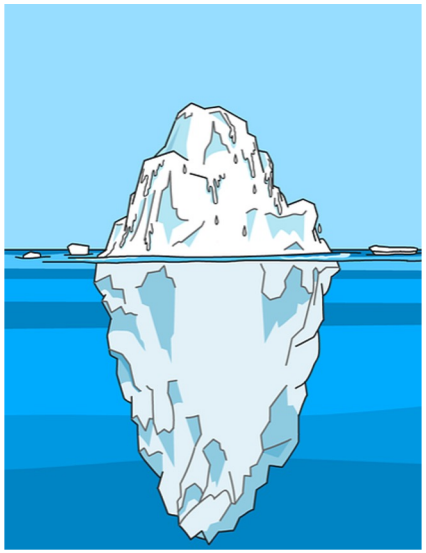
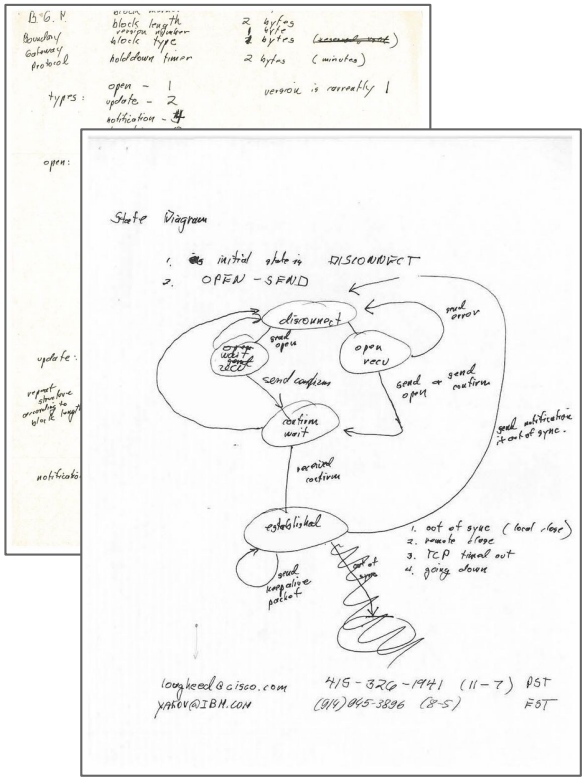


Experiences in increasing Internet security through research

Cristian Hesselman

Risk and Resilience Festival
University of Twente, Nov 11, 2022

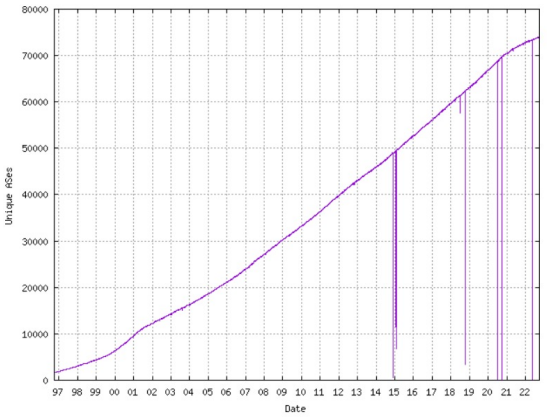
The early days of the Internet



https://computerhistory.org/blog/the-two-napkin-protocol/

Birthplace of the Internet
UCLA, Sep 2017

The ARPANET in December 1969

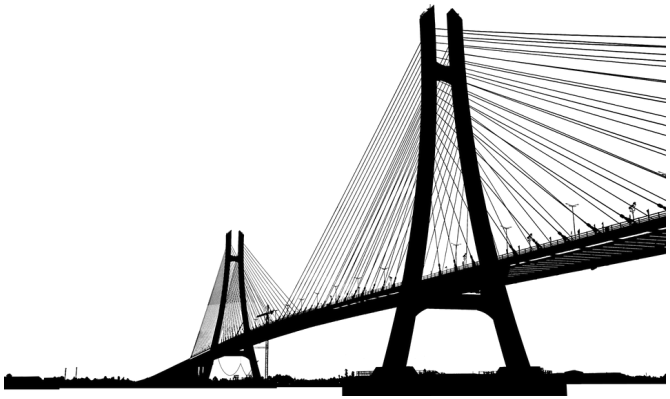


https://www.cidr-report.org/as2.0/

SDN LABS

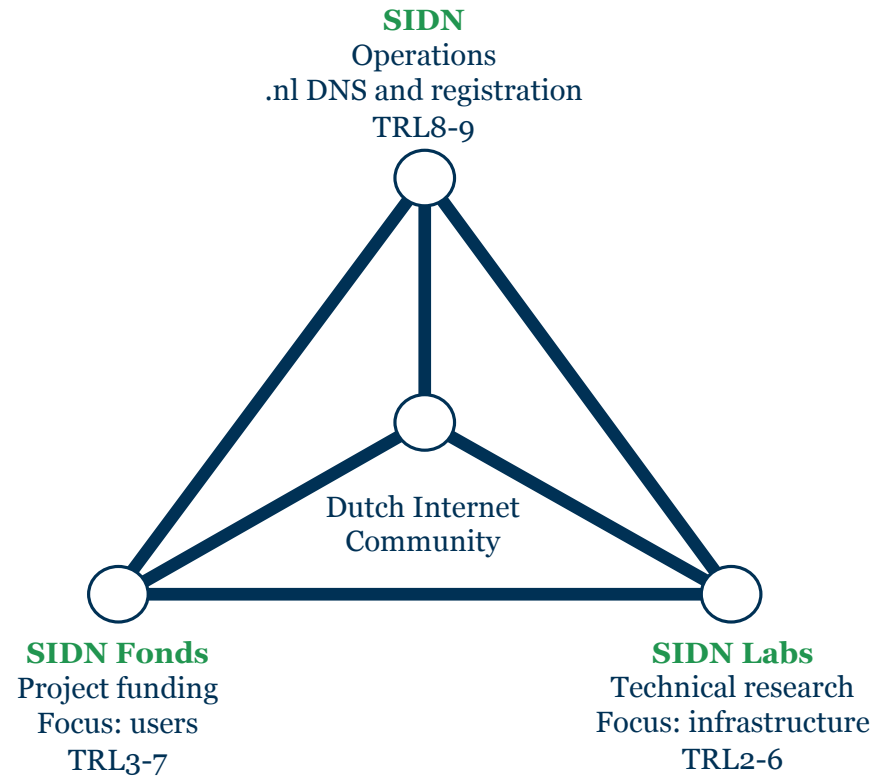
Today's goal

- Showcase how we increase Internet security based on research and share lessons learned
- Learn from each other by discussing your experience in this space
- Targeted result: new insights in how to use research in your daily work



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

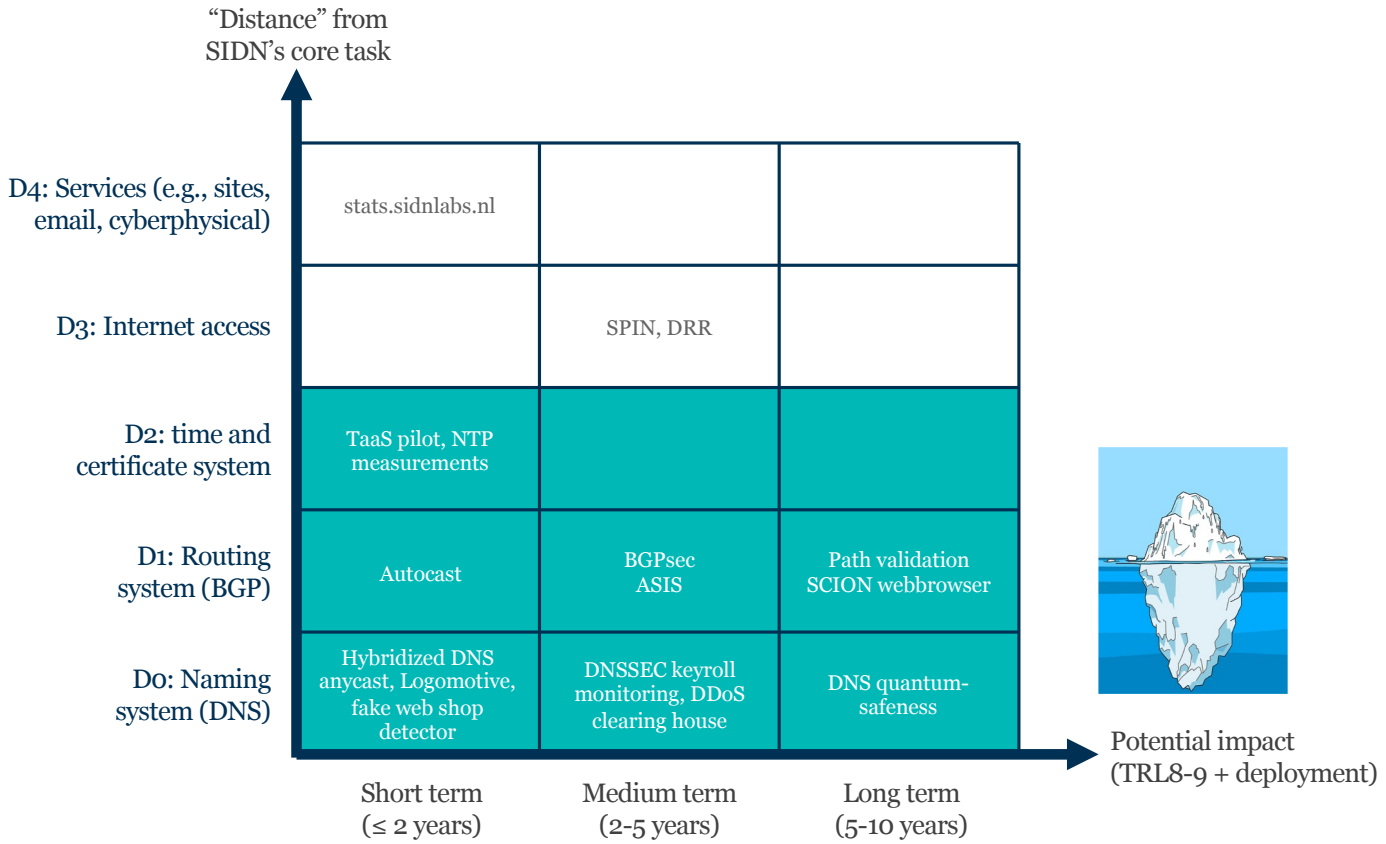
- Not-for-profit private organization for the benefit of Dutch society
- Securely manage .nl, the Dutch national extension on the internet (63% market share)
- Critical service provider: DNS infrastructure and domain name registration (6.3M names)
- Increase the value of the Internet in the Netherlands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



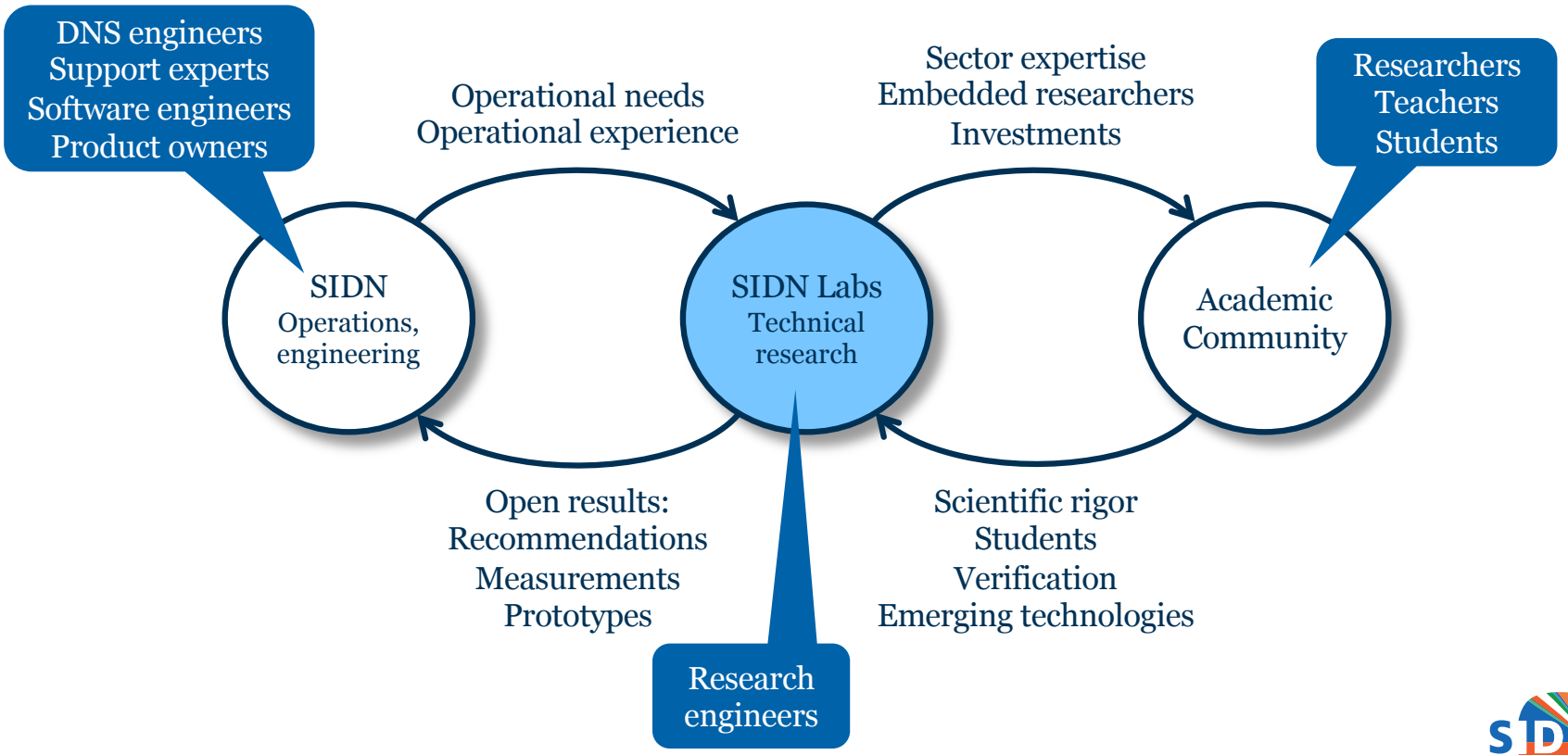
I ♥ .nl

SIDN LABS

SIDN Labs research space for more Internet security

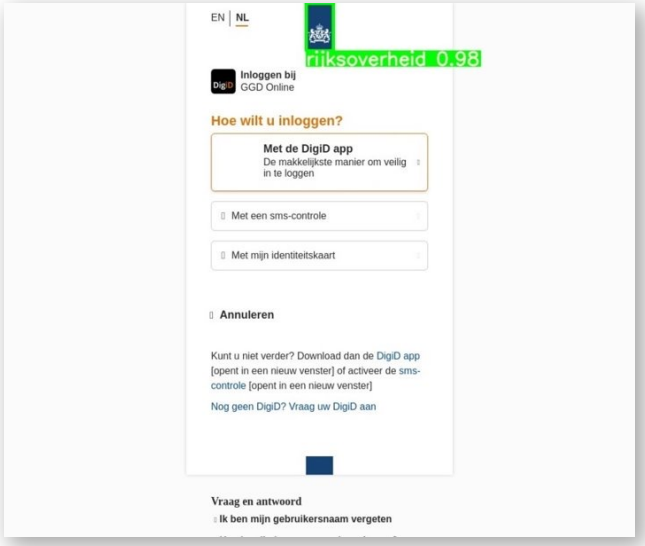


Our way of working



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%)

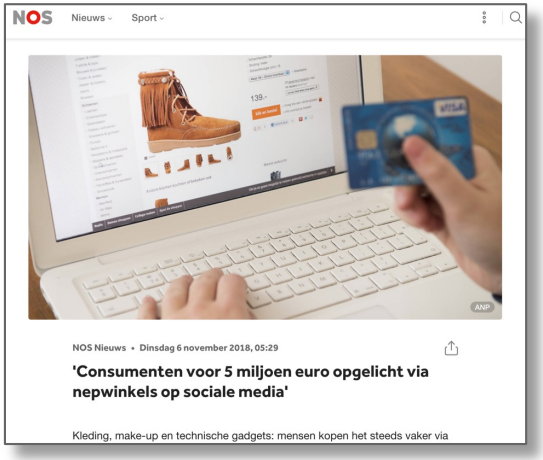
Case study #2: fake web shops

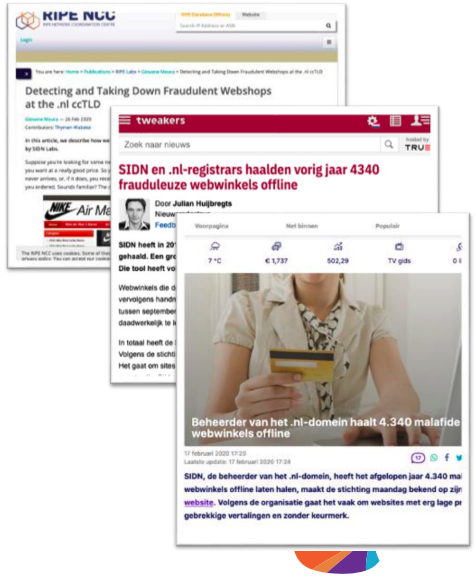
- Sales of fake shoes was a big problem in the .nl zone back in 2016-2018

- 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

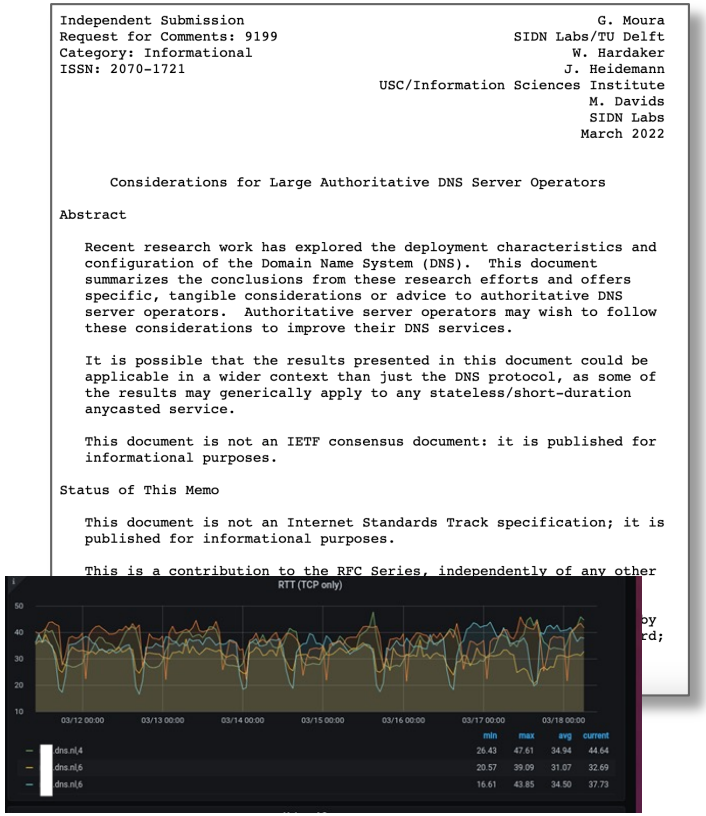
Year	Taken down
2022	192
2021	224
2020	481
2019	4,340
2018	~12,000





Case study #3: 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
Request for Comments: 9199
Category: Informational
ISSN: 2070-1721

G. Moura
SIDN Labs/TU Delft
W. Hardaker
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

Selected lessons learned

- Combine scientists, engineers, and operators (in one team/under one roof)
- Set up a dedicated research network, such as for measurements, prototypes, pilots
- Define problems and validate preliminary results with (external) users/domain experts
- Articulate a clear long-term research goal and a few focused research areas
- Set up long-term relationships with selected universities (e.g., by seconding staff)
- 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

SDN LABS

What are your experiences in using research to address your organization's security challenges?

Volg ons

SIDN.nl

@SIDN

SIDN

Q&A

www.sidnlabs.nl | stats.sidnlabs.nl

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

Member of TUCCR.

SIDN LABS