Whose Cloud Is Your Country On?

Single-provider dependencies of Romanian critical services

25th RoEduNet Conference · Iași · 19–21 November 2026

Vlad-Ștefan Dieaconu
National University of Science and Technology POLITEHNICA Bucharest
vlad.dieaconu@stud.acs.upb.ro

Carol-Luca Gasan
University of Cambridge
clg72@cam.ac.uk

Andreea-Loredana Dieaconu-Ușurelu
National University of Science and Technology POLITEHNICA Bucharest
andreea.dieaconu95@upb.ro

Răzvan Victor Rughiniș
National University of Science and Technology POLITEHNICA Bucharest
razvan.rughinis@upb.ro

18 November 2025

DNSC, Romania’s cybersecurity authority, reported its own website unavailable during a Cloudflare outage

The data may remain

Intact

and under the intended jurisdiction

While the public service becomes

Unreachable

through a dependency elsewhere in its delivery path

A roughly three-hour outage, caused by a faulty configuration file [1], [2]

The problem

Sovereignty clauses do not ask who keeps a service reachable

Sovereignty clauses ask

- Where are the data stored?
- Under whose law?

Reachability depends on

- Who operates each layer?

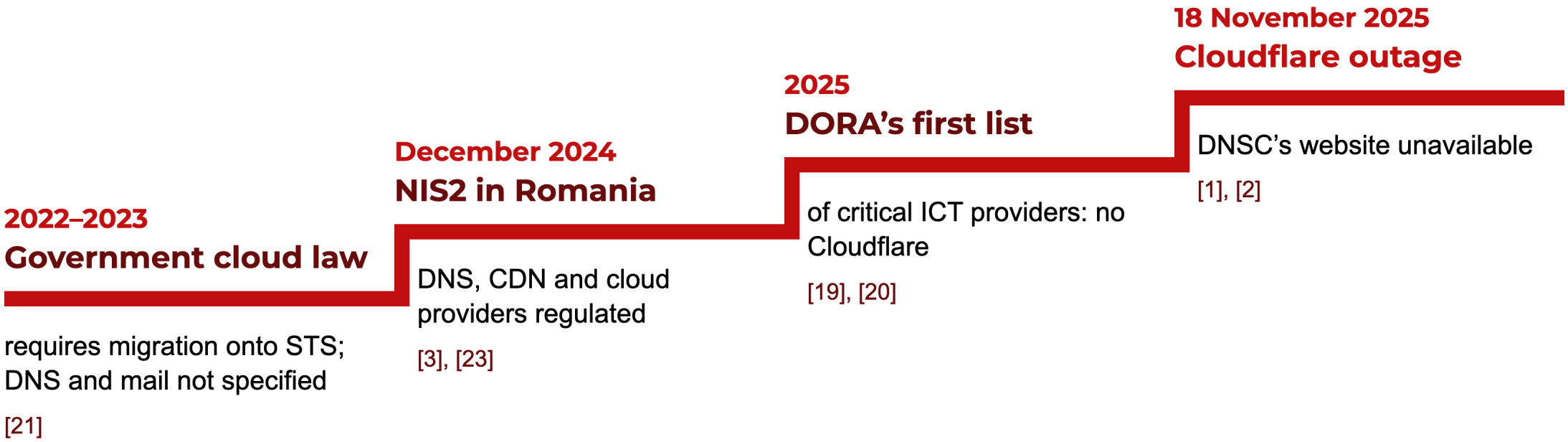
  Authoritative DNS · edge or CDN · hosting

We ask

At each layer, which organisation is the sole observed provider?

Why now

New rules since 2022 and a 2025 outage; no rule observes, per domain, who keeps a service reachable



STS: Special Telecommunications Service, the state operator

What was missing | What we ask

For Romania's sectors, earlier work does not show which single organisation is observed at each layer

Earlier work measures

- **One layer at a time** [4]–[8]
- **The Web at large, or popular sites** [9]–[11]
- **Government infrastructure** [12]–[14]

We ask

RQ1 How concentrated is each layer?

RQ2 Who are the sole observed providers?

RQ3 Does that survive other assumptions?

Our contribution

A reproducible audit, a measurement of 192 Romanian public services, and a test of what holds

01

A method

An audit unit we defined and built: service × layer × operating organisation. Five layers per service, one rule for every operator.

02

A measurement

192 public services in ten NIS2 sector groups: layer concentration, sole observed providers, reach across sectors, jurisdiction.

03

Its limits, tested

A second vantage point and 15 variants show what holds. Plus a four-question check an operator can run.

Open and reproducible [25]

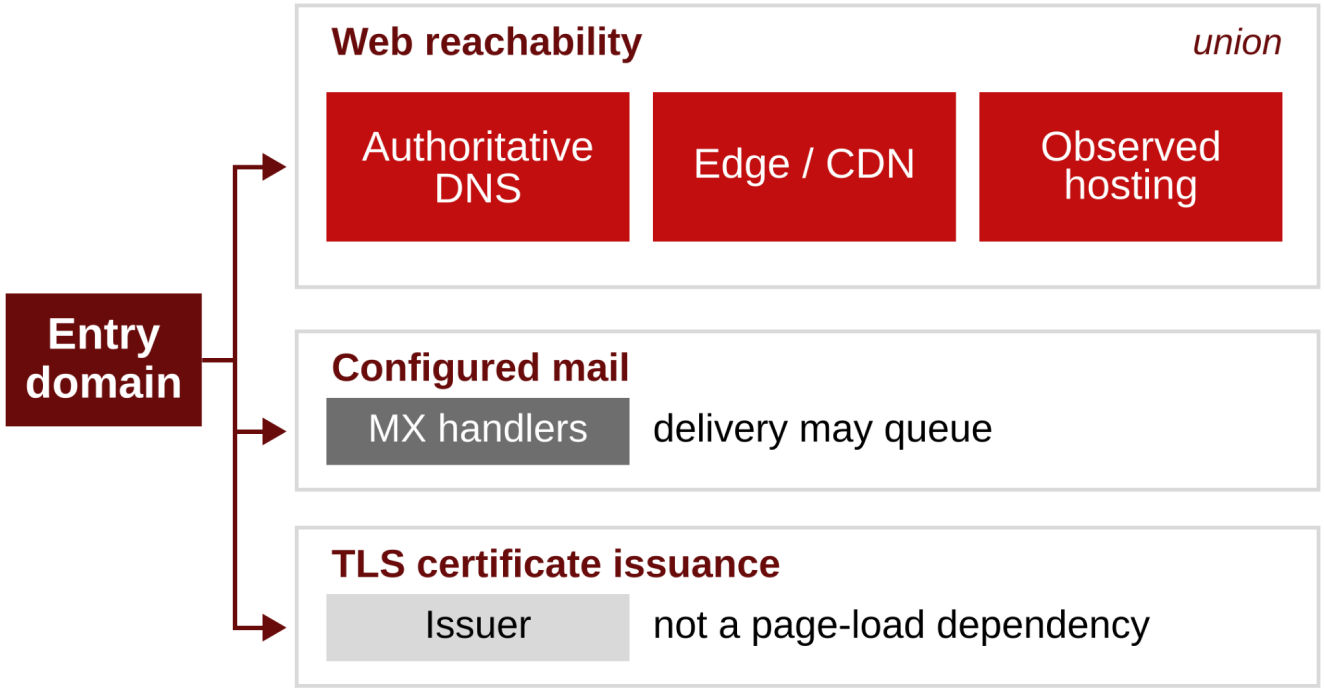
code, attribution rules, raw records, per-service tables: every table and figure can be regenerated

What it shows

Cloudflare 53 of 192;
STS, the state operator, second with 35

What we measured | Five layers

Five layers per service, one test for every operator



Layer verdict: sole observed when exactly one operator is attributed

Sole observed provider

the only organisation observed at a layer of a service

test adapted from Kashaf et al. [10]

Web, mail and certificate issuance are reported apart.

One test for commercial providers, the state operator and own networks

How we measured | Four steps

From a domain name to the organisations behind it, using only public answers

01

Ask

Ordinary DNS lookups for each domain: name servers, addresses, CNAME, MX. One certificate read. One landing-page request.

02

Attribute

Each name and each address goes to the organisation that operates it: rules on names, then the network (AS) that announces the address [24].

03

Test

Count the organisations at each layer.
One: sole observed provider
Two or more: redundant
Only the operator's own network: self-hosted

04

Stress

Repeat the count under 15 variants of scope and attribution, and from a second vantage point.

Example a name server under cloudflare.com → Cloudflare · an address announced by AS31313 → STS

Snapshot 7 September 2026 · from Bucharest (all 192 services) and from a non-Romanian cloud (186) · 3,317 DNS lookups in total

How to read one service

Example: dnsc.ro has a single organisation per layer

Layer	Sole provider, AS	HQ	Table II cell
Web reachability: one test over three layers			
Authoritative DNS	STS, AS31313	RO-S	DNS (31)
Edge / CDN	Cloudflare, AS13335	US	Edge (42)
Observed hosting			Host (41)
	Web column: Cloudflare (53) and STS (35)		
Configured mail: a separate test			
Configured MX	STS, AS31313	RO-S	MX (32)
	Web/MX column: Cloudflare (53) and STS (37)		
Certificate issuance: not a sole-provider test			
TLS issuer	DigiCert	US	Table I only

STS alone at DNS and at mail

Cloudflare alone at the edge and at hosting

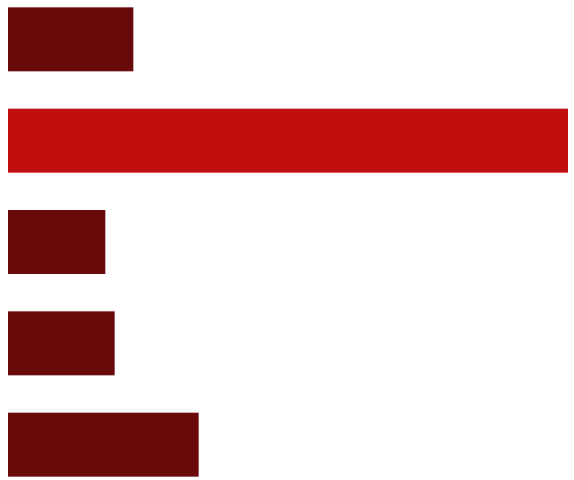
dnsc.ro is in STS's set and in Cloudflare's set: the sets overlap and are never summed

Snapshot of 7 September 2026, not the outage-day configuration

RQ1 | Concentration

The edge is the most concentrated layer (HHI 4,802)

Layer	HHI, 0–10,000	Providers
Authoritative DNS	**1,072**	72
Edge / CDN	**4,802**	9
Observed hosting	**829**	65
Configured MX	**911**	67
TLS issuer	**1,635**	13



67.7%

of the edge layer goes to its largest provider

Only 62 of 192 services have an identifiable edge

HHI: Herfindahl–Hirschman index.
A sample, not an antitrust market.

RQ2 | Sole observed providers

Cloudflare is the sole observed provider for 53 of 192 services; STS is second

53

Cloudflare

27.6%, at one or more web layers

35

STS, the state operator

18.2%, at the web layers; 37 at web or mail

36

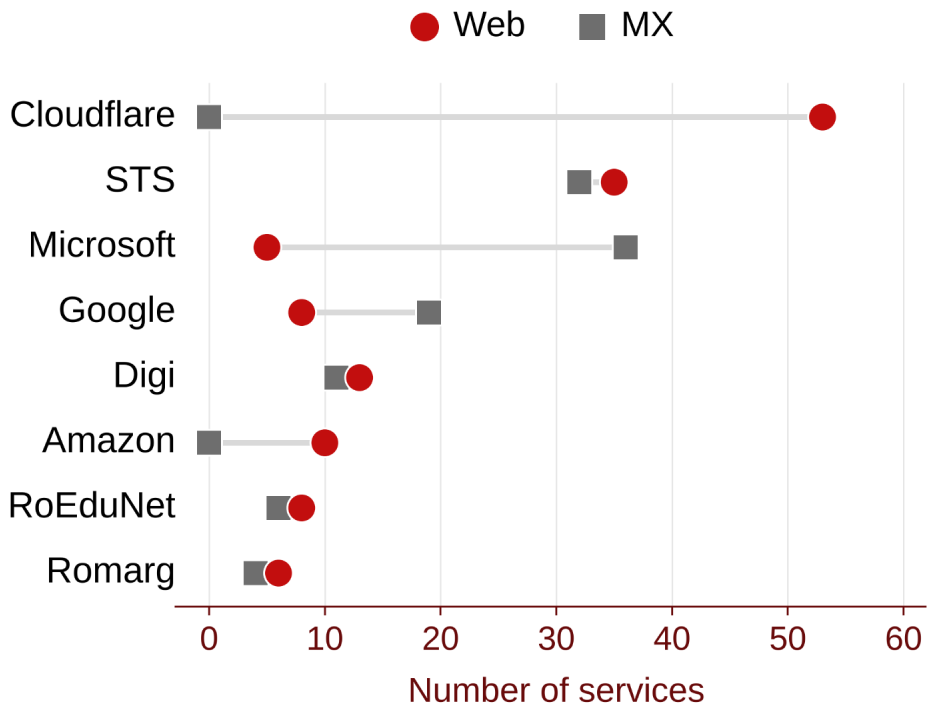
Microsoft, once mail counts

only 5 at the web layers

Exposure indicators, not proof of failure. The sets overlap and are never summed.

RQ2 | Web and mail

Mail reorders providers: Microsoft goes from 5 to 36

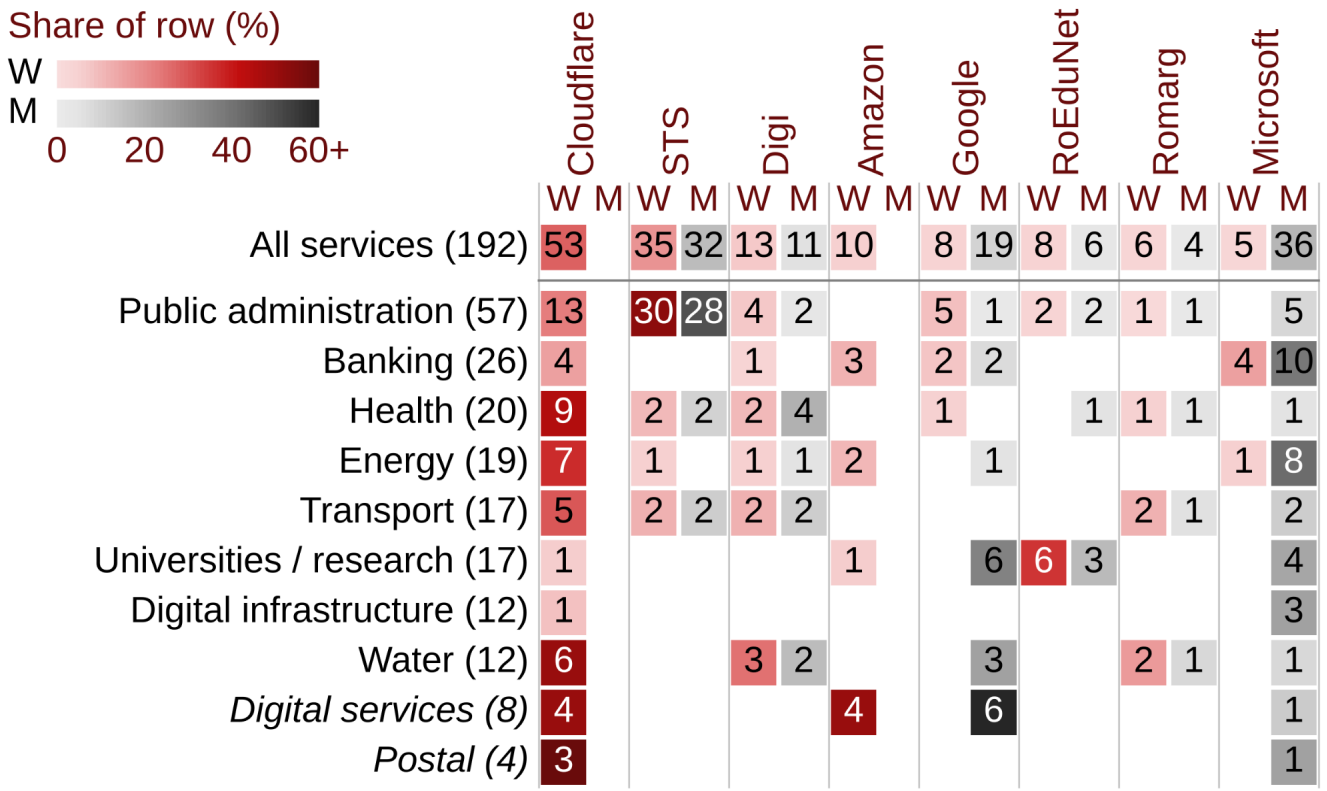


Organisation	Web	MX
Cloudflare	53	0
STS	35	32
Microsoft	5	36
Google	8	19
Digi	13	11

Number of services; two tests, never added.

RQ2 | By sector

STS's exposure set is mostly public administration



32 of 37

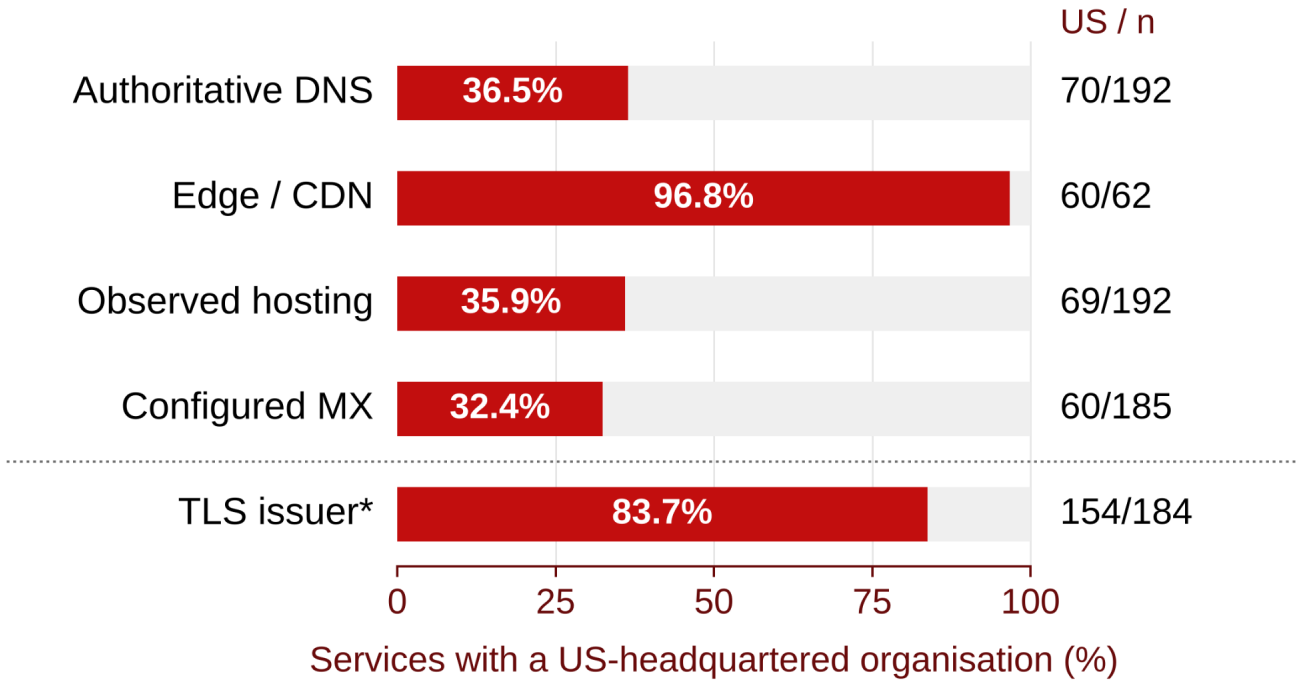
STS services (web or mail) are in public administration: 32 of the 57 services there (56.1%)

Cloudflare's web set and Microsoft's mail set reach all ten sector groups

W: web layers · M: mail · cells count services

Jurisdiction

107 of 192 services have a US-headquartered web or mail provider



55.7%

at one or more web or mail layers

Edge: 60 of the 62 services that use one

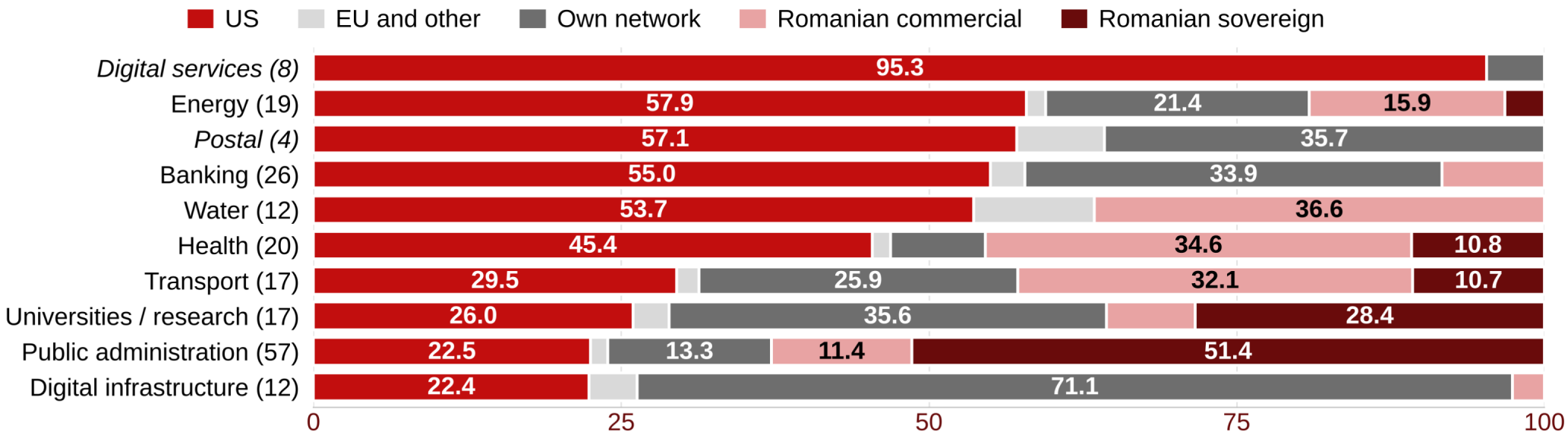
57 services (29.7%) are sovereign or self-hosted at every such layer

Headquarters of the operating company, not server location

* TLS issuer: supplementary, not counted in the 107

Jurisdiction by sector

Public administration is 51.4% Romanian sovereign; energy is 57.9% US-headquartered



% of the sector's DNS, edge, hosting and MX observations, by headquarters of the operating company
in brackets: number of services · italics: fewer than ten services

RQ3 | Robustness · web or mail counts

Cloudflare stays first in all 15 variants; STS stays second only at the web layers

Four of the 15 variants	Cloudflare	STS	Microsoft	Second place
Stated rule	53	37	36	STS
Strictest scope (n = 144)	44	27	27	tie
MX address cap applied	53	36	36	tie
Mail gateways read by their network	53	37	39	Microsoft

Holds

Cloudflare first; the web order Cloudflare, STS, Digi

Does not hold

STS second once mail counts

Second vantage

3 of 186 services differ (1.6%), all at DNS

What this tells us

Four things a data-location clause cannot show

01 Sovereign is not redundant

STS, the state operator, is a sole observed provider for 32 of the 57 public-administration services (56.1%).

02 The front door is the narrowest point

Nine edge providers; one holds 67.7% of the layer, and 60 of the 62 edges are US-headquartered.

03 A website audit misses the mail

Microsoft: 5 services at the web layers, 36 once mail counts.

04 No service has a second organisation at every layer

157 of 192 (81.8%) have a sole observed provider at a web or mail layer; the other 35 have a layer only their own network answers.

For operators

Four questions an operator can ask; the aim is a distinct organisation with tested failover

01 **Who answers for the authoritative zone?**

02 **Does an edge front the origin?**

03 **Is hosting the same organisation as the edge?**

04 **Who handles configured mail (MX)?**

In this sample

A second DNS provider [12] would take at most 11 of Cloudflare's 53 services out of its web set; the other 42 keep it as sole edge.

For 37 of the 53, Cloudflare is sole at DNS and edge: the switch away runs through its own control plane [1].

Conclusion

Jurisdictional sovereignty does not imply provider diversity

01 **A method:** a reproducible audit unit, service × layer × operating organisation, with public code and data [25]

02 **A first picture:** Cloudflare is the sole observed web provider for 53 of 192 services; the state operator is second; mail orders providers differently

03 **Its limits:** Cloudflare's lead holds in all 15 variants, the second place does not once mail counts; one snapshot, a chosen sample, an outside view

Next repeat the measurement over time, to see what cloud migration changes; then failover exercises with operators

Thank you

Questions?

vlad.dieaconu@stud.acs.upb.ro

The paper

V.-Ș. Dieaconu, C.-L. Gasan, A.-L. Dieaconu-Ușurelu, R. V. Rughiniș, “Whose Cloud Is Your Country On? Single-Provider Dependencies of Romanian Critical Services,” 25th RoEduNet Conference: Networking in Education and Research, Iași, November 2026, paper #449.

Code, data, results [25]

doi:10.5281/zenodo.23706262

Backup | Method in detail

What each step does, as in the paper

Step	How
Probes	dnspython over UDP/53; 12–29 DNS lookups per service (median 16; 3,317 in total); one certificate; one landing-page request chain
Authoritative DNS	zone-cut walk, stopping at the registrable domain
Edge / CDN	a CNAME rule or, for 41 of 62 edge services, the AS serving the entry domain; response headers support 45 of 47
Hosting	organisations serving the IPv4 addresses of the entry name and its www host; behind a proxy, the proxy network
Mail	explicit MX handlers of the service name
Attribution	rules on CNAME, name-server and MX names; then AS names, from Team Cymru's IP-to-ASN service [24]; a 22-entry parent map
Jurisdiction	headquarters of the operating company: 106 operator entries, 61 observed here

Rules hand-reviewed, not independently validated · code, rules and raw records are in the public archive [25]

Backup | Data

A purposive sample of public services, measured from outside on 7 September 2026

192

public-facing services

10

sector groups, from the NIS2 annexes

2

vantages: Bucharest (all 192), non-Romanian cloud (186)

Active but low-rate: no scanning, authentication or crawling.

Shares describe this sample, not all Romanian critical entities.

Backup | Table II

The eight largest exposure sets, in services where the organisation is the sole observed provider

Organisation	HQ	DNS	Edge	Host	Web	MX	Web/MX	Share
Cloudflare	US	48	42	41	53	0	53	27.6%
STS	RO-S	31	0	27	35	32	37	19.3%
Digi	RO-C	8	0	12	13	11	17	8.9%
Amazon	US	5	6	7	10	0	10	5.2%
Google	US	2	0	6	8	19	25	13.0%
RoEduNet	RO-S	8	0	6	8	6	9	4.7%
Romarg	RO-C	5	0	5	6	4	7	3.6%
Microsoft	US	5	1	2	5	36	36	18.8%

Share: Web/MX of all 192 · HQ: operating company's headquarters · RO-S, RO-C: Romanian sovereign, commercial

Backup | Table III

Jurisdiction by sector, % of observations, by headquarters of the operating company

Sector	n	Self	RO-S	RO-C	EU	US	Oth.
Public administration	57	13.3	51.4	11.4	1.1	22.5	0.3
Banking	26	33.9	0.0	8.3	2.2	55.0	0.6
Health	20	7.7	10.8	34.6	1.5	45.4	0.0
Energy	19	21.4	3.2	15.9	1.6	57.9	0.0
Transport	17	25.9	10.7	32.1	1.8	29.5	0.0
Universities / research	17	35.6	28.4	7.2	2.9	26.0	0.0
Digital infrastructure	12	71.1	0.0	2.6	3.9	22.4	0.0
Water	12	0.0	0.0	36.6	9.8	53.7	0.0
Digital services	8	4.7	0.0	0.0	0.0	95.3	0.0
Postal	4	35.7	0.0	0.0	0.0	57.1	7.1

n: services · Self: operator’s own network · RO-S, RO-C: Romanian sovereign, commercial · 631 observations, no certificates

Backup | Table IV

Sole-observed-provider counts: six of the 15 variants

Variant	Cloudflare	STS Web	STS Web/MX	STS MX	Microsoft
Stated rule	53	35	37	32	36
Scope, n = 156	46	31	33	28	28
Scope, strictest (n = 144)	44	26	27	23	27
Both cap readings at once	53	35	36	16	36
Own network out	53	39	41	32	37
Transitive mail	53	35	37	32	39

Cloudflare, Microsoft: Web/MX. Other n = 192 variants: Cloudflare 53; STS Web 34–35, Web/MX 36–37, MX 16–32; Microsoft 36.

Backup | 18 November 2025

The 2025 outage is an illustration, not an outage count

Post-mortem [1]	Proxy core, key-value store and access-control product failed; authoritative DNS is not identified as affected
2026 snapshot	11 of Cloudflare’s 53 services: sole observed provider only at DNS. The other 42: sole observed edge
Incident date	The other 52 services were not observed that day

Backup | Sample scope

The sample is wider than the Directive's mandatory scope, on purpose

Rows	Outside the strict frame
17	universities
7	municipalities
3	county councils
7	excluded state functions
6	private financial firms
1	ministry

41 of 192

rows (21.4%) are outside the strict frame; up to 48 (25.0%) are outside or ambiguous

Recounted without them: n = 156, 152, 157 and 144

Backup | Limits and ethics

Limits: one snapshot, an outside view, hand-reviewed rules

Limitations

- One snapshot: 7 September 2026
- Anycast and reverse proxies hide origins
- IPv6 not attributed; parent zones not measured
- 40 services: no successful landing-page response

Ethics and data

- Low rate: 12–29 DNS lookups per service
- No scanning, authentication or crawling
- No personal data; results by sector
- Only dnsc.ro is named: its outage was public

Backup | Sources

Sources cited on these slides, by the paper's numbers

[1] M. Prince, Cloudflare outage of 18 November 2025, Cloudflare Blog

[2] AGERPRES, DNSC statement on unavailable websites, 18 Nov. 2025

[3] Directive (EU) 2022/2555 (NIS2), Off. J. Eur. Union, 2022

[4] Moura et al., DNS centralisation, ACM IMC 2020

[5] Zembruzki et al., hosting consolidation, IEEE/IFIP NOMS 2022

[6] Doan et al., Web consolidation, ACM Trans. Internet Technol., 2022

[7] Liu et al., mail-provider usage, ACM IMC 2021

[8] Azevedo et al., certificate centralisation, IEEE GLOBECOM 2025

[9] Habib et al., web infrastructure dependence, ACM SIGCOMM 2025

[10] Kashaf et al., third-party service dependencies, ACM IMC 2020

[11] Kumar et al., third-party dependency around the world, Proc. ACM Meas. Anal. Comput. Syst., 2023

[12] Sommese et al., e-government DNS resilience, CNSM 2022

[13] Kumar et al., government hosting, ACM IMC 2024

[14] Carisimo et al., subnational government hosting, PAM 2026

[19] Regulation (EU) 2022/2554 (DORA), Off. J. Eur. Union, 2022

[20] EBA, EIOPA, ESMA, designated critical ICT providers, 2025

[21] OUG 89/2022, HG 112/2023 (government cloud), Monitorul Oficial

[23] OUG 155/2024 (NIS2 transposition), Monitorul Oficial, 2024

[25] Dieaconu et al., measurement code, data and results, Zenodo, 2026