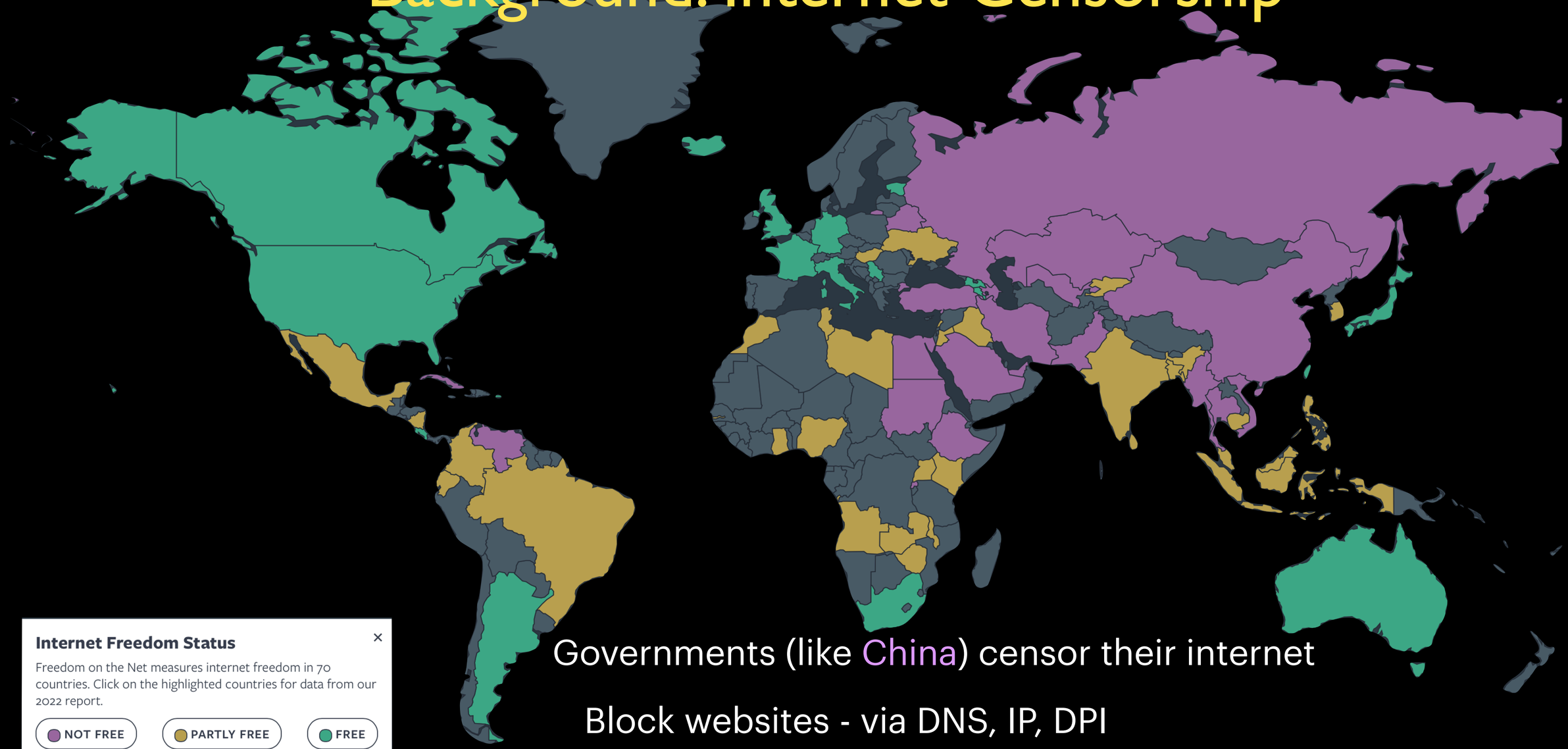
How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic

Mingshi Wu (GFW Report)
Jackson Sippe, Danesh Sivakumar, Jack Burg,
Peter Anderson, Xiaokang Wang, Kevin Bock,
Amir Houmansadr, Dave Levin, Eric Wustrow

Homepage

https://gfw.report/publications/usenixsecurity23/en/

Background: Internet Censorship



Internet Freedom Status

Freedom on the Net measures internet freedom in 70 countries. Click on the highlighted countries for data from our 2022 report.

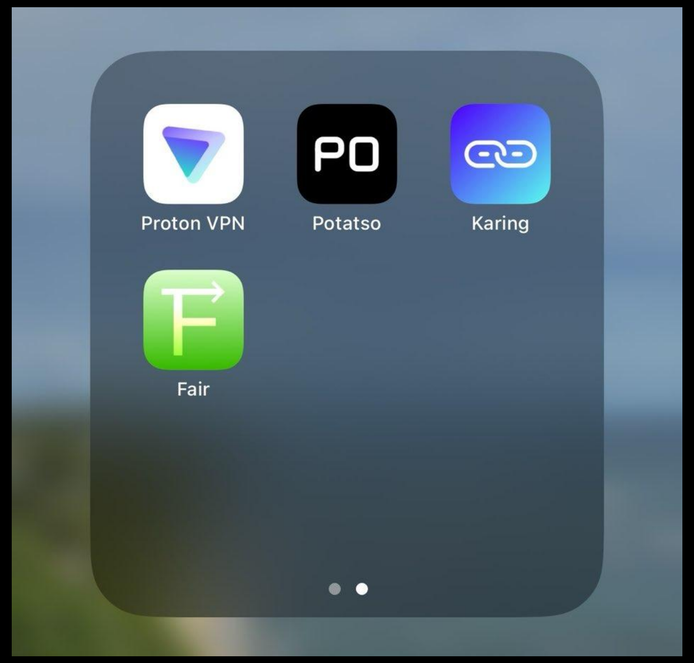
NOT FREE	PARTLY FREE	FREE
Score: 0-39	Score: 40-69	Score: 70-100

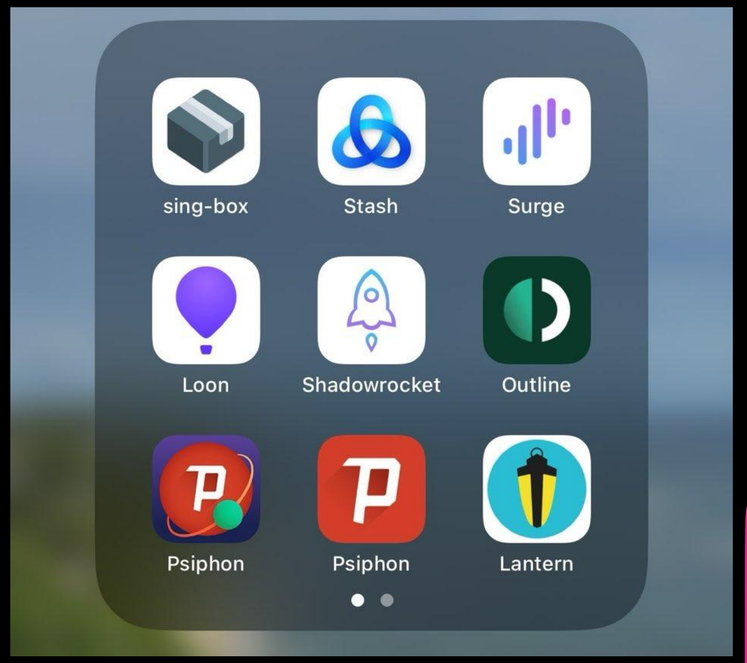
Source: https://freedomhouse.org/explore-the-map?type=fotn&year=2022

Governments (like China) censor their internet

- Block websites - via DNS, IP, DPI
- Block proxies - e.g. Tor, VPN, Shadowsocks, ...

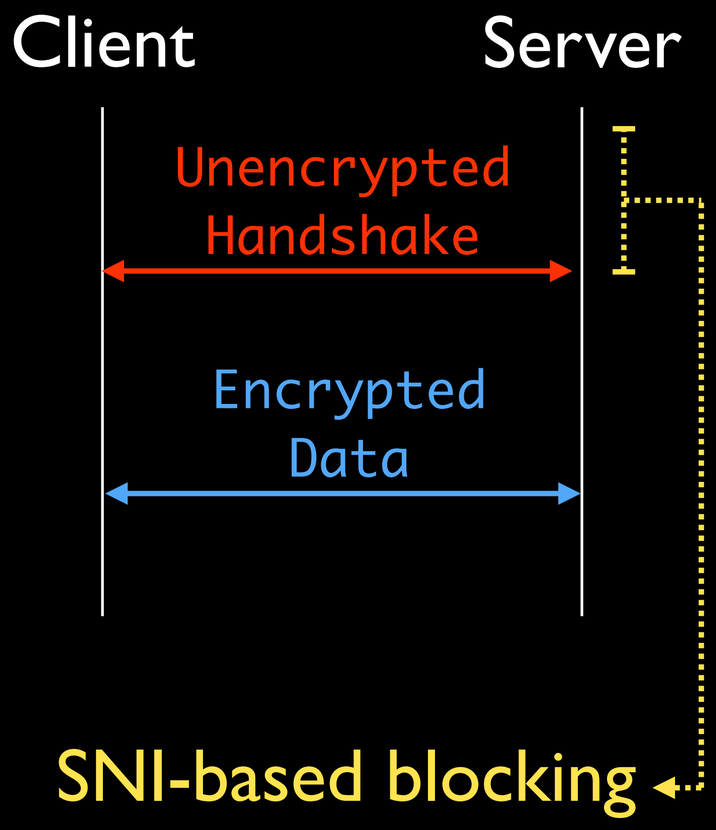
Fully-encryption is “The” Cornerstone of Circumvention



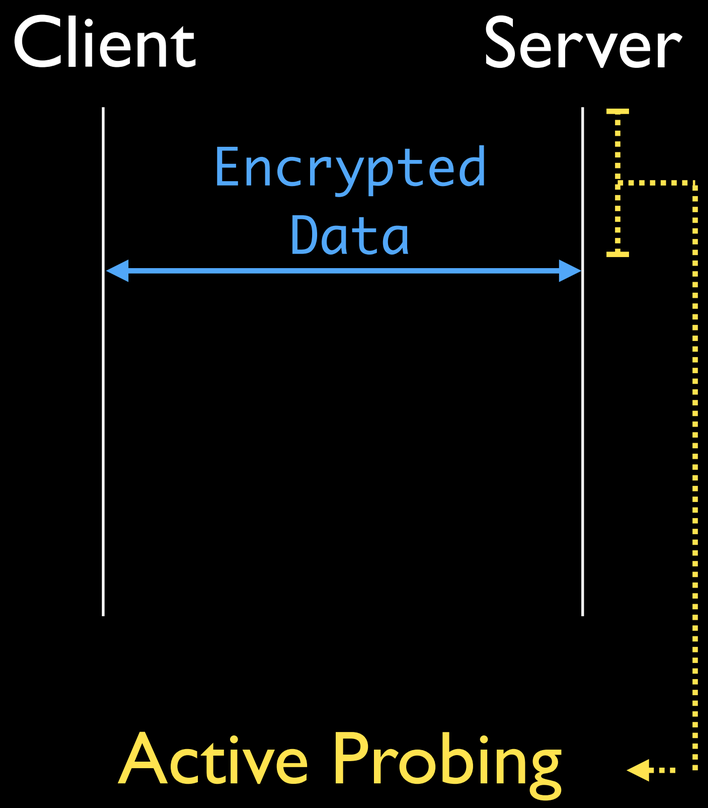


Fully-encrypted traffic

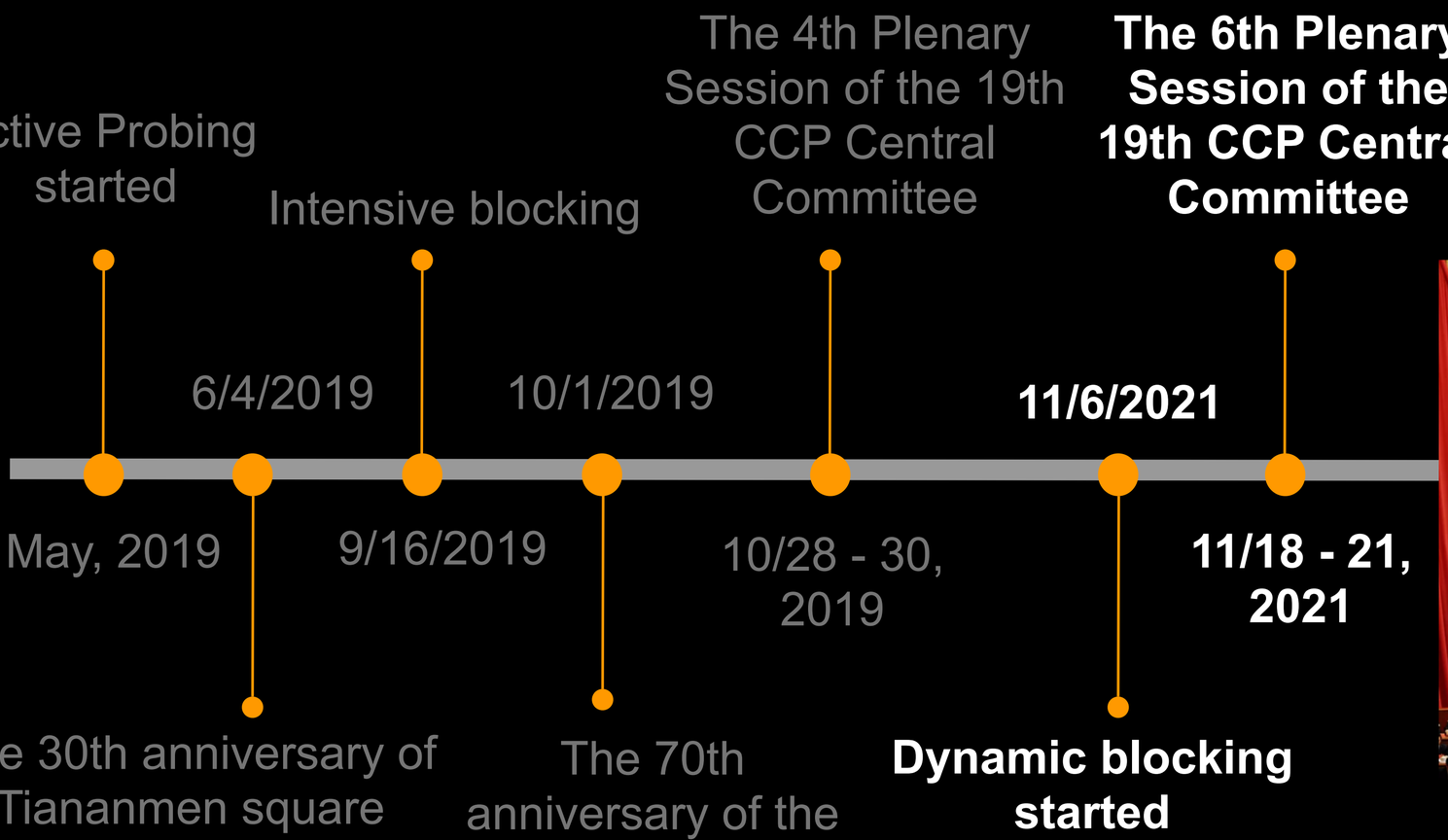
TLS is not *fully*-encrypted



Obfs4, Shadowsocks, VMess are

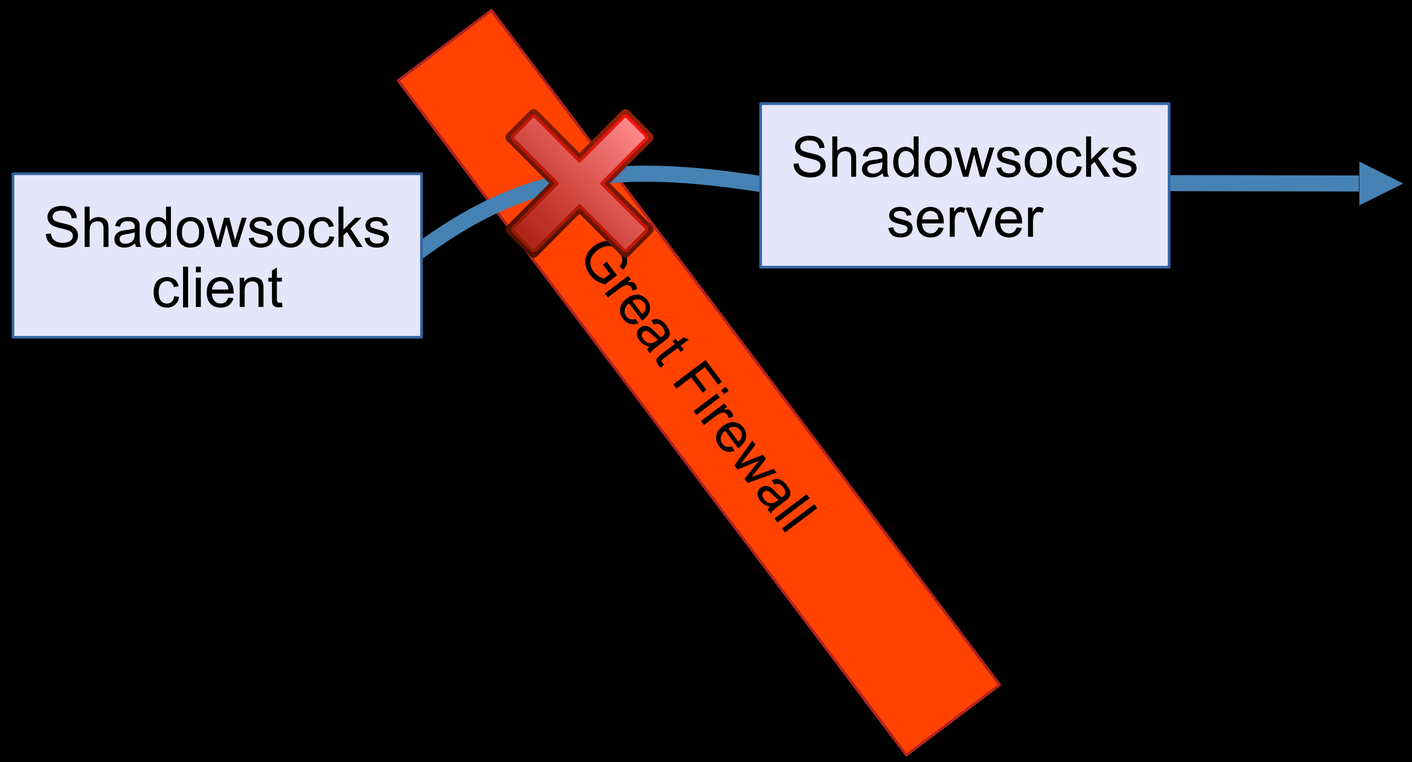


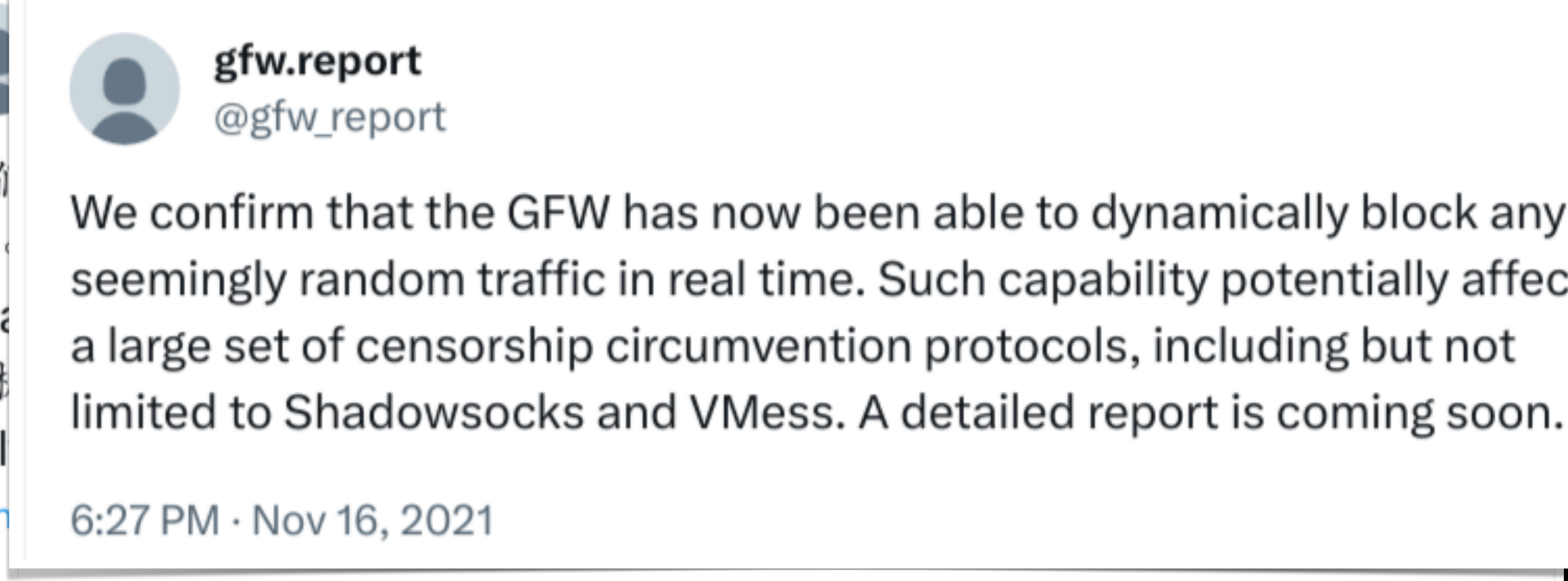
The censor started dynamic blocking of fully encrypted traffic



Dynamic Blocking of Fully Encrypted Traffic

1. Identify fully encrypted connections with traffic analysis.
2. Immediately block all connections with the same three tuple (client IP, server IP, server Port) for 180 seconds.





6:43 PM · Nov 16, 2021

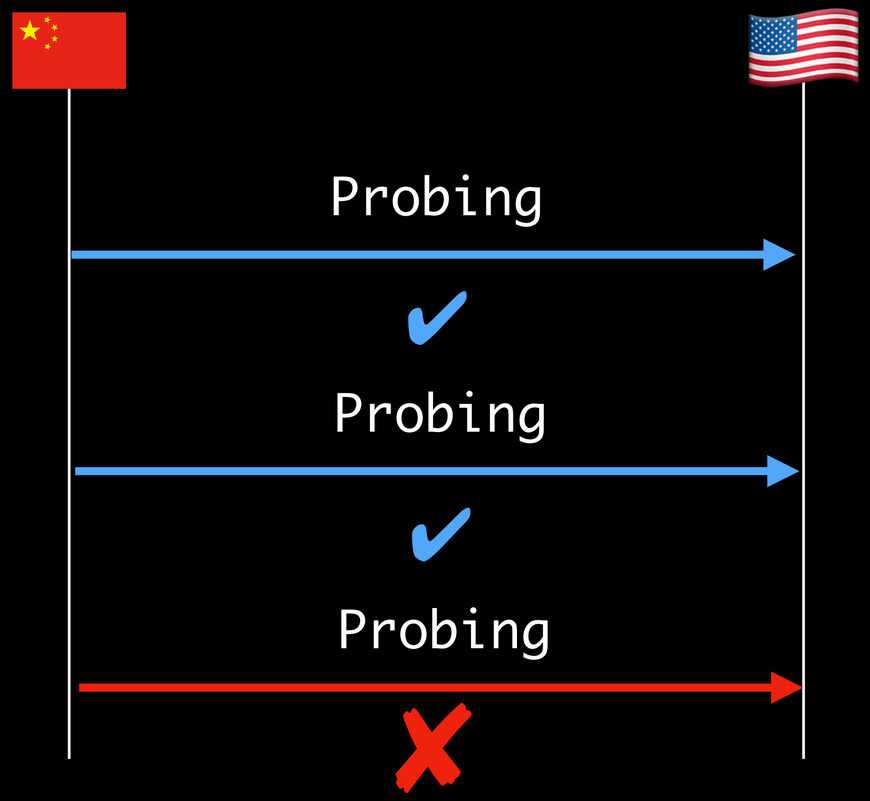
532 Reposts **35** Quotes **2,434** Likes **266** Bookmarks

Censor's Traffic Analysis Algorithm

Block the connection *unless any of the following hold*

- Fraction of zeroes ≤ 42.5% or ≥ 57.5%
- The first six bytes are printable ASCII
- >50% of bytes are printable ASCII
- 20 contiguous bytes are printable ASCII
- Matches the fingerprint for HTTP or TLS

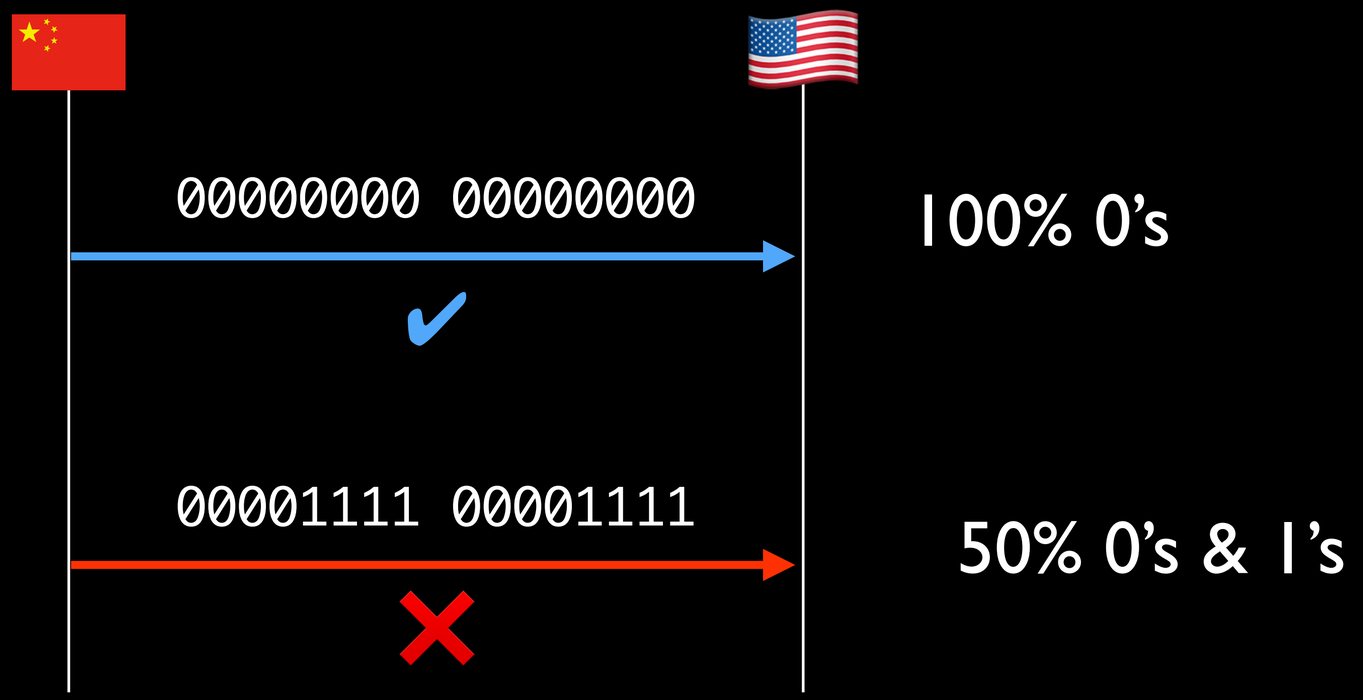
Analyzing how China blocks fully encrypted proxies



Identifying Random

Bytes	State
01 01 01 01 01 01 01 01	ALLOWED
02 02 02 02 02 02 02 02	ALLOWED
• • •	
0E 0E 0E 0E 0E 0E 0E 0E	ALLOWED
0F 0F 0F 0F 0F 0F 0F 0F	BLOCKED
10 10 10 10 10 10 10 10	ALLOWED
• • •	
16 16 16 16 16 16 16 16	ALLOWED
17 17 17 17 17 17 17 17	BLOCKED
18 18 18 18 18 18 18 18	ALLOWED

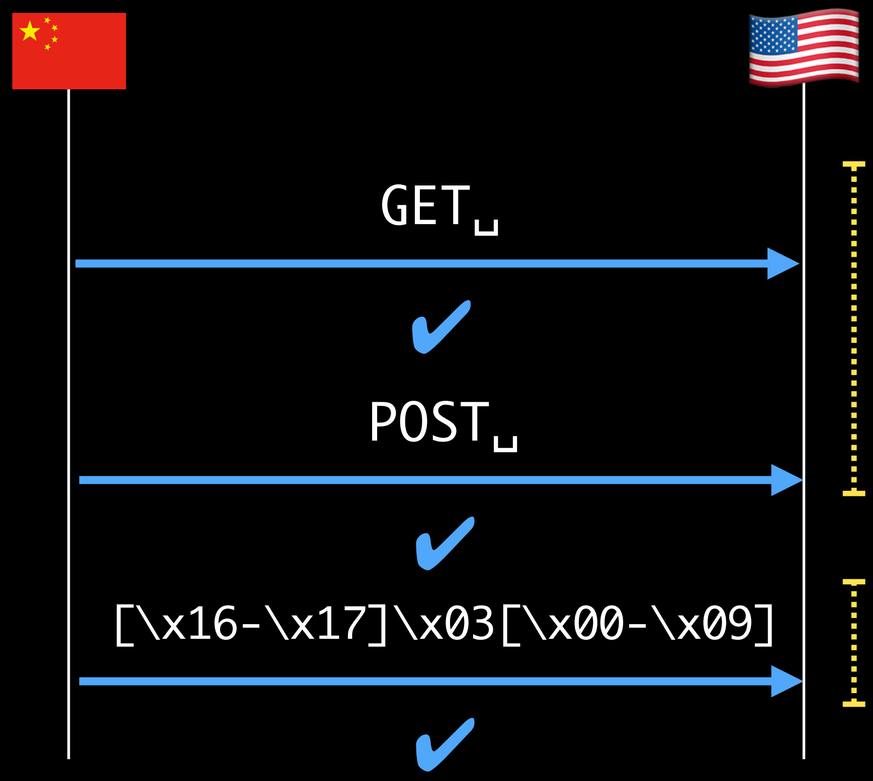
Entropy test



Blocking Exemption

Fraction of zeroes ≤ 42.5% or ≥ 57.5%

Exemption: Protocol signatures



HTTP fingerprint

TLS fingerprint

Blocking Exemption

Matches the fingerprint for HTTP or TLS

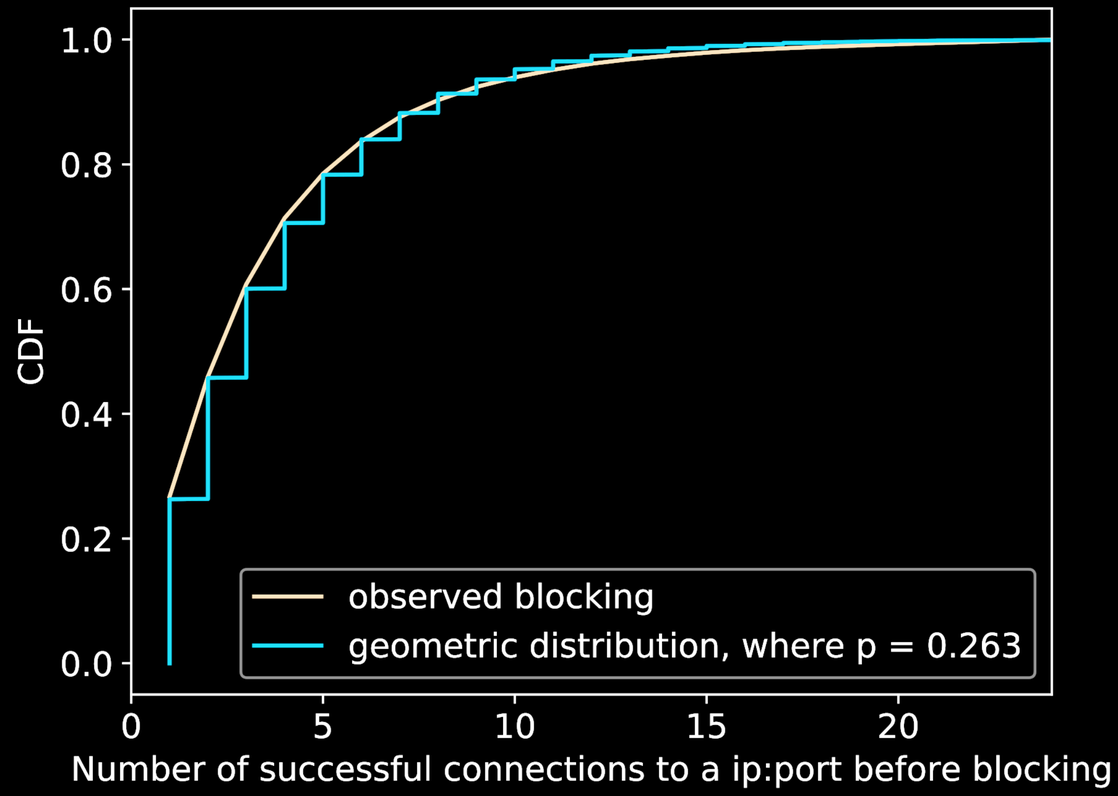
Which connections are affected?

Blocking happens intermittently

We observe blocking 26.3% of the time

Why?

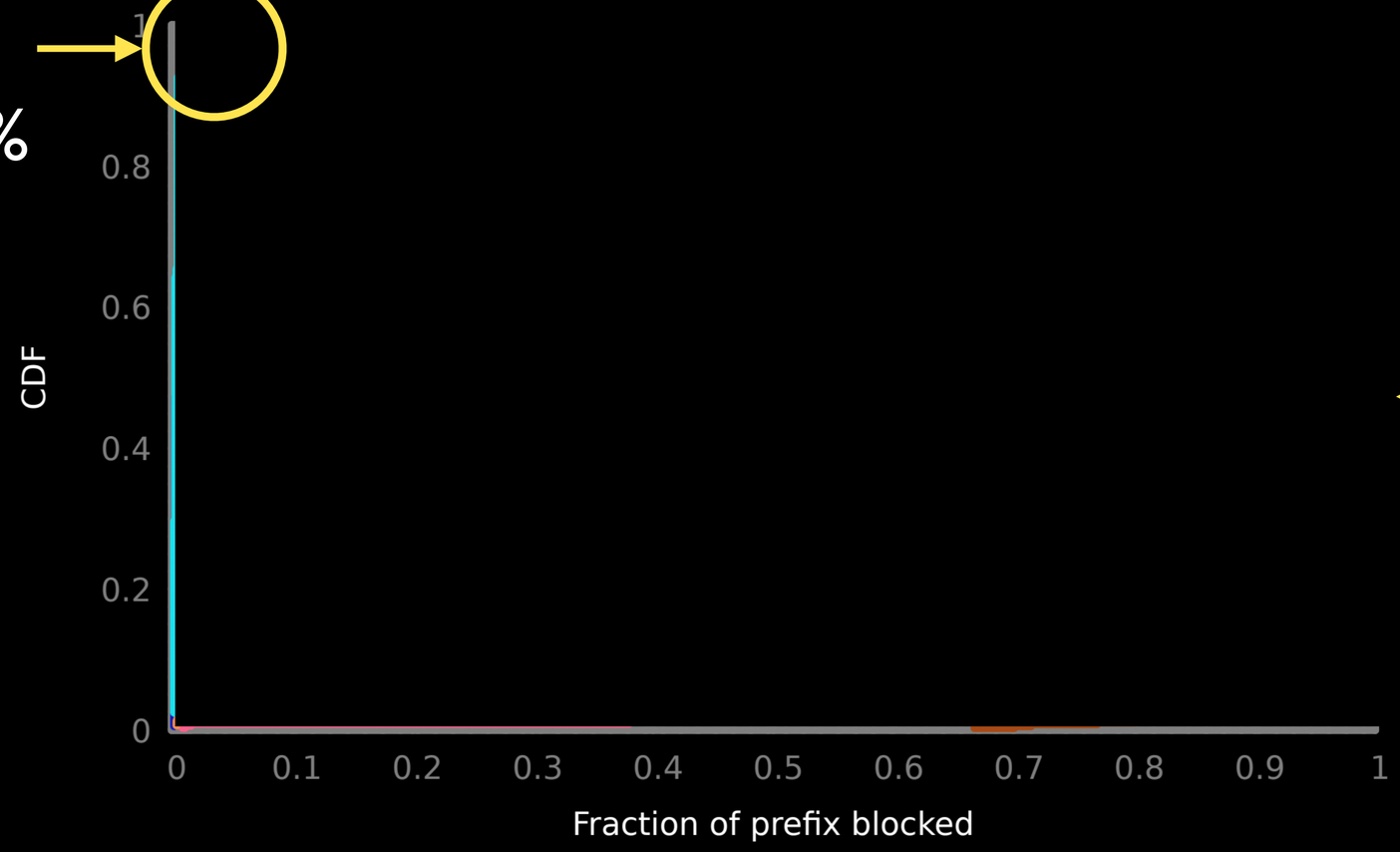
- Sample observed traffic
- Reduce false positives



Which IP addresses are affected?

98% of IP addresses are unaffected

95% of ASes affected <10%



A few ASes affected >30%

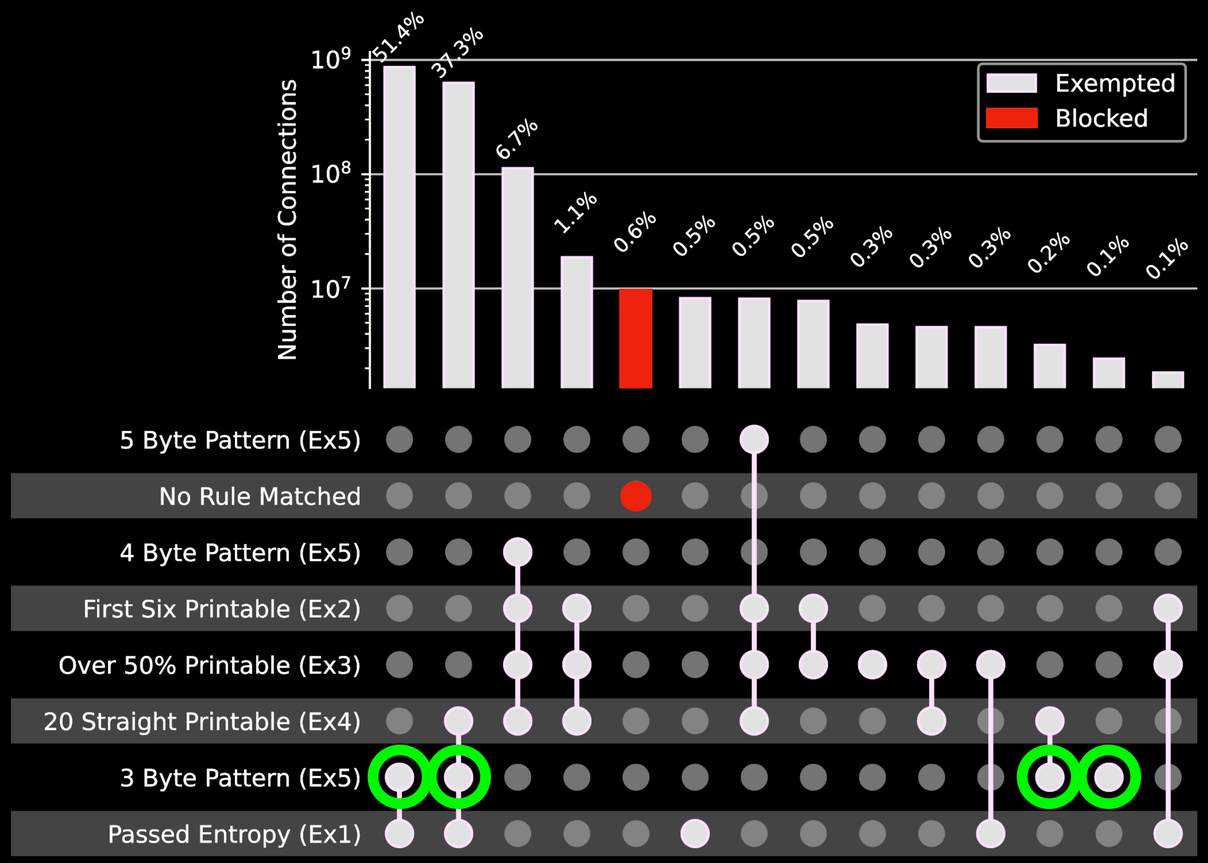
All of the affected ASes are popular VPS providers

How Good is the Censor's Detection Algorithm?

Utilize university network tap to test the rules

Estimate 0.6% false positive rate

89% of traffic is exempt by matching TLS

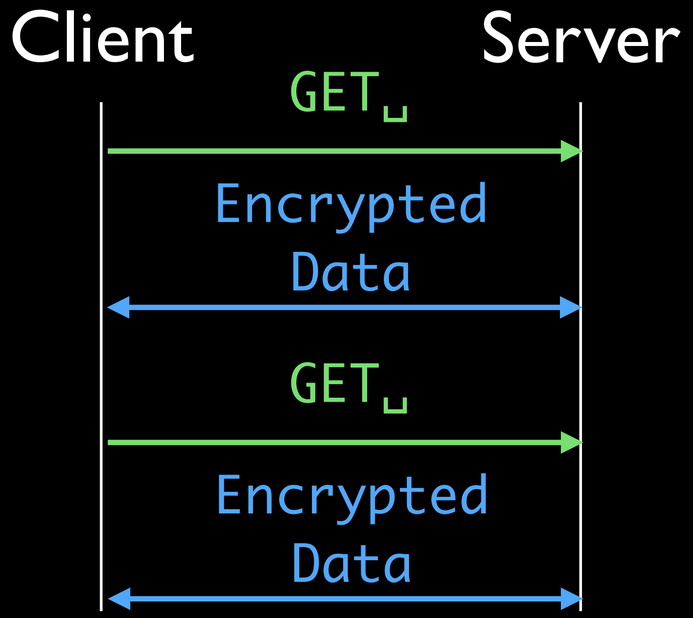


Mitigations

Short Term

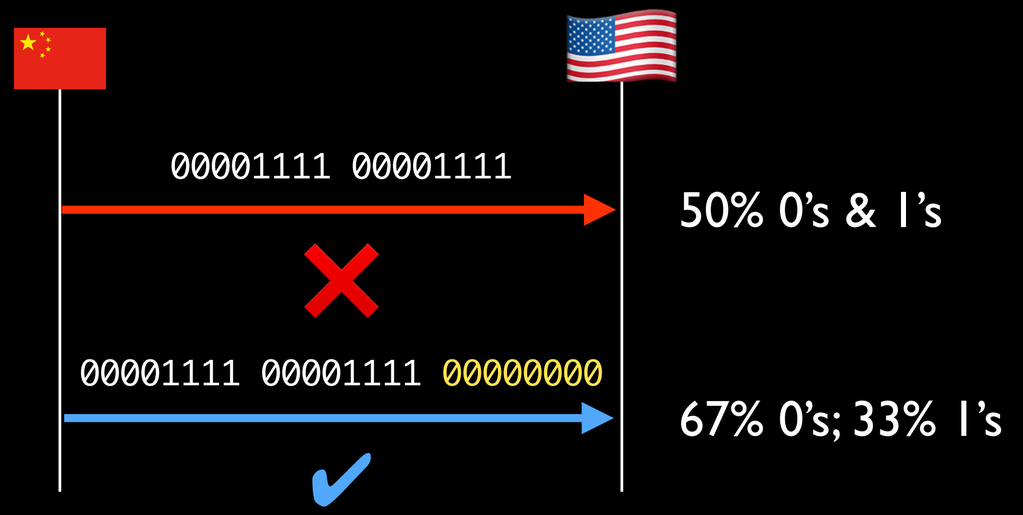
Match an exemption

Eg. TLS or plaintext prefix



Long Term

Modify entropy of the payload



Bypassing Censors' Detection

Block the connection *unless any of the following hold*

Fraction of zeroes ≤ 42.5% or ≥ 57.5%	Pad & Permute
The first six bytes are printable ASCII	Prepending
>50% of bytes are printable ASCII	
20 contiguous bytes are printable ASCII	Prepending
Matches the fingerprint for HTTP or TLS	Prepending

Circumvention Adoption

Adopted by tools with millions of users

Entropy modification


anonymized


shadowsocks-rust*


shadowsocks-android*

Protocol prefix


Outline


Lantern


Psiphon

First six bytes are printable ASCII


shadowsocks-rust


shadowsocks-go

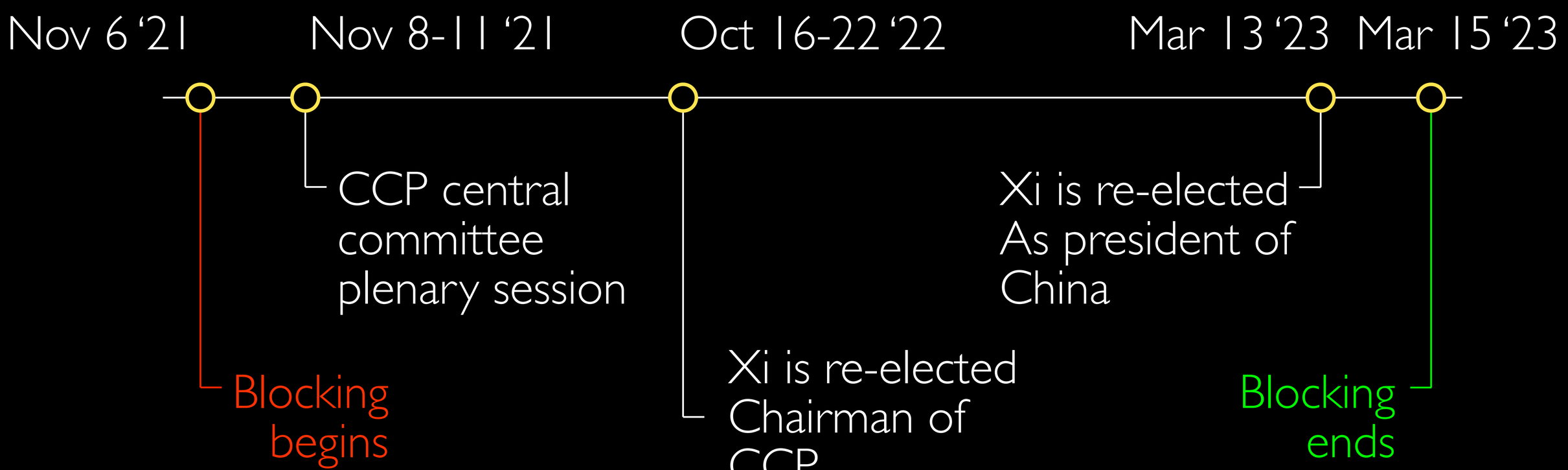

shadowsocks-android


Outline

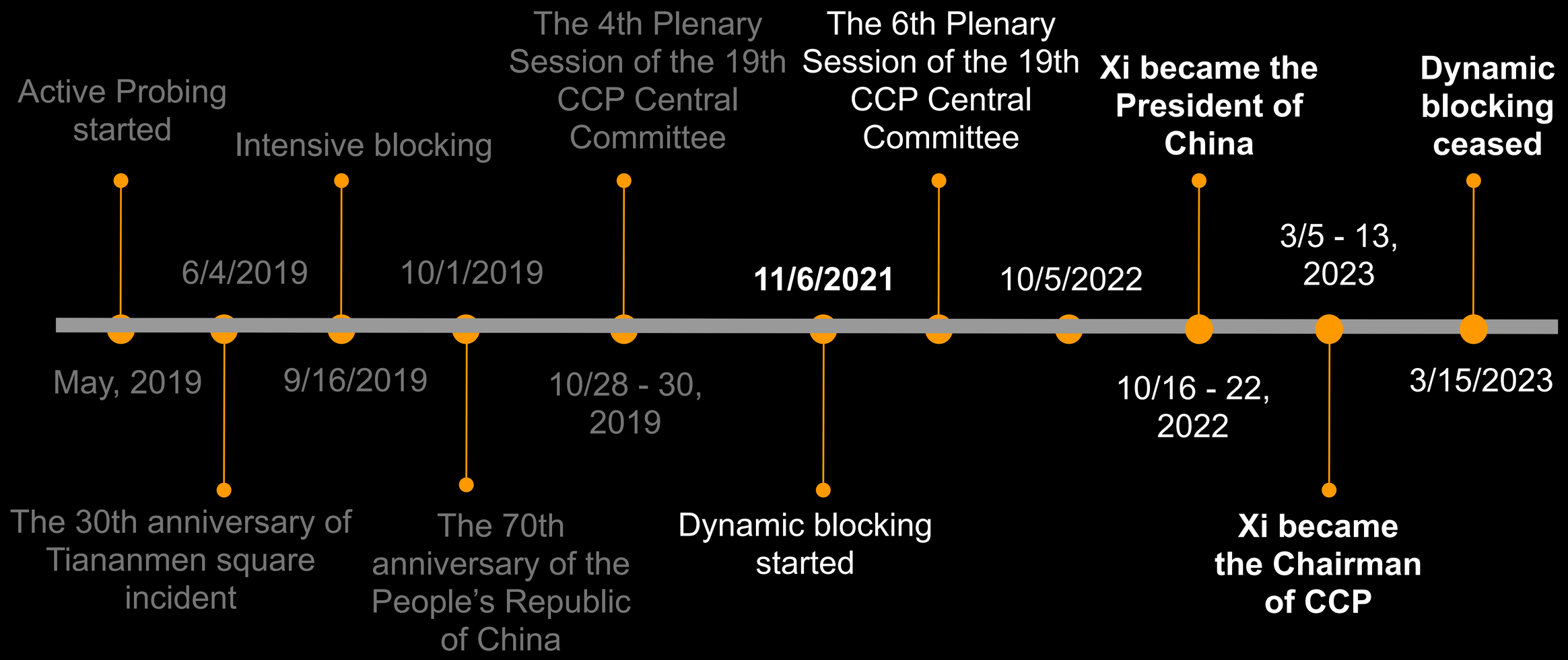

V2Ray (VMess)

* Unofficial feature: https://github.com/net4people/bbs/issues/136

How Political Events Influence Censorship in China?



How Political Events Influence Censorship in China?



How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic

Project Homepage

Questions?

gfw.report@protonmail.com

https://gfw.report/publications/usenixsecurity23/en/

How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic

Find our paper here!
https://gfw.report/publications/usenixsecurity23/en/

Mingshi Wu, Jackson Sippe, Danesh Sivakumar,
Jack Burg, Peter Anderson, Xiaokang Wang, Kevin Bock,
Amir Houmansadr, Dave Levin, Eric Wustrow