

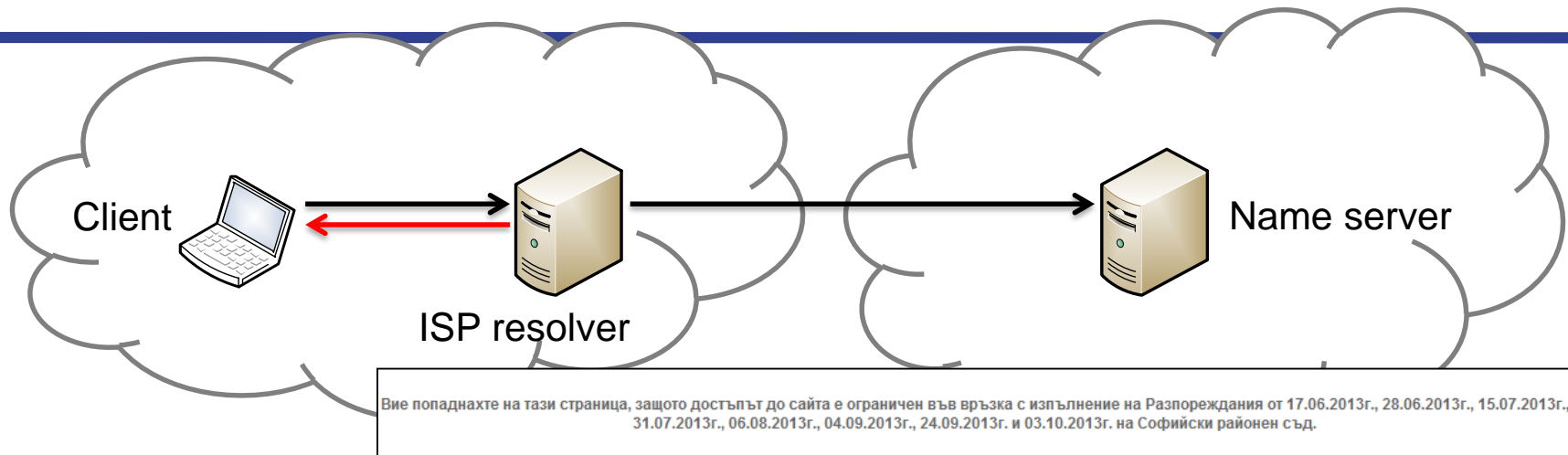
DNS Censorship

Matthäus Wander

<matthaeus.wander@uni-due.de>

Internet-Technology & Web Engineering

DNS Filtering on ISP Resolver



internet positif  

 Click me NOW

*Situs terlarang tidak dapat diakses melalui jaringan ini karena terindikasi mengandung salah satu unsur Pornografi, Judi, Phising, SARA atau PROXY.
Jika anda merasa situs ini tidak termasuk ke dalam kategori diatas, silahkan menghubungi aduankonten@lat.depkominfo.go.id.*



The website which you are trying to access is restricted by the Media Development Authority (MDA).

Find out more information on [MDA regulations](#).

Best viewed with IE 7.0 © Copyright StarHub 2011. All rights reserved

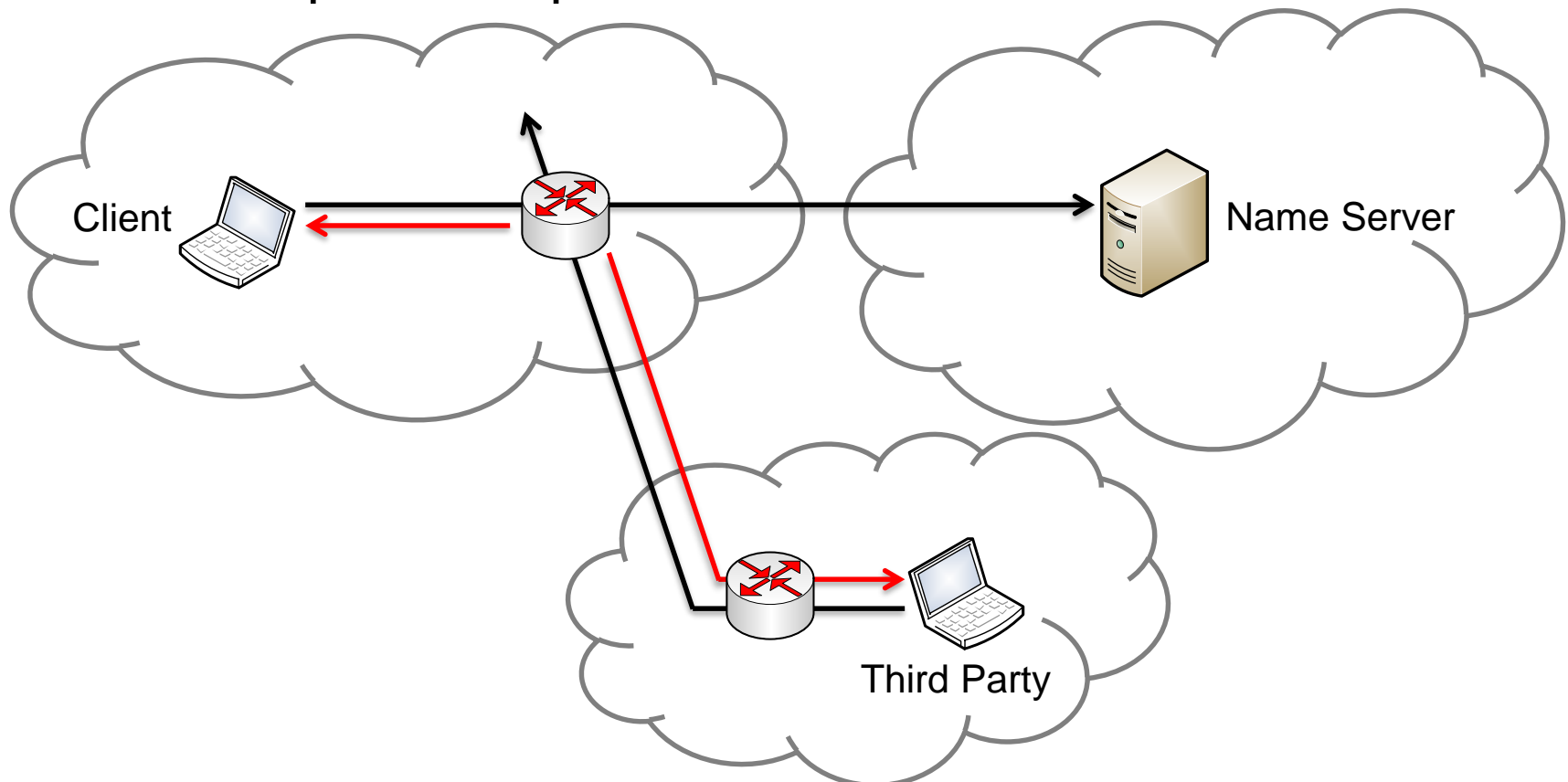
Case Study: Twitter/Youtube filter in Turkey

- Turkish ISPs ordered to filter Twitter/Youtube
- DNS filtering on ISP resolver
 - Easily bypassed
 - Public open resolvers
- Block access to 8.8.8.8
 - Later, ISPs hijack 8.8.8.8
- IP filtering of websites
 - High maintenance cost

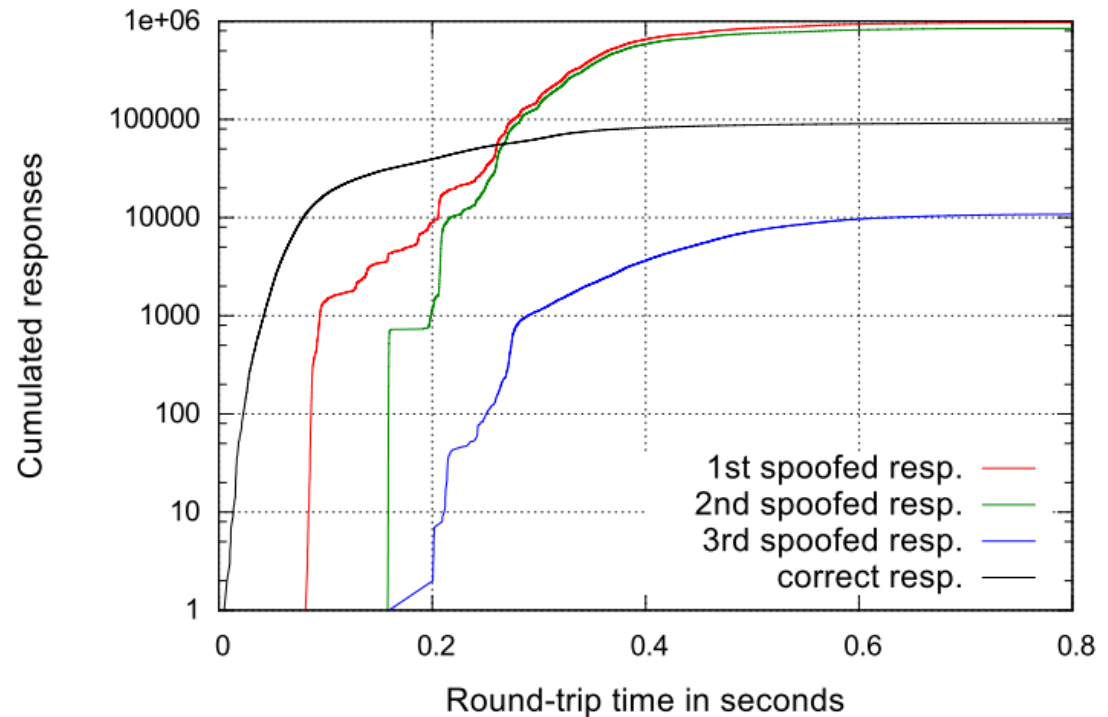
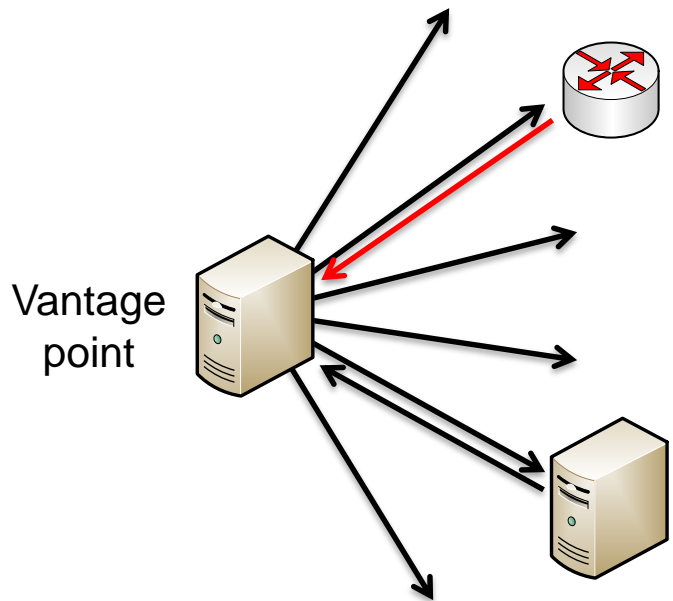


DNS Filtering by Packet Injection

- Deep Packet Inspection of all DNS queries
 - Router spoofs responses for unwanted domain names

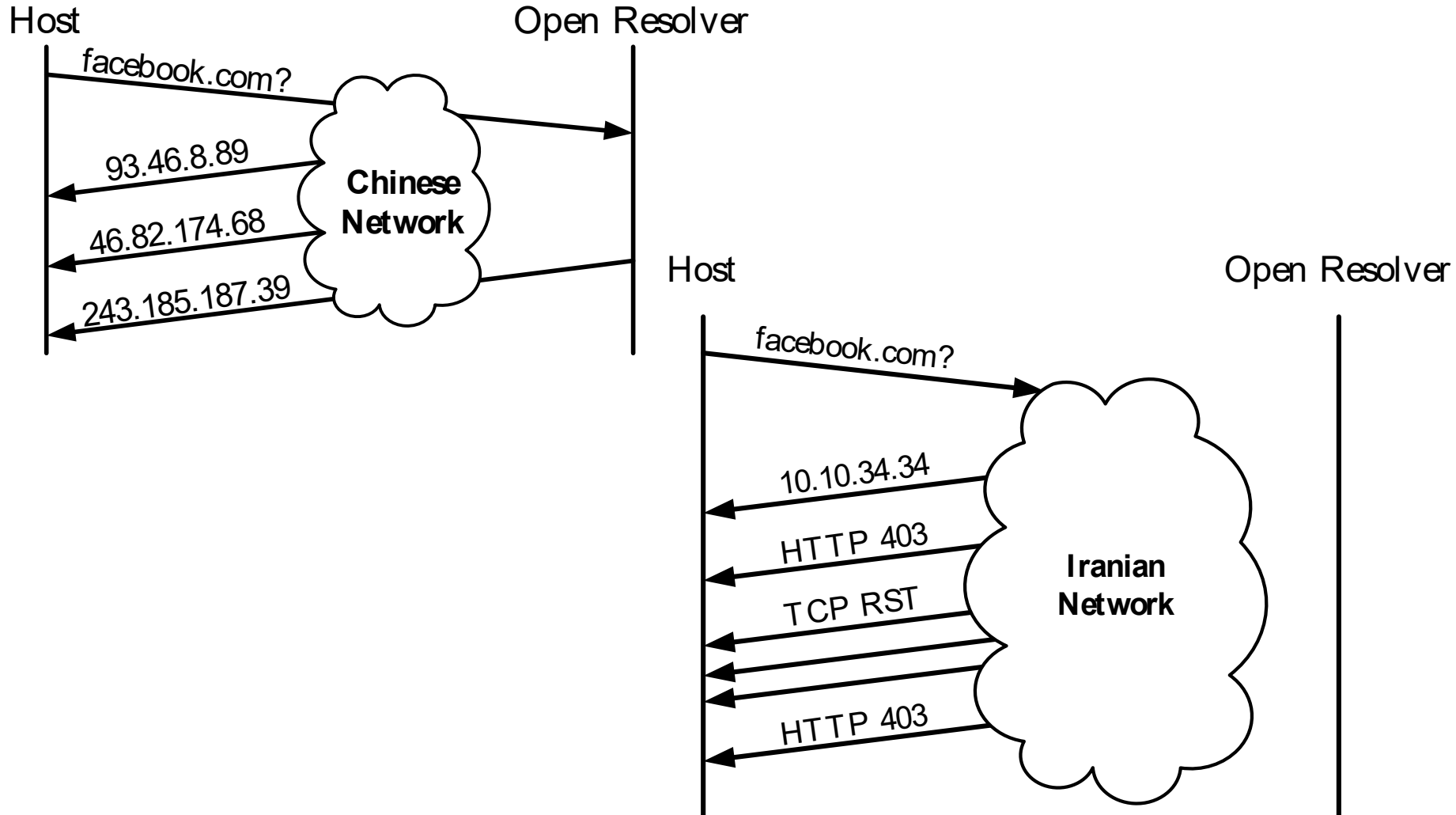


Probing for DNS Injectors

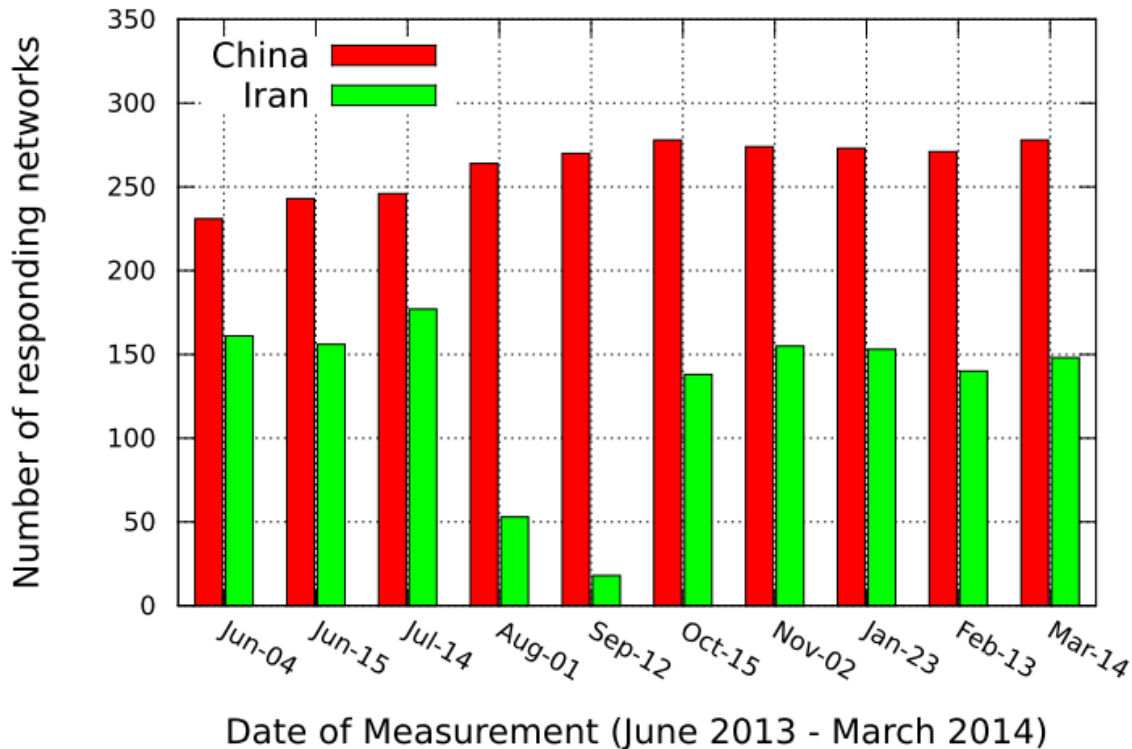


- 100k correct responses from open resolvers
- 1.9M spoofed responses from 1.1M addresses

DNS Injection in China and Iran



Injected „facebook.com“ Responses over Time



theguardian

News Sport Comment Culture Business Money Life & style

News World news Iran

Iran's president signals softer line on web censorship and Islamic dress code

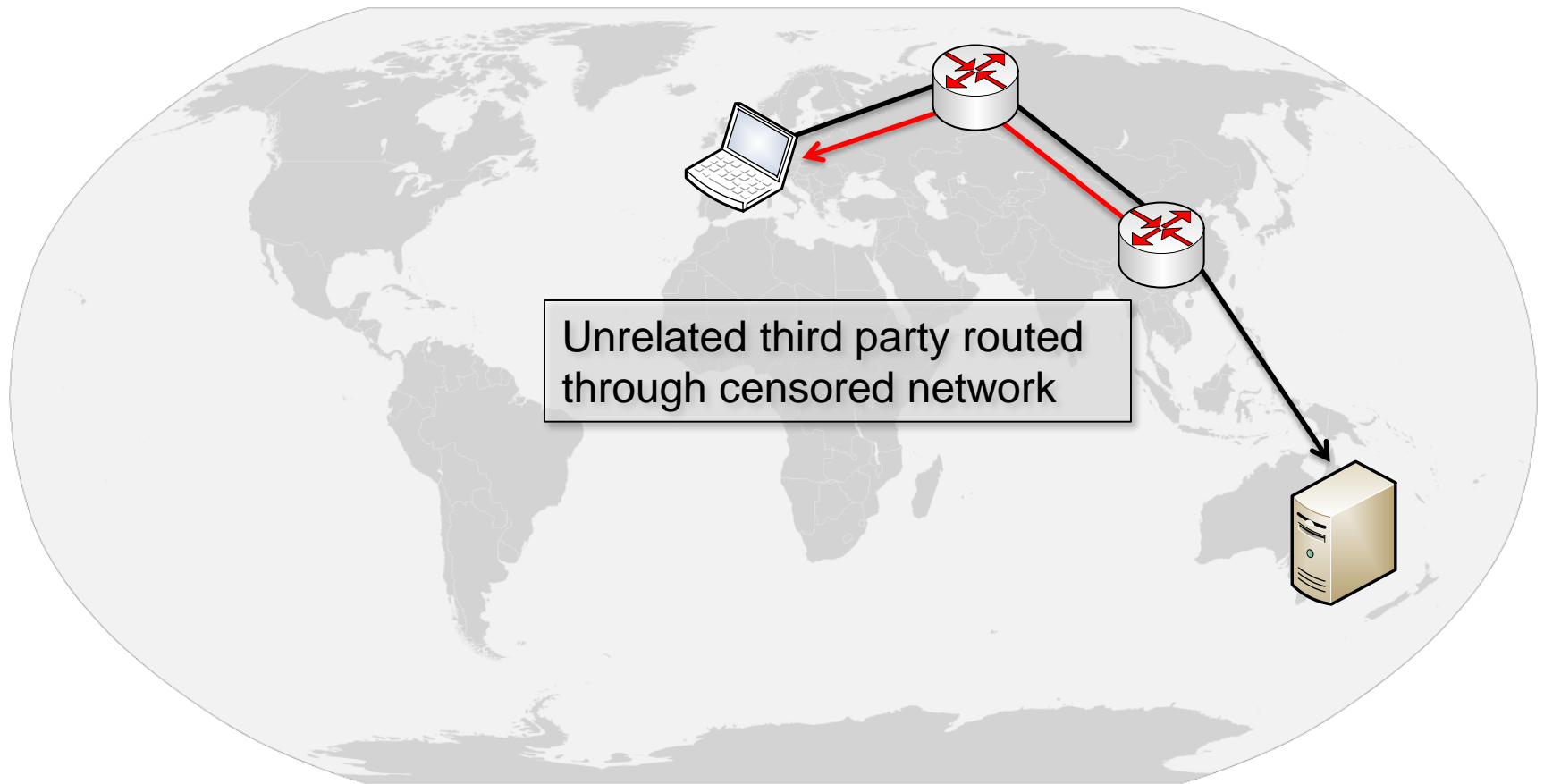
Newly elected Hassan Rouhani, an opponent of segregation by gender, says Iranians' freedoms and rights have been ignored

Saeed Kamali Dehghan

theguardian.com, Tuesday 2 July 2013 18.28 BST



What if... ? Impact on Third Parties



Measurement with RIPE Atlas for „de“

- Measure impact with RIPE Atlas network
 - Few thousand hardware probes worldwide



- Send DNS query to „de“ top-level domain server
 - Check if response is spoofed

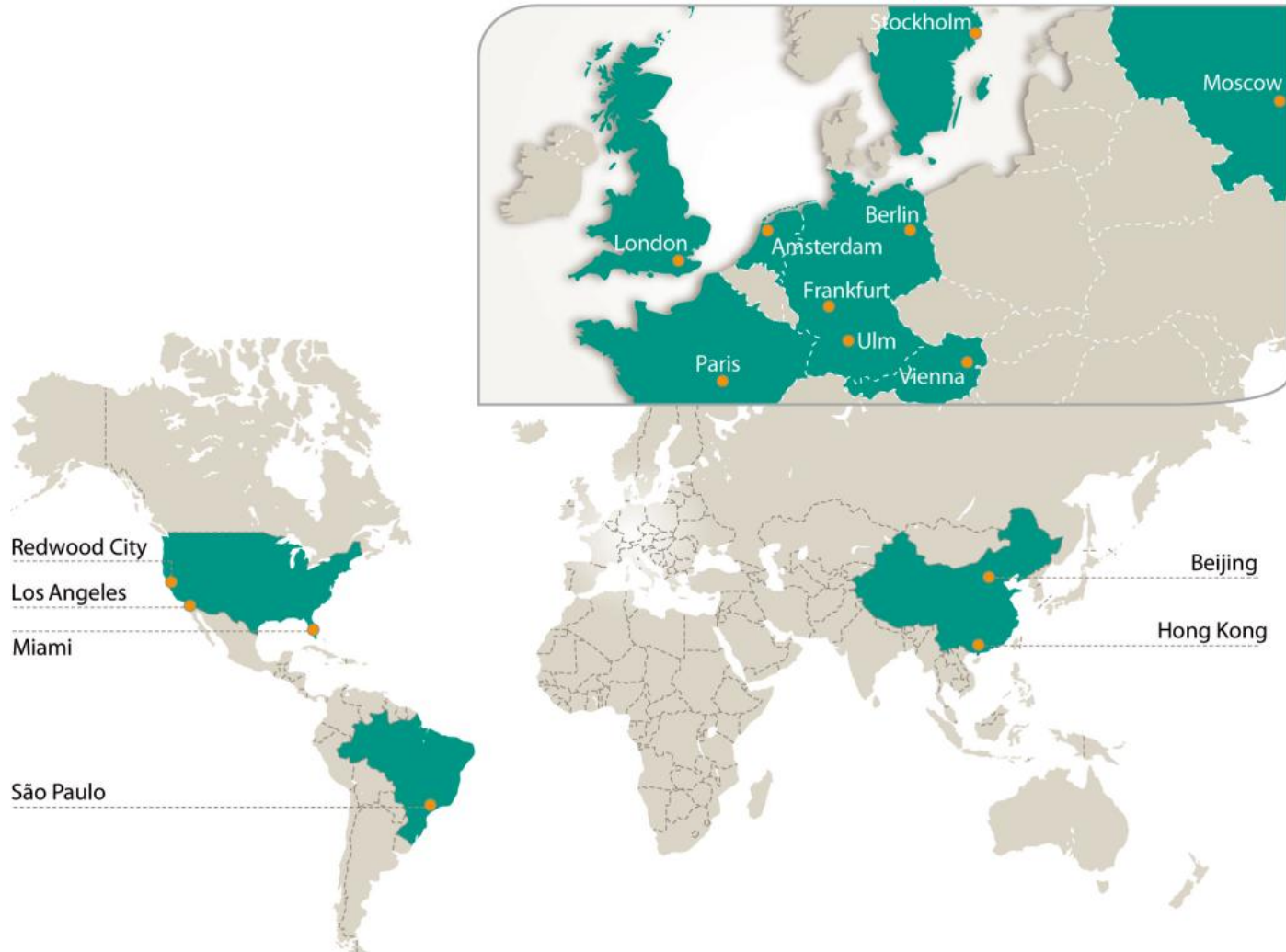
Measurement with RIPE Atlas for „de“



Sep
2012

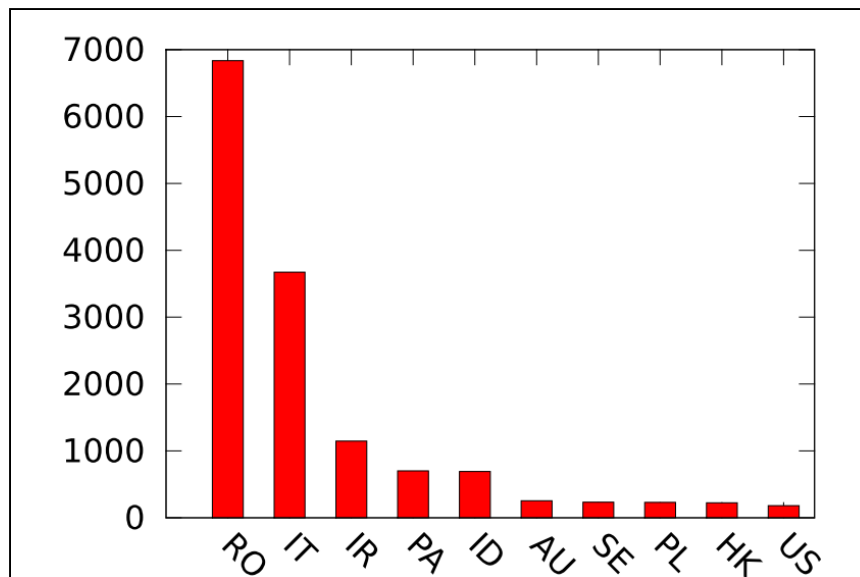
- **Green**: all good
- **Red**: affected
- **Yellow**: routed to China but not affected

Anycast Locations of „de“



Measurement with Open Resolvers for all TLDs

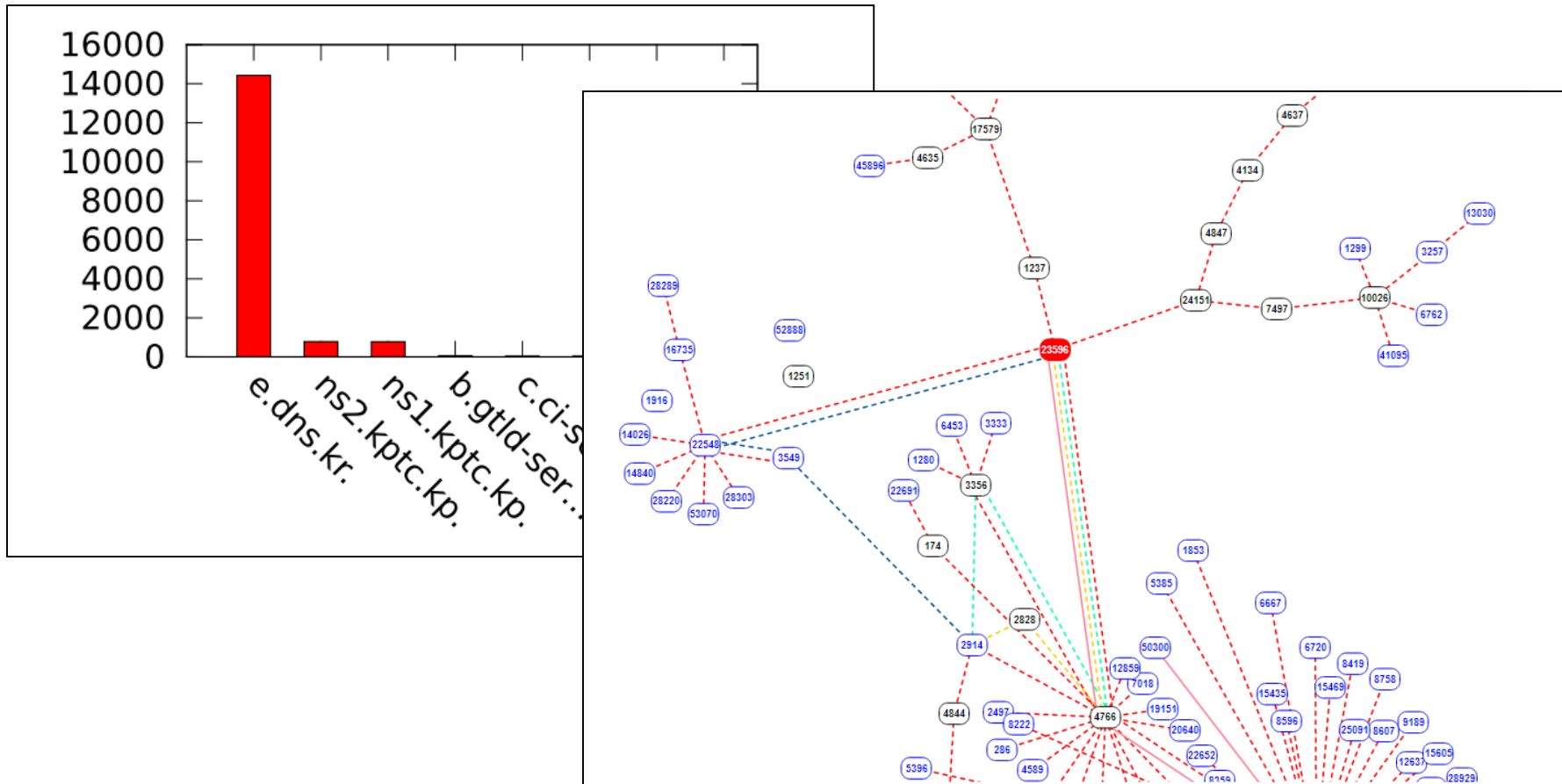
- Test 270k open resolvers with all TLDs
 - 15k in China, all affected from DNS injection
 - 245k outside of China in 188 countries/regions
- 15k affected by Chinese DNS injection (6%)



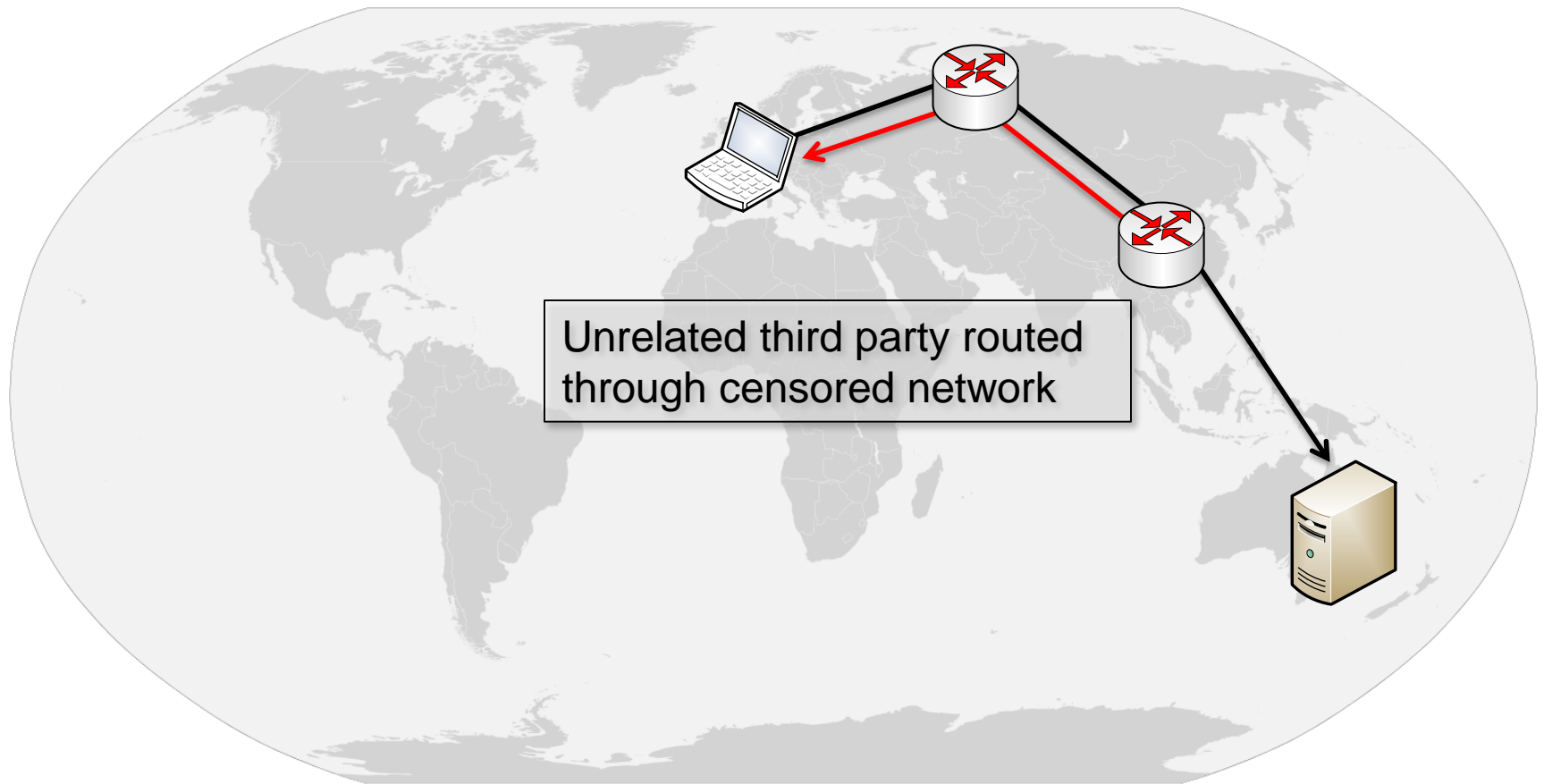
Affected CC	AS#	Organization
6826 RO	9050	Romtelecom
3455 IT	3269	Telecom Italia
701 PA	11556	C&W Panama
263 IR	12880	ITC Iran
231 SE	3301	TeliaSonera
166 IR	48159	TIC Iran

Affected Destination Name Servers

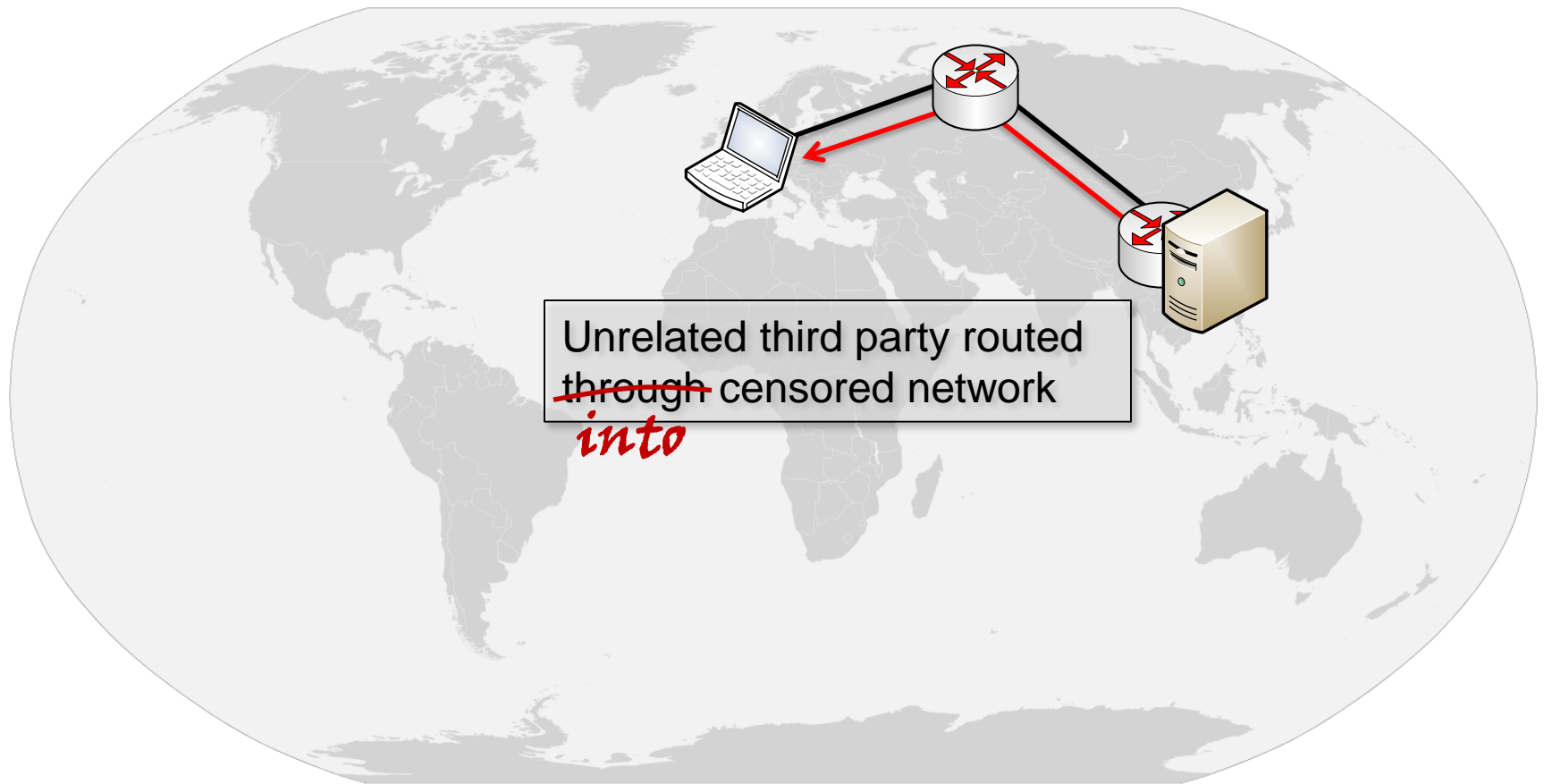
- 14k resolvers affected from e.dns.kr (5.7%)



What if... ? Impact on Third Parties



What if... ? Impact on Third Parties



Conclusion

- DNS filtering on ISP resolver
 - Ineffective
- DNS filtering by packet injection
 - Can affect foreign third-parties
- DNSSEC mitigates effect of DNS injection

