Faculty of Electrical Engineering, Computer Science, and Mathematics

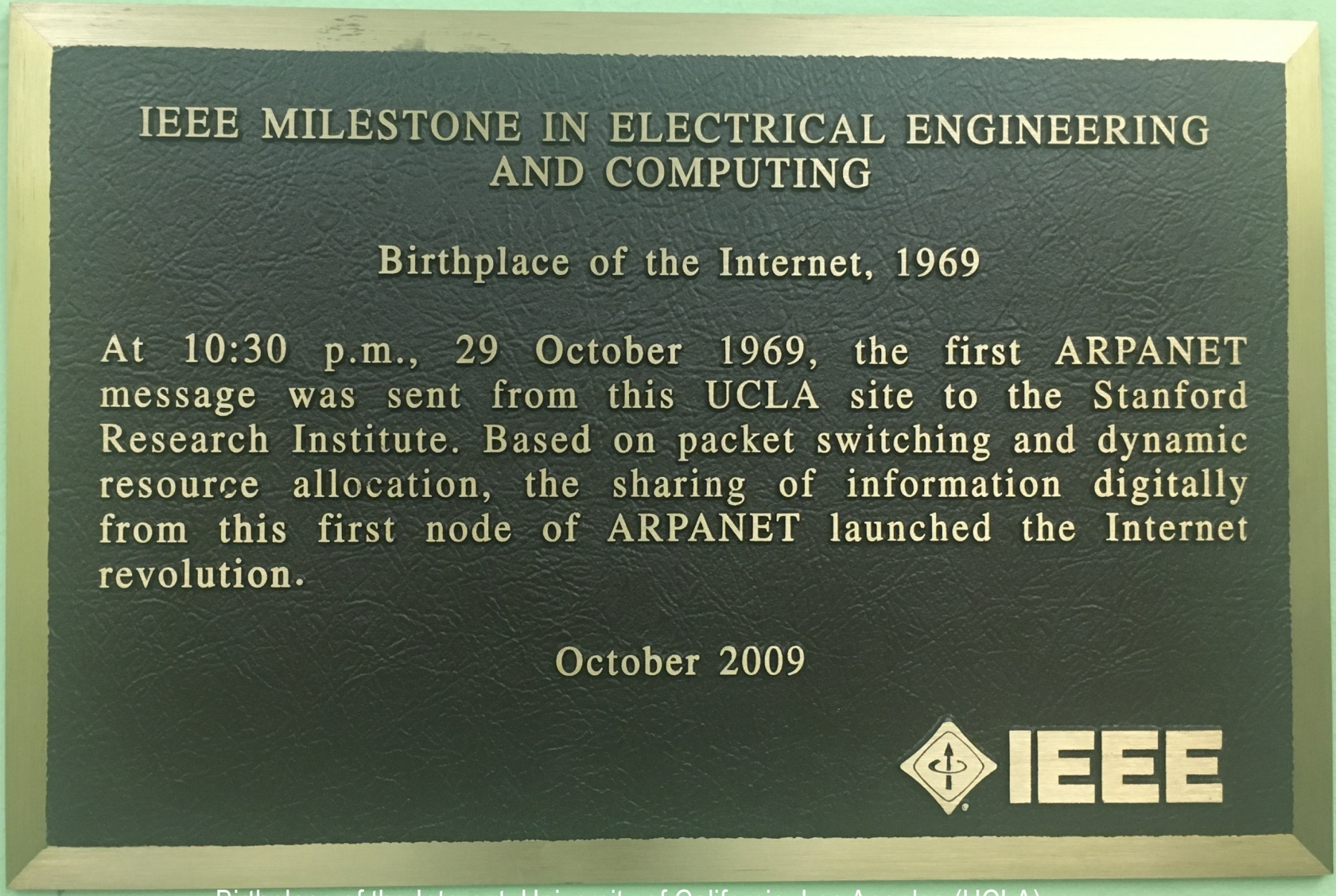
TRUST IN TRANSIT: INTERNET SECURITY FOR THE NEXT GENERATION

INAUGURAL LECTURE

PROF.DR.IR. CRISTIAN HESSELMAN

FRI NOV 3, 2023

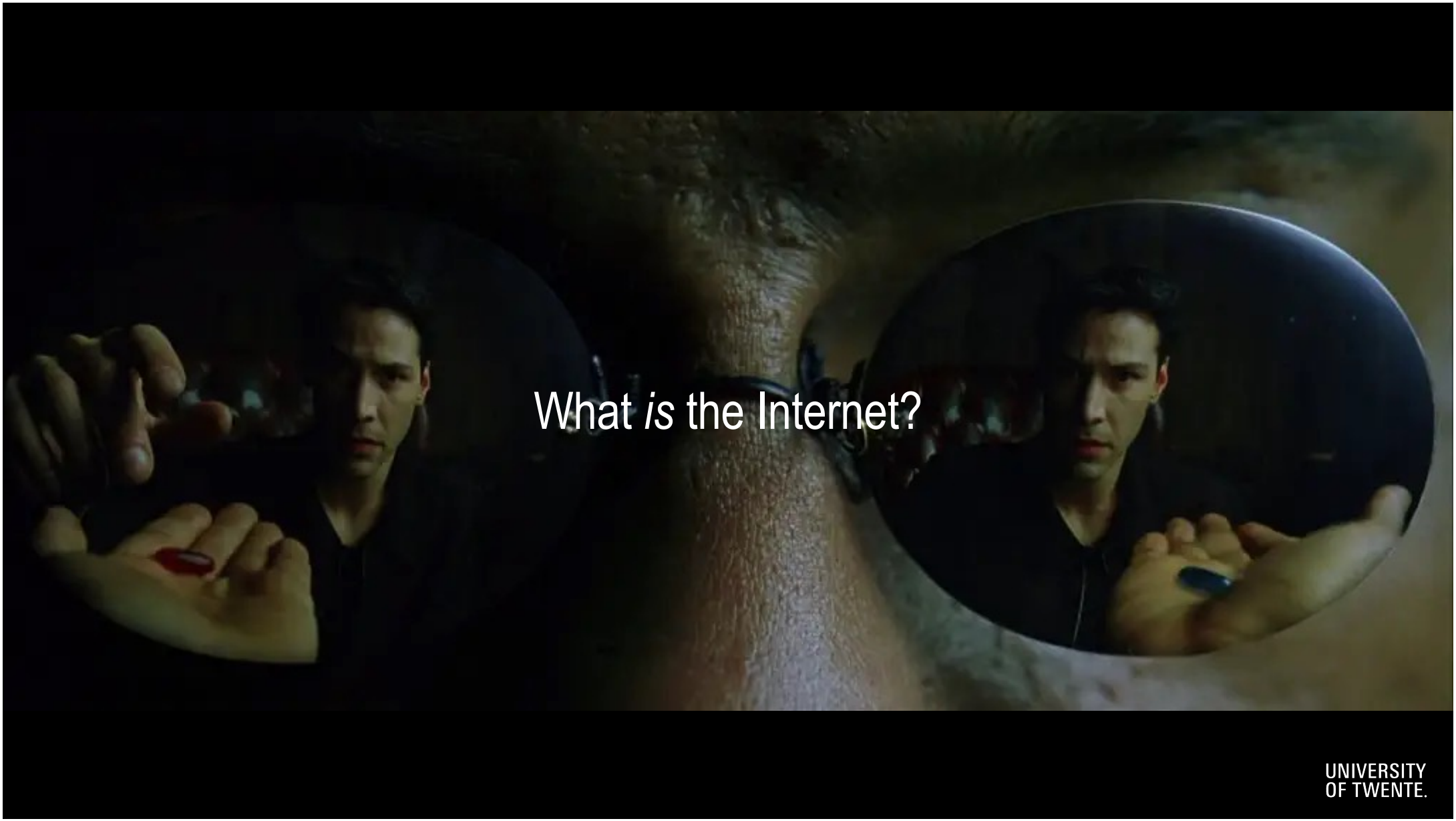
TUCCR. DACS SIDN LABS UNIVERSITY OF TWENTE.



Birthplace of the Internet, University of California, Los Angeles (UCLA)

TODAY'S OBJECTIVE

- Help you explain how the Internet works, so you can impress others :-)
- Outline my research field "Trusted Open Networking" in the form of 5 case studies
- Look ahead at future challenges

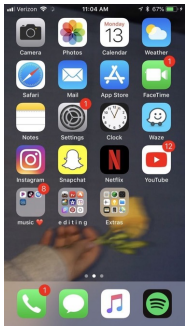


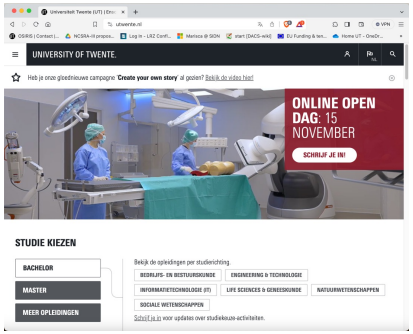
UNIVERSITY
OF TWENTE.

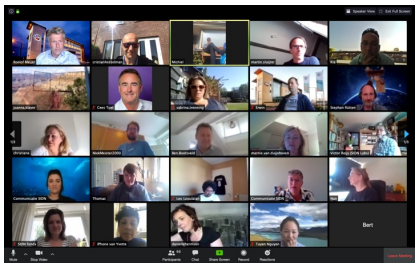
https://www.youtube.com/watch?v=xqvna9t9uB4

The Internet in the 1990s

TODAY'S DEPENDENCE ON THE INTERNET



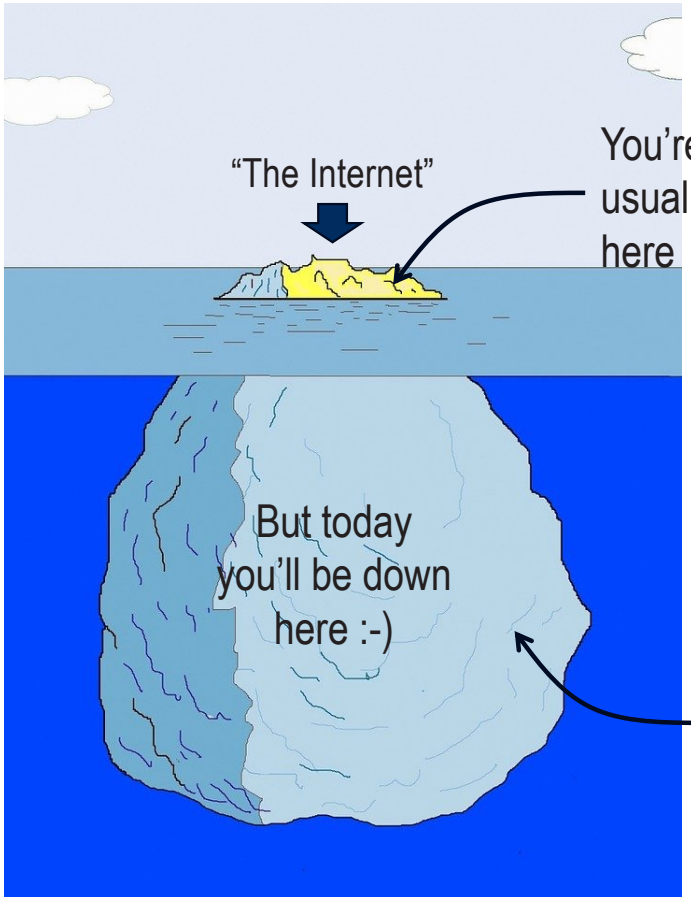




5G

UNIVERSITY OF TWENTE.

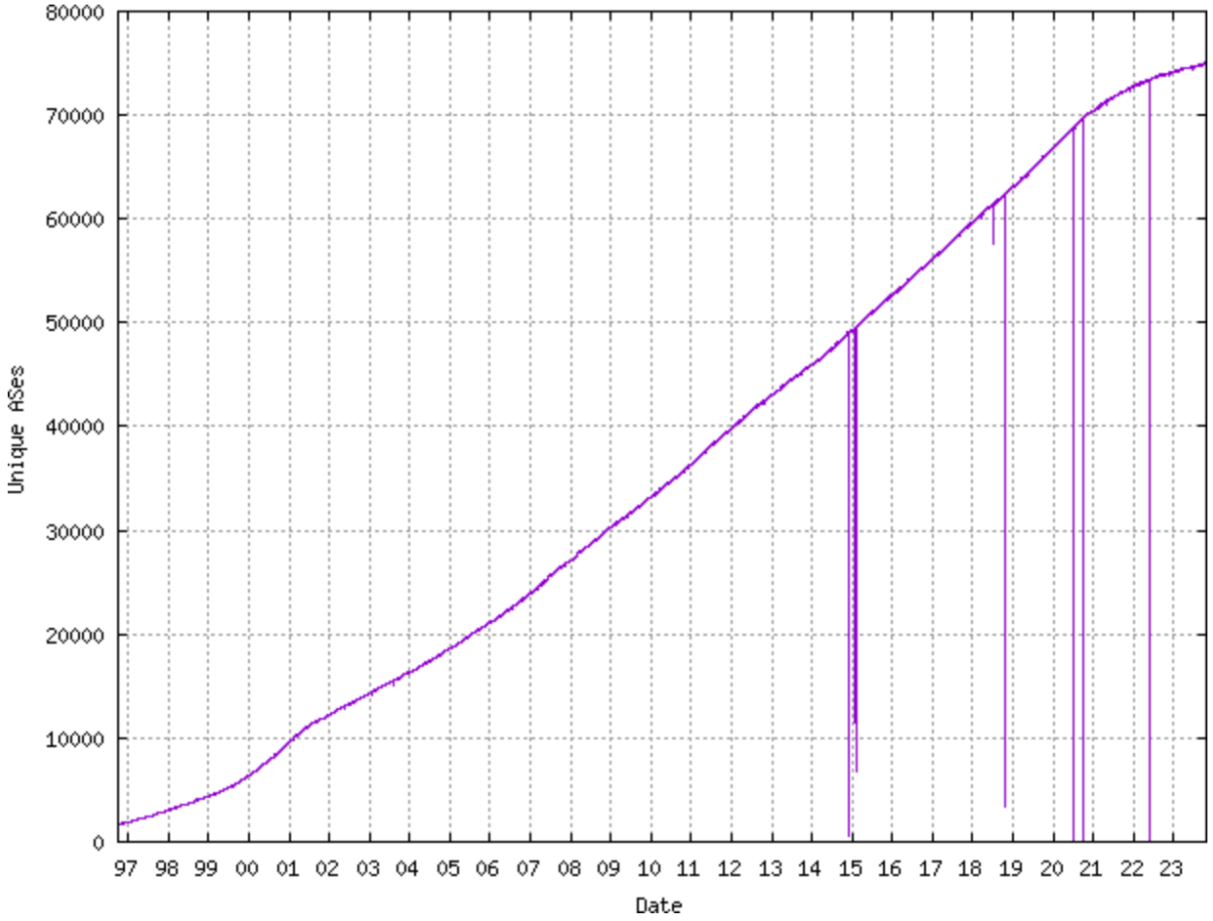
BUT THAT'S JUST THE TIP OF THE ICEBERG



Barrett Lyon / The Opte Project
Visualization of the routing paths of the Internet
https://www.opte.org/the-internet

A complex and ever-changing network of networks (hence *inter*net)

INTERNET GROWTH 1996-2023



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

UNIVERSITY
OF TWENTE.

THE TANGIBLE INTERNET IN THE 1960S/70S

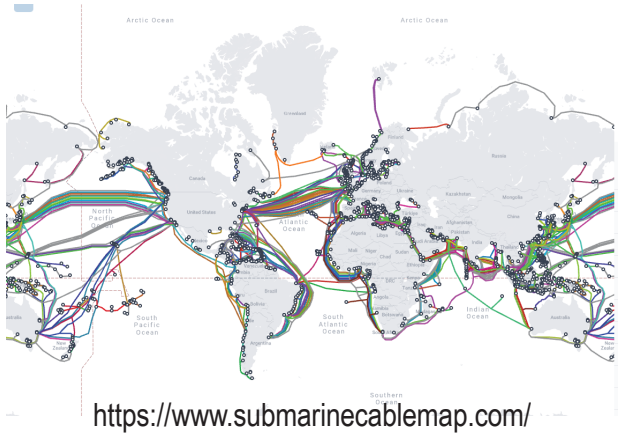
Birthplace of the Internet @UCLA

UNIVERSITY
OF TWENTE.

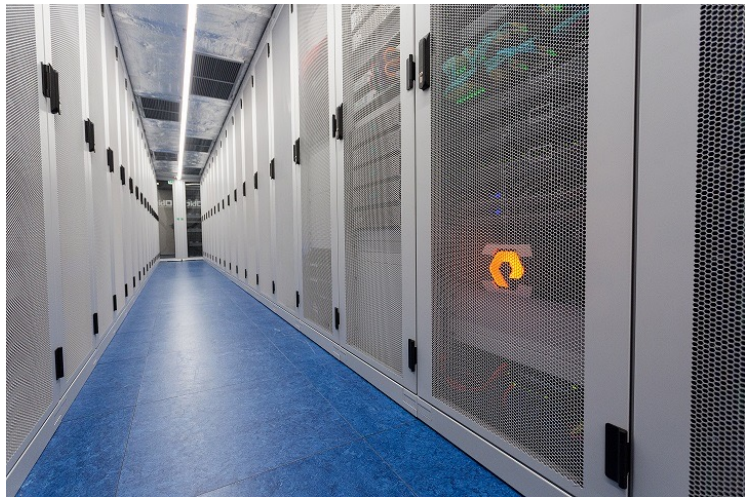
THE TANGIBLE INTERNET TODAY

Cisco router

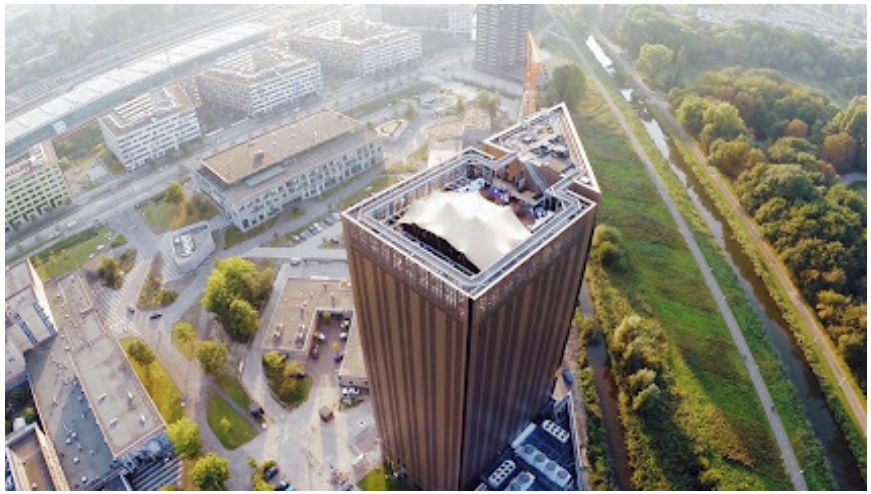
GL-iNet mini router



https://www.submarinecablemap.com/



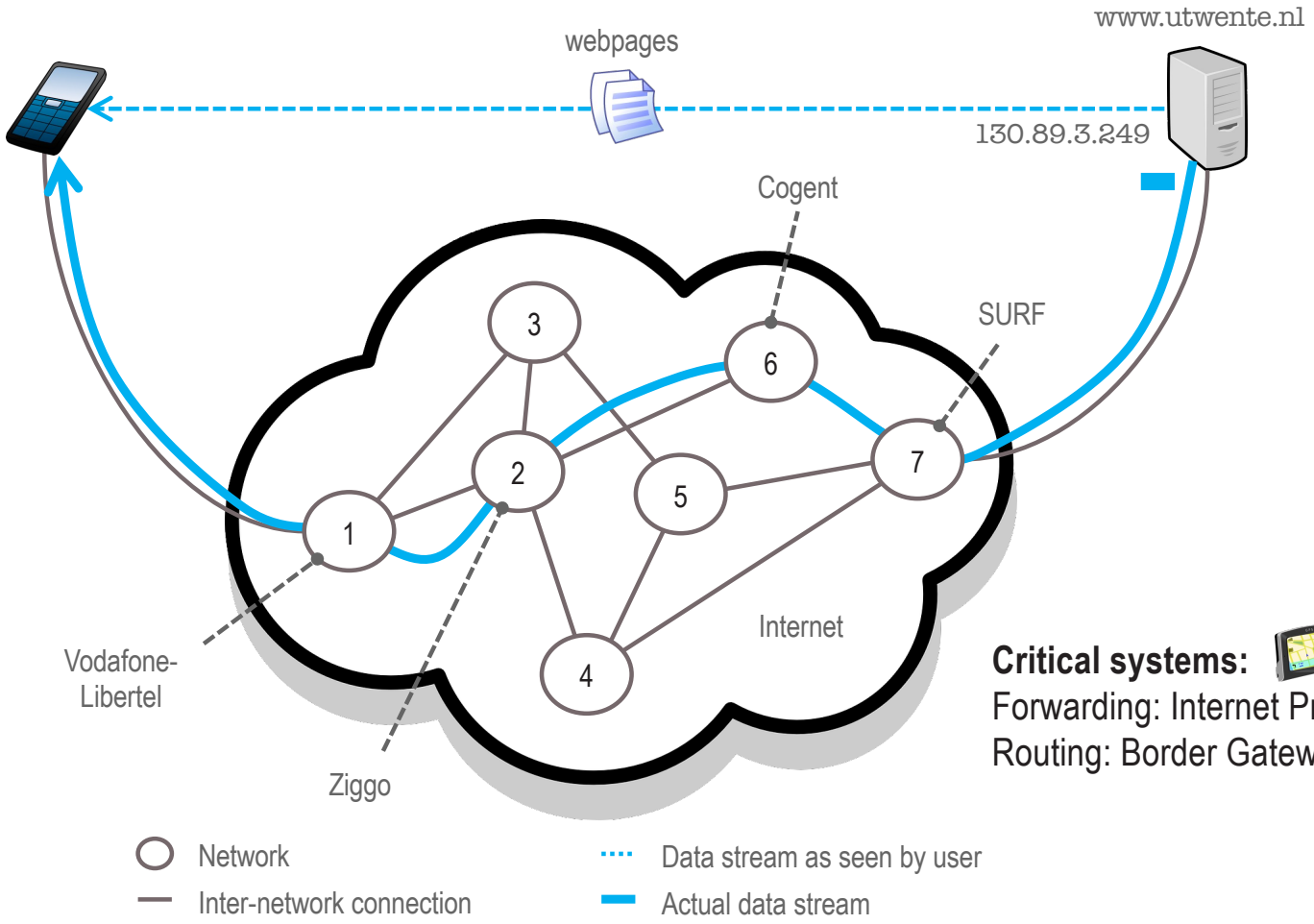
BIT data center, Ede



Data Tower, Amsterdam Science Park

UNIVERSITY
OF TWENTE.

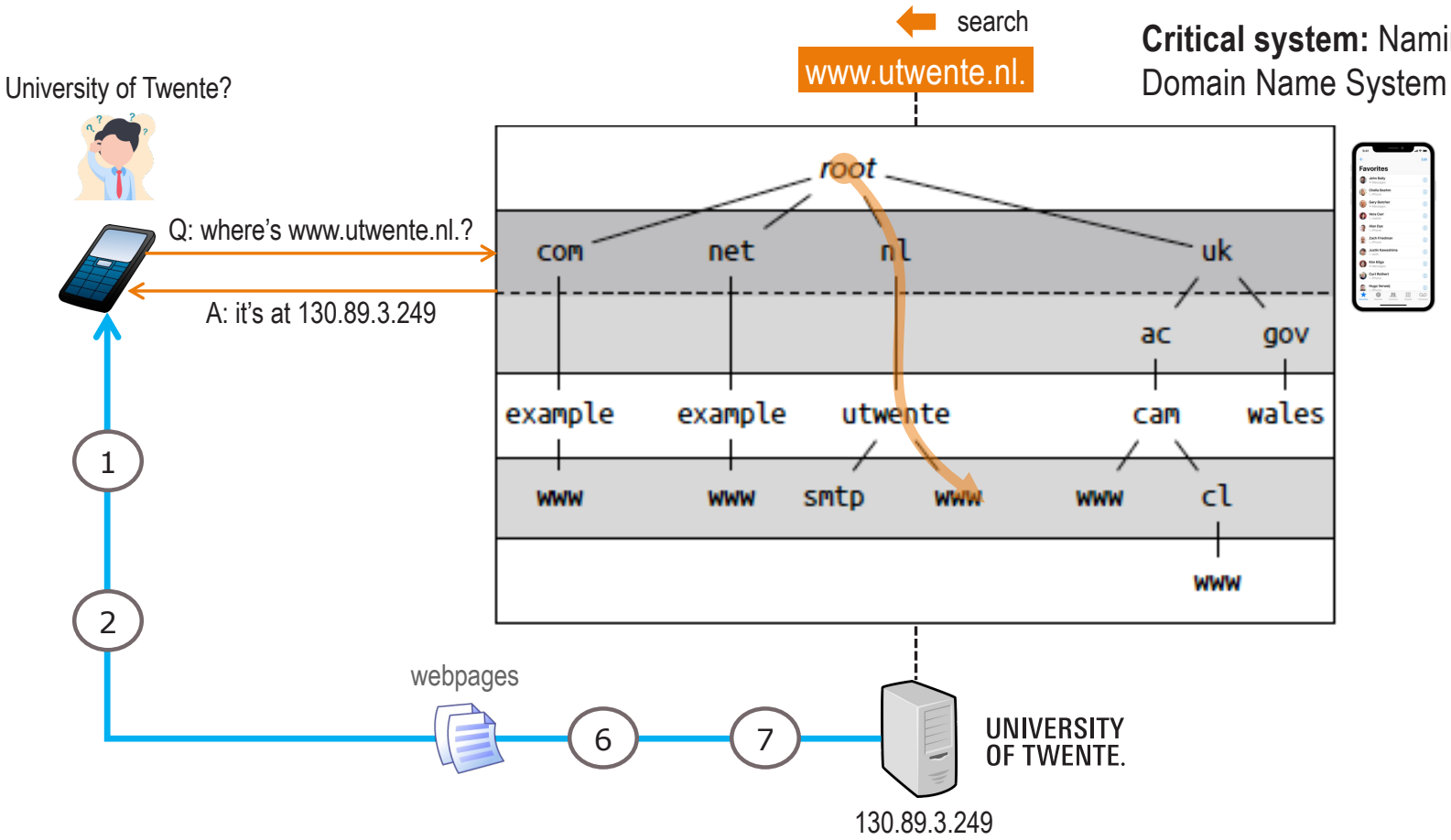
TRANSPORT ACROSS NETWORKS AND OPERATORS



Critical systems:
Forwarding: Internet Protocol (IP)
Routing: Border Gateway Protocol (BGP)

[Shosh78] [ISOC20] [Lehr19]

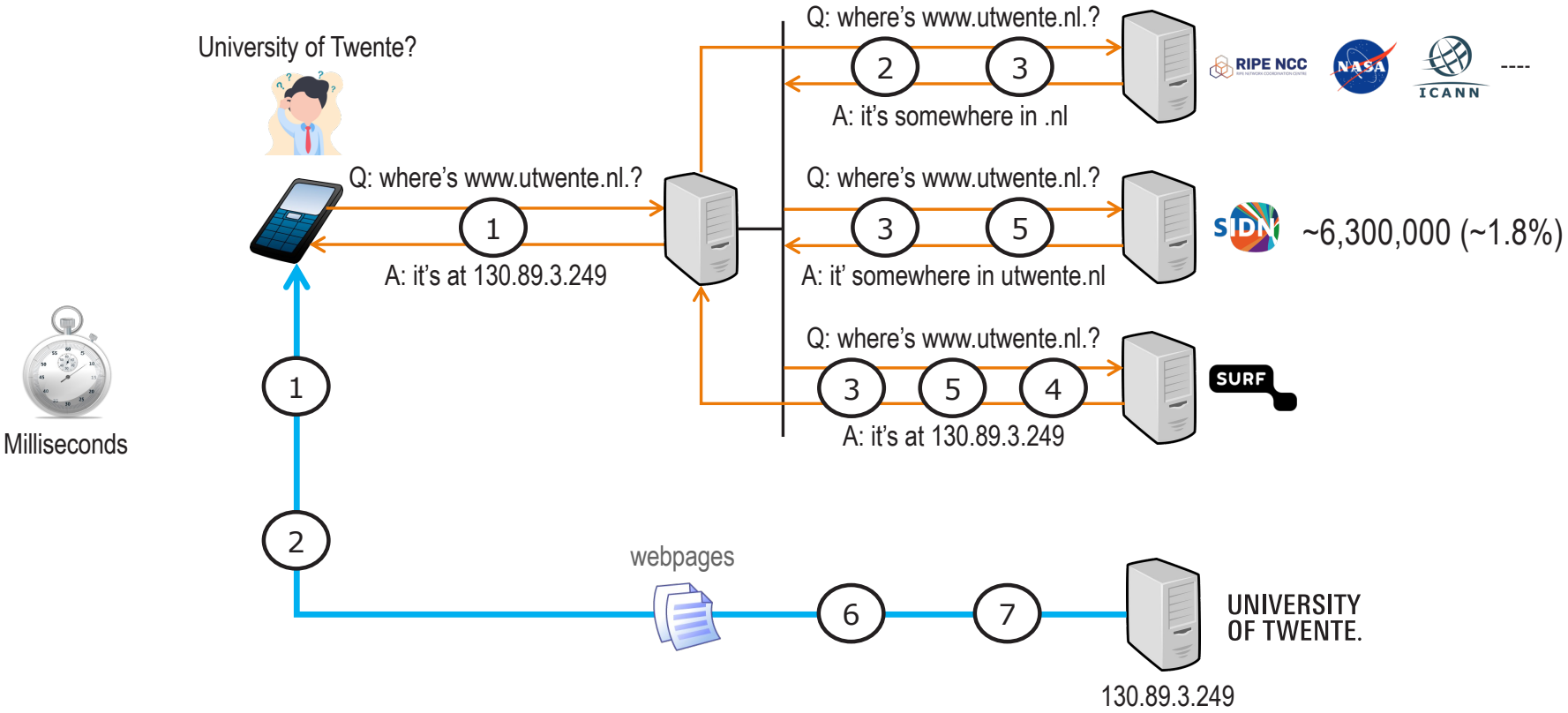
FROM NAMES TO NUMBERS



Critical system: Naming: Domain Name System (DNS)

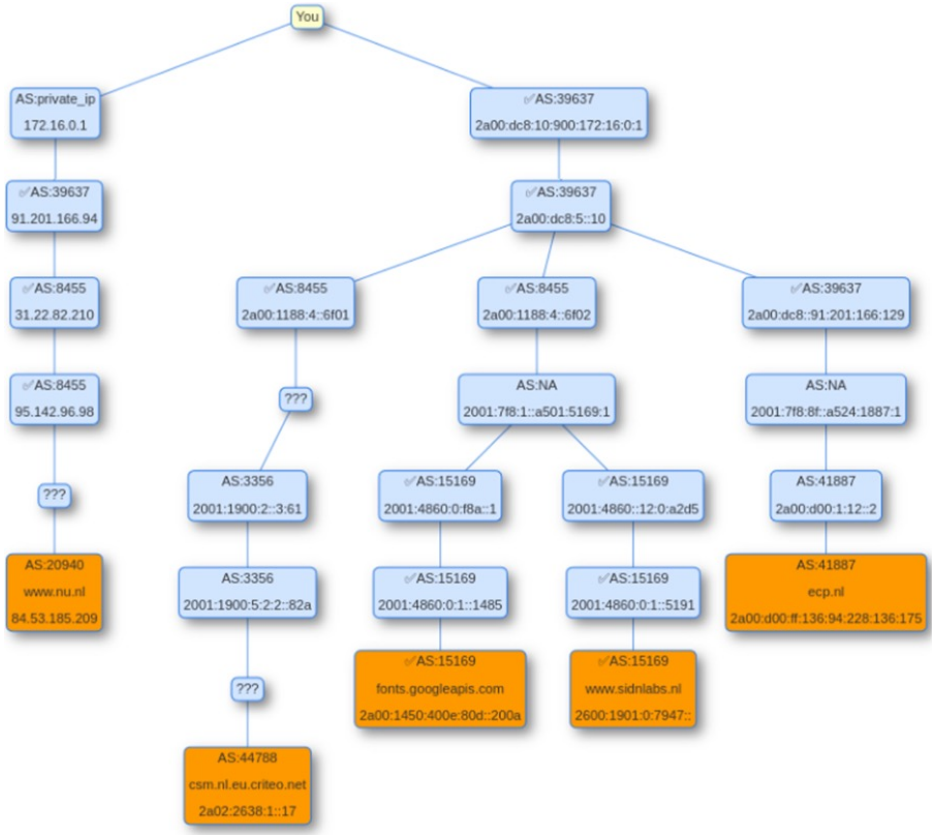
[Toorn22]

TECHNICAL AND ORGANIZATIONAL COMPLEXITY



[Toorn22]

HAVE A LOOK YOURSELF AT THE RECEPTION

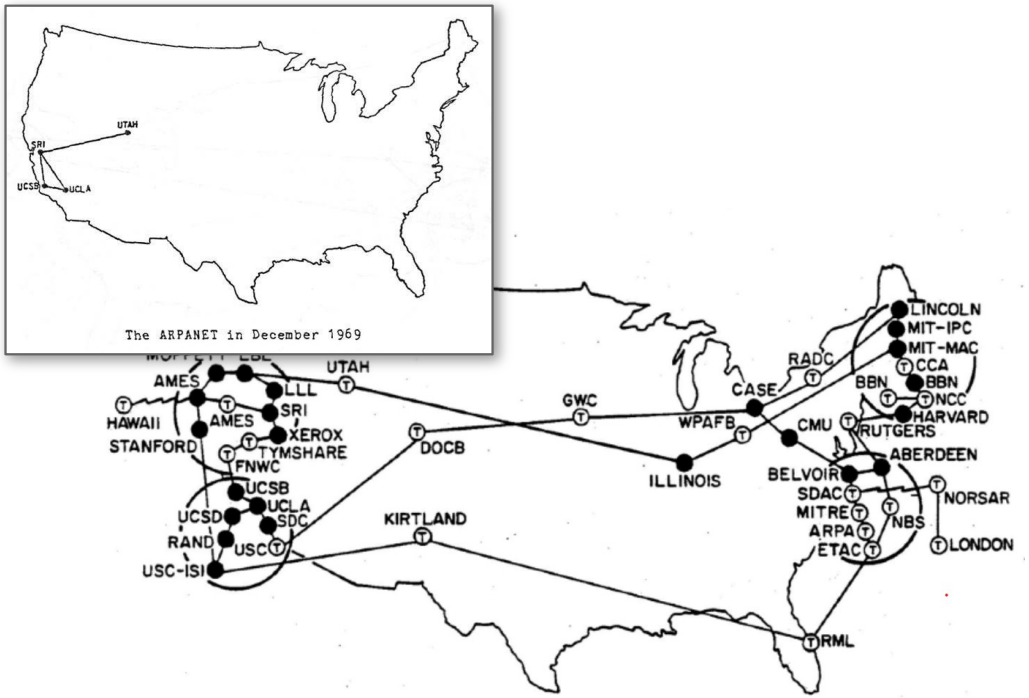


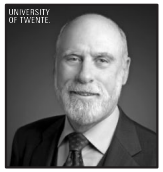
PathVis: visualization of Internet paths

Internet security protocols

UNIVERSITY
OF TWENTE.

EARLY DAYS: PERSONAL TRUST AND NO “BAD ACTORS”




Vint Cerf


Steve Crocker

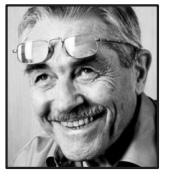

Robert Kahn


Jon Postel


Leonard Kleinrock


Paul Mockapetris


Kc Claffy


Louis Pouzin


Kees Neggers


Jaap Akkerhuis

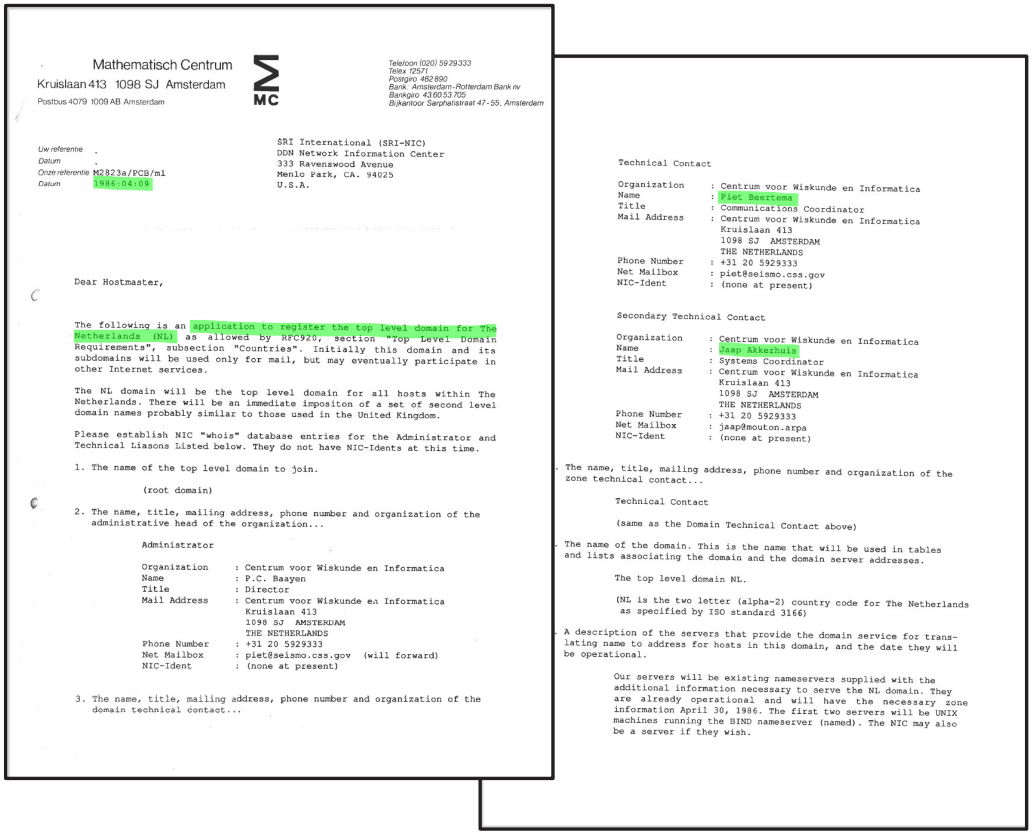

Erik Huizer


Daniel Karrenberg

https://en.wikipedia.org/wiki/ARPANET
https://www.internethalloffame.org/

UNIVERSITY OF TWENTE.

EXAMPLE: .NL DELEGATION (APR 25, 1986)



Mathematisch Centrum
Kruislaan 413 1098 SJ Amsterdam
Postbus 4079 1009 AB Amsterdam

MC

Telefoon (020) 5929333
Telex 12571
Postgiro 462890
Bank Amsterdam-Rotterdam Bank nv
Bankgiro 4360.53.705
Bijkantoor Sarphatistraat 47-55, Amsterdam

Uw referentie .
Datum .
Onze referentie M2823a/PCB/ml
Datum 1986:04:09

SRI International (SRI-NIC)
DDN Network Information Center
333 Ravenswood Avenue
Menlo Park, CA. 94025
U.S.A.

Dear Hostmaster,

The following is an application to register the top level domain for The Netherlands (NL) as allowed by RFC920, section "Top Level Domain Requirements", subsection "Countries". Initially this domain and its subdomains will be used only for mail, but may eventually participate in other Internet services.

The NL domain will be the top level domain for all hosts within The Netherlands. There will be an immediate impositon of a set of second level domain names probably similar to those used in the United Kingdom.

Please establish NIC "whois" database entries for the Administrator and Technical Liasons Listed below. They do not have NIC-Idents at this time.

1. The name of the top level domain to join.

   (root domain)

2. The name, title, mailing address, phone number and organization of the administrative head of the organization...

   Administrator

   Organization : Centrum voor Wiskunde en Informatica
   Name : P.C. Baayen
   Title : Director
   Mail Address : Centrum voor Wiskunde en Informatica
   Kruislaan 413
   1098 SJ AMSTERDAM
   THE NETHERLANDS
   Phone Number : +31 20 5929333
   Net Mailbox : piet@seismo.css.gov (will forward)
   NIC-Ident : (none at present)

3. The name, title, mailing address, phone number and organization of the domain technical contact...

   Technical Contact

   Organization : Centrum voor Wiskunde en Informatica
   Name : Piet Beertema
   Title : Communications Coordinator
   Mail Address : Centrum voor Wiskunde en Informatica
   Kruislaan 413
   1098 SJ AMSTERDAM
   THE NETHERLANDS
   Phone Number : +31 20 5929333
   Net Mailbox : piet@seismo.css.gov
   NIC-Ident : (none at present)

   Secondary Technical Contact

   Organization : Centrum voor Wiskunde en Informatica
   Name : Jaap Akkerhuis
   Title : Systems Coordinator
   Mail Address : Centrum voor Wiskunde en Informatica
   Kruislaan 413
   1098 SJ AMSTERDAM
   THE NETHERLANDS
   Phone Number : +31 20 5929333
   Net Mailbox : jaap@mouton.arpa
   NIC-Ident : (none at present)

4. The name, title, mailing address, phone number and organization of the zone technical contact...

   Technical Contact

   (same as the Domain Technical Contact above)

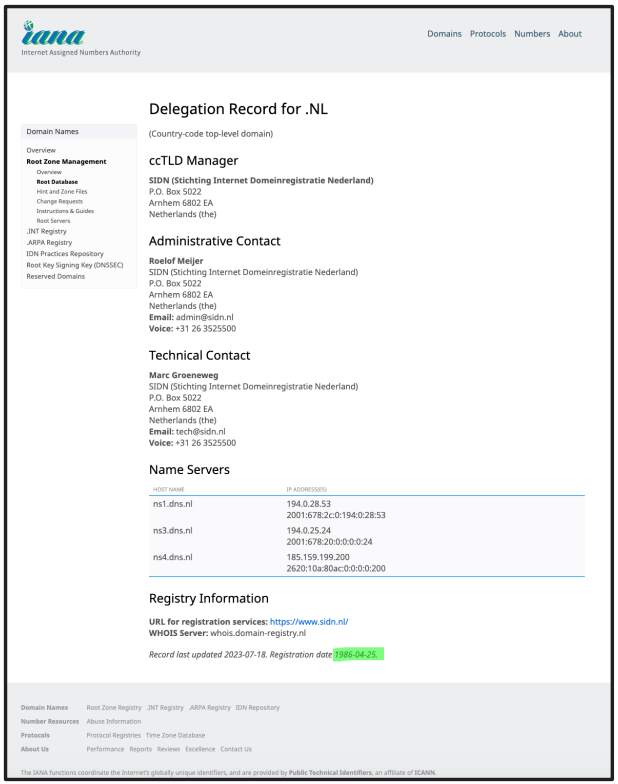
5. The name of the domain. This is the name that will be used in tables and lists associating the domain and the domain server addresses.

   The top level domain NL.

   (NL is the two letter (alpha-2) country code for The Netherlands as specified by ISO standard 3166)

6. A description of the servers that provide the domain service for translating name to address for hosts in this domain, and the date they will be operational.

   Our servers will be existing nameservers supplied with the additional information necessary to serve the NL domain. They are already operational and will have the necessary zone information April 30, 1986. The first two servers will be UNIX machines running the BIND nameserver (named). The NIC may also be a server if they wish.



iana
Internet Assigned Numbers Authority

Domains Protocols Numbers About

Domain Names
- Overview
- Root Zone Management
  - Overview
  - Root Database
  - Hint and Zone Files
  - Change Requests
  - Instructions & Guides
  - Root Servers
- .INT Registry
- .ARPA Registry
- IDN Practices Repository
- Root Key Signing Key (DNSSEC)
- Reserved Domains

Delegation Record for .NL

(Country-code top-level domain)

ccTLD Manager

SIDN (Stichting Internet Domeinregistratie Nederland)
P.O. Box 5022
Arnhem 6802 EA
Netherlands (the)

Administrative Contact

Roelof Meijer
SIDN (Stichting Internet Domeinregistratie Nederland)
P.O. Box 5022
Arnhem 6802 EA
Netherlands (the)
Email: admin@sidn.nl
Voice: +31 26 3525500

Technical Contact

Marc Groeneweg
SIDN (Stichting Internet Domeinregistratie Nederland)
P.O. Box 5022
Arnhem 6802 EA
Netherlands (the)
Email: tech@sidn.nl
Voice: +31 26 3525500

Name Servers

HOST NAME	IP ADDRESSES
ns1.dns.nl	194.0.28.53 2001:678:2c:0:194:0:28:53
ns3.dns.nl	194.0.25.24 2001:678:20:0:0:0:0:24
ns4.dns.nl	185.159.199.200 2620:10a:80ac:0:0:0:0:200

Registry Information

URL for registration services: https://www.sidn.nl/
WHOIS Server: whois.domain-registry.nl

Record last updated 2023-07-18. Registration date 1986-04-25

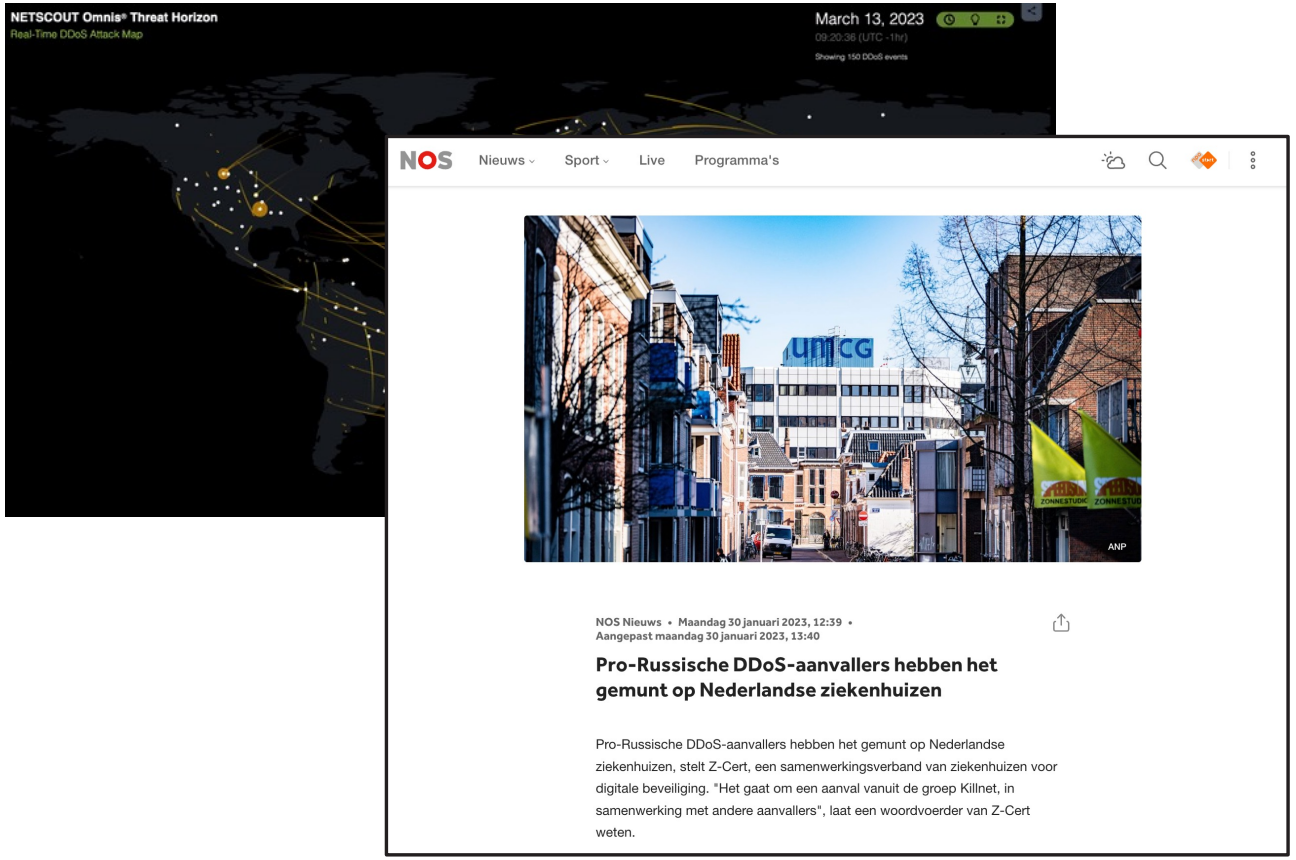
Domain Names Root Zone Registry .INT Registry .ARPA Registry IDN Repository
Number Resources Abuse Information
Protocols Protocol Registries Time Zone Database
About Us Performance Reports Reviews Excellence Contact Us

The IANA functions coordinate the Internet's globally unique identifiers, and are provided by Public Technical Identifiers, an affiliate of ICANN.

UNIVERSITY OF TWENTE.

GROWTH INTRODUCED SECURITY RISKS

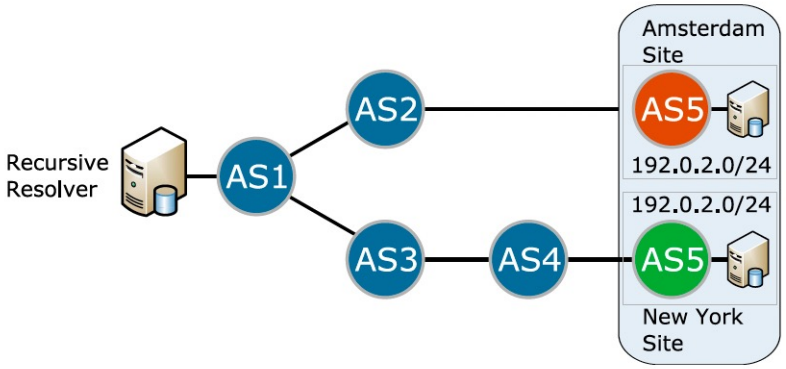
- Phishing
- Fake webshops
- **DDoS attacks**
- Malware
- Routing hijacks
- Cache poisoning



[Moura20a] [Moura16]

IMPERSONAL TRUST THROUGH SECURITY MECHANISMS

- Encryption so that only the receiver can read a message and not an adversary
- Signatures so that receivers can validate the source and message integrity
- **Additional** availability mechanisms, such as service replication and “DDoS scrubbing”
- Together referred to as “CIA”: confidentiality, integrity, and availability
- Implemented through techniques like DNS-over-HTTPS, DNSSEC, RKPI, anycast

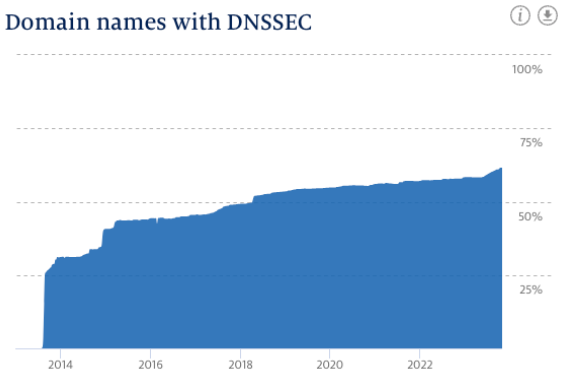


Core system: BGP (anycast)

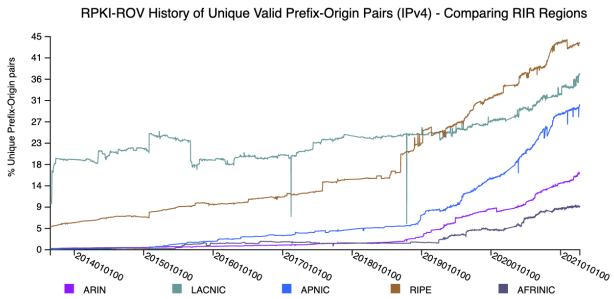
[Toorn22] [Moura20b]

OPERATORS ARE INCREMENTALLY ADDING SECURITY

75,000+
autonomous
networks



stats.sidnlabs.nl



NIST RPKI Deployment Monitor

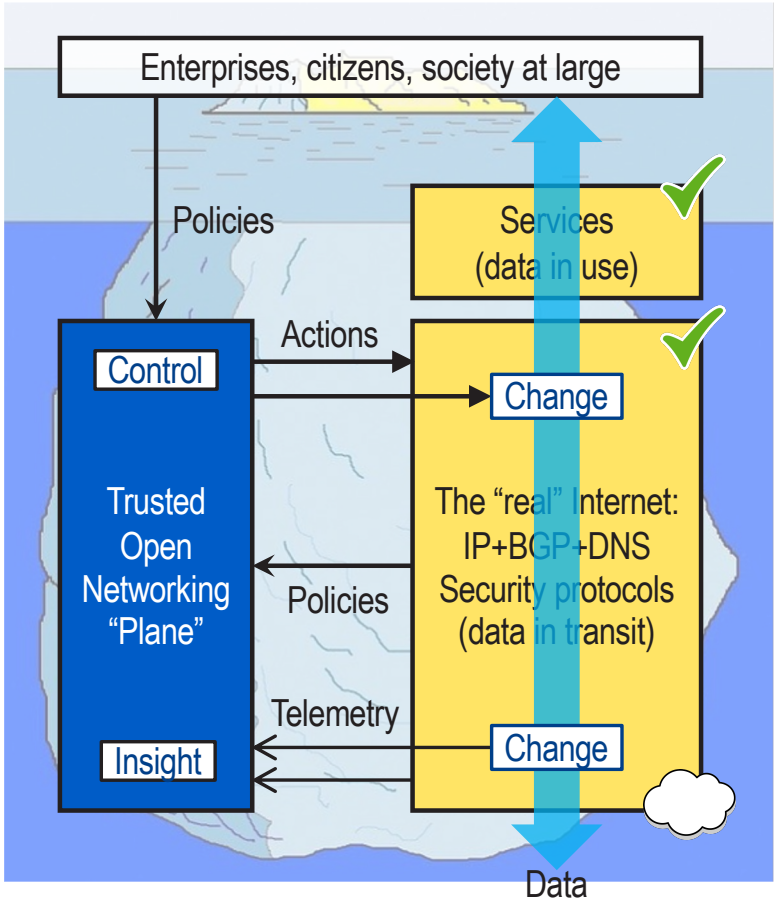
[Moura14]

UNIVERSITY
OF TWENTE.


The field of Trusted Open Networking
UNIVERSITY
OF TWENTE.

GOAL: ENHANCE TRUST IN TRANSIT

- Logical **extension** of the Internet
- Key concepts: security-related **insight** and **control**
  - Insights through measurements
  - Control actions to mitigate incidents or risks
- **Open** technologies for wide-scale deployment
- May require changes to the Internet itself
- Work: design & analysis and science & practice
- A bit high-level? Examples ahead :-)

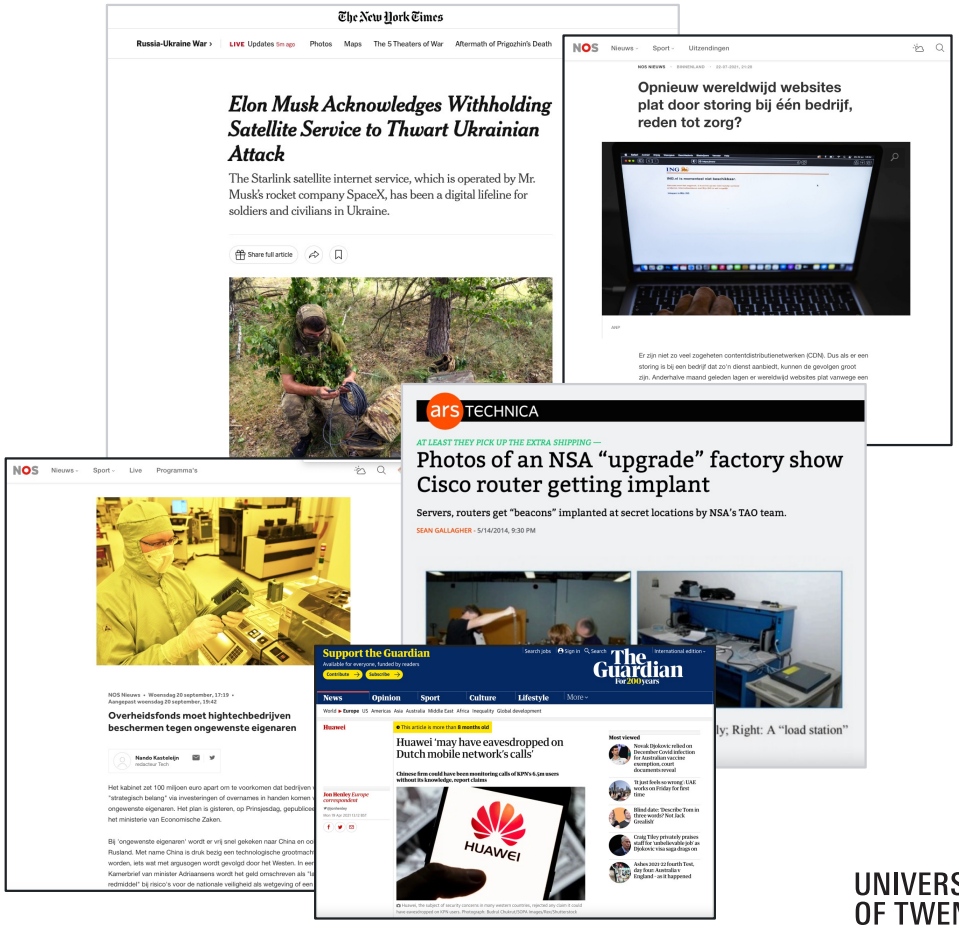


[Hesselman20a]

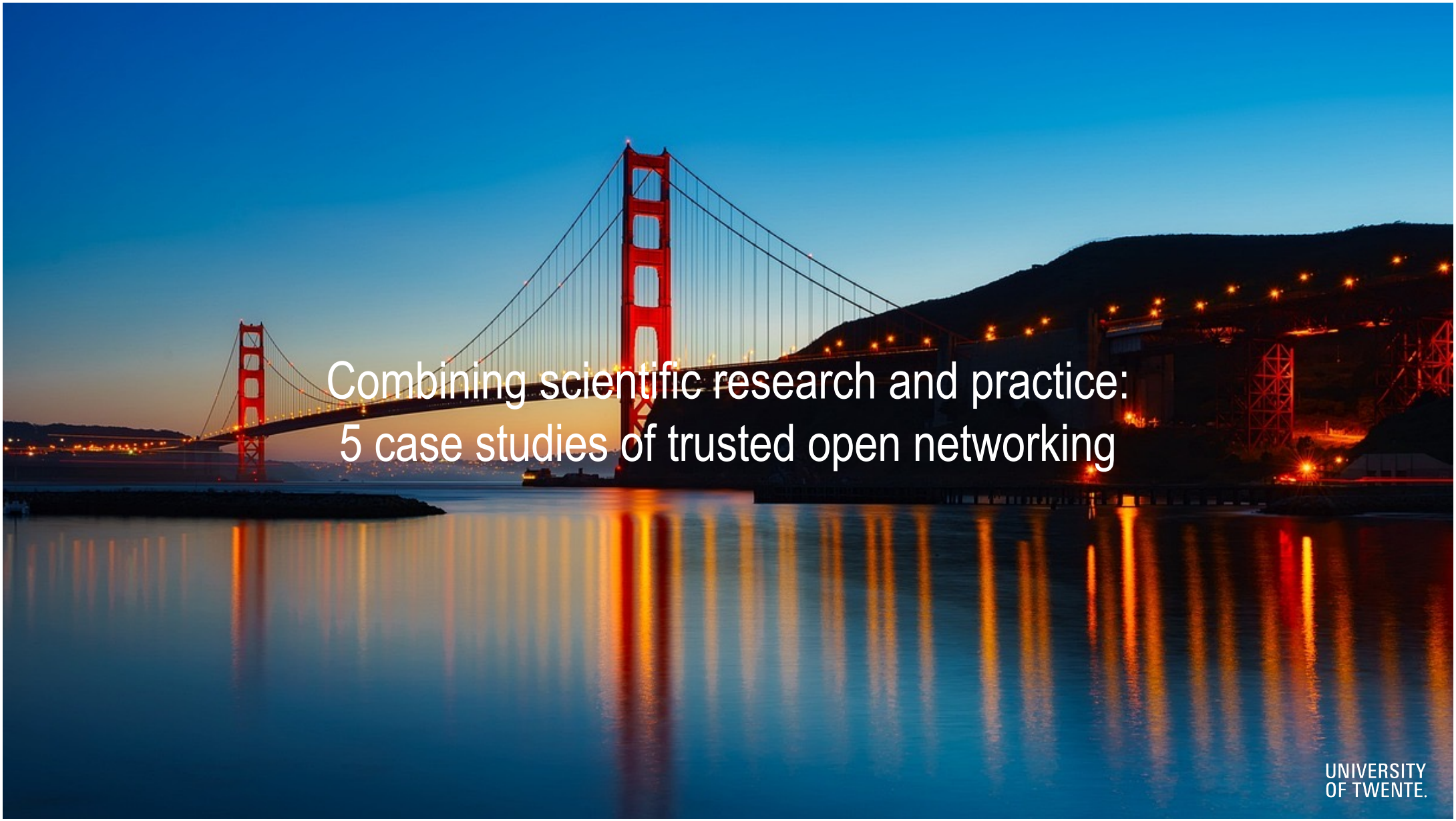
ALSO CONTRIBUTES TO PUBLIC POLICY

CSR Cyber Security Raad

- Insight and control are also key in open strategic digital autonomy
  - Responsible AI, 5G certification, GAIA-X
  - NIS2, CRA, Chips Act
- Goal: strengthen grip on EU's digital infrastructure
- Motivation: BigTech US/China and untrusted equipment, which is a **risk** for in terms of:
  - Upholding public values
  - Available technical expertise
  - Equal trade possibilities (lack of reciprocity)
  - Resilience of the Union's digital infrastructure



UNIVERSITY OF TWENTE.


Combining scientific research and practice:
5 case studies of trusted open networking
UNIVERSITY
OF TWENTE.

CASE STUDY #1: SECURITY SERVICES FOR THE IOT

- IoT senses and interact with people's physical space
- Insight into and control over IoT security is essential
- Teaching
  - Scientific papers to understand key concepts
  - Lab: insight in IoT traffic through measurements, control over traffic through MUD technology
- Results
  - Educated 135 students 2018-2023
  - Average student rating: 7.8

IP address	Used by
api-eu.roborock.com, EUiot.roborock.com	
18.198.13.146	Roborock
52.28.134.206	Companion app
18.195.39.22	Roborock
mqtt-eu.roborock.com	
52.29.111.255	Companion app
52.57.14.190	Companion app
3.64.102.186	Roborock
3.65.76.56	Roborock, Companion app
awsde0.fds.api.xiaomi.com	
3.121.13.133	Roborock
35.156.105.161	Companion app
3.122.185.108	Roborock
18.198.60.243	Companion app
v-eu-2.roborock.com	
3.125.156.2	Roborock, Companion app

MUD

https://courses.sidnlabs.nl/ssi/

[Hesselman20b]

SIDN LABS UNIVERSITY OF TWENTE.

CASE STUDY #2: FAKE WEBSHOPS

- Many fake shops in the .nl zone back in 2016-2018
- Developed tools to detect them
- Partnered with registrars and ISC to remove them
- Results
  - Fake shops virtually gone from the .nl zone
  - Dashboard in use at SIDN's anti-abuse desk
  - Peer-reviewed scientific paper at PAM2020

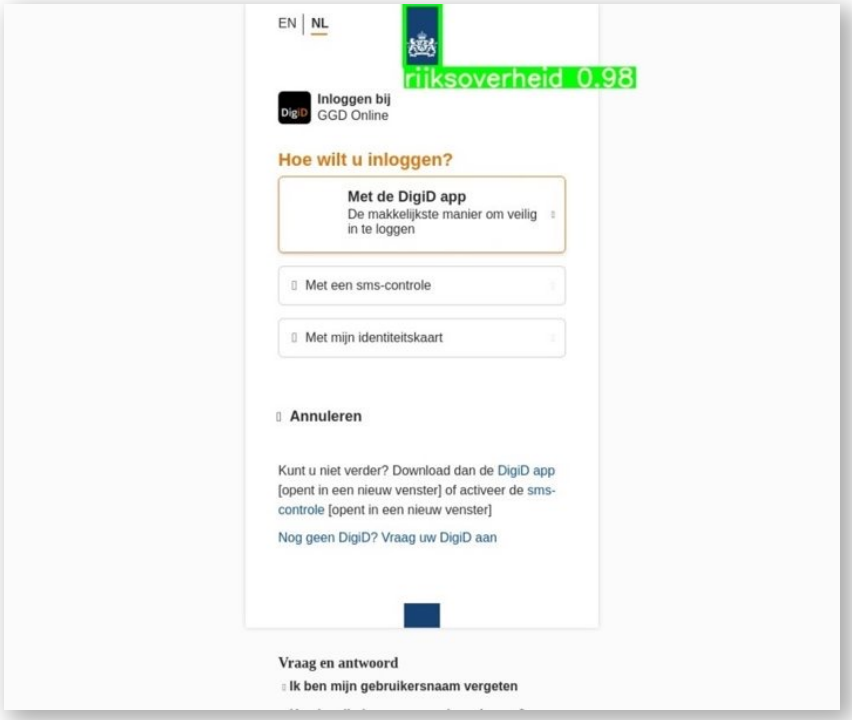
Year	Taken down
2023	241
2022	192
2021	224
2020	481
2019	4,340
2018	~12,000

[Wabeke20]

SIDN LABS UNIVERSITY OF TWENTE.

CASE STUDY #3: ONLINE IMPERSONATION

- Misuse of logos is an indicator for abuse
- Logomotive detects logo usage in the .nl zone
- Pilots with the 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 scientific paper at PAM2022



[Hout22]

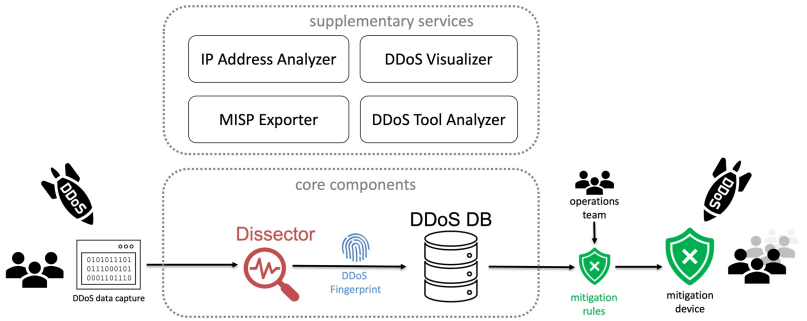
SIDN LABS UNIVERSITY OF TWENTE.

CASE STUDY #4: SHARING DDOS FINGERPRINTS

- Lack of insight in DDoS attack landscape, reduces proactiveness for (critical) service providers
- Developed concept of Anti-DDoS Coalitions (ADCs) with 7 European partners
- Results
  - NL-ADC standing organization with 18 partners from industry, government, academia
  - Technical pilots in NL and IT, cookbook, system being transferred to production at NBIP
  - Paper submitted to IEEE Communications Magazine (under review)

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Anti-DDoS-Coalitie
No More DDoS

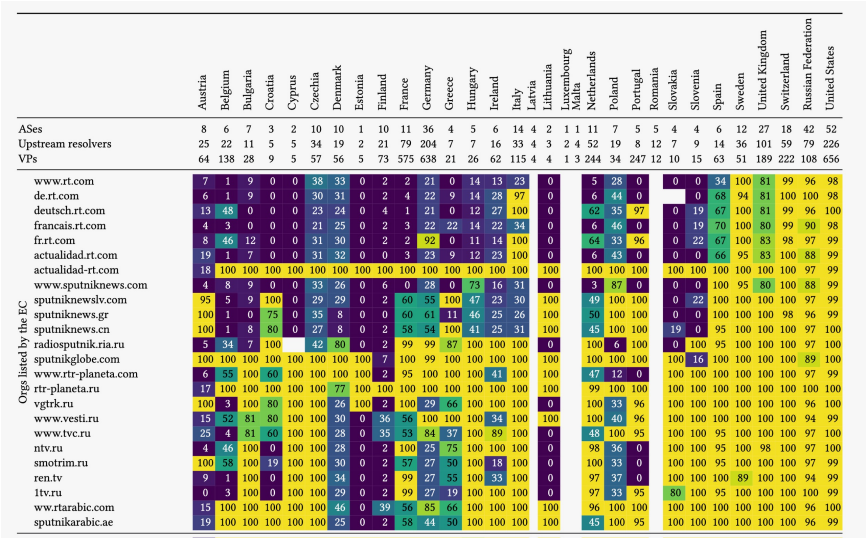


[Yazdani23]

nationale beheersorganisatie internet providers
SURF
SIDN LABS
UNIVERSITY OF TWENTE.

CASE STUDY #5: BLOCKING OF RT AND SPUTNIK

- EU mandates ban of Russian state-backed channels
- RIPE-ATLAS measurements provide insight into degree of actual blocking by ISPs across the EU
- Inconsistency partly due to lack of (tech) guidance, perhaps in combination with DNS outsourcing
- Showcases how measurement-based insights can provide input to public policy making and evaluation
- Results
  - Scientific paper (in progress)
  - Combination of technical and policy research



Orgs listed by the EC	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czechia	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom	Switzerland	Russian Federation	United States
ASes	8	6	7	3	2	10	10	1	10	11	36	4	5	6	14	4	2	1	1	11	7	5	5	4	4	6	12	27	18	42	52
Upstream resolvers	25	22	11	5	5	34	19	2	21	79	204	7	7	16	33	4	3	2	4	52	19	8	12	7	9	14	36	101	59	79	226
VPs	64	138	28	9	5	57	56	5	73	575	638	21	26	62	115	4	4	1	3	244	34	247	12	10	15	63	51	189	222	108	656
www.rt.com	7	1	9	0	0	38	33	0	2	2	21	0	14	13	23	0		5	28	0		0	0	34	100	81	99	96	98		
de.rt.com	6	1	9	0	0	30	31	0	2	4	22	9	14	28	97	0		6	44	0			0	68	94	81	100	100	98		
deutsch.rt.com	13	48	0	0	0	23	24	0	4	1	21	0	12	27	100	0		62	35	97		0	19	67	100	81	99	96	100		
francais.rt.com	4	3	0	0	0	21	25	0	2	3	22	22	14	22	34	0		6	46	0		0	19	70	100	80	99	90	98		
fr.rt.com	8	46	12	0	0	31	30	0	2	2	92	0	11	14	100	0		64	33	96		0	22	67	100	83	98	97	99		
actualidad.rt.com	19	1	7	0	0	31	32	0	0	3	23	9	12	23	100	0		6	43	0		0	0	66	95	83	100	88	99		
actualidad-rt.com	18	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100		100	100	100		100	100	100	100	100	100	97	99		
www.sputniknews.com	4	8	9	0	0	33	26	0	6	0	28	0	73	16	31	0		3	87	0		0	0	100	95	80	100	88	99		
sputniknewslv.com	95	5	9	100	0	29	29	0	2	60	55	100	47	23	30	100		49	100	100		0	22	100	100	100	100	97	99		
sputniknews.gr	100	1	0	75	0	35	8	0	0	60	61	11	46	25	26	100		50	100	100		0	0	100	100	100	98	96	99		
sputniknews.cn	100	1	8	80	0	27	8	0	2	58	54	100	41	25	31	100		45	100	100		19	0	95	100	100	100	97	100		
radiosputnik.ria.ru	5	34	7	100		42	80	0	2	99	99	87	100	100	100	0		100	6	100		0	100	95	100	100	100	97	100		
sputnikglobe.com	100	100	100	100	100	100	100	100	7	100	99	100	100	100	100	100		100	100	100		100	16	100	100	100	100	89	100		
www.rtr-planeta.com	6	55	100	60	100	100	100	100	2	95	100	100	100	41	100	100		47	12	0		100	100	100	100	100	100	97	99		
rtr-planeta.ru	17	100	100	100	100	100	77	100	100	100	100	100	100	100	100	100		99	100	100		100	100	100	100	100	100	100	100		
vgtrk.ru	100	3	100	80	100	100	26	100	2	100	29	66	100	100	100	0		100	33	96		100	100	100	100	100	100	96	100		
www.vesti.ru	15	52	81	80	100	100	30	0	36	56	100	100	100	34	100	100		100	40	96		100	100	100	100	100	100	94	99		
www.tvc.ru	25	4	81	60	100	100	28	0	35	53	84	37	100	89	100	0		48	100	95		100	100	95	100	100	100	97	100		
ntv.ru	4	46	100	0	100	100	28	0	2	100	25	75	100	100	100	0		98	36	0		100	100	95	100	98	100	97	100		
smotrim.ru	100	58	100	19	100	100	30	0	2	57	27	50	100	18	100	0		100	33	0		100	100	95	100	100	100	97	99		
ren.tv	9	1	100	0	100	100	34	0	2	99	27	55	100	33	100	0		97	37	0		100	100	100	89	100	100	94	99		
1tv.ru	0	3	100	0	100	100	29	0	2	99	27	19	100	100	100	0		97	33	95		80	100	95	100	100	100	100	99		
ww.rtarabic.com	15	100	100	100	100	100	46	0	39	56	85	66	100	100	100	100		96	100	100		100	100	100	100	100	100	96	100		
sputnikarabic.ae	19	100	100	100	100	100	25	0	2	58	44	50	100	100	100	100		45	100	95		100	100	100	100	100	100	96	99		

September 2023

[Müller23]

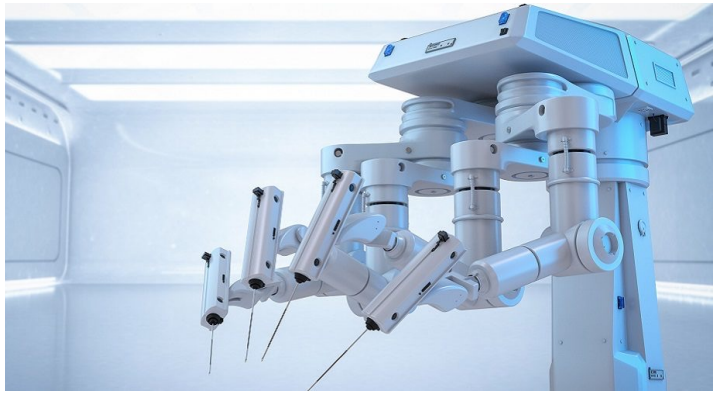
OONI UNIVERSITY OF ILLINOIS CHICAGO SIDN LABS UNIVERSITY OF TWENTE.

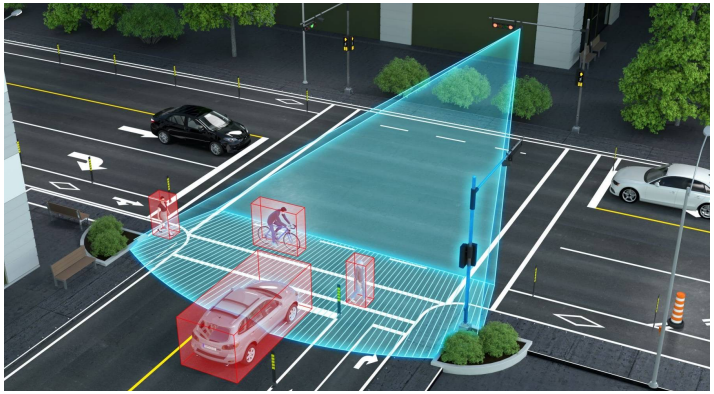

Vision: next generation Internet applications
UNIVERSITY OF TWENTE.

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

Example: remote truck driving

OTHER FUTURE CRITICAL INTERNET APPLICATIONS

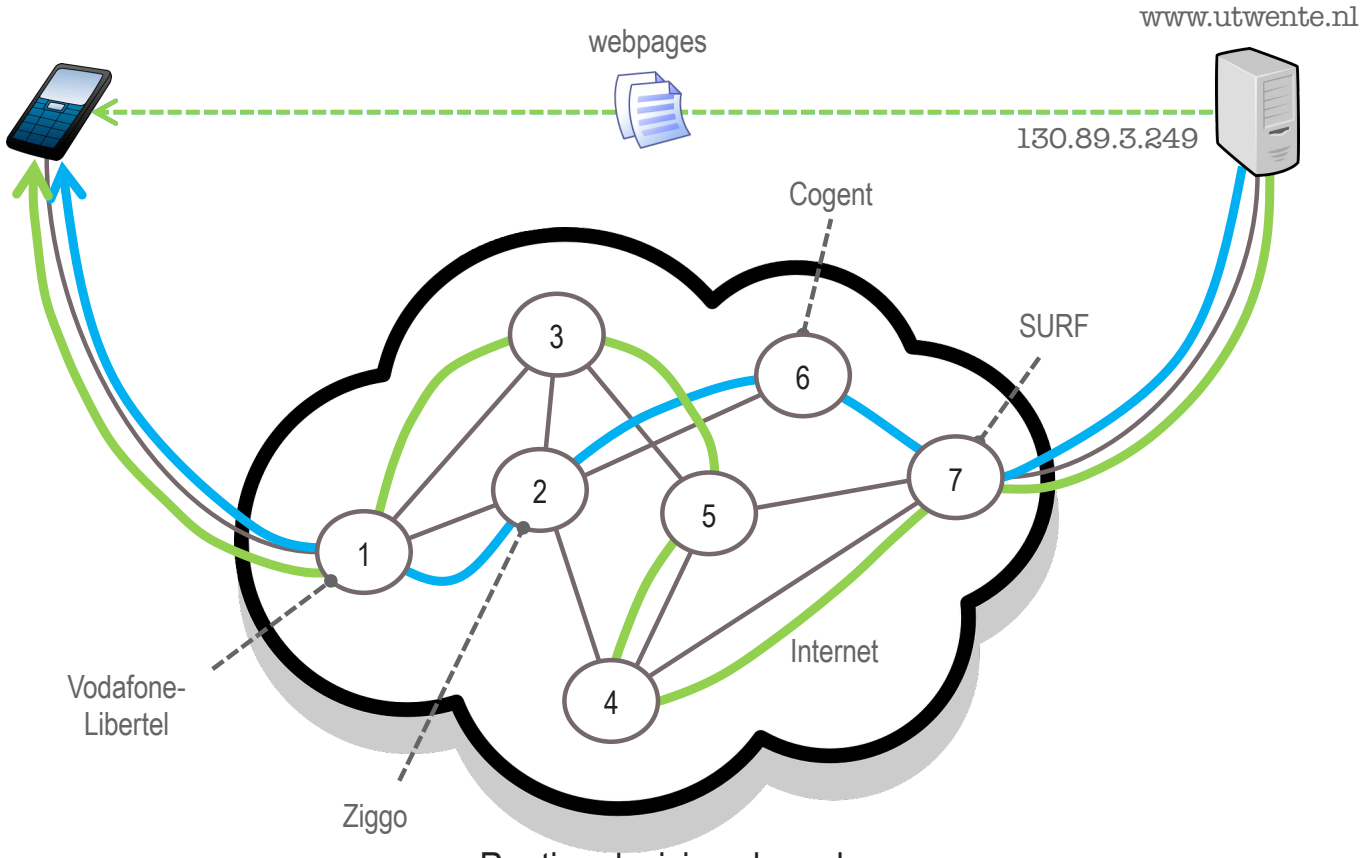




[Schulzrinne22] [TNO22]

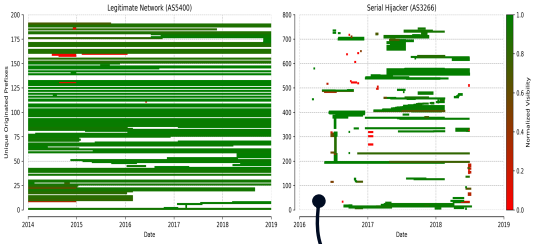

Challenge: insight and control for next generation Internet applications

CONCEPT #1: RISK-BASED ROUTING



Routing decisions based on risk profiles (control)

Routing hijacks



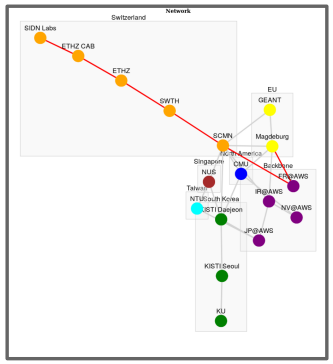
Risk Profile 5
- Network mgmt
- Routing settings
- Abuse sources
- HW/SW security

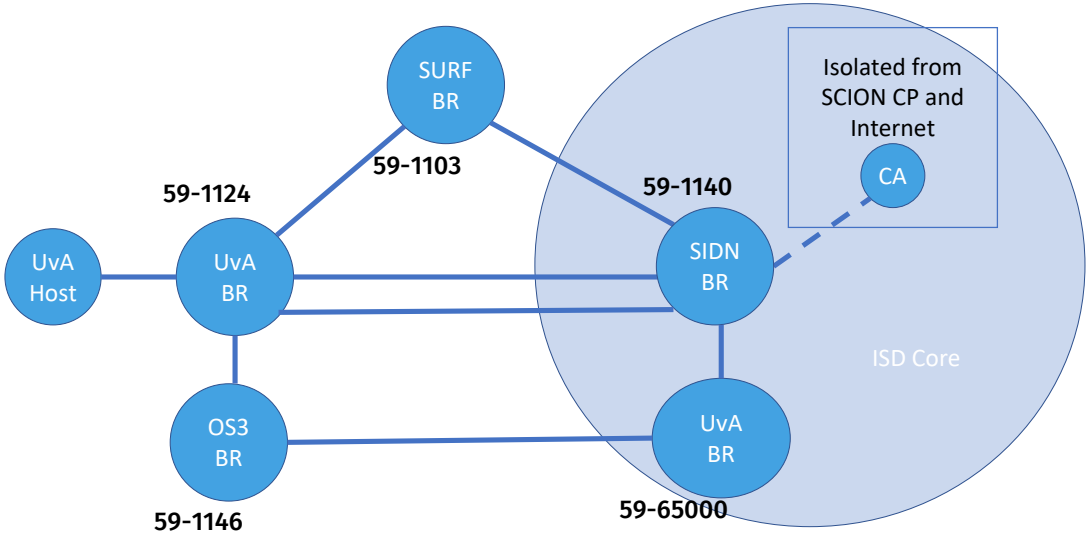
Risk profile of networks (insight)

TUCCR. UNIVERSITY OF TWENTE.

CONCEPT #2: END-USER INSIGHT AND CONTROL

“Network receipt”

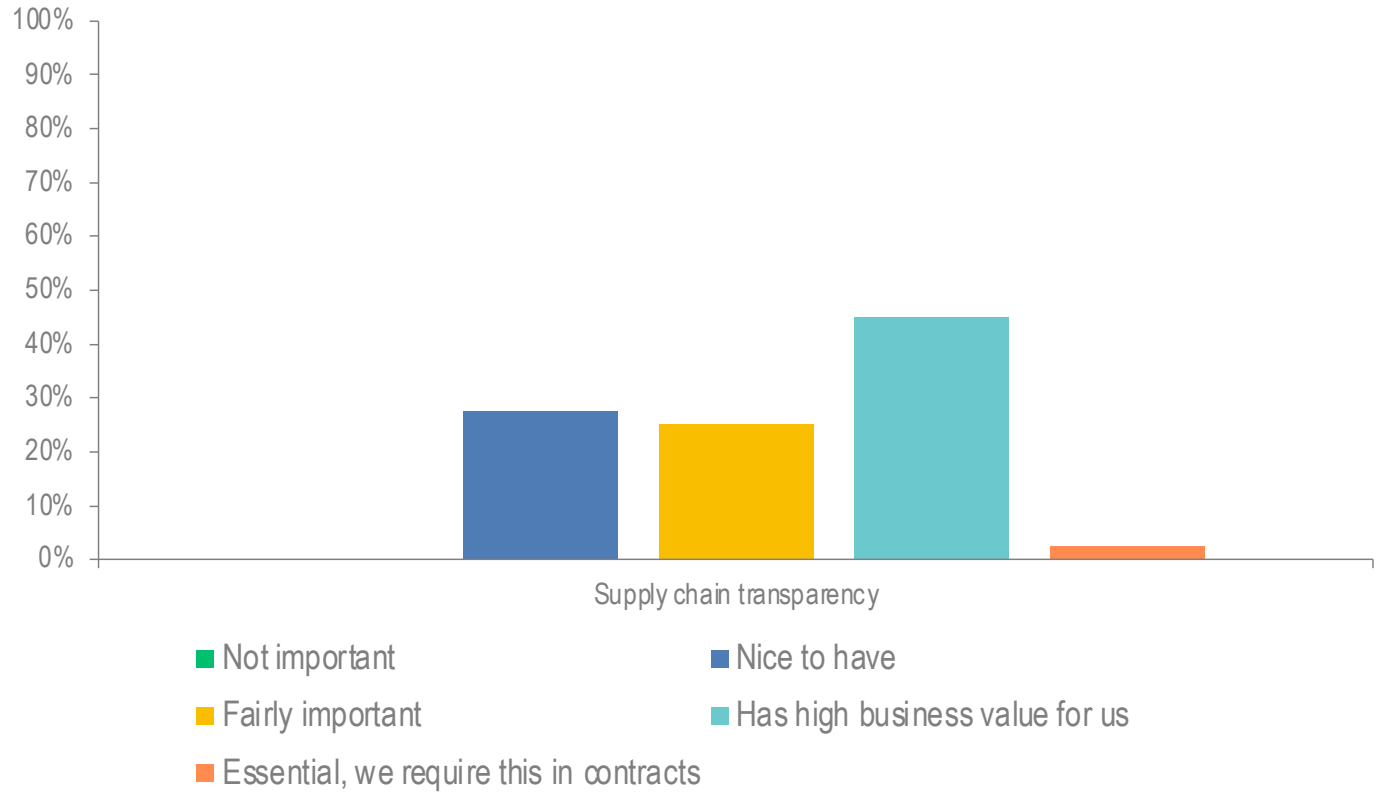




SCION-NL for student projects

Universiteit van Amsterdam · SURF · SIDN Labs · University of Twente.

FIRST INDICATION OF NEED (MANRS+)



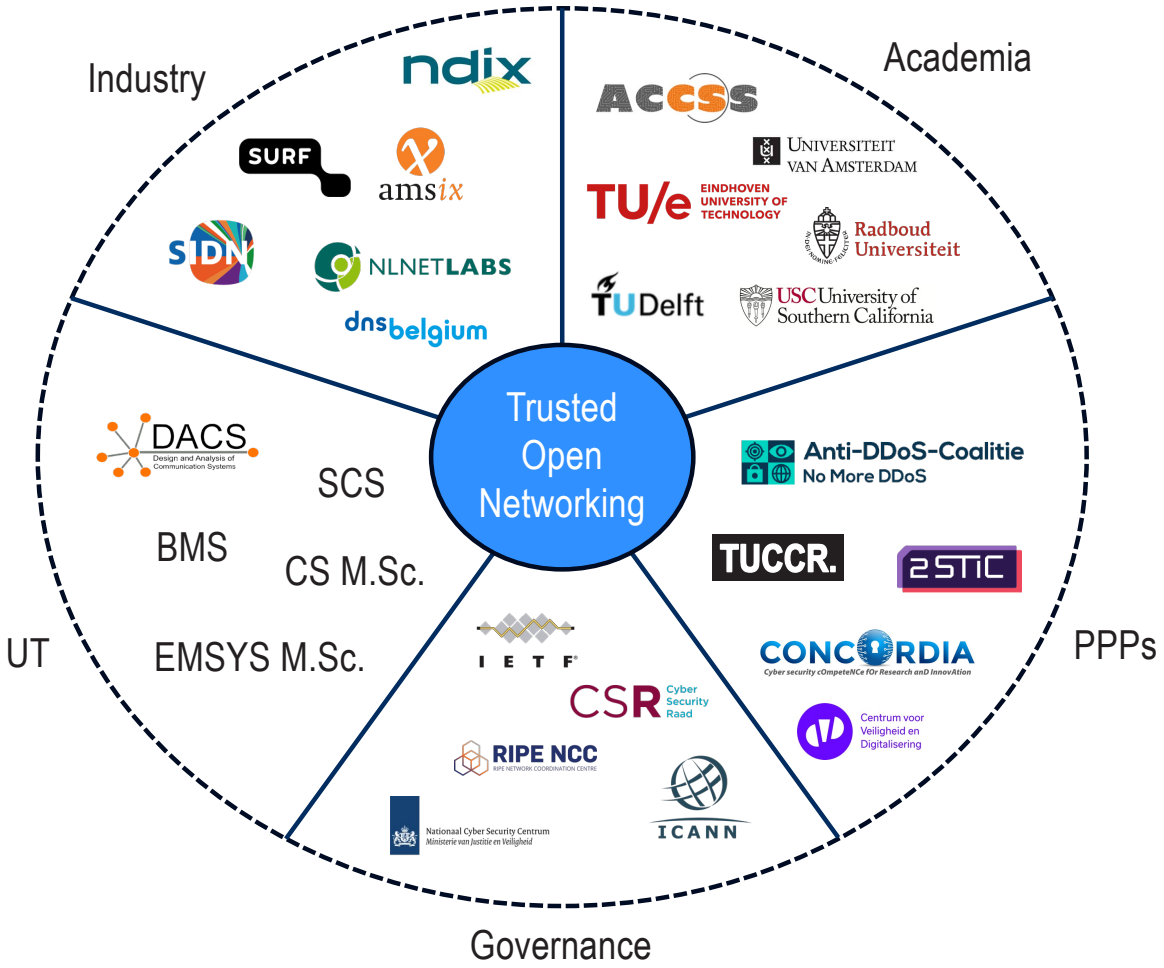
https://www.manrs.org/2023/08/survey-shows-enterprises-value-routing-security-may-underestimate-their-ability-to-influence-vendors/

UNIVERSITY OF TWENTE.

FURTHER TRUSTED OPEN NETWORKING CHALLENGES

- **Education:** Internet security and open strategic digital autonomy → B.Sc. students, professionals, boards
- **Research:** technical (see previous), incentives (with BMS), policy (Cyber Security Council)
- **Innovation:** bring research results to operations (SIDN and elsewhere), multi-disciplinary cookbooks

EMBEDDING AND COLLABORATION



UNIVERSITY OF TWENTE.

TODAY'S OBJECTIVE REVISITED

- Help you explain how the Internet works, so you can impress others :-)
- Outline my research field "Trusted Open Networking" in the form of 5 case studies
- Look ahead at future challenges

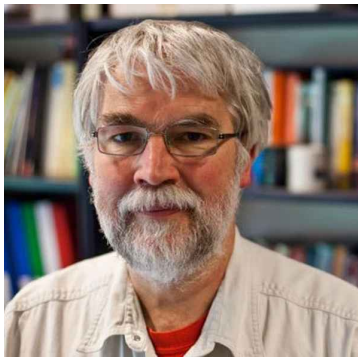
Feedback welcome at the reception and afterwards!


Standing on the shoulders of giants
UNIVERSITY
OF TWENTE.

Prof. Aiko Pras (UT)

Roelof Meijer (SIDN)

Kees Neggers



Prof. Cees de Laat (UvA)

RvT en managementteam SIDN

UNIVERSITY
OF TWENTE.

UNIVERSITY
OF TWENTE.

Ik heb gezegd

Thank you!

c.e.w.hesselman@utwente.nl

TUCCR. DACS SIDN LABS UNIVERSITY OF TWENTE.

FURTHER READING

[Shosh78] J. Shosh, “Inter-Network Naming, Addressing, and Routing”, Internet Experiment Note #19, Jan 1978
[ISOC20] ISOC, “The Internet Way of Networking – Defining the critical properties of the Internet”, Sep 2020
[Lehr19] W. Lehr, D. Clark, S. Bauer, A. Berger, P. Richter, “Whither the public Internet?”, Journal of Information Policy 9, Aug 2019
[Toorn22] O. van der Toorn, M. Müller, S. Dickinson, C. Hesselman, A. Sperotto, and R. van Rijswijk-Deij, “Addressing the Challenges of Modern DNS: A Comprehensive Tutorial”, Elsevier Computer Science Review, 2022
[Moura20a] G. Moura, C. Hesselman, G. Schaapman, N. Boerman, and O. de Weerdt, “Into the DDoS maelstrom: a longitudinal study of a scrubbing service”, International Workshop on Traffic Measurements for Cybersecurity (WTMC), 2020
[Moura20b] G. Moura, J. Heidemann, W. Hardaker, P. Charnsethikul, J. Ceron and C. Hesselman, "Old but Gold: Prospecting TCP to Engineer and Live Monitor DNS Anycast", Passive and Active Measurement Conference (PAM2022), March 2022
[Moura14] G.. Moura, R. Sadre, A. Pras, “Bad neighborhoods on the internet”, IEEE Communications Magazine, Vol 52, Issue 7, Jul 2014
[Moura16] G. Moura, R. de O. Schmidt, J. Heidemann, W. de Vries, M. Müller, L. Wei, C. Hesselman, “Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event”, ACM Internet Measurement Conference (IMC 2016)
[Hesselman20a] C. Hesselman, P. Grosso, R. Holz, F. Kuipers, J. Hui Xue, M. Jonker, J. de Ruiter, A. Sperotto, R. van Rijswijk-Deij, G. Mour, A. Pras, C. de Laat, “A Responsible Internet to Increase Trust in the Digital World”, Invited paper, Journal of Network and Systems Management (JNSM), Sep 2020
[Hesselman20b] C. Hesselman, M. Kaeo, L. Chapin, kc claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour, and R. Rasmussen, “The DNS in IoT: Opportunities, Risks, and Challenges”, IEEE Internet Computing, 2020
[Hout22] T. van den Hout, T. Wabeke, G. Moura, C. Hesselman, “LogoMotive: detecting logos on websites to identify online scams - a TLD case study”, PAM2022, Mar 2022
[Wabeke20] T. Wabeke, G. Moura, N. Franken, C. Hesselman, “Counterfighting Counterfeit detecting and taking down fraudulent webshops at a ccTLD”, PAM2020, Mar 2020
[Müller23] M. Müller, N. ten Oever, J. Kristoff, C. Kanich, A. Filastò, M. Resing, “Online Sanctions Against Russian Media: Implementation and Effects” Work in Progress
[Schulzrinne22] H. Schulzrinne, “Networking: The Newest Civil Engineering Challenge”, SIGCOMM 2022, Amsterdam, August 2022, https://www.youtube.com/watch?v=5lvXIqI_mQ4
[TNO22] “Bridging the Dutch and European Digital Sovereignty gap”, TNO Technical Report R10507, May 2022