Passively detecting Connection tampering

Dave Levin

We don't know how users are experiencing connection tampering

How we measure tampering

OONI

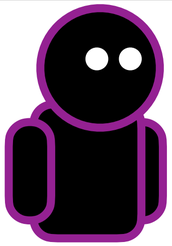
Censored Planet

Mint

How we measure tampering

OONI Censored Planet Mint

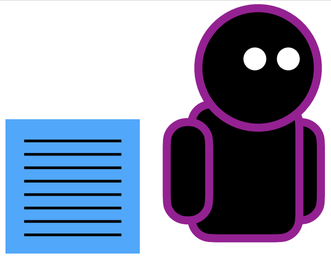
1. Get vantage point, volunteer, or target in a region of interest



How we measure tampering

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest



2. Come up with a “test list” to measure

How we measure tampering

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest

2. Come up with a "test list" to measure

3. Query for items on the test list; Observe what's tampered

How we measure tampering

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest

2. Come up with a "test list" to measure

3. Query for items on the test list; Observe what's tampered

This measures the test list = What *could* be tampered with

How we measure tampering

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest

2. Come up with a "test list" to measure

3. Query for items on the test list; Observe what's tampered

This measures the test list = What *could* be tampered with

It does not measure user traffic = What *is* being tampered with

What we are missing

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest

2. Come up with a "test list" to measure

3. Query for items on the test list; Observe what's tampered

What we are missing

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest

Soliciting participation is difficult

2. Come up with a "test list" to measure

3. Query for items on the test list; Observe what's tampered

What we are missing

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest

Soliciting participation is difficult

2. Come up with a "test list" to measure

How do we know test lists are complete?

3. Query for items on the test list; Observe what's tampered

What we are missing

OONI Censored Planet Mint

1. Get vantage point, volunteer, or target in a region of interest

Soliciting participation is difficult

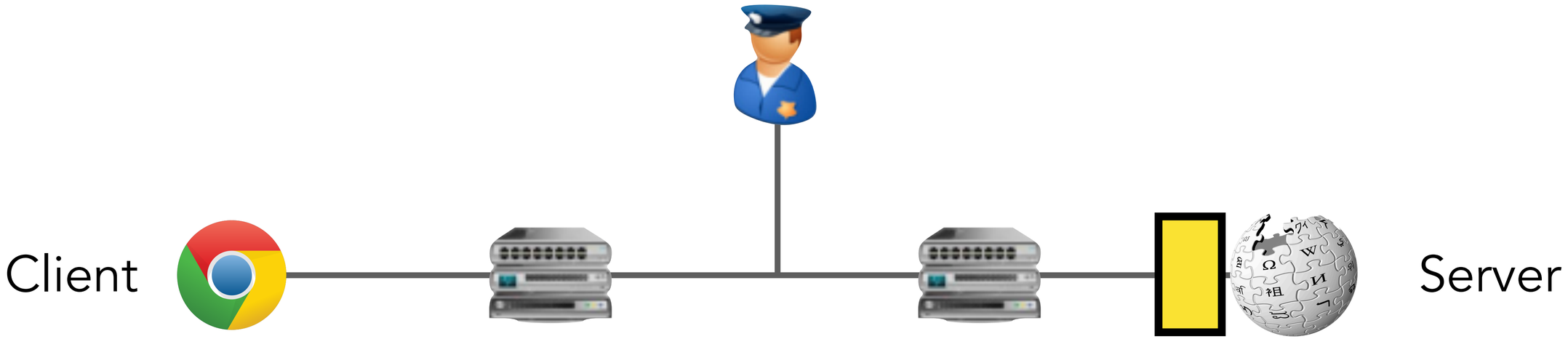
2. Come up with a "test list" to measure

How do we know test lists are complete?

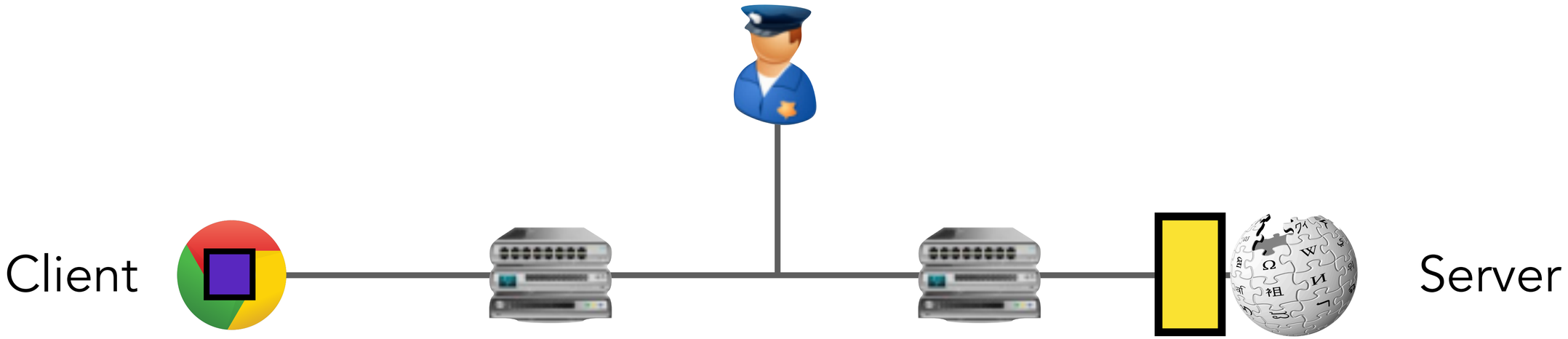
3. Query for items on the test list; Observe what's tampered

What *could* be tampered ≠ What tampering users are *experiencing*

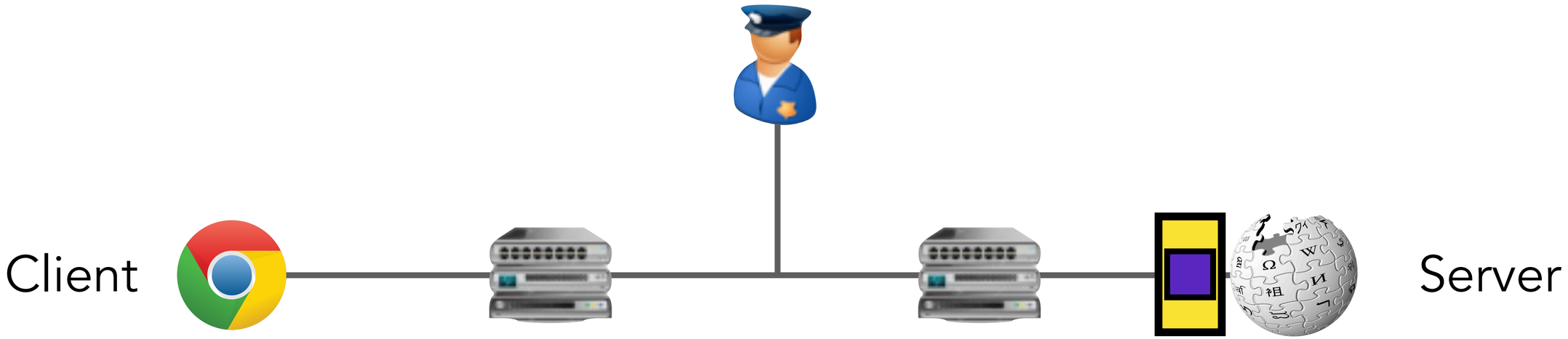
Passively detecting connection tampering



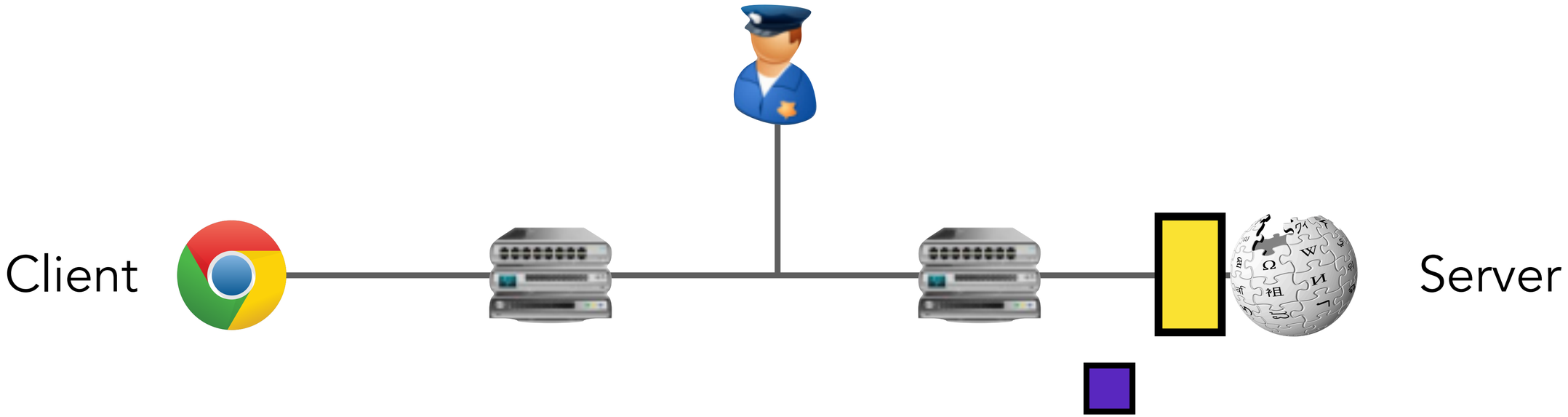
Passively detecting connection tampering



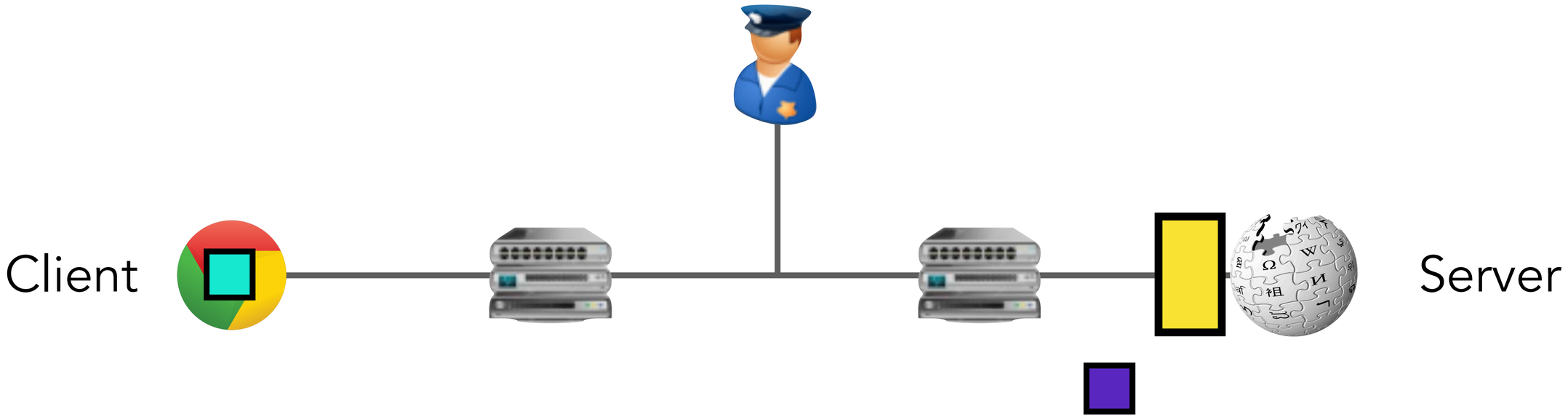
Passively detecting connection tampering



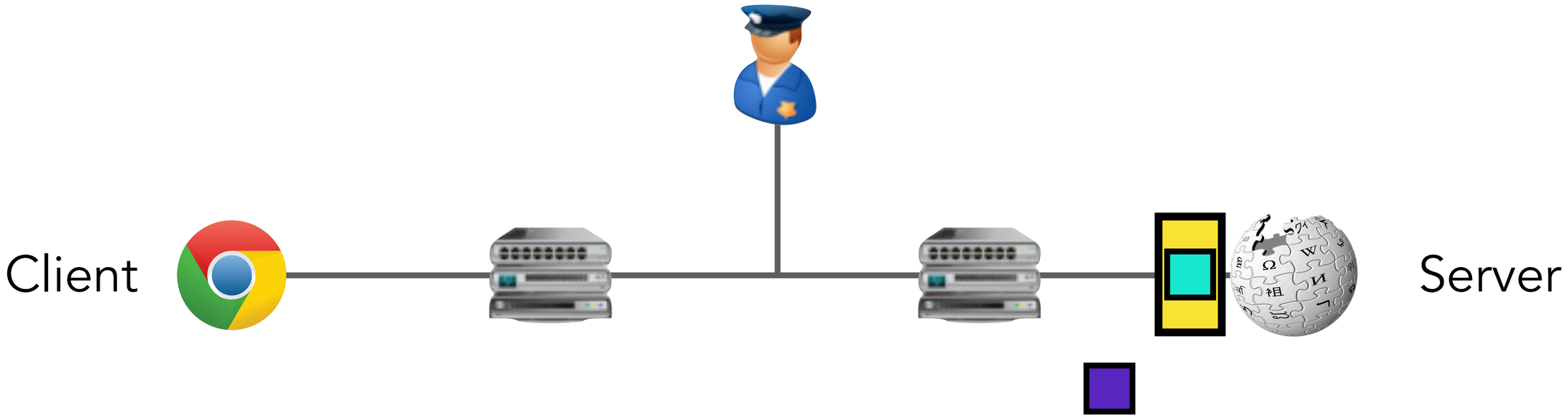
Passively detecting connection tampering



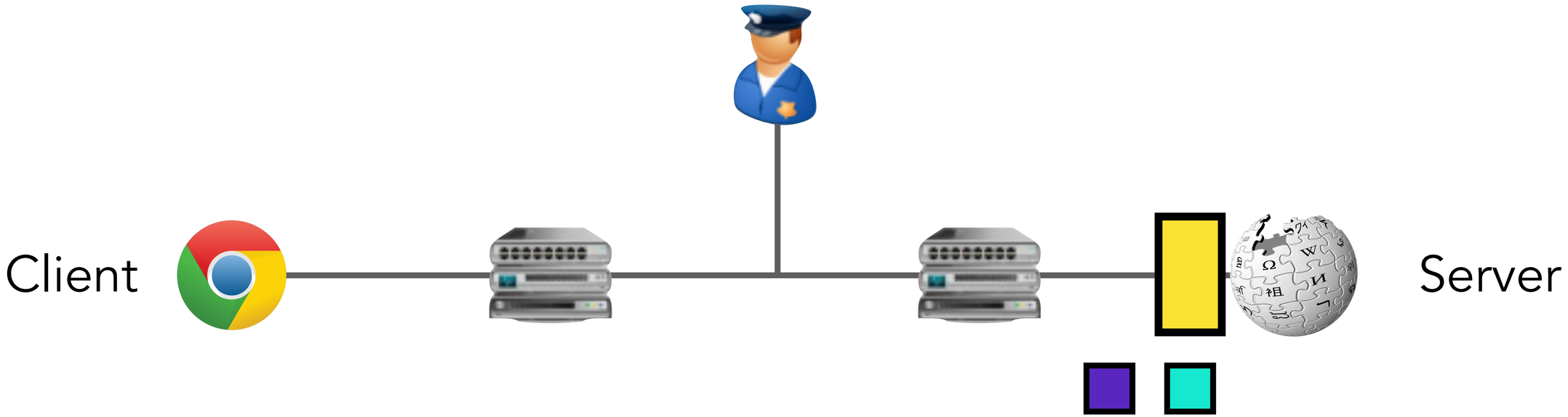
Passively detecting connection tampering



Passively detecting connection tampering

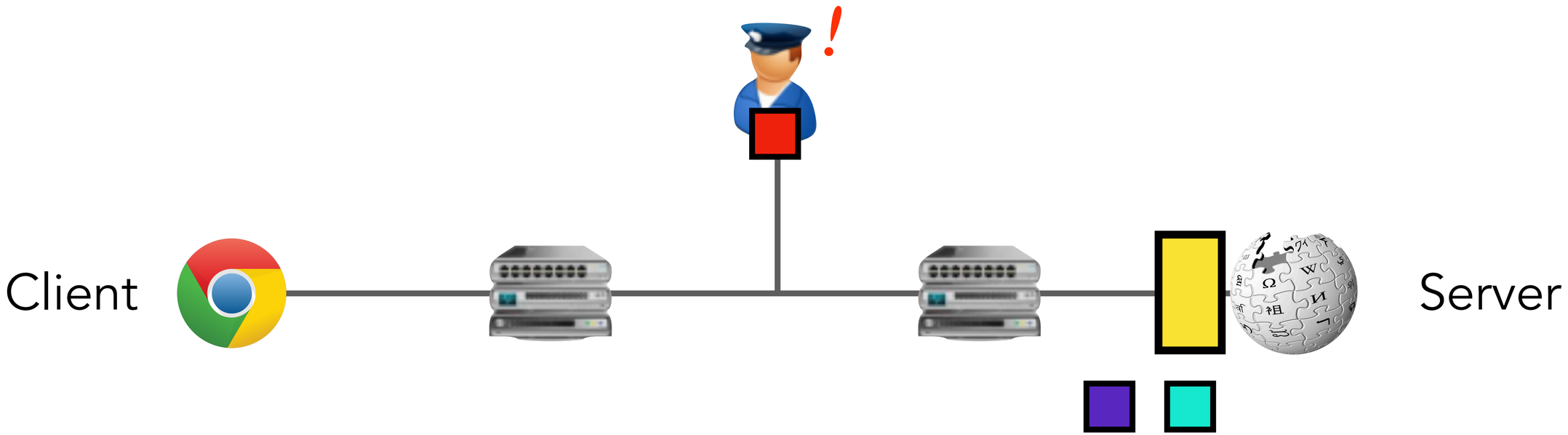


Passively detecting connection tampering



Passively detecting connection tampering

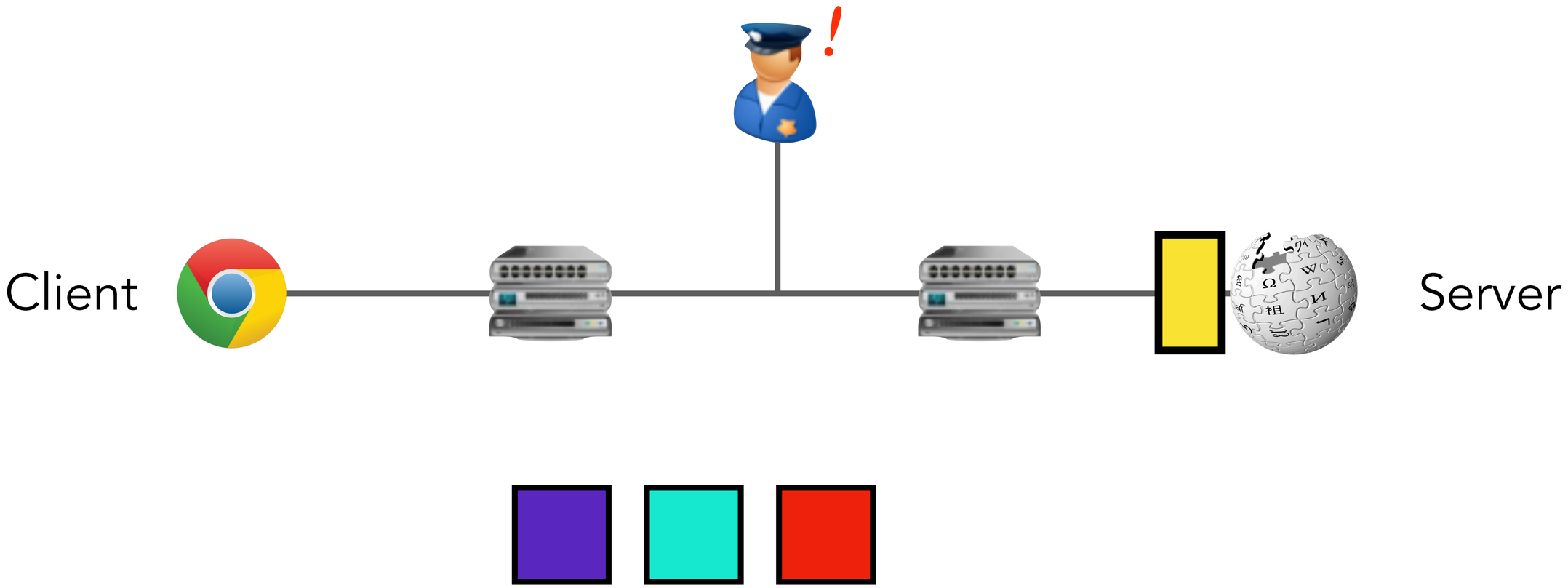
Passively detecting connection tampering



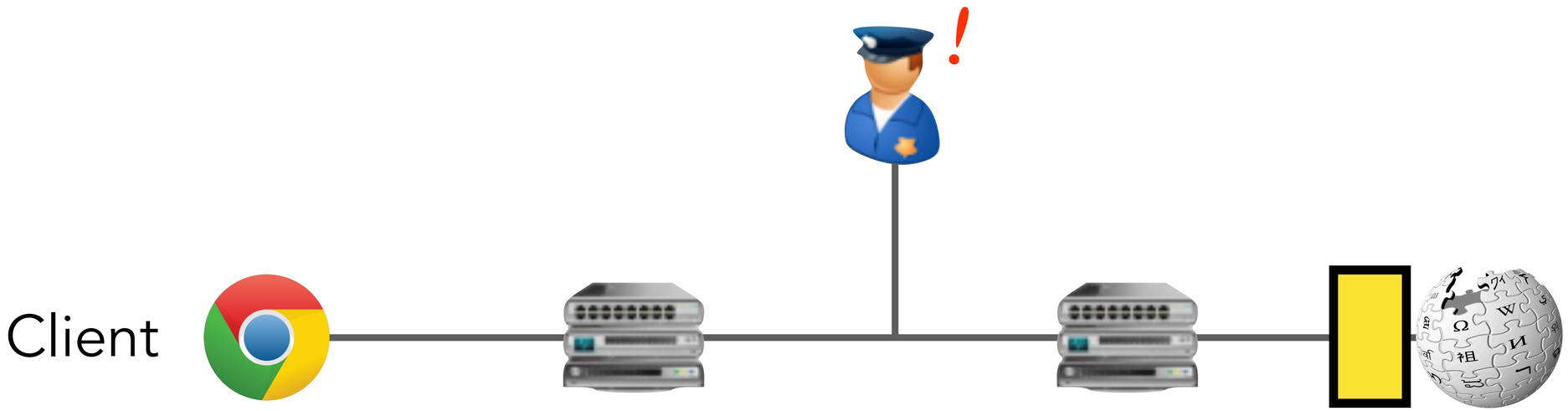
Passively detecting connection tampering

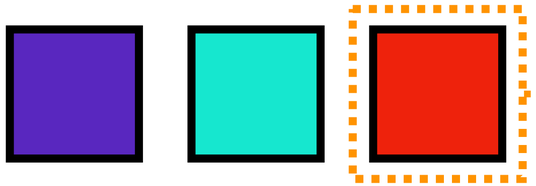
Passively detecting connection tampering

Passively detecting connection tampering



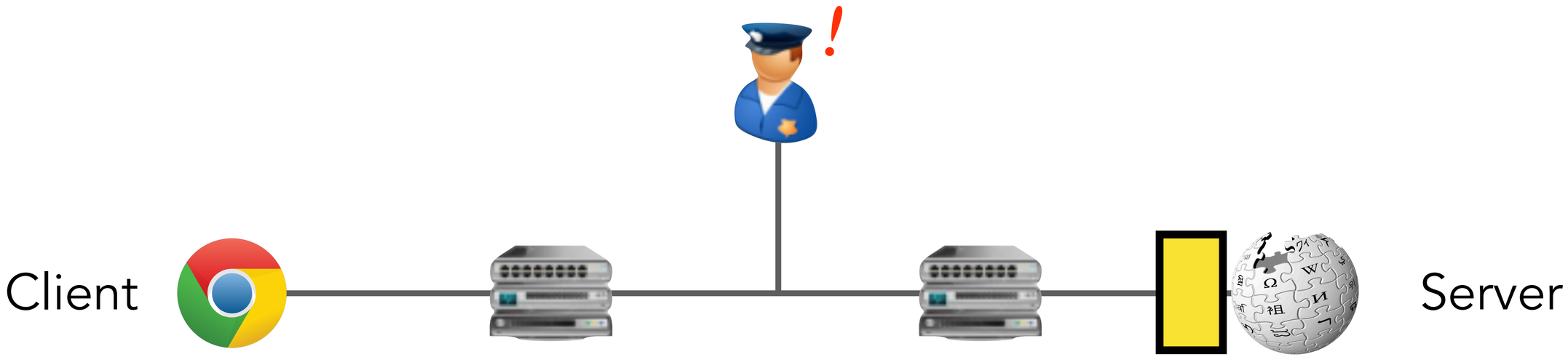
Passively detecting connection tampering



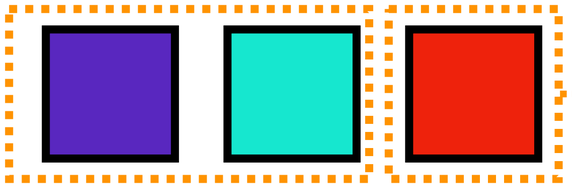


How does that region tamper?

Passively detecting connection tampering

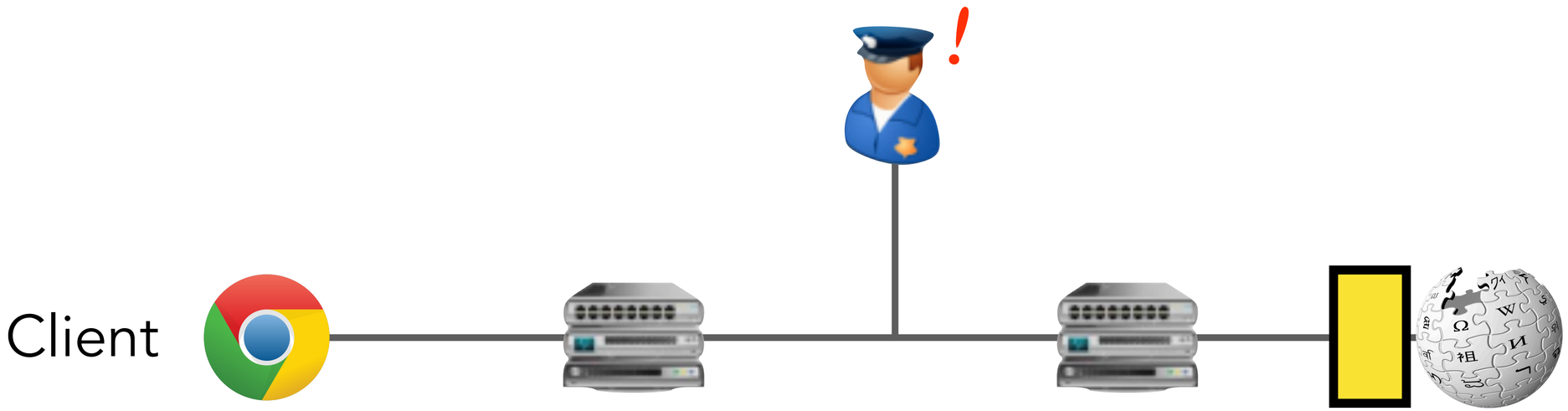


What precipitated the tampering?

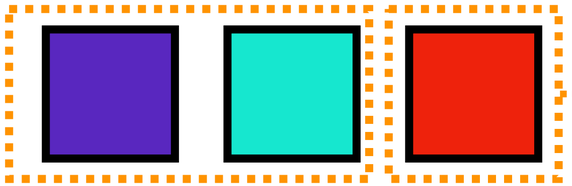


How does that region tamper?

Passively detecting connection tampering



What precipitated the tampering?

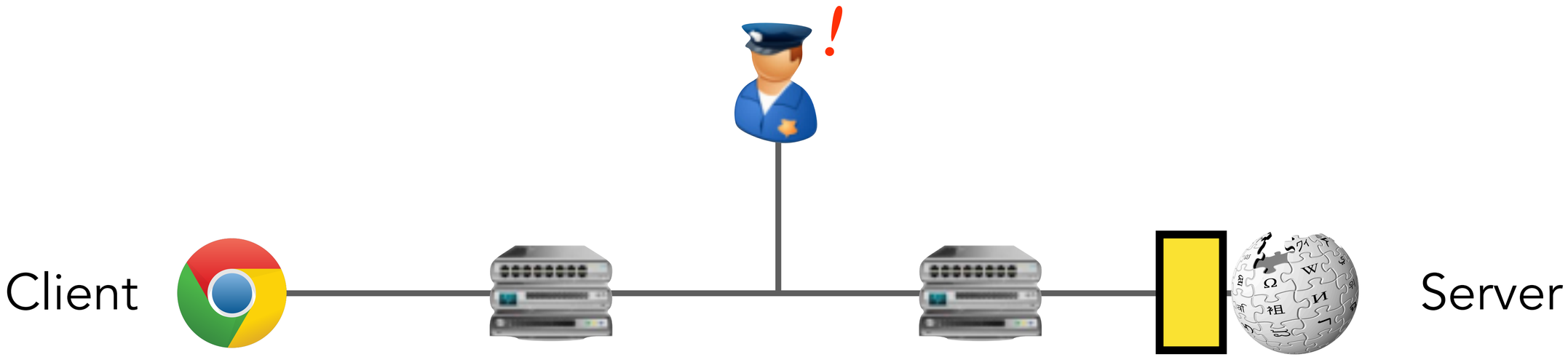


How does that region tamper?

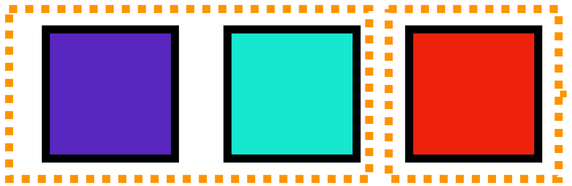
SNI in ClientHello

HTTP GET request

Passively detecting connection tampering



What precipitated the tampering?



How does that region tamper?

SNI in ClientHello

HTTP GET request

This technique lets us *populate test-lists!*

Cloudflare deployment

Cloudflare servers
~17-20% of Internet
websites, 275+ PoPs

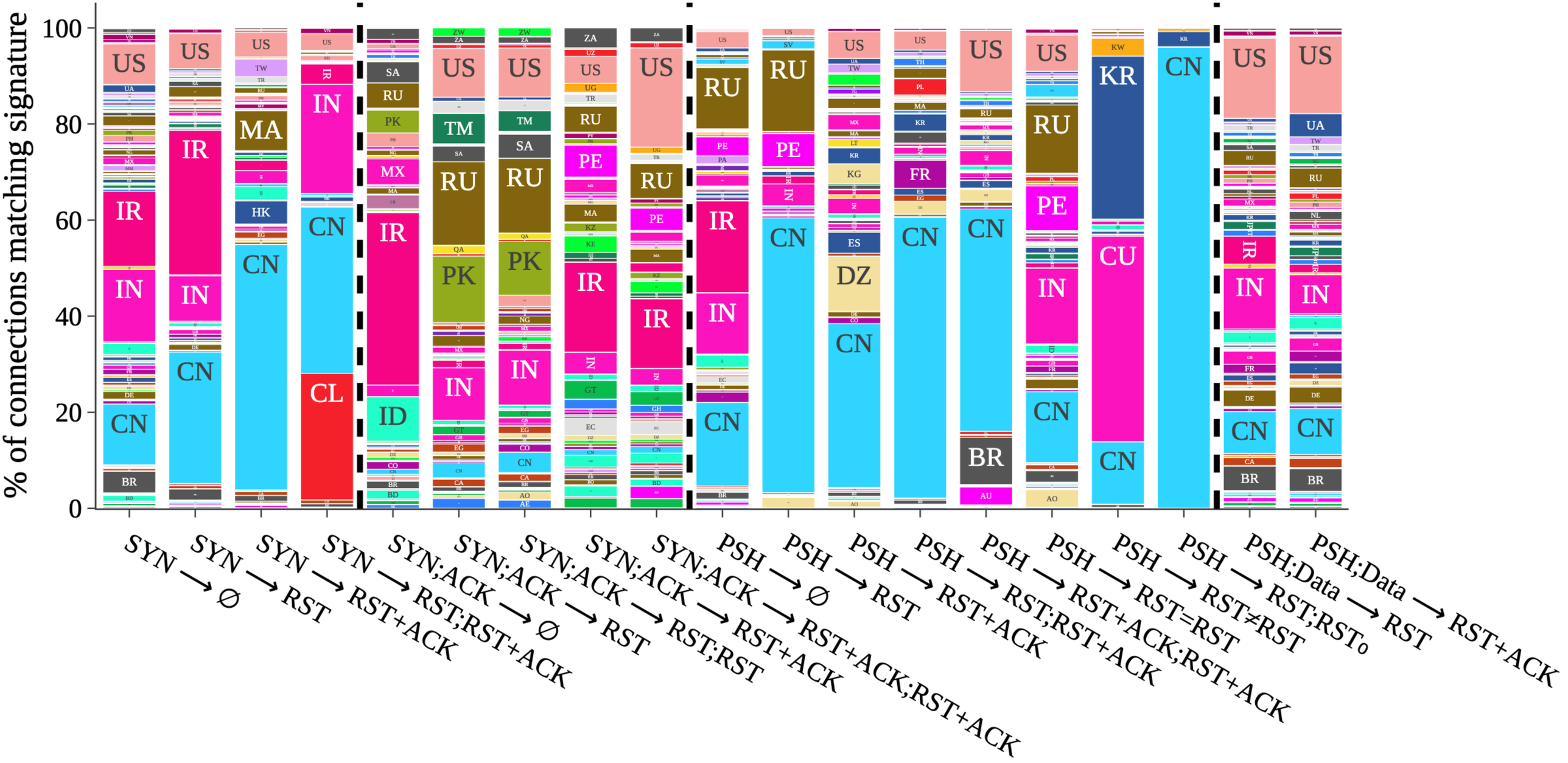
0.01% sample of all
incoming connections

2 weeks of
longitudinal data from
247 countries

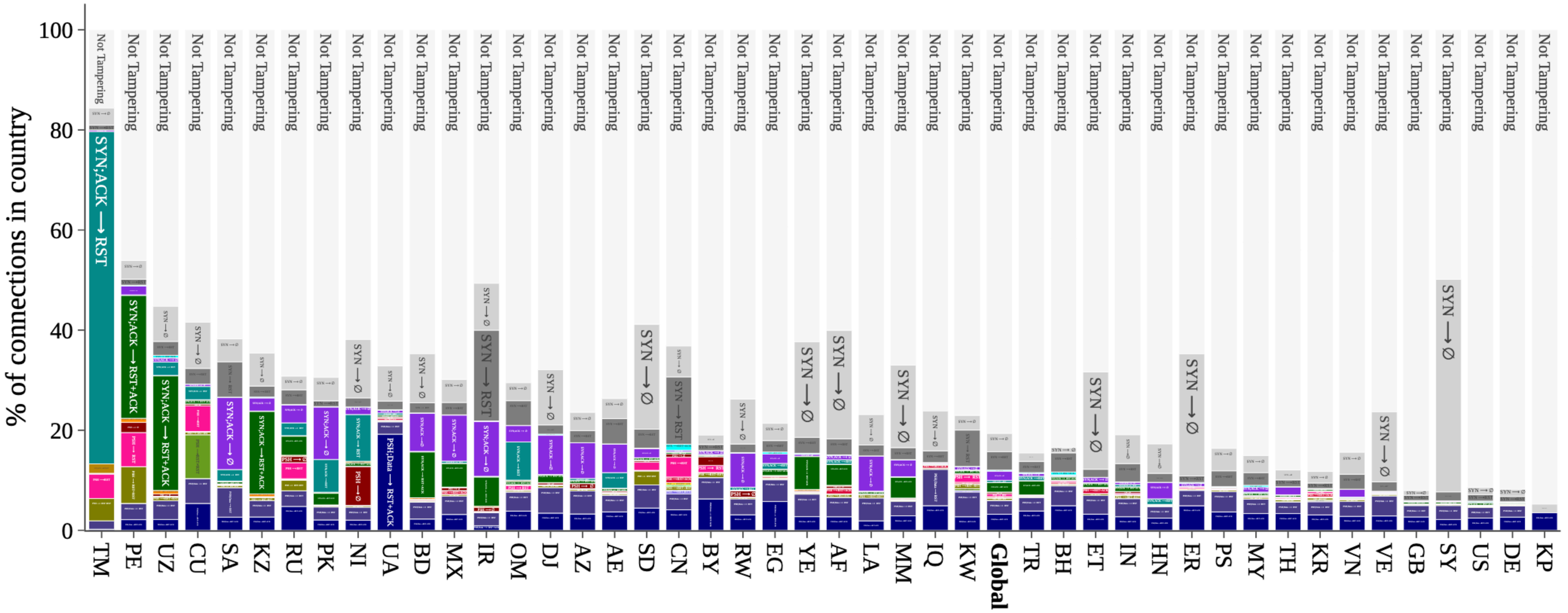
No decryption, and
results in aggregate

Tampering fingerprints

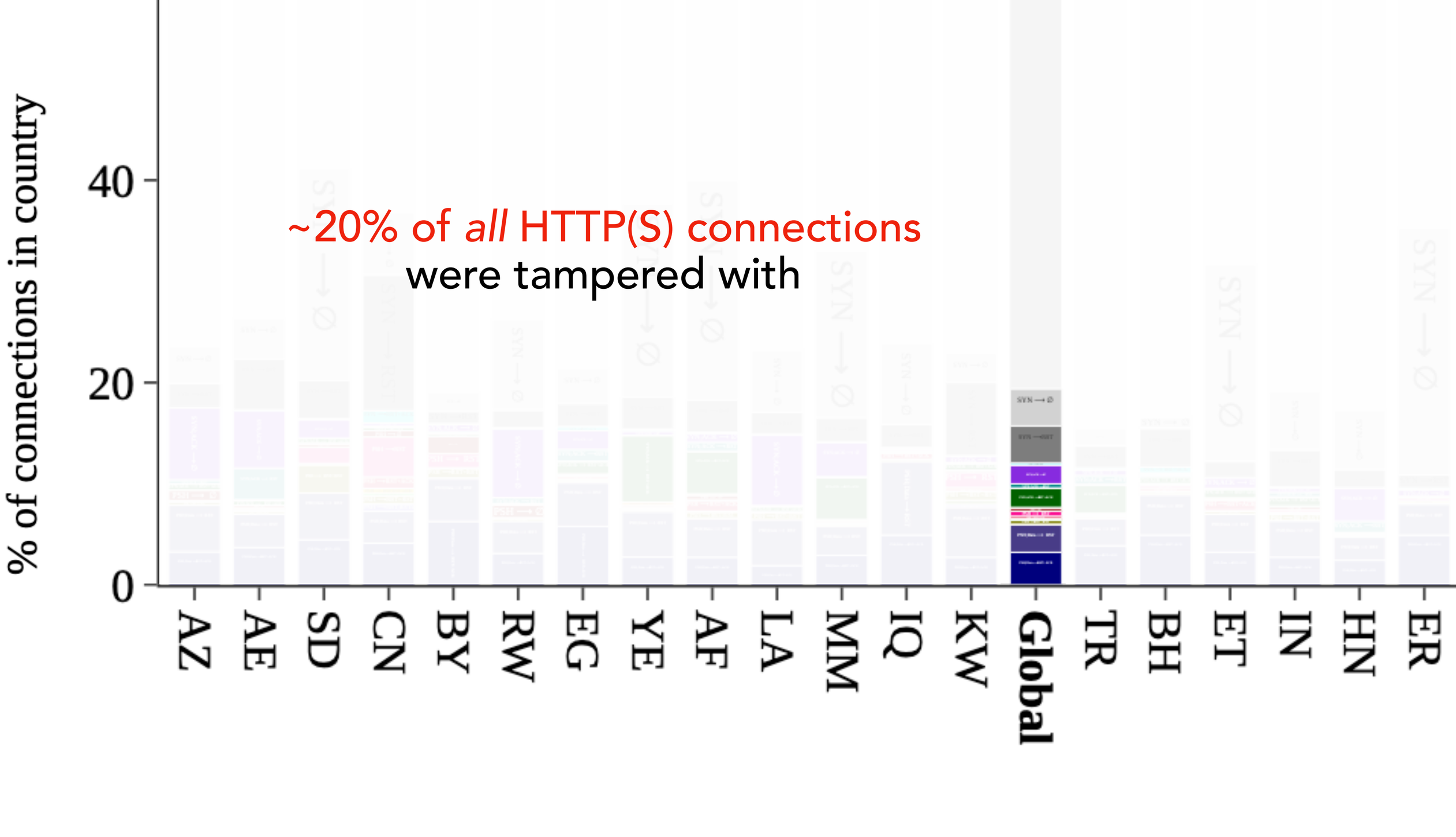
Type	Signature
Post-SYN	⟨SYN → ∅⟩
	⟨SYN → RST⟩
	⟨SYN → RST+ACK⟩
	⟨SYN → RST; RST+ACK⟩
Post-ACK	⟨SYN; ACK → ∅⟩
	⟨SYN; ACK → RST⟩
	⟨SYN; ACK → RST; RST⟩
	⟨SYN; ACK → RST+ACK⟩
	⟨SYN; ACK → RST+ACK; RST+ACK⟩
Post-PSH	⟨PSH+ACK → ∅⟩
	⟨PSH+ACK → RST⟩
	⟨PSH+ACK → RST+ACK⟩
	⟨PSH+ACK → RST; RST+ACK⟩
	⟨PSH+ACK → RST+ACK; RST+ACK⟩
	⟨PSH+ACK → RST = RST⟩
	⟨PSH+ACK → RST ≠ RST⟩
	⟨PSH+ACK → RST; RST_0⟩
Post-Multiple Data Packets	⟨PSH+ACK; Data → RST⟩
	⟨PSH+ACK; Data → RST+ACK⟩

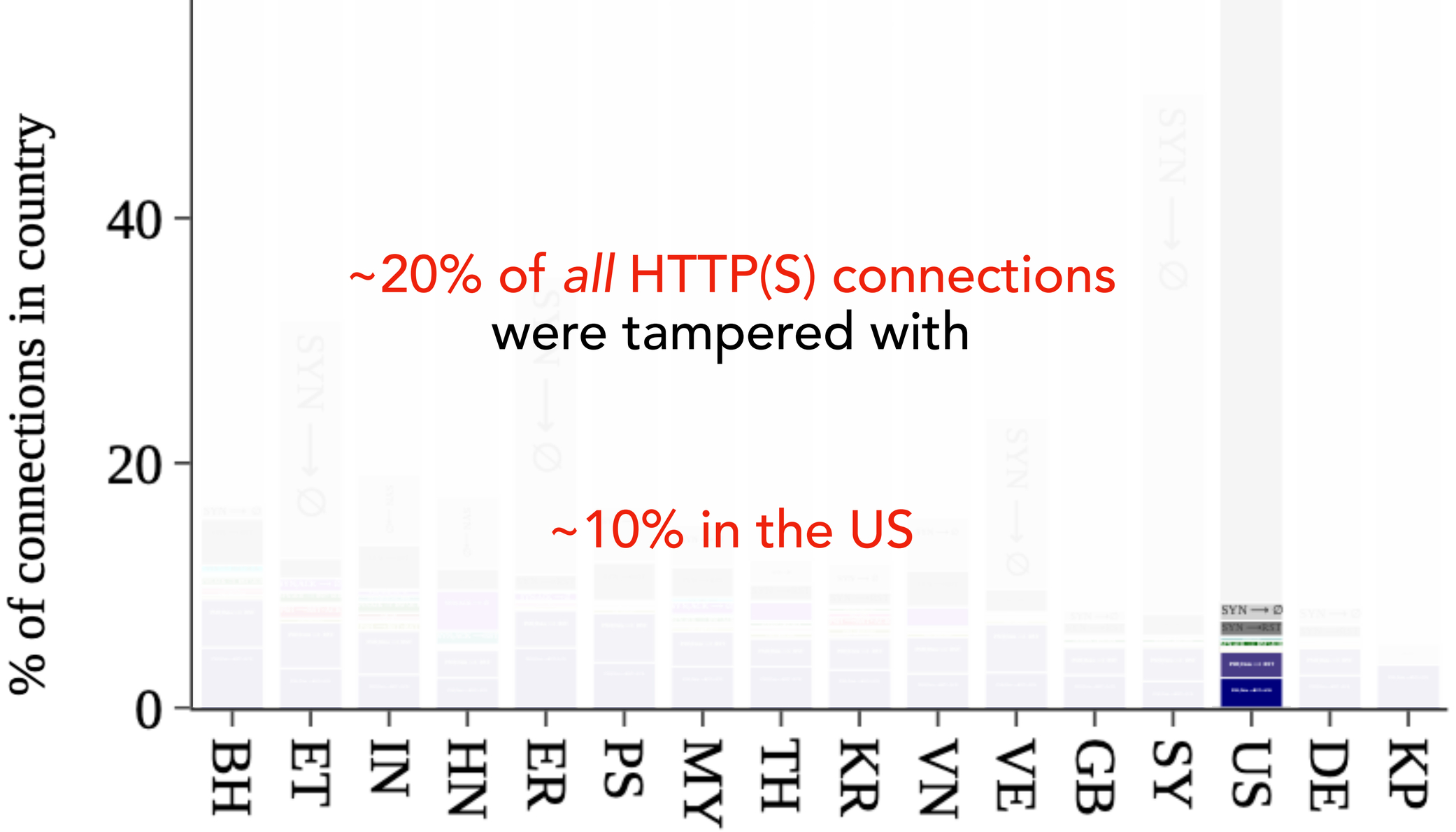


Users in different regions experience tampering in different ways



There is a wide diversity in how countries experience tampering

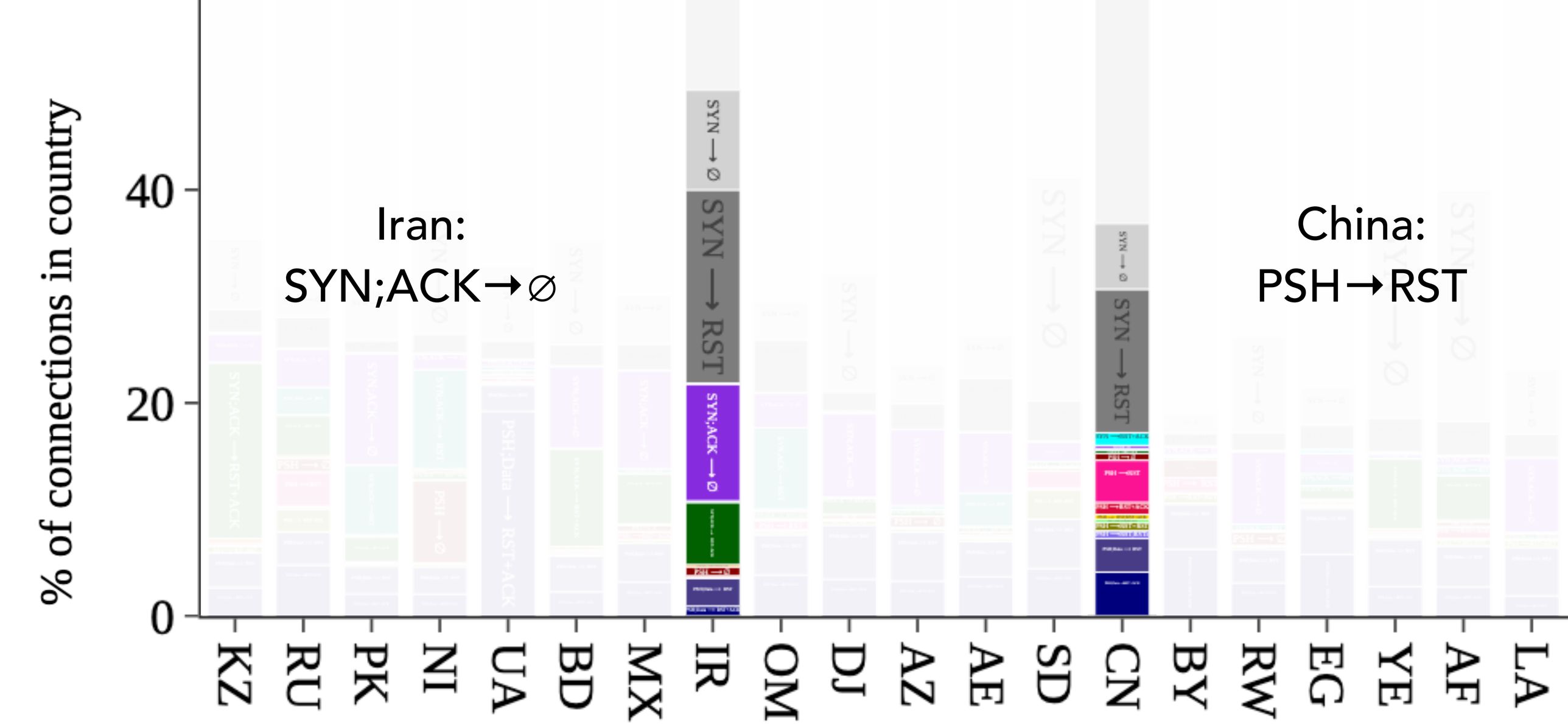

~20% of *all* HTTP(S) connections
were tampered with
% of connections in country
0
20
40
AZ
AE
SD
CN
BY
RW
EG
YE
AF
LA
MM
IQ
KW
Global
TR
BH
ET
IN
HN
ER



~20% of *all* HTTP(S) connections were tampered with

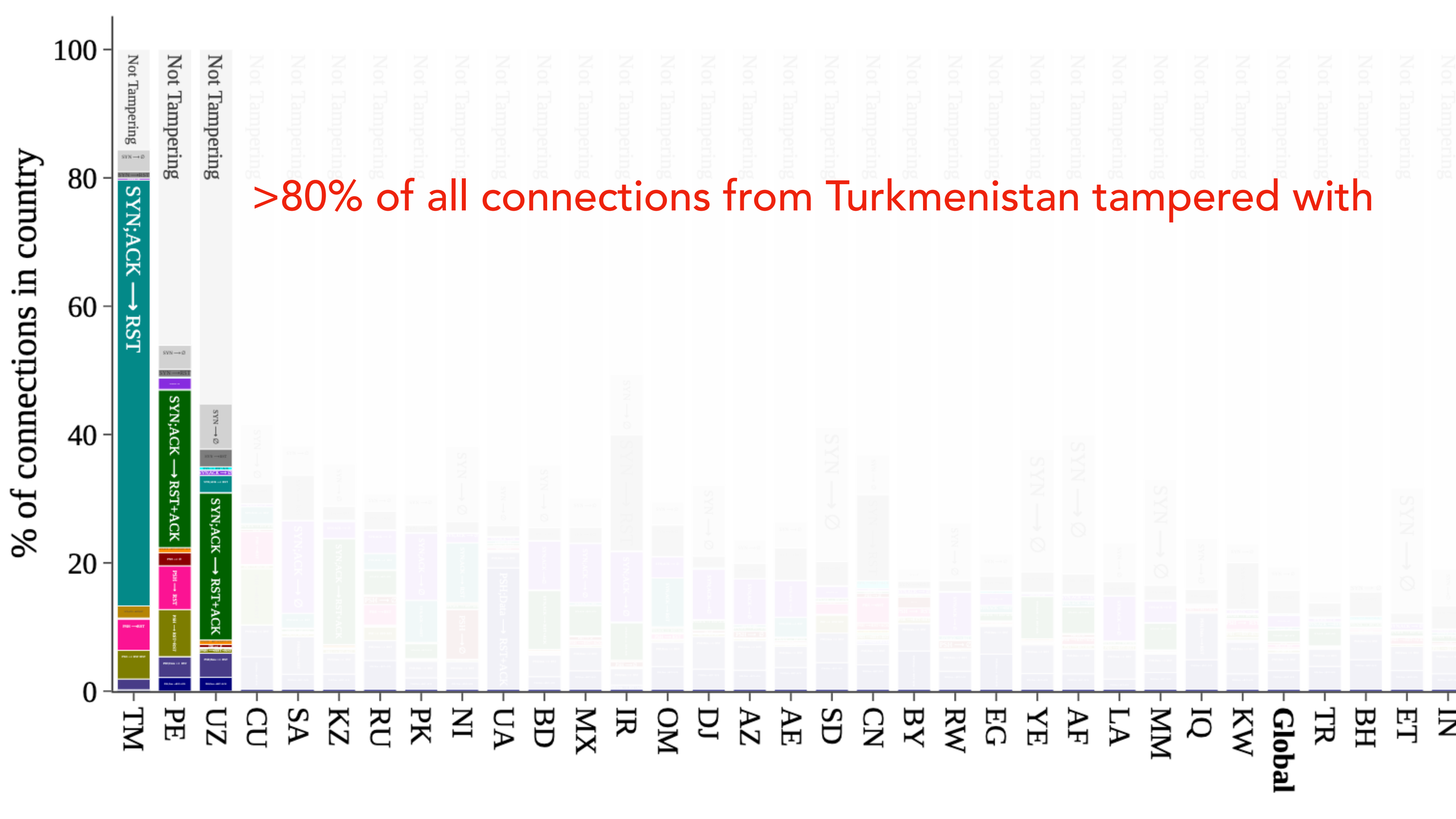
~10% in the US

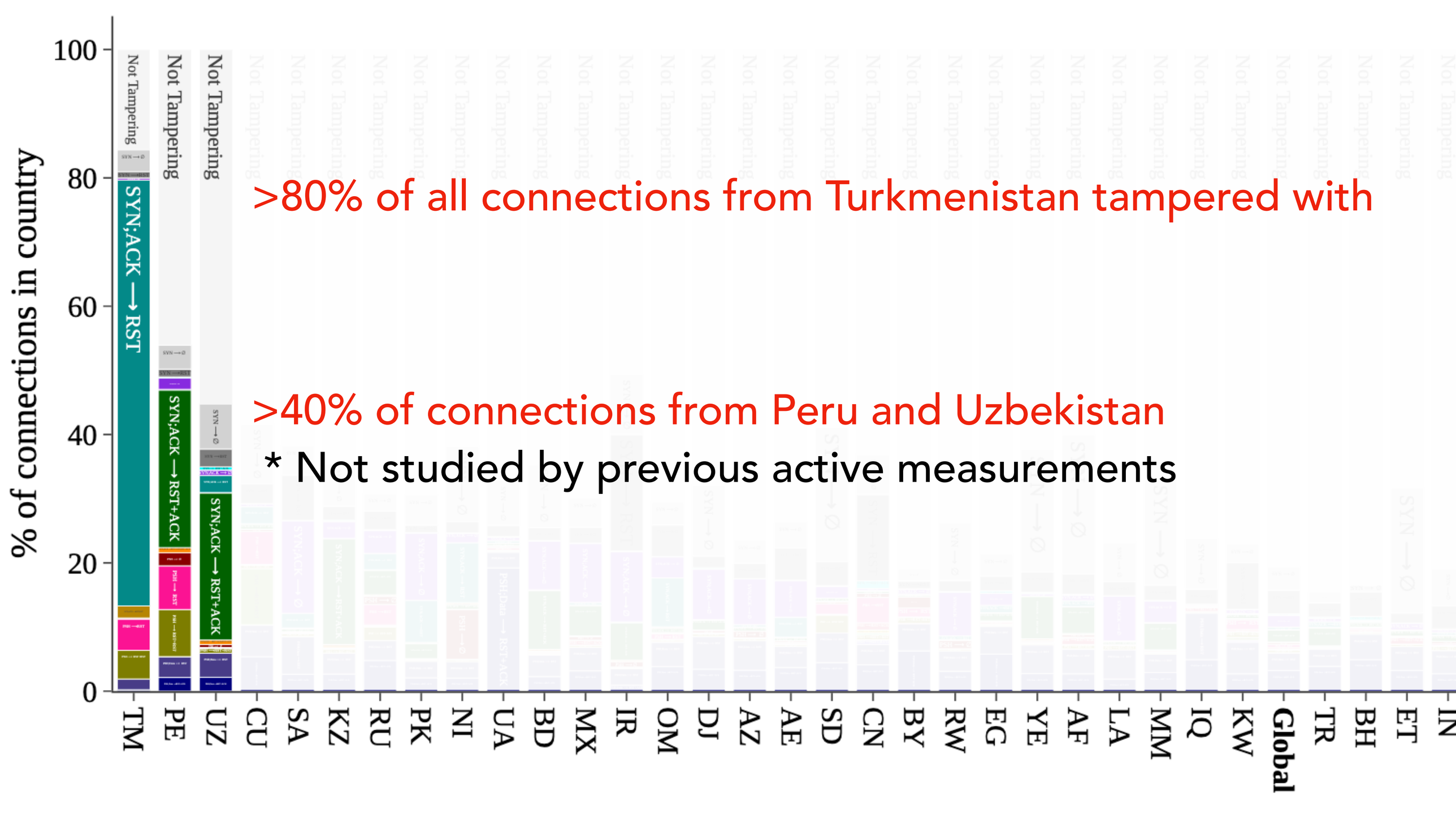
Connection tampering is a *global* phenomenon



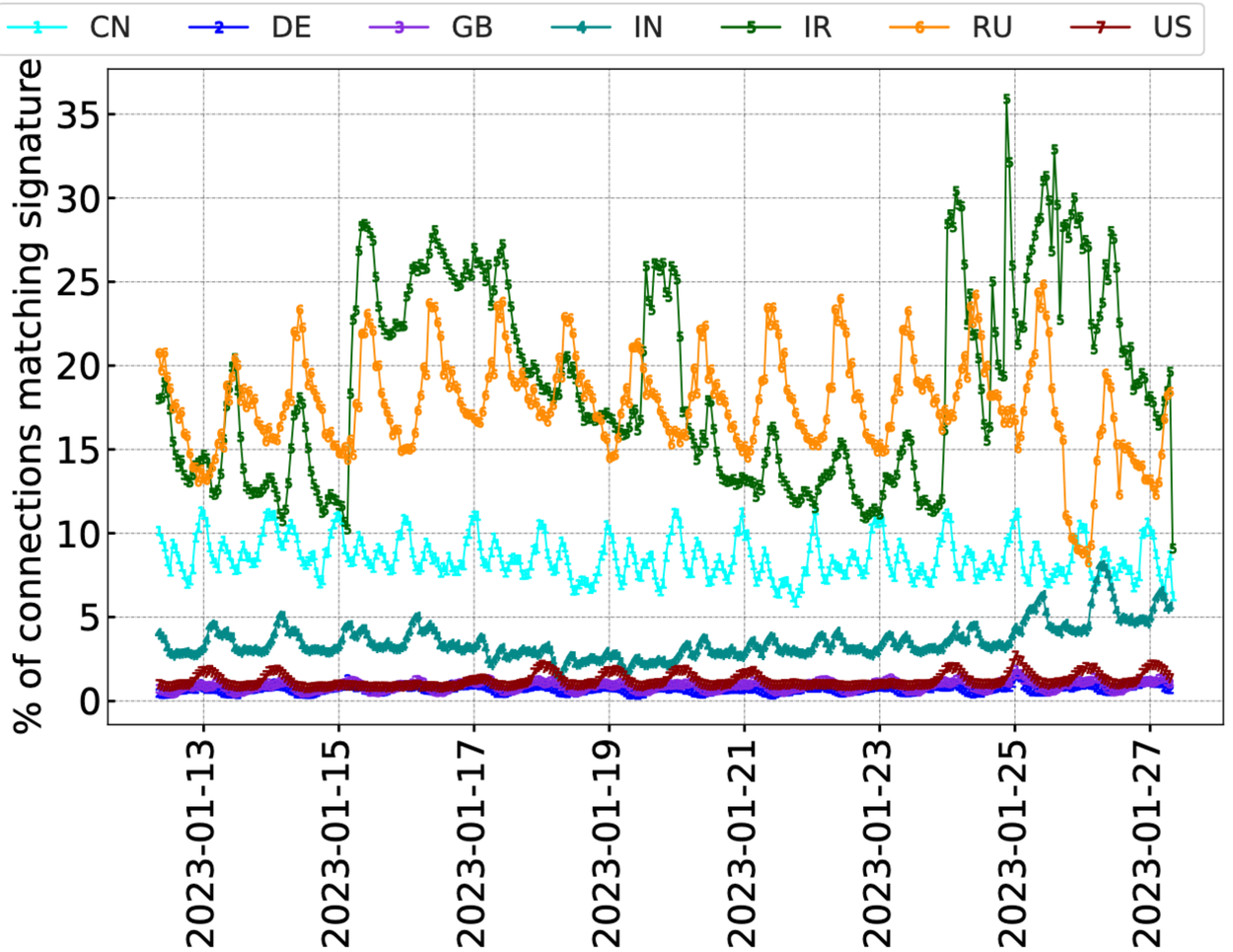
Reflects known censorship behavior

% of connections in country
0
20
40
60
80
100
TM
PE
UZ
CU
SA
KZ
RU
PK
NI
UA
BD
MX
IR
OM
DJ
AZ
AE
SD
CN
BY
RW
EG
YE
AF
LA
MM
IQ
KW
Global
TR
BH
ET
IN
Not Tampering
SYN;ACK → RST
SYN;ACK → RST+ACK
SYN → ∅


% of connections in country
100
80
60
40
20
0
Not Tampering
SYN;ACK → RST
SYN;ACK → RST+ACK
SYN → ∅
>80% of all connections from Turkmenistan tampered with
TM
PE
UZ
CU
SA
KZ
RU
PK
NI
UA
BD
MX
IR
OM
DJ
AZ
AE
SD
CN
BY
RW
EG
YE
AF
LA
MM
IQ
KW
Global
TR
BH
ET
IN


% of connections in country
100
80
60
40
20
0
Not Tampering
SYN;ACK → RST
SYN;ACK → RST+ACK
SYN → ∅
TM
PE
UZ
CU
SA
KZ
RU
PK
NI
UA
BD
MX
IR
OM
DJ
AZ
AE
SD
CN
BY
RW
EG
YE
AF
LA
MM
IQ
KW
Global
TR
BH
ET
IN
>80% of all connections from Turkmenistan tampered with
>40% of connections from Peru and Uzbekistan
* Not studied by previous active measurements

When do users experience tampering?



Tampering follows a diurnal pattern in many regions

How comprehensive are our test lists?

List Name	# Entries	Global	CN	IN	IR	KR	MX	PE	RU	US
Tranco_1K	1,000									
Tranco_10K	10,000									
Tranco_100K	100,000									
Tranco_1M	1,000,000									
Majestic_1K	1,000									
Majestic_10K	10,000									
Majestic_100K	100,000									
Majestic_1M	1,000,000									
Greatfire_all	214,406									
Greatfire_30d	22,427									
Citizenlab	23399									
Citizenlab_global	1,388									
Citizenlab_country	Variable									
Union: Citizenlab + Greatfire	233,359									
Union: All lists	1,627,447									
Substring: Citizenlab + Greatfire	-									
Substring: All lists	-									

How comprehensive are our test lists?

List Name	# Entries	Global	CN	IN	IR	KR	MX	PE	RU	US
Tranco_1K	1,000	4.7%	1.7%	8.3%	0.0%	33.3%	9.1%	0.0%	20.8%	17.0%
Tranco_10K	10,000	20.1%	6.8%	39.2%	12.5%	44.4%	45.5%	23.5%	50.0%	69.5%
Tranco_100K	100,000	47.0%	16.7%	76.3%	31.3%	55.6%	81.8%	52.9%	87.5%	86.44%
Tranco_1M	1,000,000	69.8%	45.4%	97.9%	43.8%	72.2%	100.0%	94.1%	95.8%	93.22%
Majestic_1K	1,000	2.5%	1.0%	4.1%	0.0%	11.1%	0.0%	0.0%	4.2%	10.17%
Majestic_10K	10,000	7.5%	2.4%	9.3%	0.0%	16.7%	9.1%	0.0%	20.8%	28.8%
Majestic_100K	100,000	15.3%	5.1%	20.6%	0.0%	33.3%	18.2%	11.8%	33.3%	45.8%
Majestic_1M	1,000,000	31.2%	13.0%	66.0%	12.5%	33.3%	36.4%	23.5%	54.2%	62.7%
Greatfire_all	214,406	22.7%	10.9%	43.3%	6.3%	44.4%	27.3%	5.9%	50.0%	54.2%
Greatfire_30d	22,427	10.1%	5.5%	22.7%	0.0%	27.8%	9.1%	0.0%	20.8%	11.9%
Citizenlab	23399	7.5%	3.1%	12.4%	0.0%	22.2%	18.2%	0.0%	25.0%	11.9%
Citizenlab_global	1,388	3.6%	1.7%	5.2%	0.0%	11.1%	9.1%	0.0%	12.5%	10.2%
Citizenlab_country	Variable	-	0.7%	2.1%	0.0%	0.0%	0.0%	0.0%	8.3%	0.0%
Union: Citizenlab + Greatfire	233,359	23.1%	10.9%	43.3%	6.3%	44.4%	27.3%	5.9%	50.0%	54.2%
Union: All lists	1,627,447	71.5%	48.1%	99.0%	43.8%	72.2%	100.0%	94.12%	95.8%	93.2%
Substring: Citizenlab + Greatfire	-	53.6%	36.9%	62.9%	56.3%	61.1%	54.5%	35.3%	58.3%	71.2%
Substring: All lists	-	87.7%	77.5%	100.0%	93.8%	83.3%	100.0%	100.0%	95.8%	96.6%

How comprehensive are our test lists?

List Name	# Entries	Global	CN
Tranco_1K	1,000	4.7%	1.7%
Tranco_10K	10,000	20.1%	6.8%
Tranco_100K	100,000	47.0%	16.7%
Tranco_1M	1,000,000	69.8%	45.4%
Majestic_1K	1,000	2.5%	1.0%
Majestic_10K	10,000	7.5%	2.4%
Majestic_100K	100,000	15.3%	5.1%
Majestic_1M	1,000,000	31.2%	13.0%
Greatfire_all	214,406	22.7%	10.9%
Greatfire_30d	22,427	10.1%	5.5%
Citizenlab	23399	7.5%	3.1%
Citizenlab_global	1,388	3.6%	1.7%
Citizenlab_country	Variable	-	0.7%
Union: Citizenlab + Greatfire	233,359	23.1%	10.9%
Union: All lists	1,627,447	71.5%	48.1%
Substring: Citizenlab + Greatfire	-	53.6%	36.9%
Substring: All lists	-	87.7%	77.5%

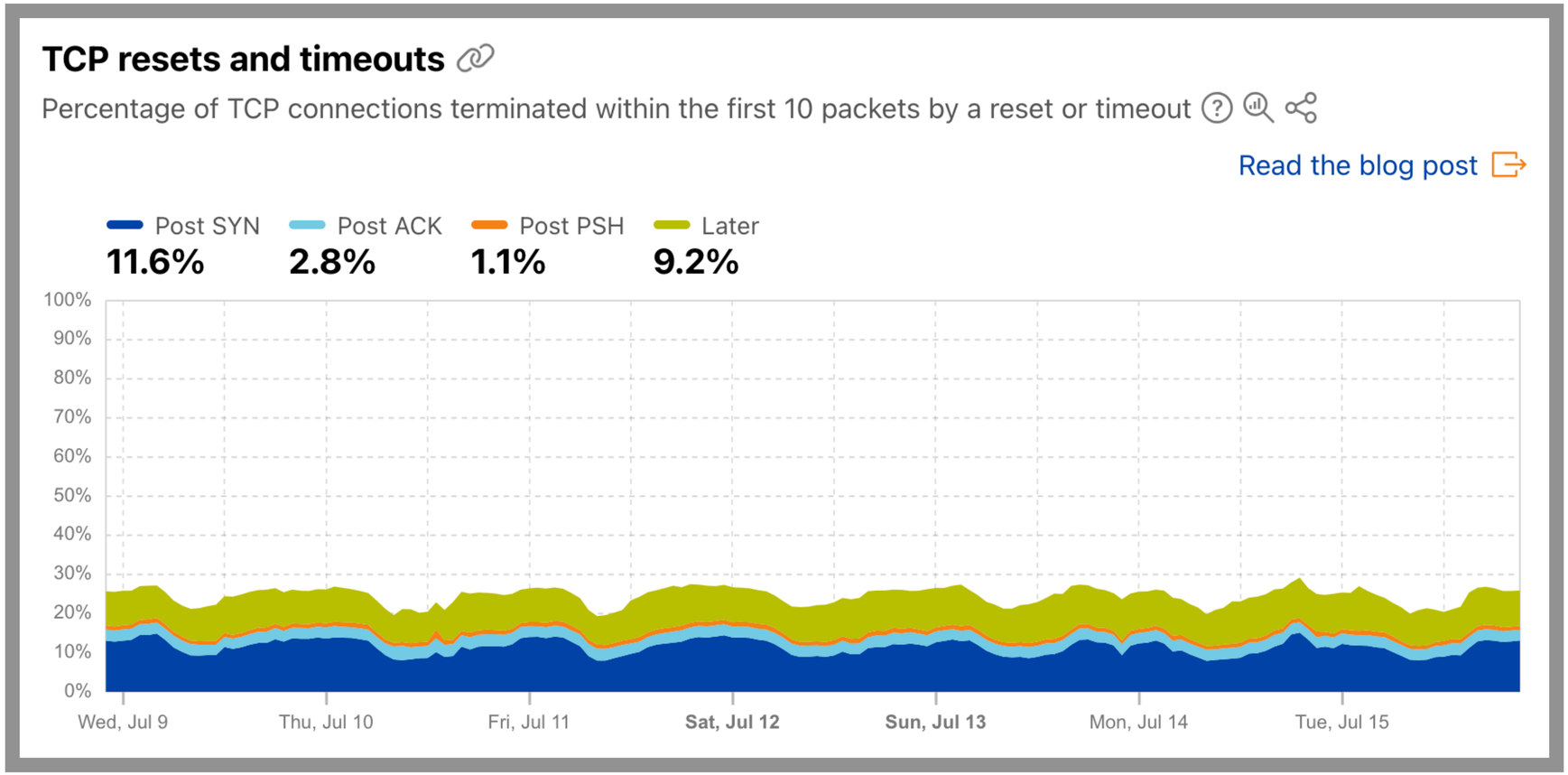
All lists together cover 48.1%

of China's tampered domains

How comprehensive are our test lists?

List Name	# Entries	Global	CN	IN	IR	KR	MX	PE	RU	US
Tranco_1K	1,000	4.7%	1.7%	8.3%	0.0%	33.3%	9.1%	0.0%	20.8%	17.0%
Tranco_10K	10,000	20.1%	6.8%	39.2%	12.5%	44.4%	45.5%	23.5%	50.0%	69.5%
Tranco_100K	100,000	47.0%	16.7%	76.3%	31.3%	55.6%	81.8%	52.9%	87.5%	86.44%
Tranco_1M	1,000,000	69.8%	45.4%	97.9%	43.8%	72.2%	100.0%	94.1%	95.8%	93.22%
Majestic_1K	1,000	2.5%	1.0%	4.1%	0.0%	11.1%	0.0%	0.0%	4.2%	10.17%
Majestic_10K	10,000	7.5%	2.4%	9.3%	0.0%	16.7%	9.1%	0.0%	20.8%	28.8%
Majestic_100K	100,000	15.3%	5.1%	20.6%	0.0%	33.3%	18.2%	11.8%	33.3%	45.8%
Majestic_1M	1,000,000	31.2%	13.0%	66.0%	12.5%	33.3%	36.4%	23.5%	54.2%	62.7%
Greatfire_all	214,406	22.7%	10.9%	43.3%	6.3%	44.4%	27.3%	5.9%	50.0%	54.2%
Greatfire_30d	22,427	10.1%	5.5%	22.7%	0.0%	27.8%	9.1%	0.0%	20.8%	11.9%
Citizenlab	23399	7.5%	3.1%	12.4%	0.0%	22.2%	18.2%	0.0%	25.0%	11.9%
Citizenlab_global	1,388	3.6%	1.7%	5.2%	0.0%	11.1%	9.1%	0.0%	12.5%	10.2%
Citizenlab_country	Variable	-	0.7%	2.1%	0.0%	0.0%	0.0%	0.0%	8.3%	0.0%
Union: Citizenlab + Greatfire	233,359	23.1%	10.9%	43.3%	6.3%	44.4%	27.3%	5.9%	50.0%	54.2%
Union: All lists	1,627,447	71.5%	48.1%	99.0%	43.8%	72.2%	100.0%	94.12%	95.8%	93.2%
Substring: Citizenlab + Greatfire	-	53.6%	36.9%	62.9%	56.3%	61.1%	54.5%	35.3%	58.3%	71.2%
Substring: All lists	-	87.7%	77.5%	100.0%	93.8%	83.3%	100.0%	100.0%	95.8%	96.6%

Cloudflare Radar



https://radar.cloudflare.com/security/network-layer

What can passive measurement teach us?

Active techniques

Permit controlled experiments

Expose censors' policies

Help populate test lists

Expose users' experiences

Passive techniques

What can passive measurement teach us?

Active techniques

Permit controlled experiments

Expose censors' policies

Complementary

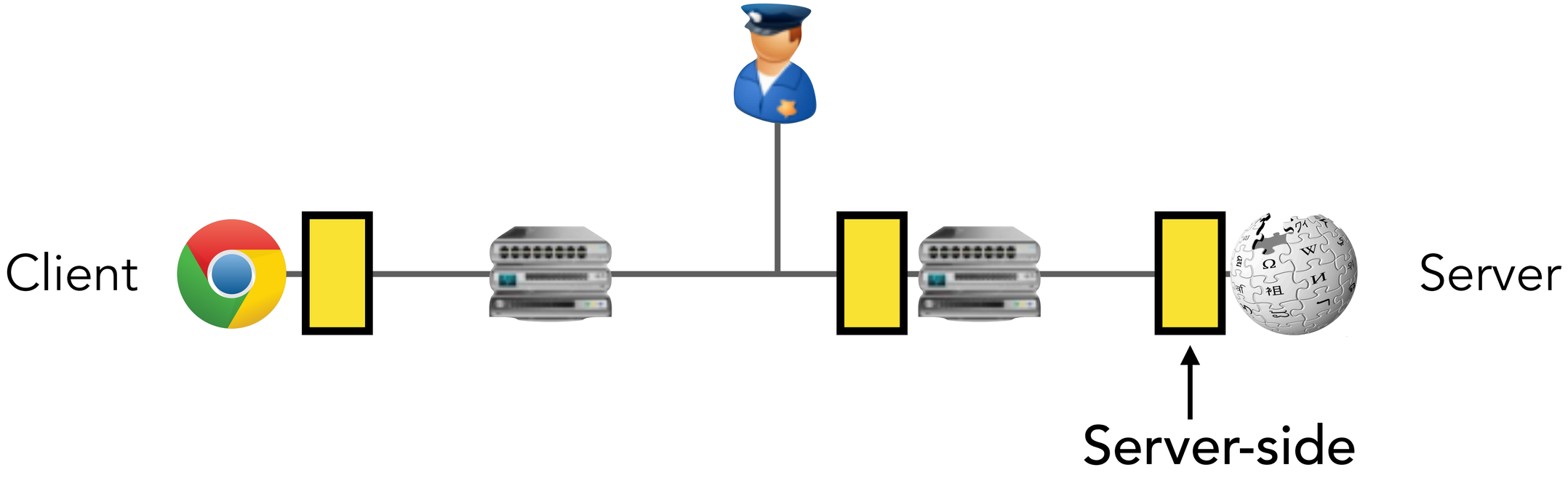
Help populate test lists

Expose users' experiences

Passive techniques

Join us in passive measurements!

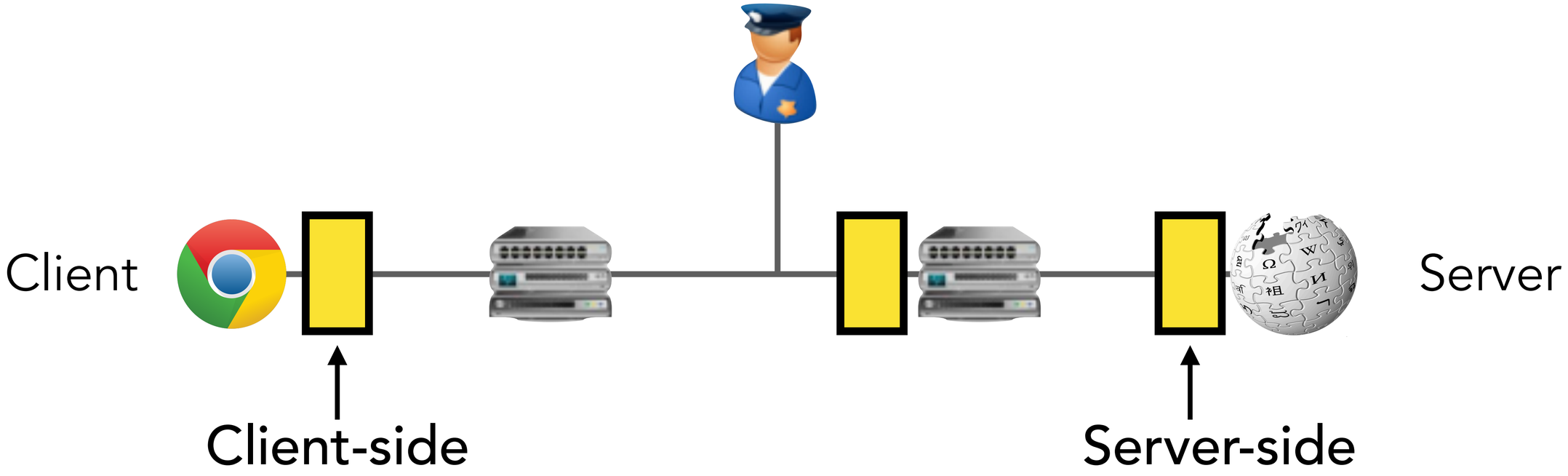
We are building passive detection tools for multiple deployment points



https://censorship.ai

Join us in passive measurements!

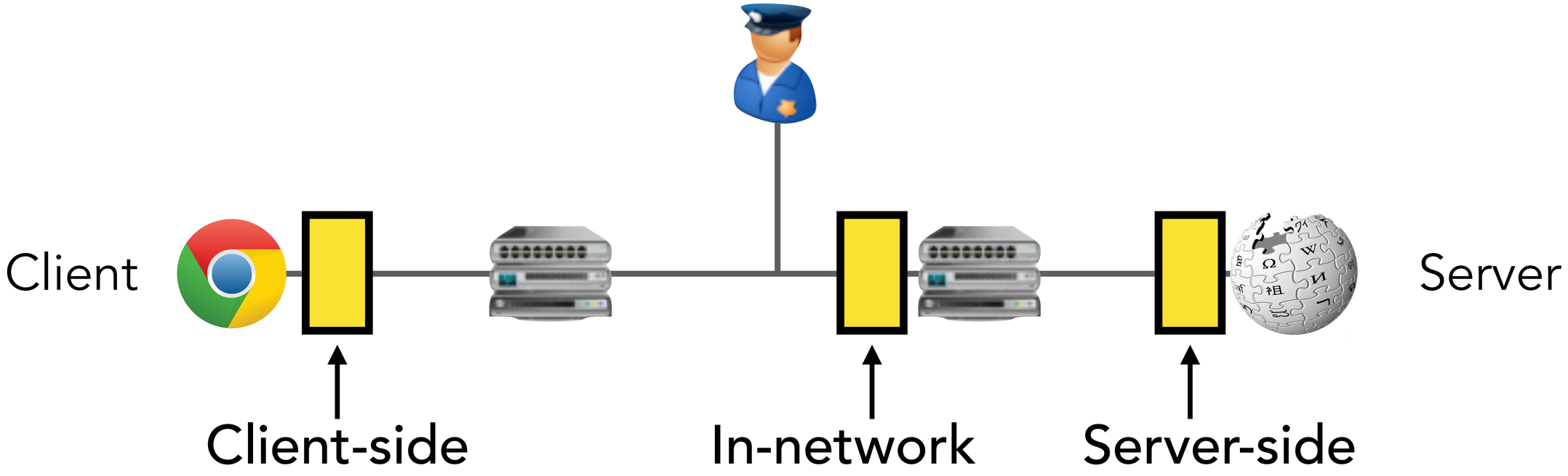
We are building passive detection tools for multiple deployment points



https://censorship.ai

Join us in passive measurements!

We are building passive detection tools for multiple deployment points



https://censorship.ai