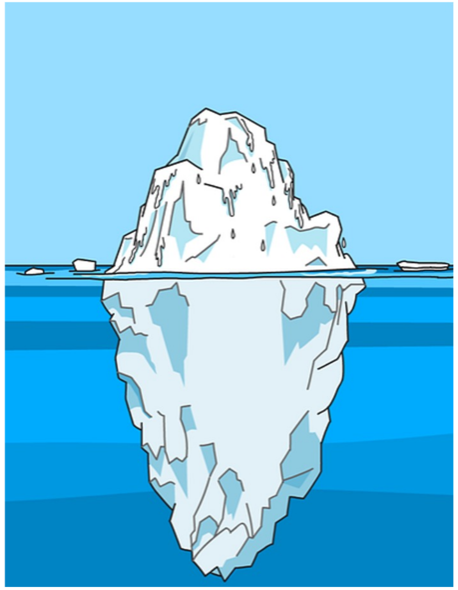


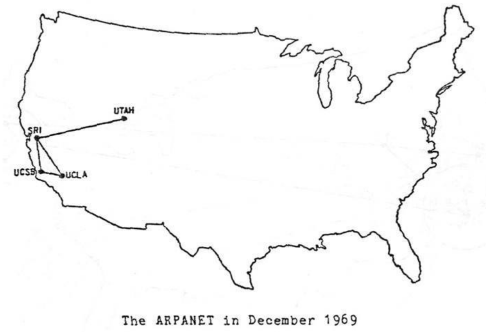
Increasing Internet security by bridging research and operations

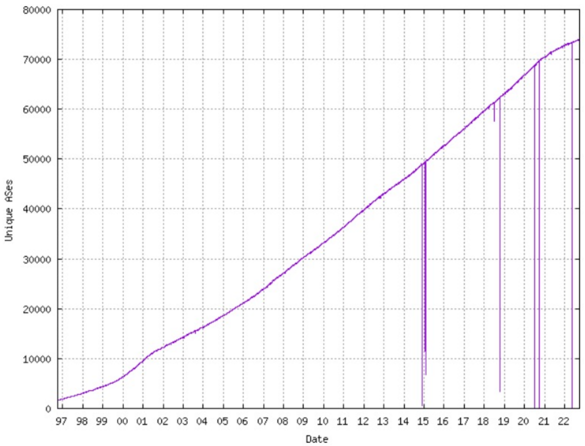
Cristian Hesselman

NLUUG spring conference
Utrecht, May 11, 2023

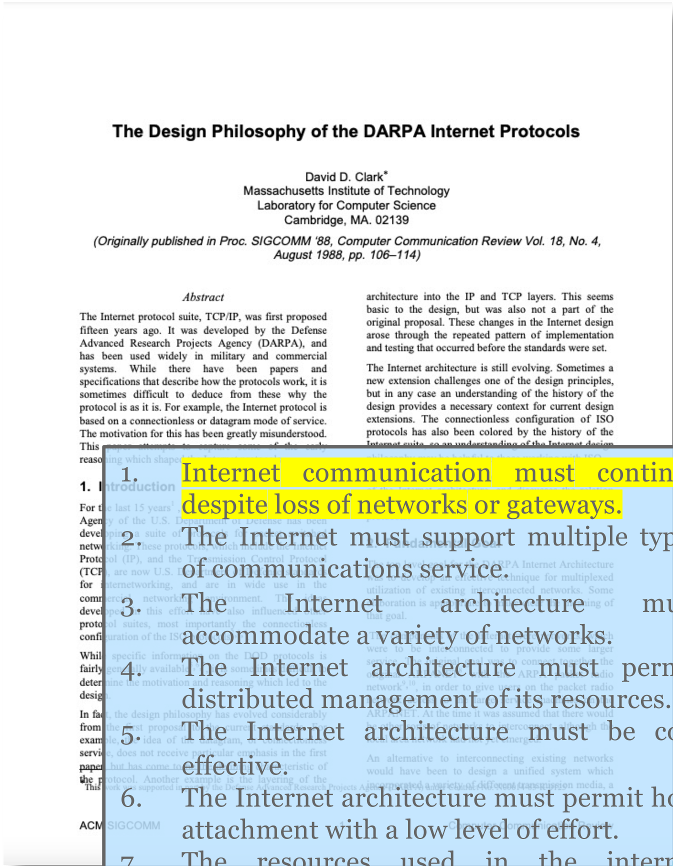
Internet security focused on availability (as in CIA)

Birthplace of the Internet
UCLA, Sep 2017





https://www.cidr-report.org/as2.0/



The Design Philosophy of the DARPA Internet Protocols

David D. Clark*
Massachusetts Institute of Technology
Laboratory for Computer Science
Cambridge, MA. 02139

(Originally published in Proc. SIGCOMM '88, Computer Communication Review Vol. 18, No. 4, August 1988, pp. 106–114)

Abstract

The Internet protocol suite, TCP/IP, was first proposed fifteen years ago. It was developed by the Defense Advanced Research Projects Agency (DARPA), and has been used widely in military and commercial systems. While there have been papers and specifications that describe how the protocols work, it is sometimes difficult to deduce from these why the protocol is as it is. For example, the Internet protocol is based on a connectionless or datagram mode of service. The motivation for this has been greatly misunderstood. This …

… architecture into the IP and TCP layers. This seems basic to the design, but was also not a part of the original proposal. These changes in the Internet design arose through the repeated pattern of implementation and testing that occurred before the standards were set.

The Internet architecture is still evolving. Sometimes a new extension challenges one of the design principles, but in any case an understanding of the history of the design provides a necessary context for current design extensions. The connectionless configuration of ISO protocols has also been colored by the history of the …

1. Internet communication must continue despite loss of networks or gateways.
2. The Internet must support multiple types of communications service.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit distributed management of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. The resources used in the internet architecture must be accountable.

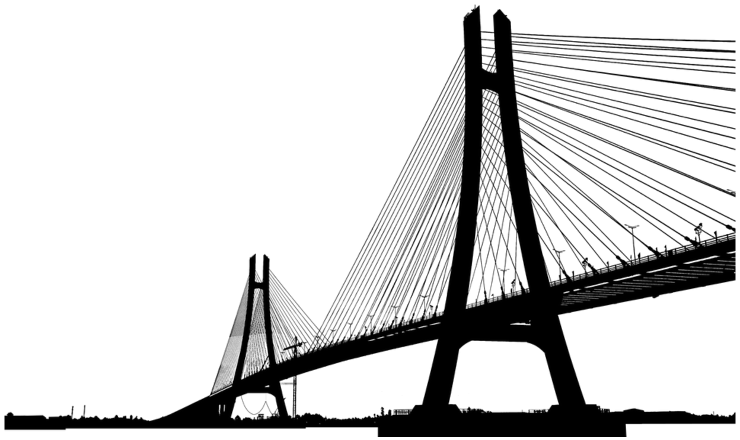
UNIVERSITY OF TWENTE.

DACS LABS

Today’s goal

- Showcase how we increase security of the Internet infrastructure by bridging the worlds of research and operations

- Get your feedback on a few of our long-term Internet research concepts (as apposed to short-term reality)



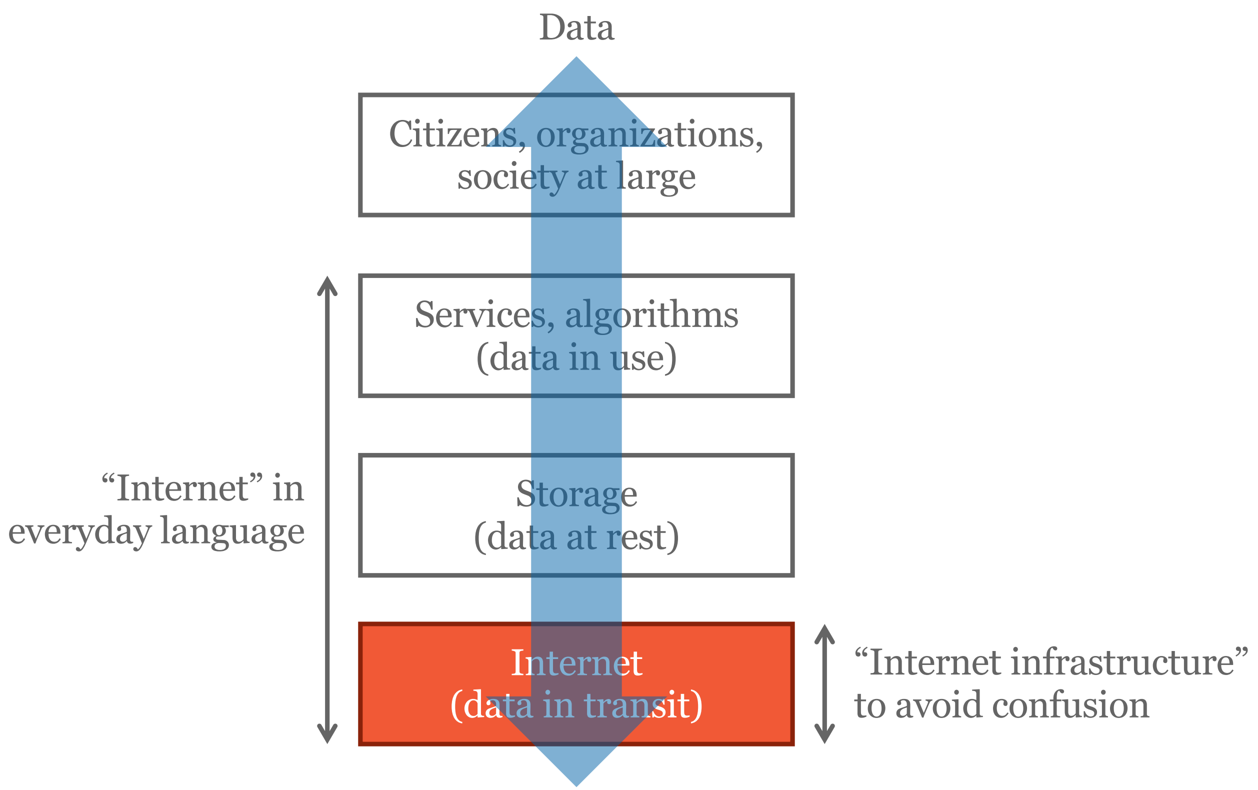
UNIVERSITY OF TWENTE.

SIDN LABS

The Internet

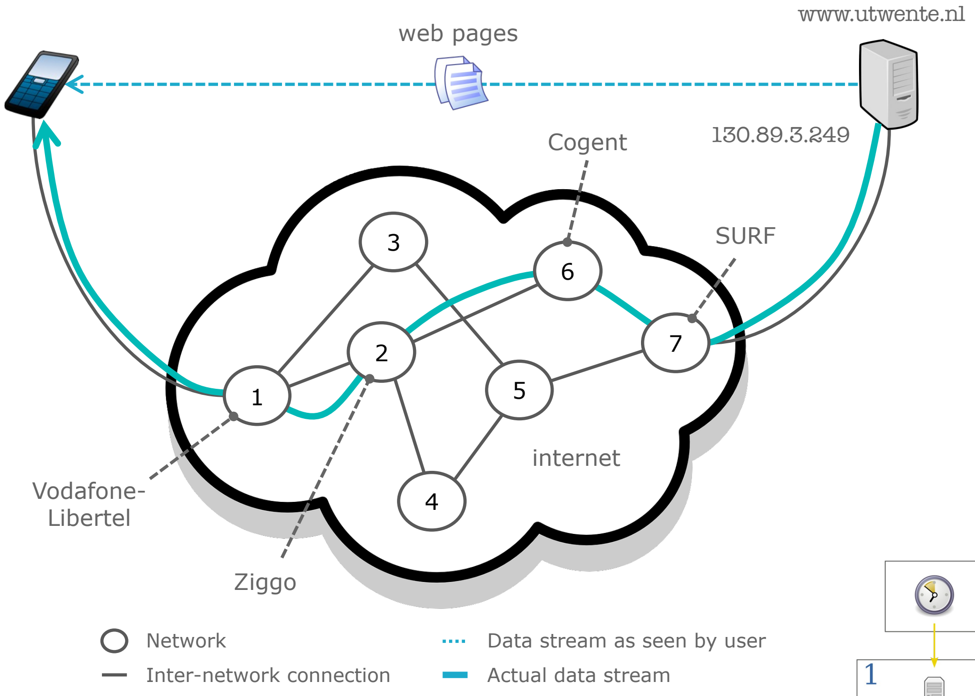
(I assume we can skip this part, but just in case)

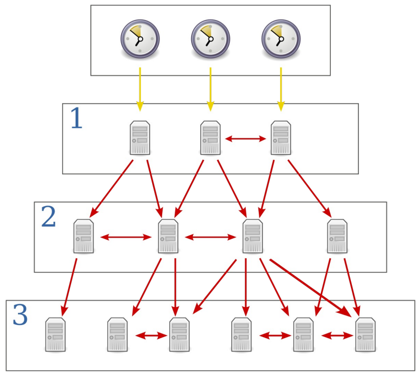
The invisible foundation of our digital world



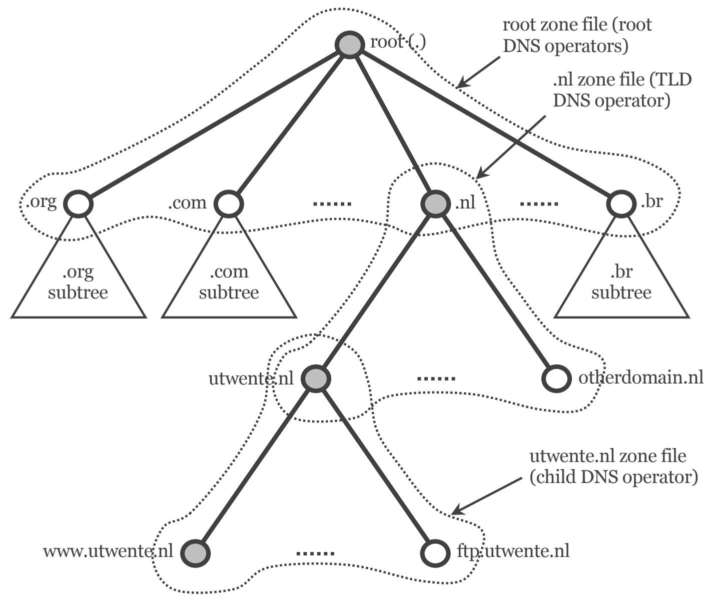
Recommended viewing: Henning Schulzrinne (Columbia University), “Networking: The Newest Civil Engineering Challenge”, SIGCOMM Lifetime Achievement Award keynote, SIGCOMM 2022, Amsterdam, August 2022, https://www.youtube.com/watch?v=5lvXIqI_mQ4

Under the hood: names, numbers, routes, time





https://en.wikipedia.org/wiki/Network_Time_Protocol



DNS naming hierarchy and DNS operators [1]

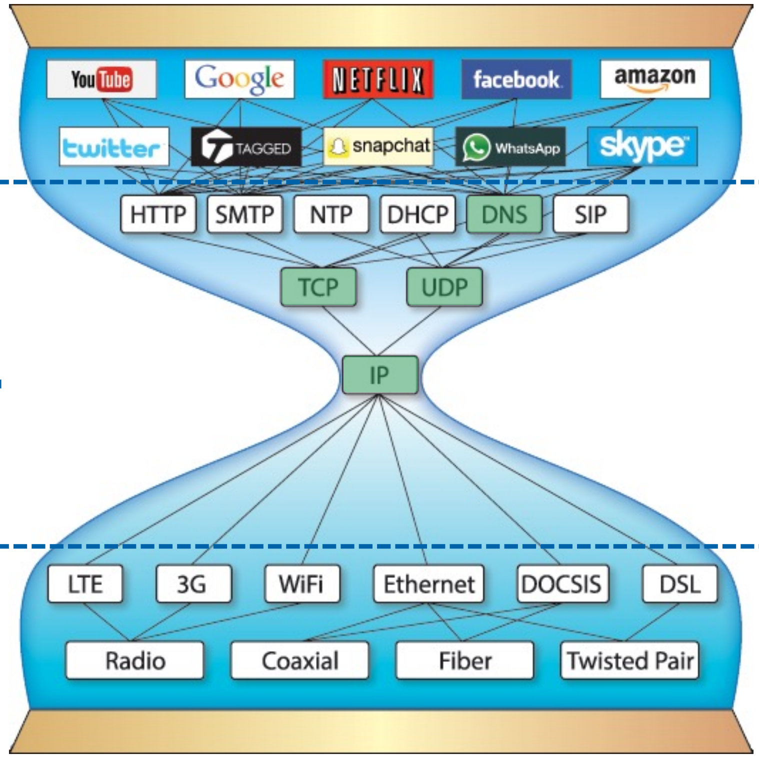
References: [1-4]

UNIVERSITY OF TWENTE. SIDN LABS

The Internet hourglass

Most people

Services



Orgs such as SIDN,
RIPE, ICANN, IETF

Names, addresses,
routes, transports

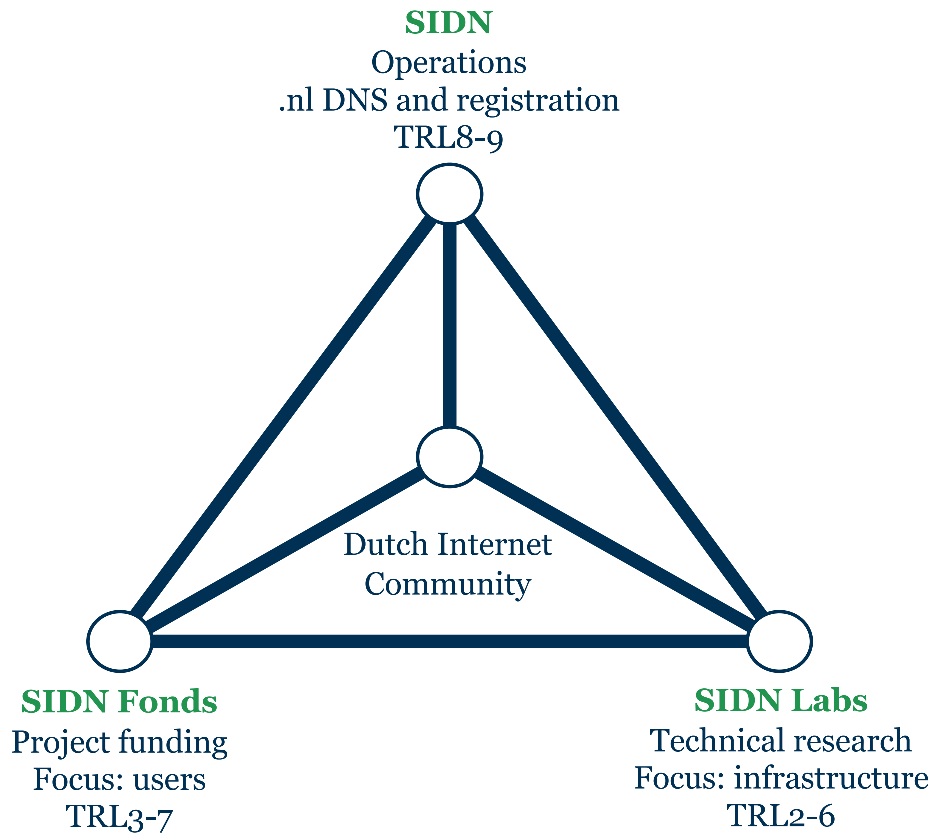
Transmission

UNIVERSITY OF TWENTE. SIDN LABS

SIDN and SIDN Labs

SIDN is the operator of the .nl top-level domain

- Not-for-profit private organization for the benefit of Dutch society (public role)
- Securely manage .nl, the Dutch national extension on the internet (63% market share)
- Critical service provider: DNS infrastructure and domain name registration (6.3M names)
- Increase the value of the Internet in the Netherlands and elsewhere



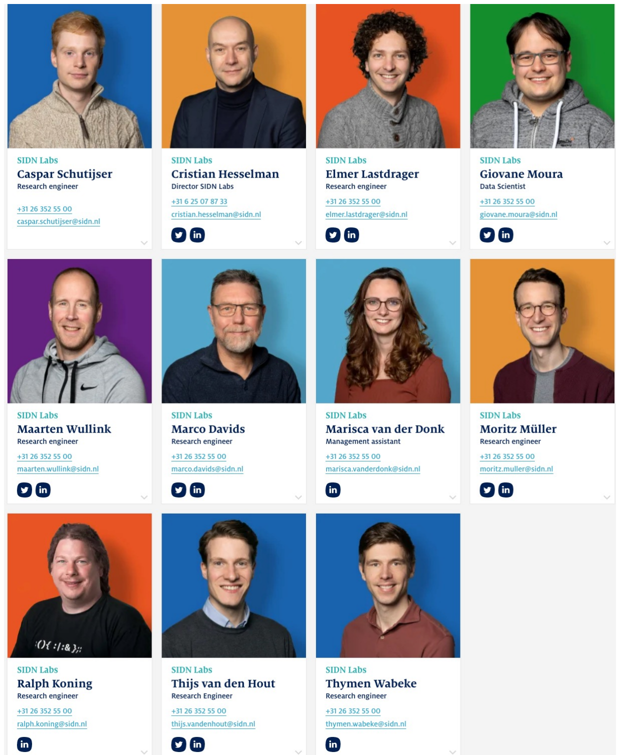
I ♥.nl

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs is the research arm of SIDN

- Goal: increase Internet infrastructure security through applied technical research, special focus on .nl and the Netherlands
- Themes: domain name security, infrastructure security, emerging Internet technologies (long term research)
- Types of work: large-scale measurement studies, system design, prototyping and evaluation, contribution to standards
- Results publicly available to advance the Internet
- Bridge between academic and operational world/industry



UNIVERSITY OF TWENTE.

SIDN LABS

Internet security: 8 case studies

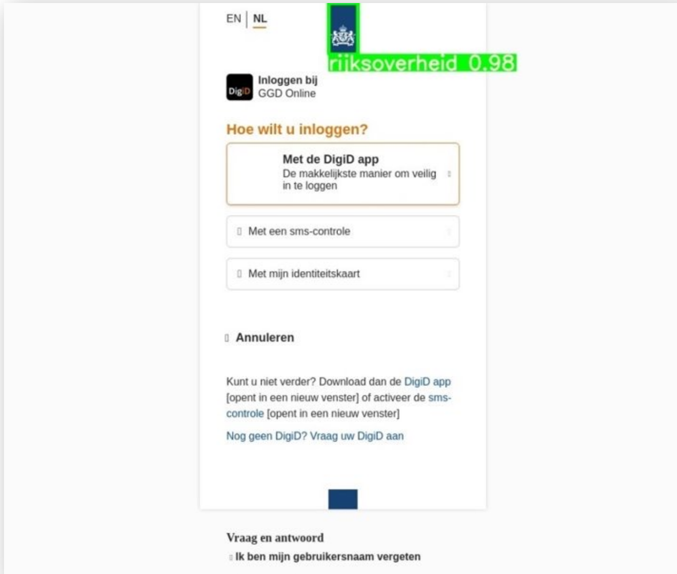
Details: www.sidnlabs.nl

Case study #1: online impersonation

- We developed Logomotive, a tool that crawls the .nl zone and detects logo usage

- Pilots with Dutch Government (DPC) and *Thuiswinkel Waarborg*

- Results:
    - Several sites removed from the zone
    - Dashboard in use at SIDN's anti-abuse desk
    - Logomotive part of SIDN's BrandGuard service
    - Peer-reviewed paper at PAM2022, blogs



Label	Full-Zone	Newly-Registered
Total	12862 (100.00%)	53
Without gov. logo (FP)	1164 (9.05%)	0 (0.00%)
With gov. logo (TP)	11698 (90.95%)	53 (100.0%)
Benign	10595 (82.37%)	32 (60.38%)
Government impersonation	151 (1.17%)	17 (32.09%)
Phishing	3 (0.02%)	3 (5.66%)
Potential threat	73 (0.57%)	9 (16.98%)
Other (false endorsements, satire, etc.)	75 (0.58%)	5 (9.43%)
Government domains	952 (7.40%)	4 (7.55%)
In portfolio	636 (4.94%)	2 (0.00%)
Not in portfolio	316 (2.46%)	2 (3.77%)
Added	109 (0.85%)	1 (1.89%)
Pending	207 (1.61%)	1 (1.89%)

UNIVERSITY OF TWENTE.

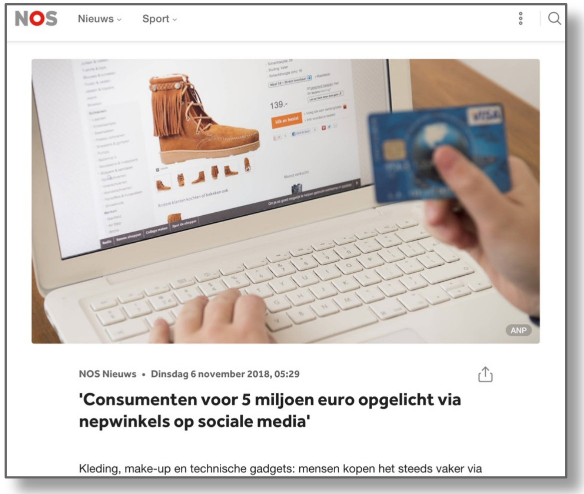
SIDN LABS

Case study #2: fake web shops

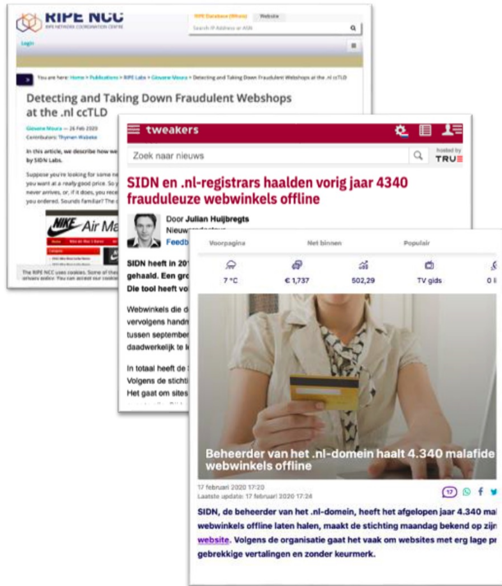
- Sales of fake shoes was a big problem in the .nl zone back in 2016-2018

- Developed tools to detect fake shops, partnered with registrars and ISC to remove them

- Results:
  - Fake shops virtually gone from the .nl zone
  - Increased online safety for users
  - Dashboard in use at SIDN's anti-abuse desk
  - Peer-reviewed paper at PAM2020, blogs



Year	Taken down
2022	199
2021	224
2020	481
2019	4,340
2018	~12,000



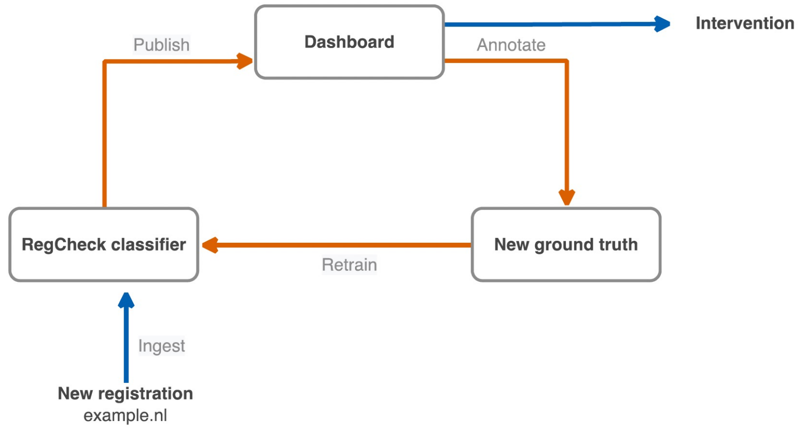
Case study #3: registration checker (RegCheck)

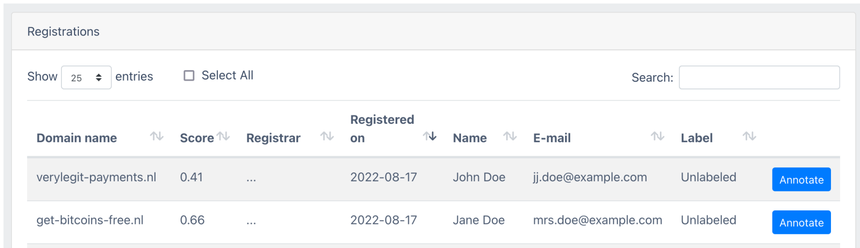
- Abuse regularly involves recent registrations

- We developed RegCheck for and with SIDN's abuse analysts to quickly inspect such domains

- Results:
  - Daily used "production prototype"
  - 3 machine learning models based on abuse reports (phishing, fake webshops, etc.)
  - User interface that gives hints about algorithm's decisions (explainable ML)

- Follow-up project with DNS Belgium (.be TLD)





Registrations

Show 25 entries ☐ Select All Search:

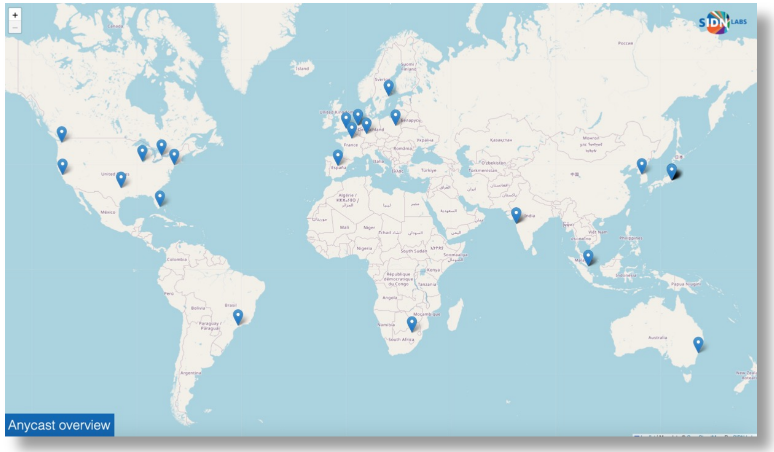
Domain name	Score	Registrar	Registered on	Name	E-mail	Label	
verylegit-payments.nl	0.41	...	2022-08-17	John Doe	jj.doe@example.com	Unlabeled	Annotate
get-bitcoins-free.nl	0.66	...	2022-08-17	Jane Doe	mrs.doe@example.com	Unlabeled	Annotate

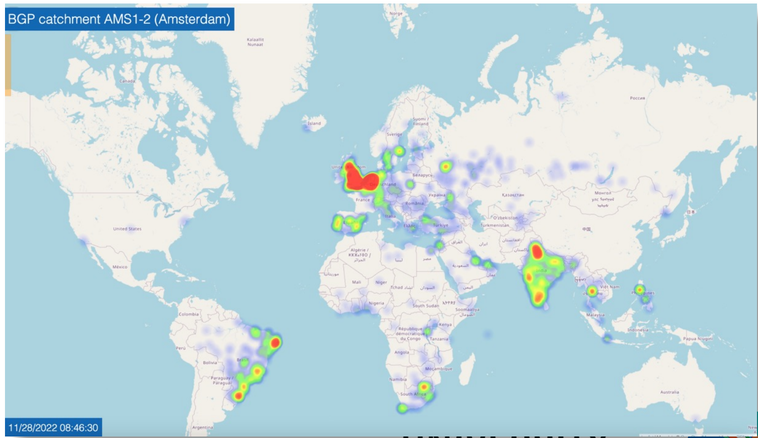
Case study #4: anycast testbed

- Send traffic to any of a set of the same nodes at different locations => increase availability

- SIDN Labs’ anycast testbed
  - 30 sites across the globe
  - Dynamically add/remove nodes
  - Catchment heatmaps
  - any.time.nl and other experimental services
  - http://dnstest.nl/anycast2020/

- Blueprint for .nl’s production anycast infrastructure, measurements with academia





UNIVERSITY OF TWENTE.

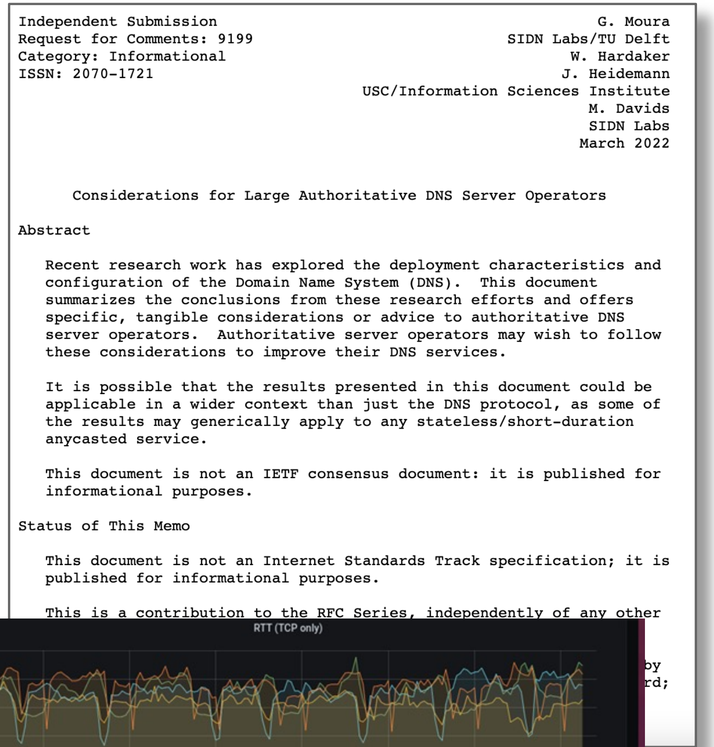
SIDN LABS

Case study #5: large-scale DNS measurements

- Help operators to make empirically-grounded DNS engineering choices (RFC9199)

- We carried out 6 studies with University of Twente and University of Southern California

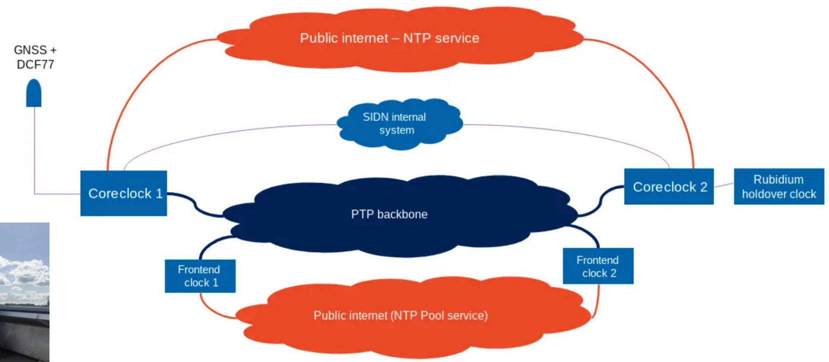
- Results:
  - Reengineering of SIDN's DNS infra
  - Recommendations for Dutch government's DNS
  - Anteater tool for DNS operators
  - 6 peer-reviewed papers, RFC9199, blogs

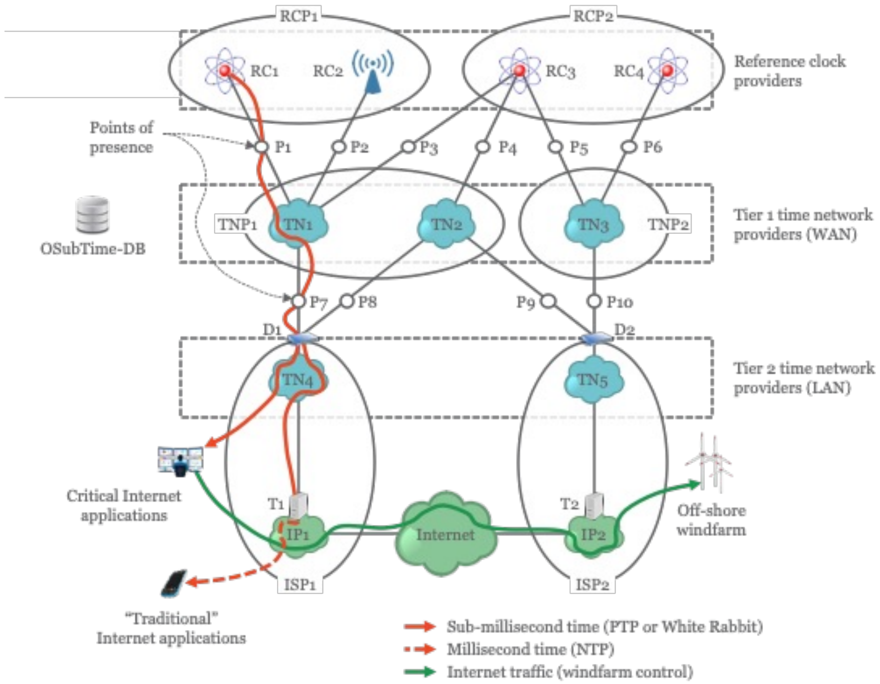


```
Independent Submission                                          G. Moura
Request for Comments: 9199                            SIDN Labs/TU Delft
Category: Informational                                      W. Hardaker
ISSN: 2070-1721                                             J. Heidemann
                                     USC/Information Sciences Institute
                                                               M. Davids
                                                               SIDN Labs
                                                              March 2022


       Considerations for Large Authoritative DNS Server Operators

Abstract

   Recent research work has explored the deployment characteristics and
   configuration of the Domain Name System (DNS).  This document
   summarizes the conclusions from these research efforts and offers
   specific, tangible considerations or advice to authoritative DNS
   server operators.  Authoritative server operators may wish to follow
   these considerations to improve their DNS services.

   It is possible that the results presented in this document could be
   applicable in a wider context than just the DNS protocol, as some of
   the results may generically apply to any stateless/short-duration
   anycasted service.

   This document is not an IETF consensus document: it is published for
   informational purposes.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This is a contribution to the RFC Series, independently of any other
```

Case study #6: TimeNL

- Accurate time is crucial for many security applications (e.g., DNSSEC, OTTP, RPKI)
- Public NTP services often ill-documented (e.g., used time sources, support levels)
- We set up TimeNL, our transparent and well-managed public NTP service
- Results: time.nl, nts.time.nl, ntp.time.nl (in Arnhem, NL), any.time.nl (anycast)
- More NTP traffic than DNS traffic for .nl ☺



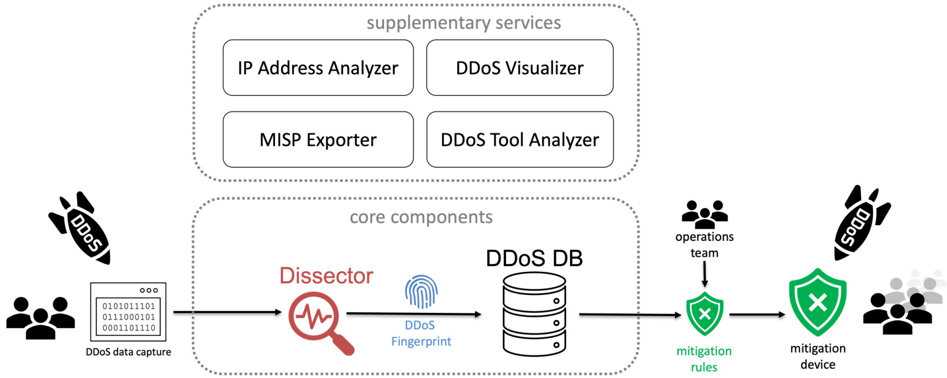


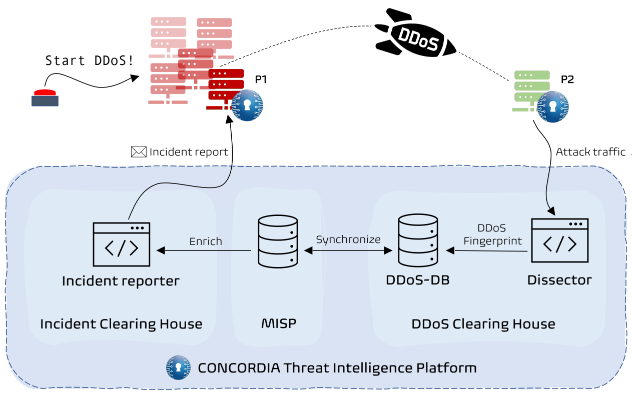
Case study #7: DDoS Clearing House

- Increase level DDoS proactiveness for (critical) service providers

- Joint work with: SURF, UT, Telecom Italia, Uni Zürich, Siemens, FORTH, NL-ADC

- Results:
  - Technical pilots in the Netherlands and Italy
  - Transition to production at NBIP (in progress)
  - Testbed, also to be used as a “cyber range”
  - Cookbook and scientific paper (in progress)

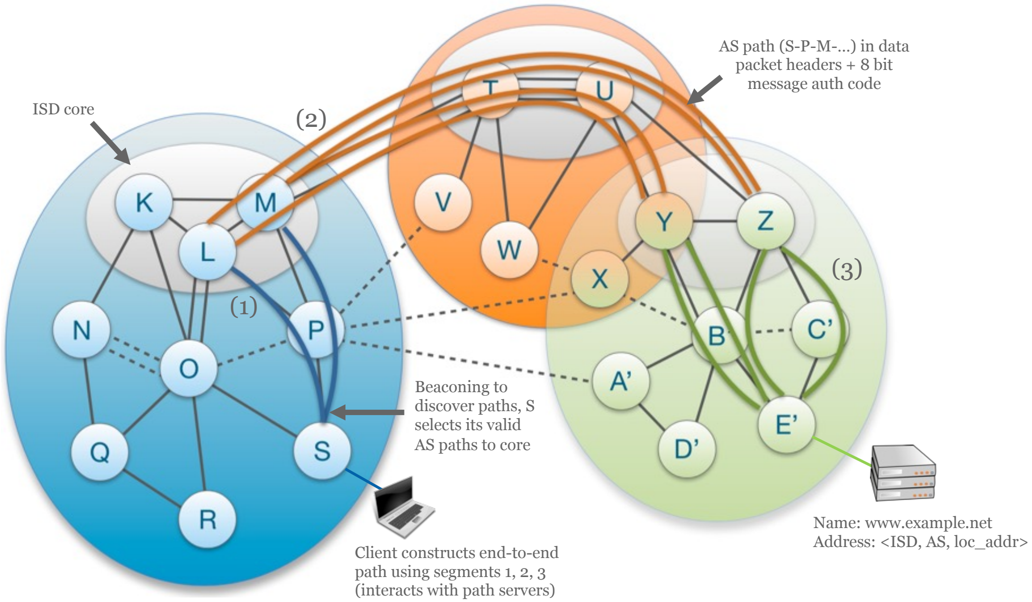




This work was funded by the European Union’s Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/

Case study #8: SCION experiments

- SCION aims to improve security of inter-domain routing and isolation of compromise
- Our goal: assess to what extent SCION concepts can improve Internet security
- Results
  - Connection to SCIONlab at ETH Zurich, P4 implementation of the SCION data plane
  - Taught students about SCION at University of Twente and University of Amsterdam
- Work in progress: SCION-NL testbed, interconnecting SURF, UvA, SIDN Labs



UNIVERSITY OF TWENTE.

SIDN LABS

Long-term Internet research

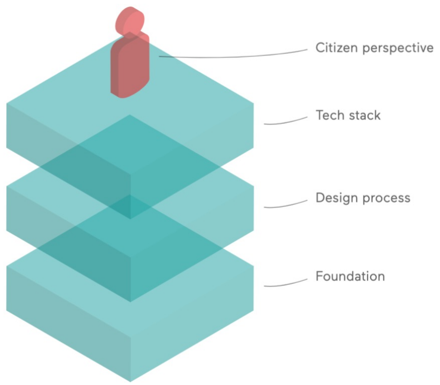
Vision: future Internet applications

https://www.youtube.com/watch?v=-7xg3DQyOXw

UNIVERSITY OF TWENTE.

SIDN LABS

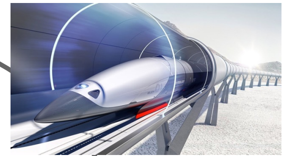
Hypothesis: require a revised networking paradigm



Increased digital autonomy
More data autonomy for users/service providers
Data-driven policy making
Joint incident analysis for network operators
Push back on Internet centralization

New levels of trust:
"Internet bill of materials": CAT
In addition to classical Internet security: CIA

Open designs:
Open source
Open hardware
Open data
Best operational practices
Legal & governance



Trusted Open Networking

UNIVERSITY OF TWENTE. SIDN LABS

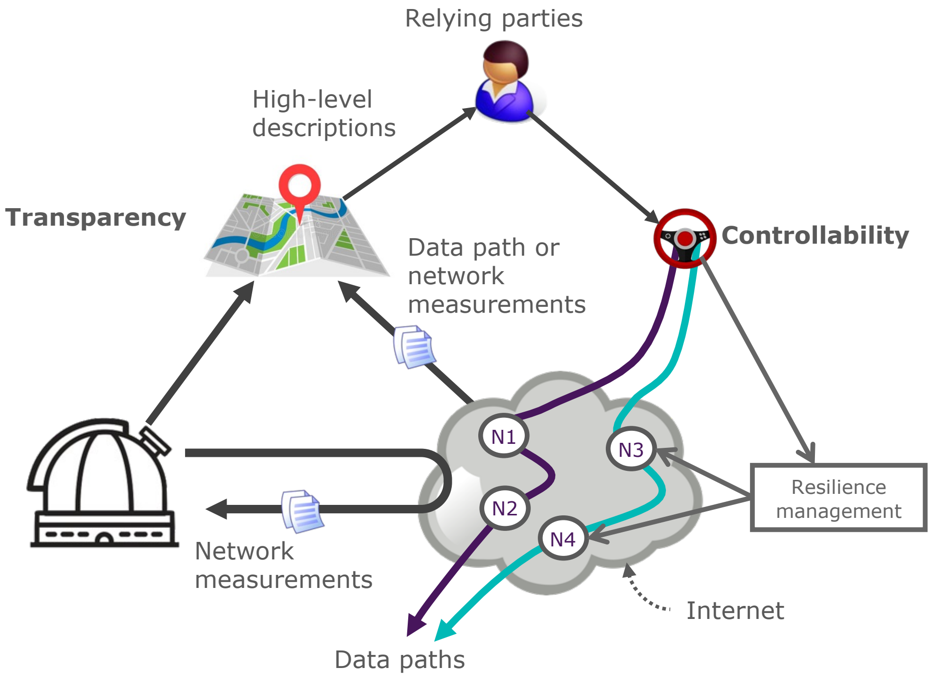
A more transparent and controllable Internet

- Transparency: logical, cryptographically verifiable data paths and "map" of the macro-level structure of the Internet

- Controllability: route data paths "around" untrusted networks or modify networks to increase resilience

- In addition to existing Internet properties, such as open, generic, distributed and decentralized

- Hypothesis: benefits critical infra, network operators, public policy makers, individuals



UNIVERSITY OF TWENTE.

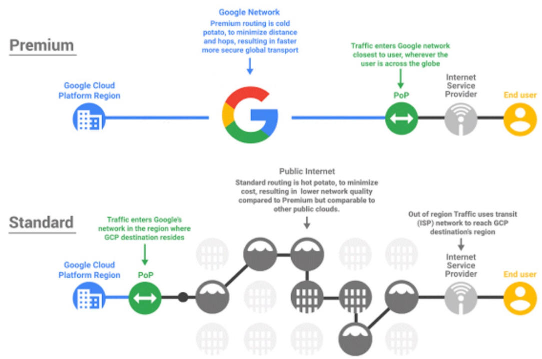
SIDN LABS

References: [6] (concept) and [7] [8] [9] [10] (potential benefits)

Network operator coalitions

- Proposed mechanism to validate value of CAT properties
  - If it works, then consider building it into the Internet's design (commitment first), unlike "clean slates"
  - Inspired by existing operator coalitions such as MANRS, NL-ADC, and SCION ISDs

- Collaborative inter-domain (security) services, such as
  - Fine-grained sharing of network properties (e.g., measurements, equipment types, jurisdiction)
  - Single-operator-like functions such as path validation, path control, packet processing (e.g., caching)



- Also helps counterbalancing hyperscalers' global WANs, such as those run by Google, Microsoft, Akamai

UNIVERSITY OF TWENTE. SIDN LABS

AS Information Service (ASIS)

- Self-hosted system for an AS to share interoperability and policy information, such as within a network operator coalition

- Disadvantages of current systems such as WHOIS/RDAP and PeeringDB:
  - Public only; lack of access control
  - Centralized
  - Rate-limited

- Result: prototype in our lab network, let us know if you'd like to work with us

Examples of ASIS information types
Technical contact information
Security contact information ("AS-wide security.txt")
Routing policies and BGP communities
Preferred peering locations and methods
Which data laws apply to the network
Information useful for path control and planning
Information about energy footprint of devices
...

UNIVERSITY OF TWENTE. SIDN LABS

CATRIN project: a small-scale responsible Internet

- www.catrin.nl: 1.9M Euros from NWO, 7 Ph.D. students, 11 partners from NL, 8 international
- Design and prototyping of network descriptions, protocol extensions, evaluation via test networks
- Developing value-added service designs for network operators and enabling them to enhance the public Internet
- Validation with organizations and individuals (e.g., via browser extensions)

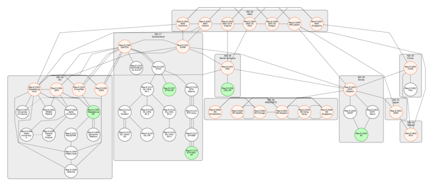
This research received funding from the Dutch Research Council (NWO) as part of the CATRIN project

Further strengthening NL as an Internet hub

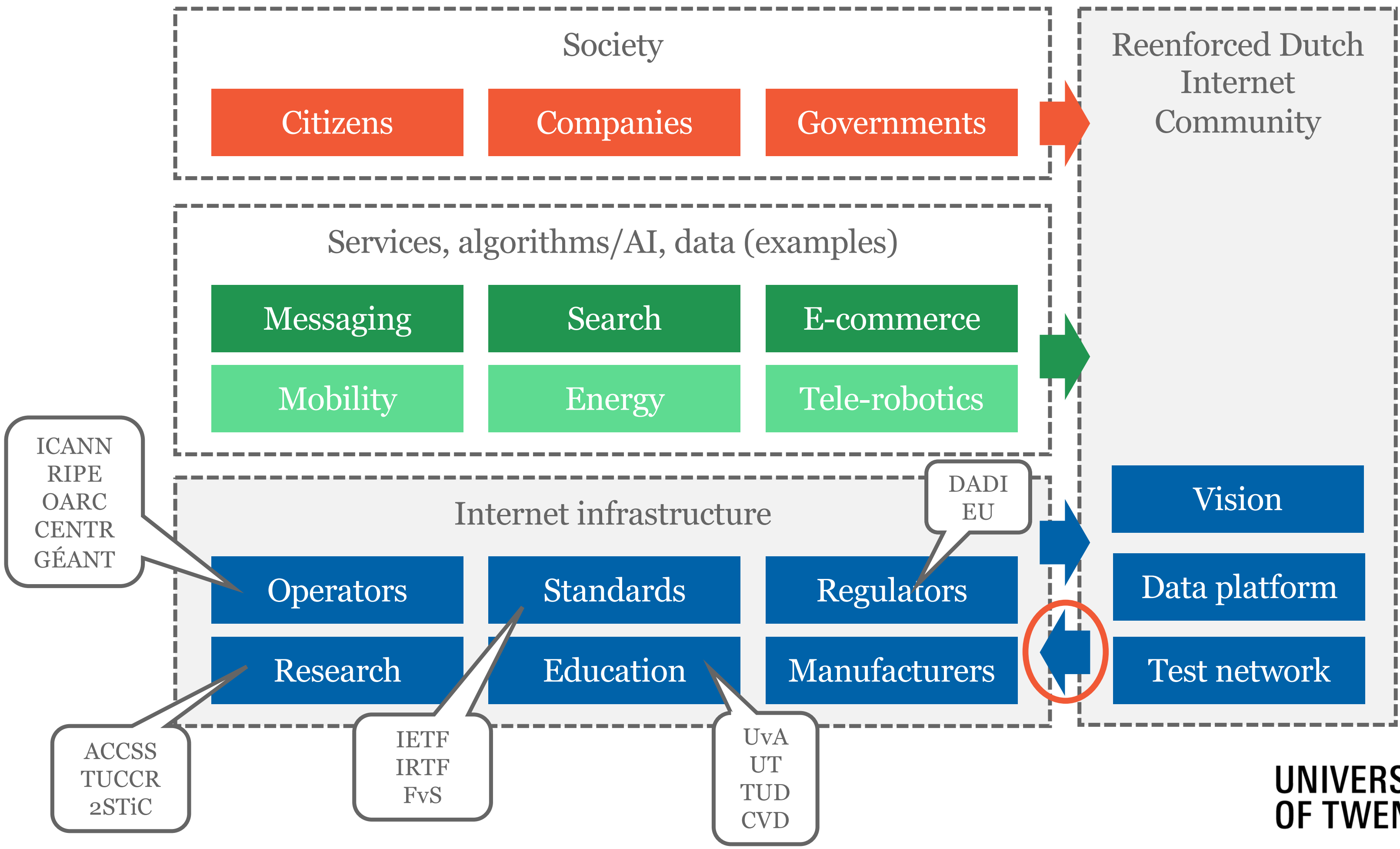
- Vision of the Internet of 2040 and its security developed by a strong, organized tech community that combines research, policy and operations

- Open federated measurement infrastructure for the ongoing analysis of Internet infrastructure robustness (cables, routing, DNS, time) with a multidisciplinary user community

- Open federated experimental network to develop, evaluate and translate new security concepts into solutions based on a “commitment first” principle

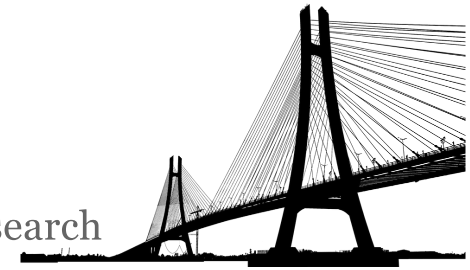


Goal: reenforced Dutch Internet community



UNIVERSITY OF TWENTE.

SIDN LABS



Lessons learned in crossing the bridge

UNIVERSITY OF TWENTE.

SIDN LABS

A few lessons learned about technology transfer

- Define problems and validate preliminary results with (external) users/domain experts
- Set up long-term relationships with academia and research labs (e.g., by seconding staff)
- Combine scientists, engineers, and operators (in one team/under one roof if possible)
- Set up a dedicated (joint) research network, such as for measurements, prototypes, pilots
- Make results generic and public, apply them yourself ("eat your own dogfood")
- Keep in mind that peer-reviewed publications are a means, not a goal

Volg ons

SIDN.nl

@SIDN

SIDN

Q&A and discussion

www.sidnlabs.nl | stats.sidnlabs.nl

Cristian Hesselman
Director of SIDN Labs
cristian.hesselman@sidn.nl
@hesselma@mastodon.social
+31 6 25 07 87 33

References

1. D. McPherson, "Routing without rumor: securing the Internet routing system", Global Commission on the Stability of Cyberspace's Cyberstability Paper Series, Dec. 2021, https://hcss.nl/report/routing-without-rumor-securing-the-internets-routing-system/
2. T. Arnold, E. Gurmericliler, G. Essig, A. Gupta, M. Calder, V. Giotsas, and E. Katz-Bassett. 2020. (How Much) Does a Private WAN Improve Cloud Performance?. In Proceedings of IEEE INFOCOM
3. P. Gigis, M. Calder, L. Manassakis, G. Nomikos, V. Kotronis, X. Dimitropoulos, E. Katz-Bassett, and G. Smaragdakis, "Seven Years in the Life of Hypergiants' off-Nets", ACM SIGCOMM, 2021.
4. G. Huston, "The Death of Transit?", RIPE Labs, Oct 2016, https://labs.ripe.net/author/gih/the-death-of-transit/
5. SSAC Briefing on Routing Security, June 2022, https://www.icann.org/en/system/files/files/sac-121-en.pdf
6. C. Hesselman, R.Holz, P. Grosso, "Three more things you need to know about the Responsible Internet", June 2021, https://www.sidnlabs.nl/en/news-and-blogs/three-more-things-you-need-to-know-about-the-responsible-internet
7. J. Chromik, "Process-aware SCADA traffic monitoring: a local approach", Ph.D. thesis, University of Twente, July 2019
8. Kc Claffy, D. Clark, "Challenges in measuring the internet for the public interest", Journal of Information Policy, Volume 12, 2022, https://par.nsf.gov/biblio/10356826-challenges-measuring-internet-public-interest
9. R. Sommese, M. Jonker, J. van der Ham, and G. C. M. Moura "Assessing e-Government DNS Resilience", 2022 International Conference on Network and Service Management (CNSM 2022), Thessaloniki, Greece
10. J. Ceron, L. Bertholdo, C. Hesselman, G. Moura, "Mapping concentrations of device vendors in IXPs", Dec 2020, https://www.sidnlabs.nl/en/news-and-blogs/mapping-concentrations-of-device-vendors-in-ixps
11. A. Davidson, M. Frei, M. Gartner, H. Haddadi, J. Subirà Nieto, A. Perrig, P. Winter, F. Wirz, "Tango or Square Dance? How Tightly Should we Integrate Network Functionality in Browsers?"
12. NCTV, "Overzicht vitale processen", https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

UNIVERSITY OF TWENTE. SIDN LABS