Assessing e-Government DNS Resilience

Raffaele Sommese[1], Mattijs Jonker[1], *Jeroen van der Ham*[1–2], Giovane C. M. Moura[3]

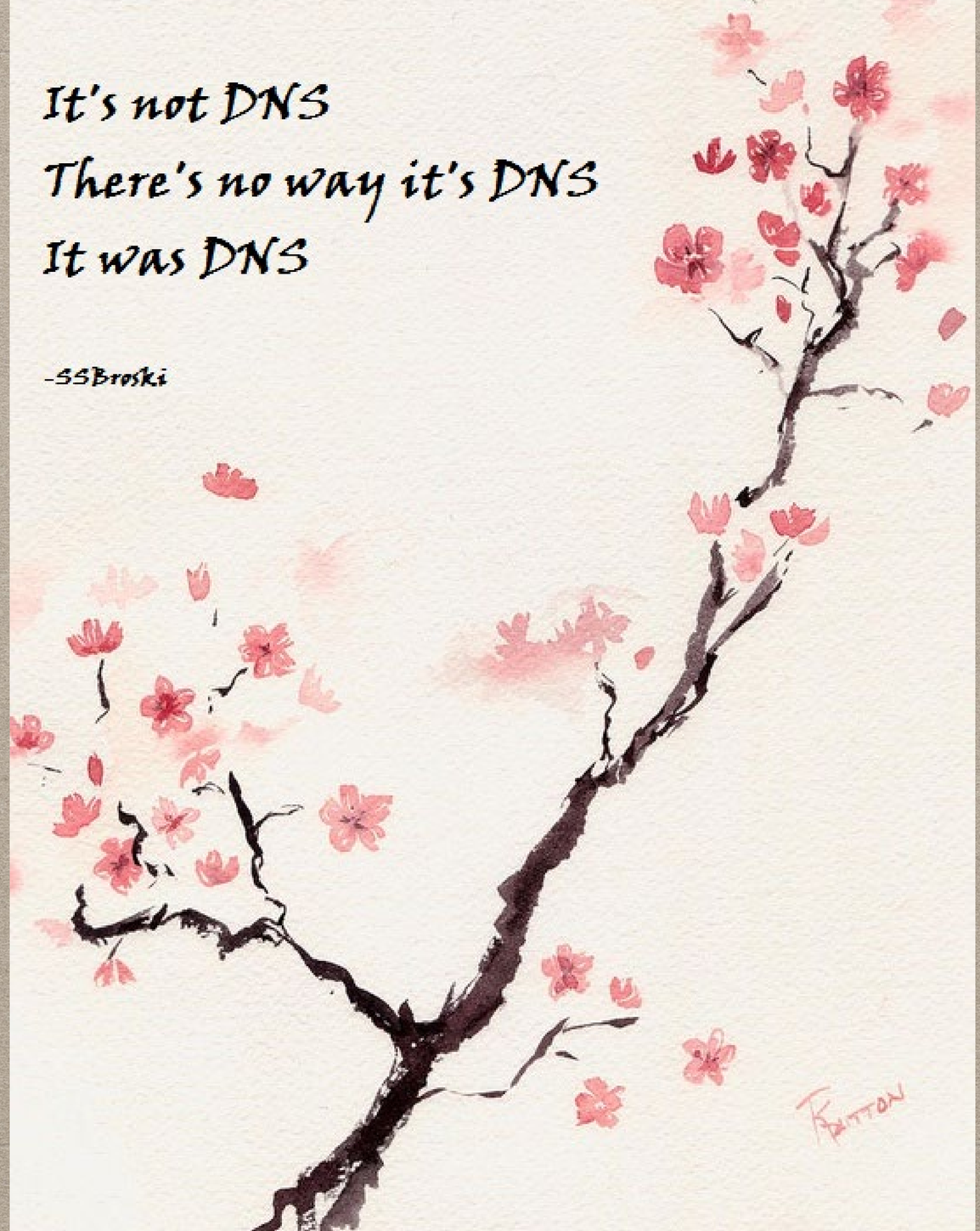
University of Twente[1], NCSC-NL[2],SIDN Labs/TU Delft[3]

It's not DNS

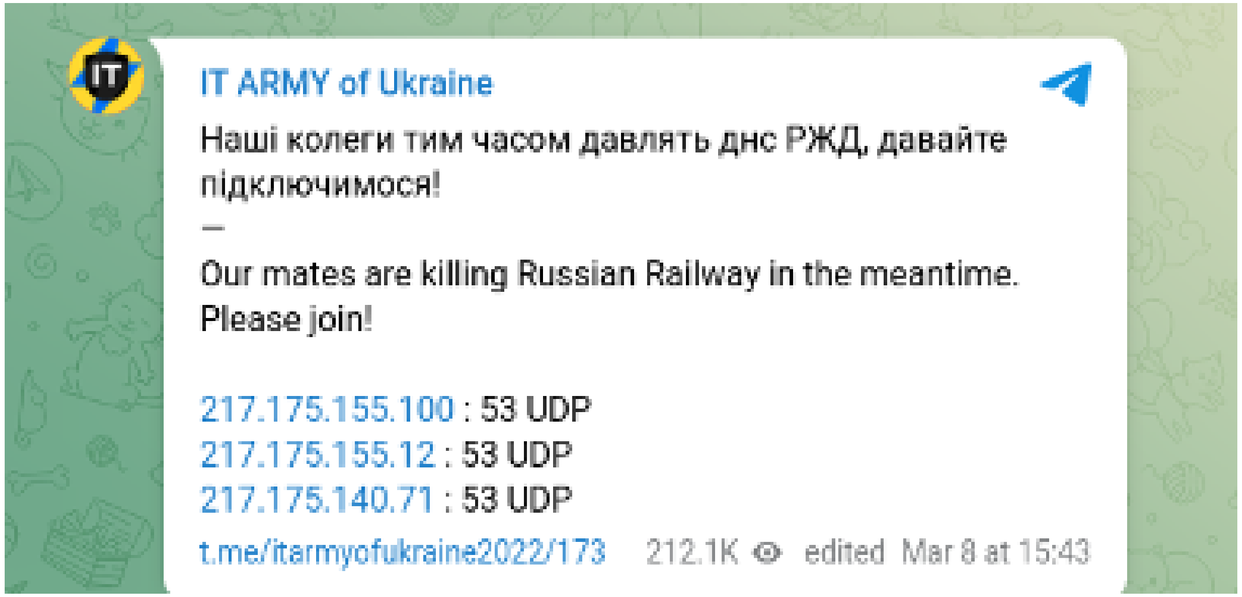
There's no way it's DNS

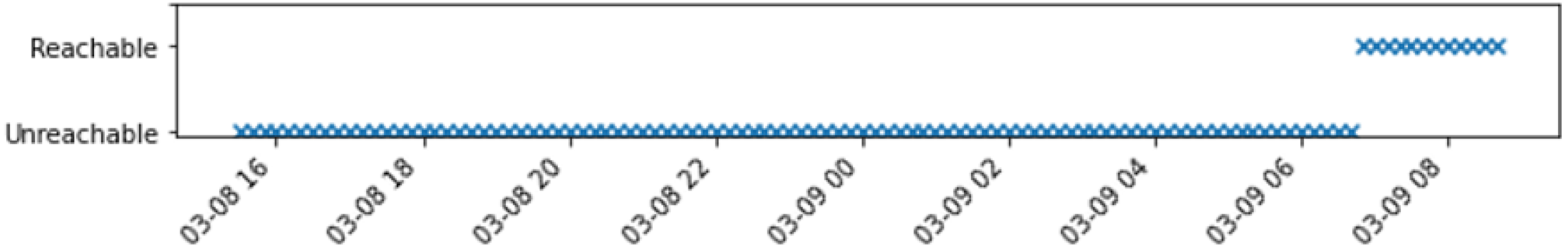
It was DNS

-SSBroski



DDoS against DNS providers





mil.ru - How to not operate a DNS server

- Nameservers of mil.ru under attack for eight consecutive days, from March 11th to 18th.
- OpenINTEL failed to resolve mil.ru during the attack.
- The three nameservers were unicast, hosted behind the same ASN/company, and even on the same /24 subnet.

The TransIP case

- December 2020, March 2021: Severe series of attacks against TransIP.
- In December 2020, the RTT increased ten-fold for eight consecutive hours.
- In March 2021, ~20% of the queries during the attack completely FAIL to resolve.
- No Anycast and a single ASN for their authoritative Nameservers

State Government Websites in DDoS Attacks

ALICIA HOPE · OCTOBER 12, 2022

Russian hackers took responsibility for a wave of cyber attacks that knocked dozens of state government websites offline.

Several states, including Colorado, Connecticut, Kentucky, and Mississippi, were impacted by the politically-motivated cyber attacks that began on W
October 6th.

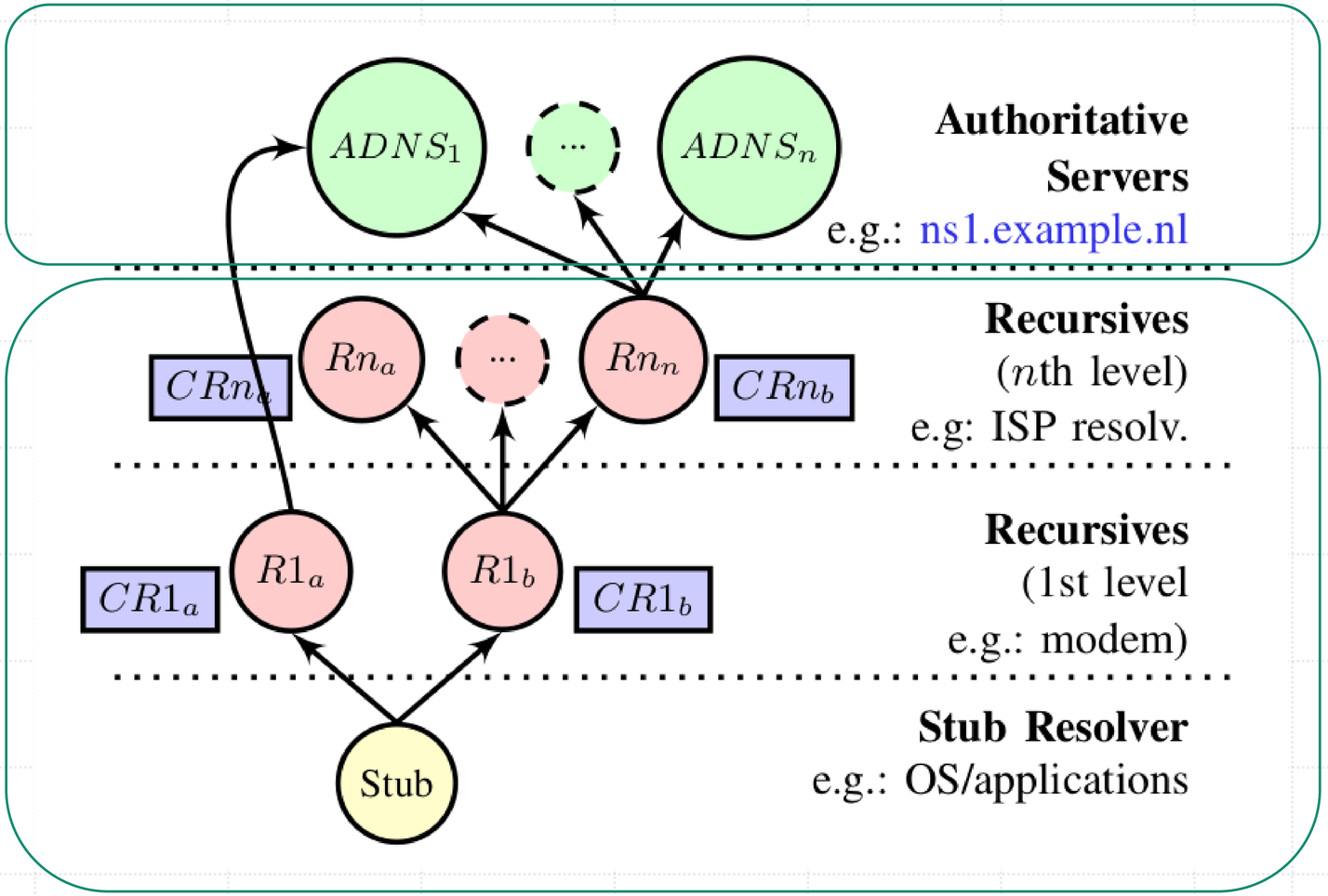
Our Contribution

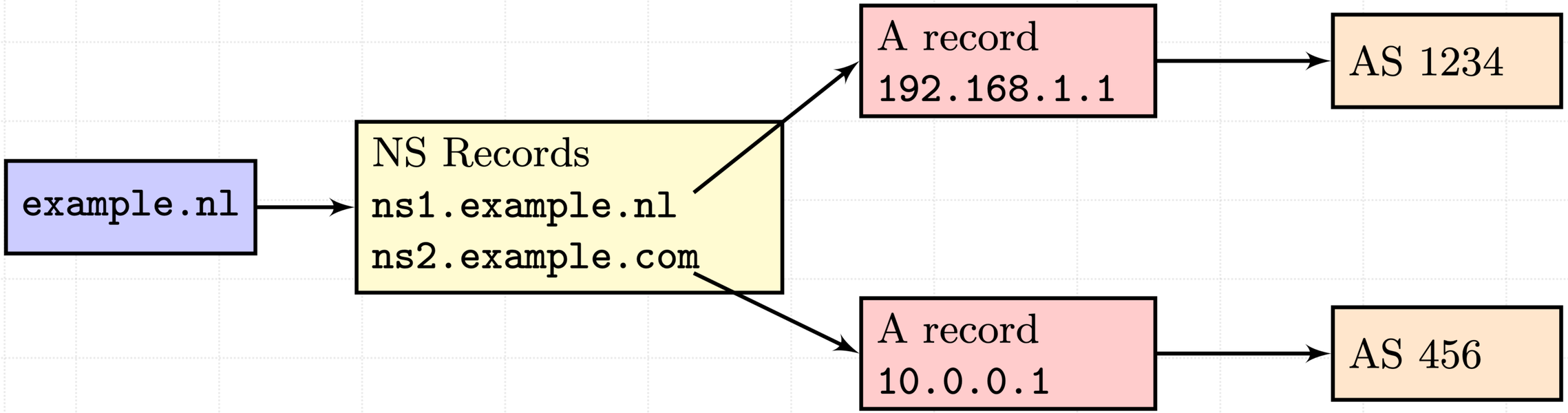
An evaluation of the infrastructure of e-gov DNS providers.

For both web and e-mail government services

Focusing on DNS and IP-based redundancy

DNS Authoritative and Recursive Nameservers




example.nl
NS Records
ns1.example.nl
ns2.example.com
A record
192.168.1.1
AS 1234
A record
10.0.0.1
AS 456

Datasets

NL.nl	FQDN E-Gov from NCSC (NL)
CH.ch	Swiss E-Gov Domains from SWITCH (.ch registry)
SE.se	Sweden E-Gov Domains from IIS (.se registry)
US.gov	US full list of government domains (public datasets)

Single Provider?

- For .nl , .se , and .ch , we notice roughly 40% of the e-gov domains have a single ADNS provider.
- For .gov , most domains (80%+) have a single ADNS provider.

	NL	SE	CH	GOV
E-gov domains	1309	615	3971	7972
SLD	602	614	3971	7972
Responsive	601	609	3546	7911
single provider(v4/v6)	268/331	249/254	1531/1923	6564/4455
multi-provider(v4/v6)	333/266	360/254	2013/344	1306/578

DNS Centralization

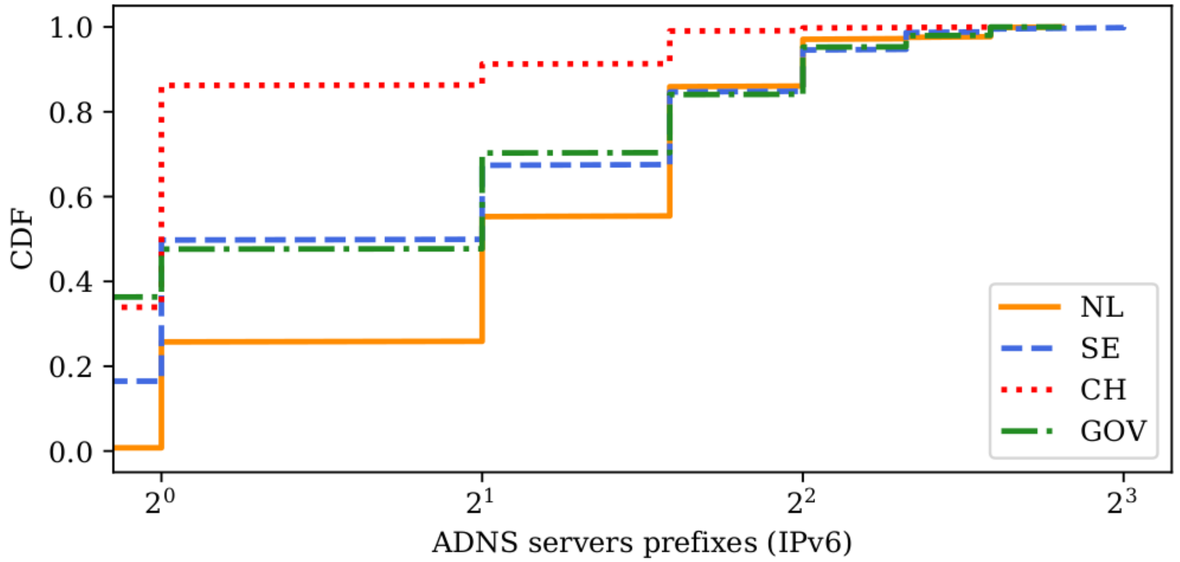
- A handful of DNS providers exclusively operate most of the domains.
- Local DNS providers provide service to most of the domains.
- A single provider (despite size) is a SPoF

	NL		SE	
	ASN	e-gov	ASN	e-gov
#1	20857 - Transip (NL)	112	39570 - Loopia (SE)	47
#2	48635 - CLDIN (NL)	39	1257 - Tele2 (SE)	23
#3	12315 - QSP (NL)	28	8068 - Microsoft (US)	21
#4	29311 - Solvinity (NL)	8	1729 - Telia (SE)	21
#5	48037 - SSC-ICT (NL)	8	3301 - Telia (SE)	19
	(195/609) = 32%		(131/614) = 21%	

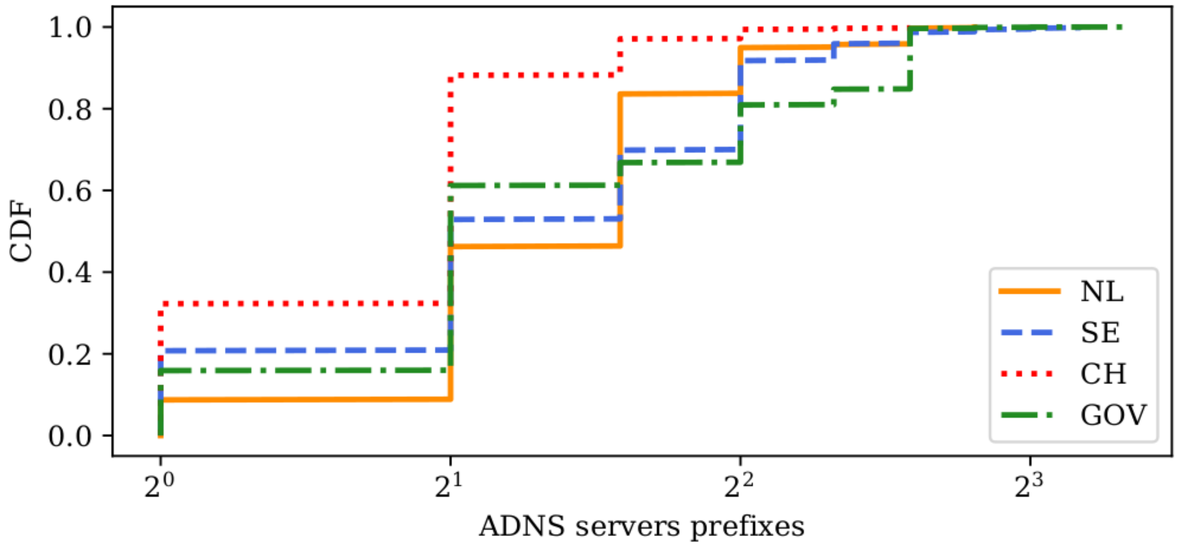
	CH		GOV	
	ASN	e-gov	ASN	e-gov
	29222 - Infomaniak (CH)	278	44273 - GoDaddy (US)	1215
	3303 - Swisscomm (CH)	115	13335 -Cloudflare (US)	909
	35206 - Novatrend (CH)	100	16509 - Amazon (US)	676
	9108 -Abraxas (CH)	97	21342 - Akamai (US)	334
	21069 - Metanet (CH)	91	16552 - Tiggee (US)	316
	(681/3971) = 17%		(3450/7972) = 43%	

Prefix NS Diversity

- One-third of .ch e-gov domains ADNS servers on the same network prefix!
- For IPv6, it is even worse: 40% of the domains with no IPv6, and another 40% from a single prefix.



(b) IPv6



(a) IPv4

TLD dependency

- Europe use mostly their own countries' ccTLD
- The US's .gov most rely on .com domains

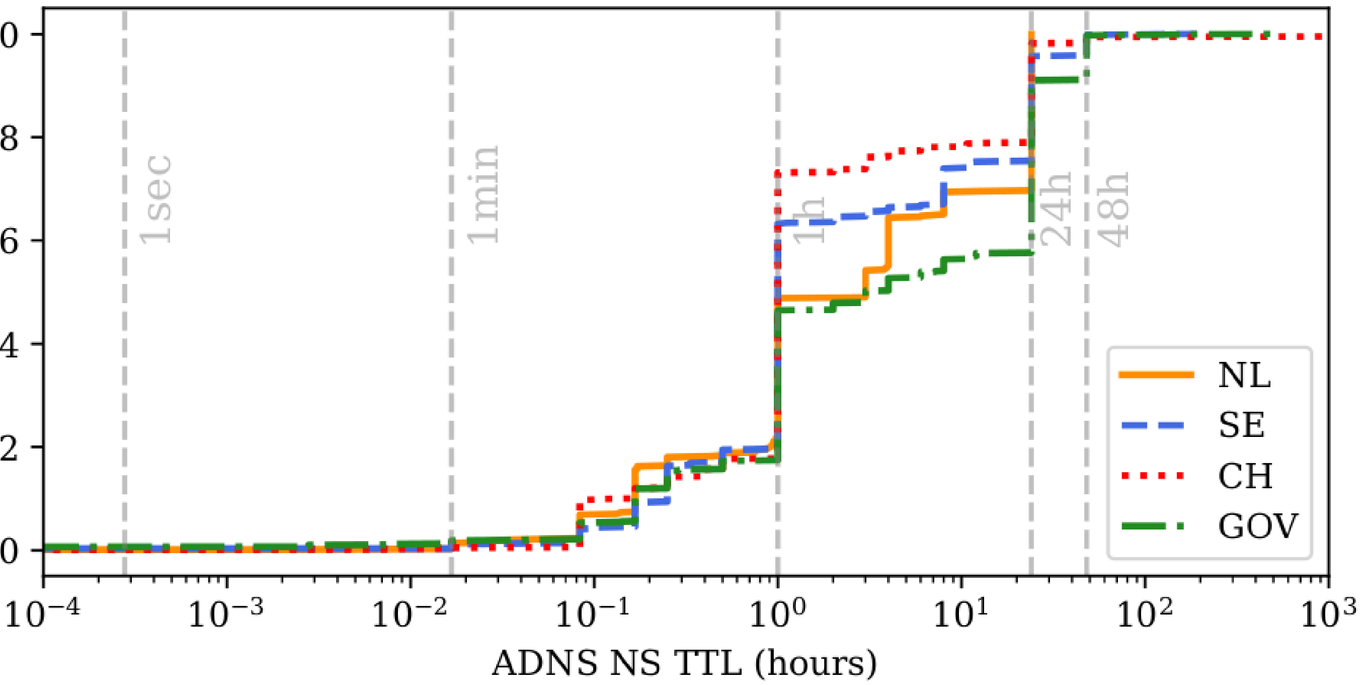
MOST USED TLD BY E-GOV ADNS SEVERS.

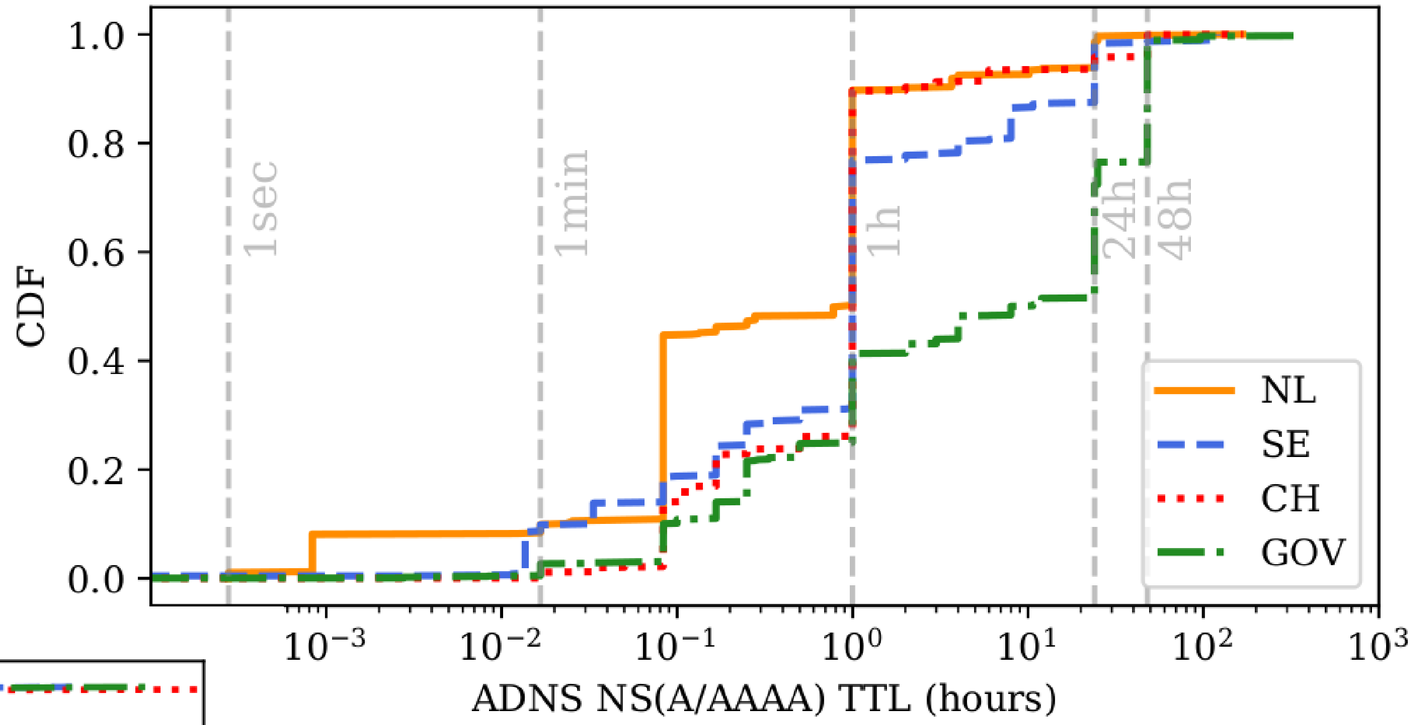
	NL	SE	CH	GOV
1	170 (.nl)	483 (.se)	609 (.ch)	2507 (.com)
2	69 (.net)	100 (.net)	190 (.com)	1541 (.net)
3	26 (.com)	82 (.com)	150 (.net)	894 (.gov)
4	12 (.eu)	14 (.info)	19 (.org)	485 (.org)
5	4 (.be)	8 (.org)	12 (.de)	302 (.us)

Anycast adoption

- Anycast for ADNS proved to be the most effective way to overcome DDoS attacks.
- Around 58% of .gov domains have one or more anycast ADNS servers.
- Very few Swiss e-gov domains do.
- The Netherlands and Sweden score in between with approximately 15–20% of domains.

TTL(s) of e-govs





- Most NS records TTL is equal to 1 h. Recommended is 24h(!)
- For A/AAAA is even worse!

Top mail providers

MX Provider	#.nl Domains	%.nl Domains	MX Provider	#.se Domains	%.se Domains
outlook.com	164	(39.0%)	outlook.com	205	(37.5%)
ezorg.nl	46	(11.0%)	mailanyone.net	69	(12.6%)
ssonet.nl	17	(4.0%)	mx25.net	52	(9.5%)
barracudanetworks.com	13	(3.1%)	staysecuregroup.com	38	(6.9%)
minvenj.nl	12	(2.9%)	staysecuregroup.net	38	(6.9%)
MX Provider	**#.ch Domains**	**%.ch Domains**	**MX Provider**	**#.gov Domains**	**%.gov Domains**
outlook.com	425	(22.1%)	outlook.com	2243	(41.4%)
infomaniak.ch	129	(6.7%)	google.com	532	(9.8%)
abxsec.com	120	(6.2%)	barracudanetworks.com	495	(9.1%)
tophost.ch	90	(4.7%)	pphosted.com	161	(3.0%)
ag.ch	78	(4.1%)	mimecast.com	157	(2.9%)

Recommendations for DNS operators

- Add at least a second DNS provider,
- Have ADNS infrastructure in different networks (physically different too!).
- Set higher TTL values of DNS records.
- Deploy more IP anycast on ADNS servers.

Thanks!

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Contact me:
j.vanderham@utwente.nl
https://jvdham.nl

UNIVERSITY OF TWENTE.

This work was supported by the DINO project, contracted by the Netherlands' National Cyber Security Center (NCSC-NL); the EU H2020 CONCORDIA project (830927); and the joint US Department of Homeland Security and Dutch Research Council DHS-NWO MADDVIPR project (628.001.031/FA8750-19-2-0004).

NWO
Netherlands Organisation for Scientific Research