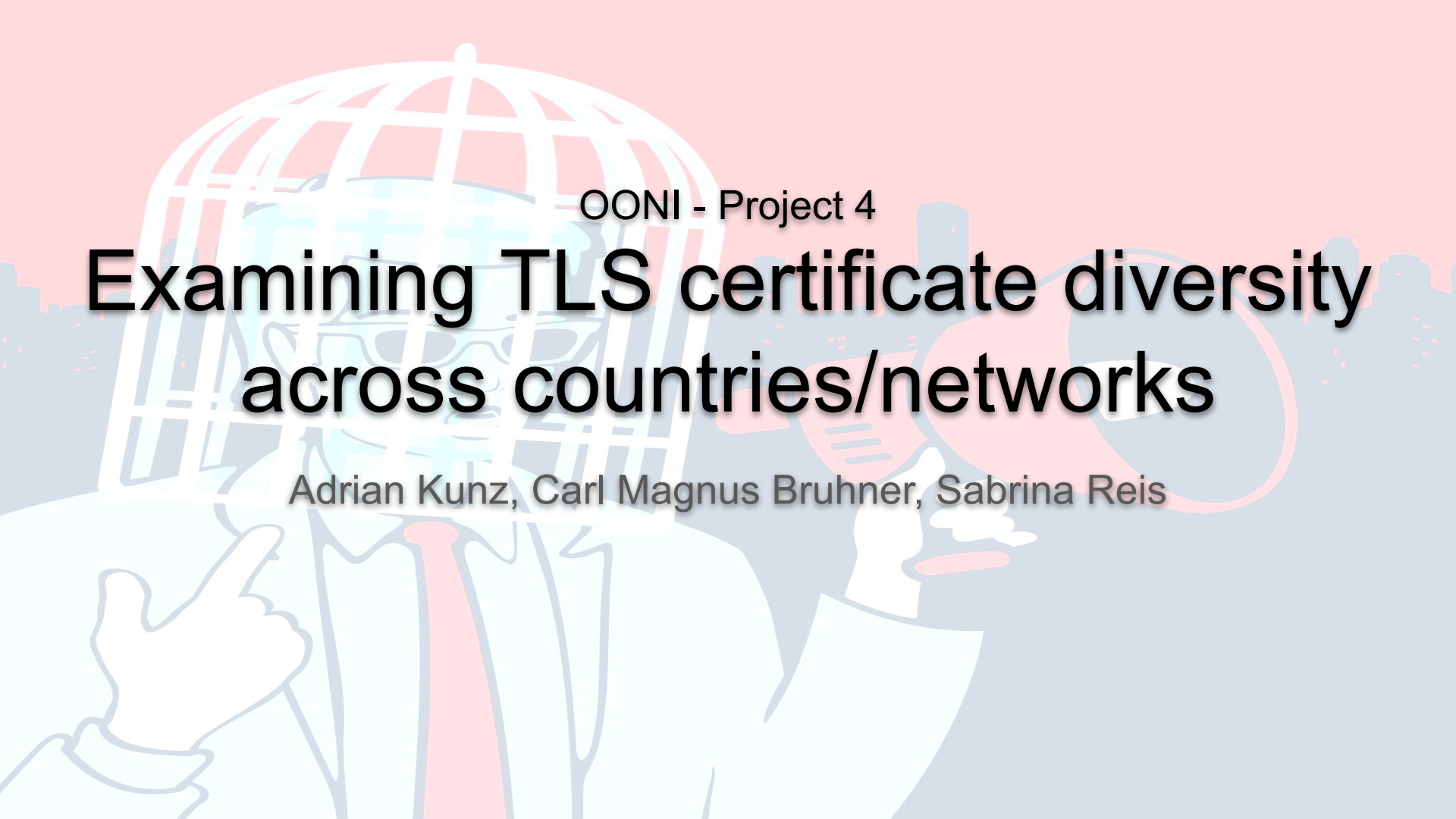


OONI - Project 4

Examining TLS certificate diversity across countries/networks

Adrian Kunz, Carl Magnus Bruhner, Sabrina Reis

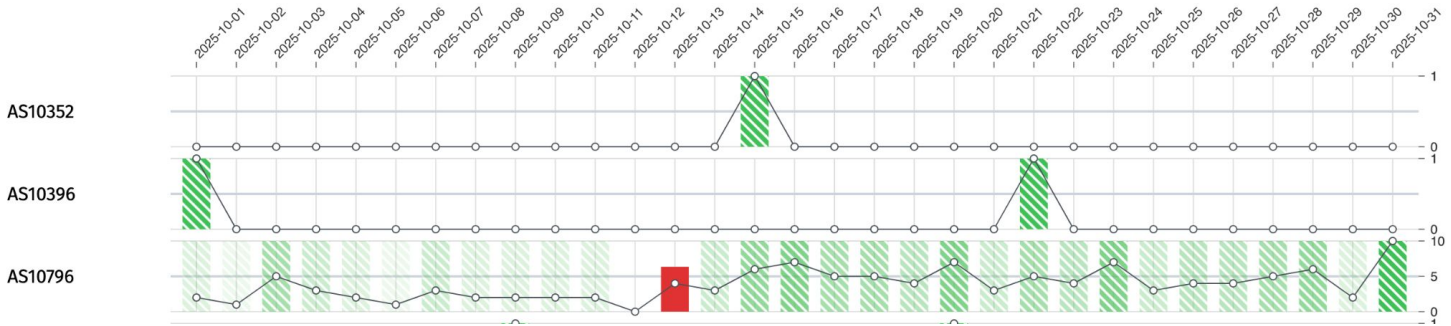
Problem + Case Study

- Investigating one signal of censorship:
  - Domain name TLS certificate varies from different vantage points
- Difficult to investigate given that this often occurs in benign circumstances
- Primary contribution: **Validating OONI findings in Kazakhstan**

Challenges

- Certificate chains are often empty
- Benign use of different certificates depending on vantage point
- Faulty configurations

US	AS 10796	2025-10-13 18:40 UTC	Web Connectivity Test	https://lgbtvacationplanners.com/	Error
US	AS 10796	2025-10-13 08:15 UTC	Web Connectivity Test	https://lgbtvacationplanners.com/	Error
US	AS 10796	2025-10-13 08:03 UTC	Web Connectivity Test	https://lgbtvacationplanners.com/	Error



Validating Past Findings

- Past study on Kazakhstan blocking of news media identified TLS MITM attacks as censorship mechanism
  - Some measurements for knews.kg originating from **Kazhakstan** produce **ssl_unknown_authority** errors
  - From neighboring countries (e.g. Kyrgyzstan KG), no errors occur

	hostname	tls_failure	probe_cc	count	fingerprints
17	knews.kg	None	KG	479	[b7a2d95c931914b077eb0edb896983e04347ea6a0e21a...
18	knews.kg	ssl_unknown_authority	KZ	41	[08897f4b9ff1ef9d419f927b2d3668820bd92463c4c67...
19	knews.kg	None	KZ	20	[982620169c62925a8e09b7d4fde691f74cbe726f62b3f...
20	knews.kg	generic_timeout_error	KZ	1	[]

Validating Past Findings

- In some cases, one certificate was valid and the other did not exist

Certificate not found

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e0:87:d5:f8:56:1b:26:65:09:10:7d:5e:36:af:89:d2
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 180754)
            commonName                = GTS CA 1D4
            organizationName          = Google Trust Services LLC
            countryName               = US
        Validity (Expired)
            Not Before: Mar  3 00:50:48 2023 GMT
            Not After : Jun  1 01:45:02 2023 GMT
        Subject:
            commonName                = knews.kg
```

Future Work / Plan

- Query for measurements, where:
  - some **TLS errors** occur (primarily ‘ssl_unknown_authority’)
  - other measurements from **the same vantage point country** succeed
  - measurements from **neighboring / other countries** don’t produce the same TLS errors
  - during a given time period / over time

- Investigate implications of multiple issuers
- Goal: Identify other countries/regions/domains with similar patterns


~~Questions~~

This slide was censored by Sabrina.