

Assessing e-Government DNS Resilience

Raffaele Sommese¹, Mattijs Jonker¹, Jeroen van
der Ham¹⁻², Giovane C. M. Moura³

University of Twente¹, NCSC-NL²,
SIDN Labs/TU Delft³

CNSM 2022, Thessaloniki, Greece
31 October - 4 November 2022



Introduction

- Governments increasingly use Internet for communication with citizens and residents.
- Internet as core communications fabric of modern societies.
- E-gov depends on the Internet, which relies on the Domain Name System (DNS).
- E-gov DNS structuring should therefore be resilient against (partial) failure to avoid service interruption.

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.

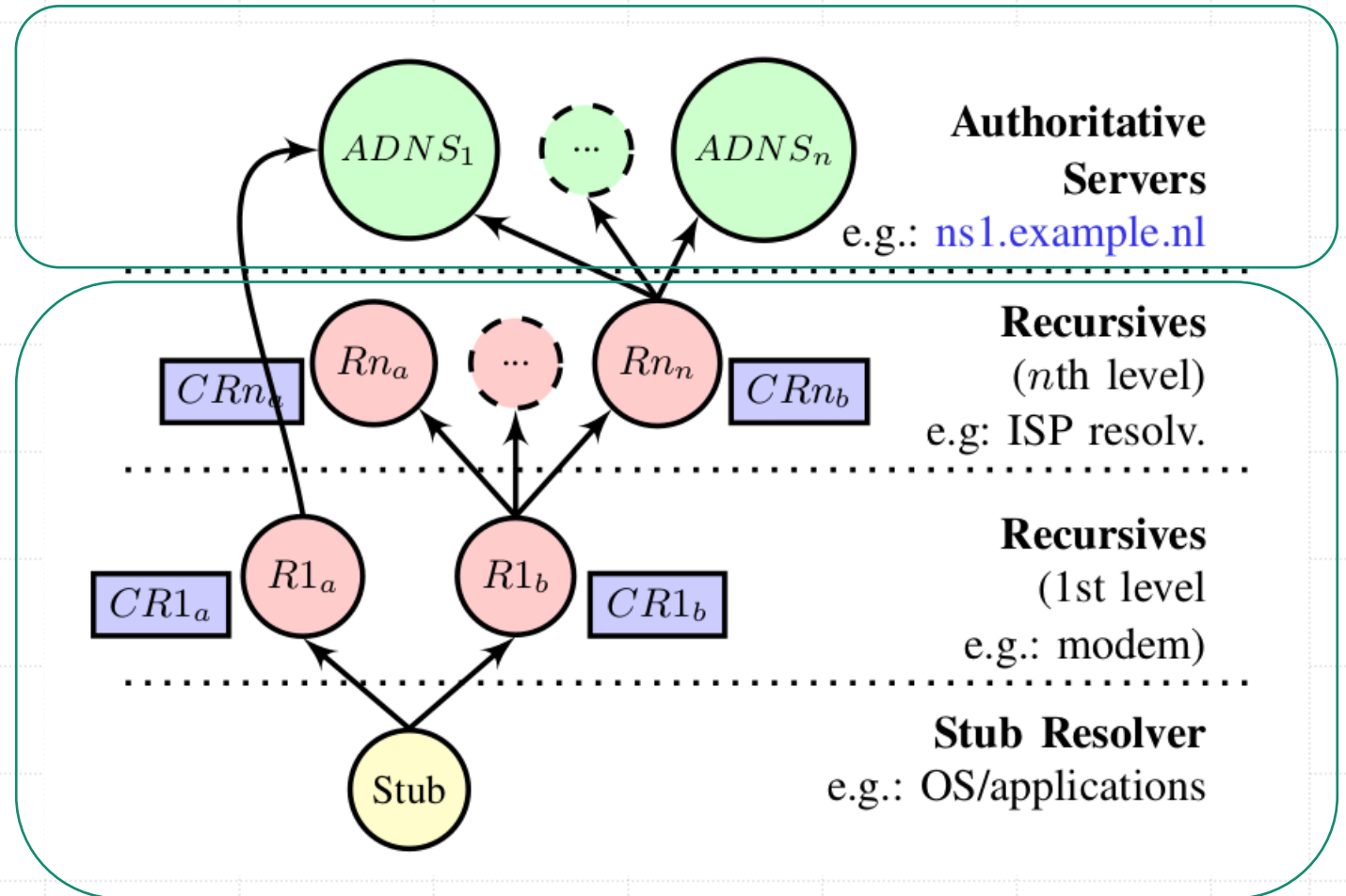
Several states, including Colorado, Connecticut, Kentucky, and Mississippi, were impacted by the politically-motivated cyber attacks that began on ~~October 6th~~ October 6th.



DNS Resilience and Misconfigurations

- The DNS supports various levels of redundancy to become more resilient against events such as DoS attacks.
- Increasing resilience is not easy task.
- The DNS is also prone to many types of configuration errors, which can lead to service unreachability.

DNS Authoritative and Recursive Nameservers





Our Contribution

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

For both web and e-mail governative services

Focusing on DNS and IP-based redundancy



Our Cases of Study

- We study three countries in continental Europe:
 1. the Netherlands
 2. Sweden
 3. Switzerland
- And the United States in North America.

We obtain the lists of e-gov domain names for these countries and use active measurements to evaluate DNS configuration and structuring



Datasets

FQDN E-Gov from National Cyber Security Center (NL)

Swiss E-Gov Domains from SWITCH (.ch registry)

Sweden E-Gov Domains from IIS (.se registry)

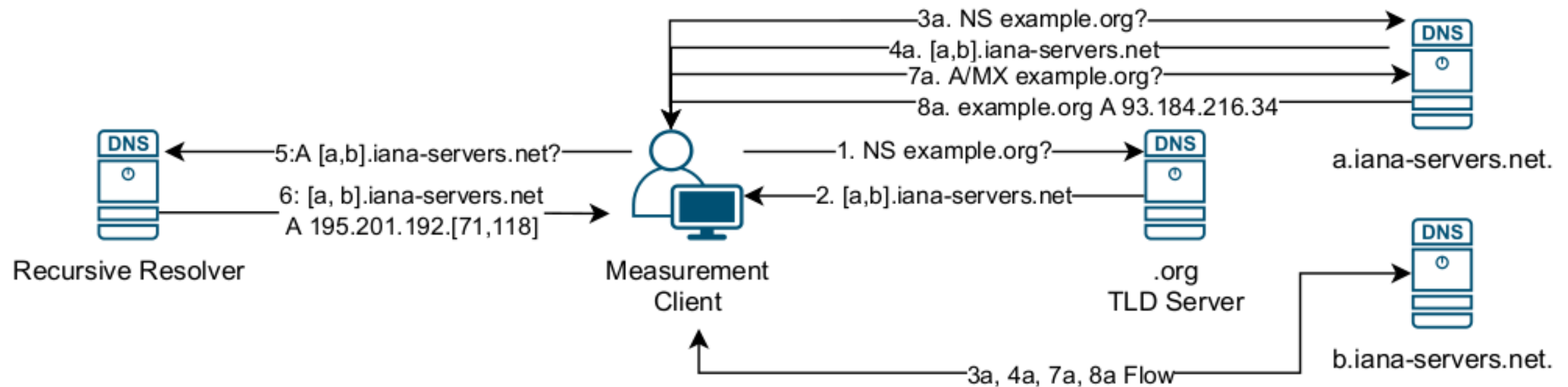
The .gov domains from US full list of governative domains (public datasets).



Our Measurements

- Conducted on 2022-06-08 from a VP in The Netherlands.
- Joined with additional anycast measurement using iGreedy (anycast census tool).
- For unicast address, we rely on IP2Location for geolocation.
- For IP to ASN mapping, we used CAIDA Prefix2AS dataset.

Measurement Step-by-step



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			CH			GOV		
	ASN	e-gov		ASN	e-gov		ASN	e-gov		ASN	e-gov
#1	20857 - Transip (NL)	112		39570 - Loopia (SE)	47		29222 - Infomaniak (CH)	278		44273 - GoDaddy (US)	1215
#2	48635 - CLDIN (NL)	39		1257 - Tele2 (SE)	23		3303 - Swisscomm (CH)	115		13335 -Cloudflare (US)	909
#3	12315 - QSP (NL)	28		8068 - Microsoft (US)	21		35206 - Novatrend (CH)	100		16509 - Amazon (US)	676
#4	29311 - Solvinity (NL)	8		1729 - Telia (SE)	21		9108 -Abraxas (CH)	97		21342 - Akamai (US)	334
#5	48037 - SSC-ICT (NL)	8		3301 - Telia (SE)	19		21069 - Metanet (CH)	91		16552 - Tiggee (US)	316

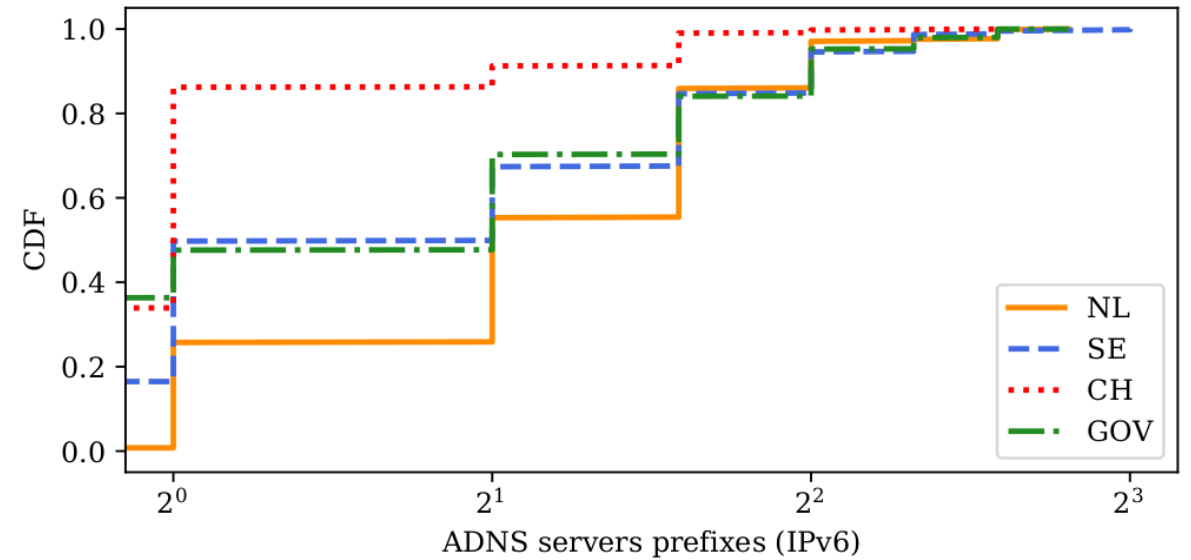


NS diversity

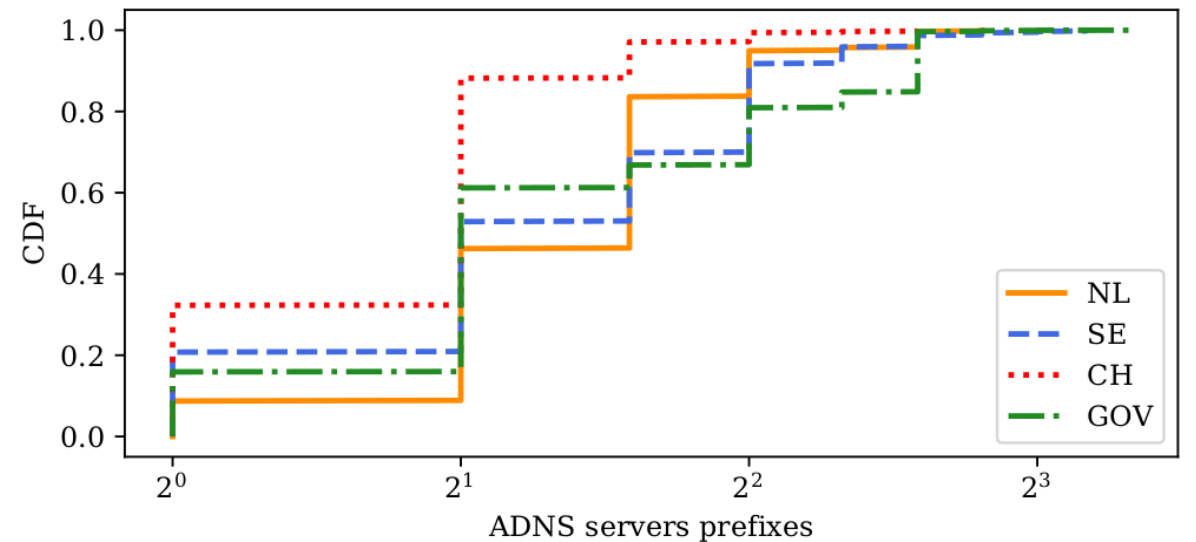
- Most e-gov domains have at least two ADNS servers (two different NS records), complying with RFC1034.
- The .gov mandate that their domains must have two ADNS servers in their operational policy.
- Six domain violated this .gov policy.
- We notified the .gov registry and registrar of this issue.

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



Implications and Suggestions

- RFC1034 states that ADNS servers for the same DNS zone should be placed in topologically distinct networks.
- We have seen that many e-gov domains depend on ADNS servers located in the same location.
- This creates an unnecessary risk in case of failures or attacks.
- We recommend operators to configure ADNS servers in distinct networks.

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 and Caching

DNS resolvers heavily deploy caching of DNS responses to improve response times to clients.

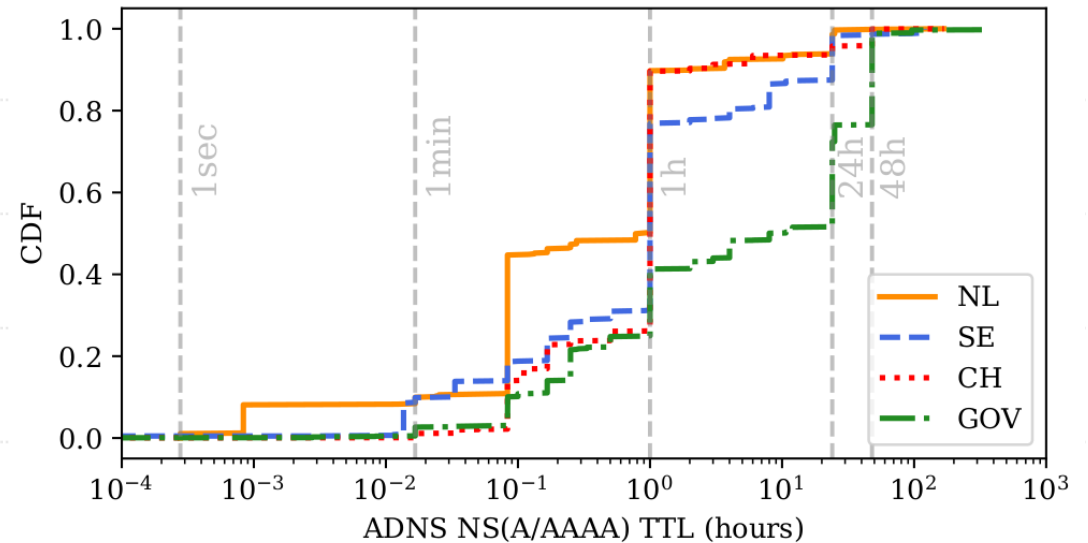
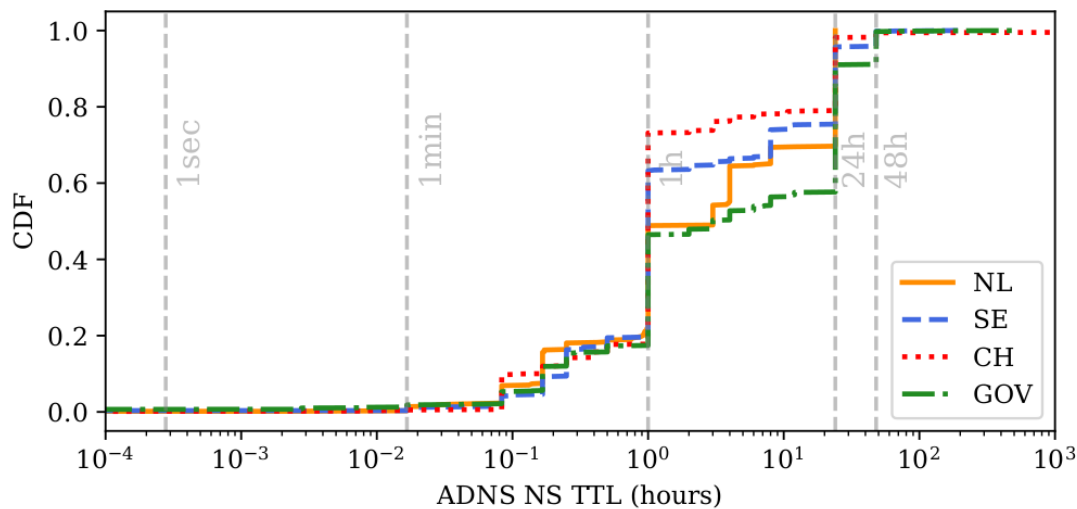
This mechanism can suppress the effects of DDoS attacks.

The ADNS controls how long records should stay in DNS resolver cache by setting a time-to-live (TTL) value.

Previous studies suggested to configure ADNS NS records to have a TTL of at least a few hours.

TTL(s) of e-govs

- Most NS records TTL is equal to 1 h, which is considered short!
- For A/AAAA is even worse!





External Mail Dependency

- MX records must be resolved to determine the location of the receiving mail server.
- This resolution can involve “external” ADNS infrastructure.
- This infrastructure should also be resilient.
- Around 80% of mail infrastructure for e-gov domain is hosted on third parties.

Top mail providers

In-country 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%)



Recommendation for operators

- There is much dependency on single DNS providers, for all countries under study.
 - The e-gov domains should add at least a second DNS provider,
- Many e-gov domains have ADNS infrastructure in the same networks.
 - We recommend e-gov domains to adhere to RFC2182 recommendations.
- We recommend operators to carefully set the TTL values of their DNS records.
- We also recommend that countries deploy more IP anycast on their ADNS servers.



Conclusion

- Our results show that many e-gov domains are not following the current recommendations for operation of large DNS providers, regardless of country.
- This behavior is not free of risks: A motivated attacker could stress specific DNS infrastructures to deteriorate the reachability of many e-gov domains.
- We hope our findings prompt the responsible operators to improve the redundancy and resilience of e-gov DNS.

Thanks for the attention

Contact me:

r.sommese@utwente.nl

<https://academia.r4ffv.info>

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).



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

**UNIVERSITY
OF TWENTE.**

The logo for the Netherlands Organisation for Scientific Research (NWO) consists of the letters 'NWO' in a bold, black, sans-serif font. A red swoosh arches over the 'O'. Below the letters, the full name 'Netherlands Organisation for Scientific Research' is written in a smaller, black, sans-serif font.

NWO
Netherlands Organisation
for Scientific Research