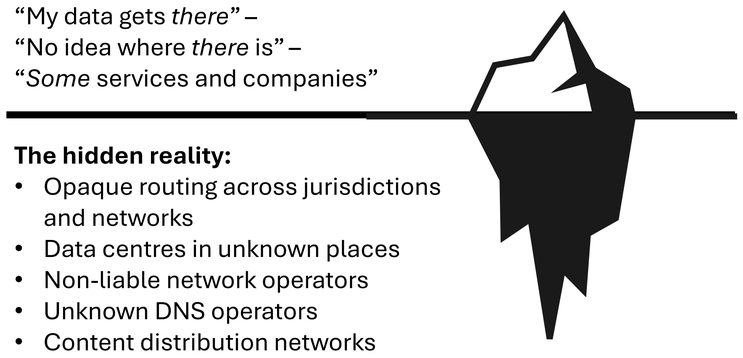
Controllable, Accountable, Transparent:
The Responsible Internet

RESPONSIBLE INTERNET

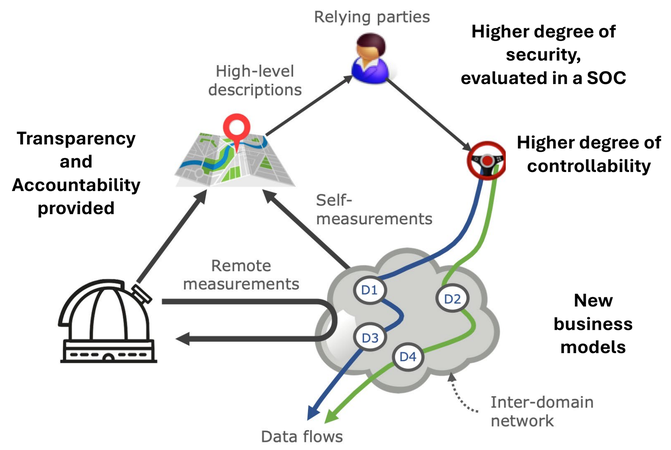
The Responsible Internet addresses the problem of Digital Sovereignty

User perception – the status quo:
"My data gets *there*" –
"No idea where *there* is" –
"*Some* services and companies"



The hidden reality:
- Opaque routing across jurisdictions and networks
- Data centres in unknown places
- Non-liable network operators
- Unknown DNS operators
- Content distribution networks
- Etc.

The Responsible Internet is to the Internet what Responsible AI is to AI



New opportunities explored and exploited

Exploration of societal impact
- Business Model Canvas
- Governance and analysis of EU policy

Opportunities with industry partners
- KPN: new business models for controllability
- NLNet Labs: novel routing
- Ciena: development of programmable networks

New collaborations with academic institutes:
University of Sydney, TU Munich, FH Münster, UC San Diego

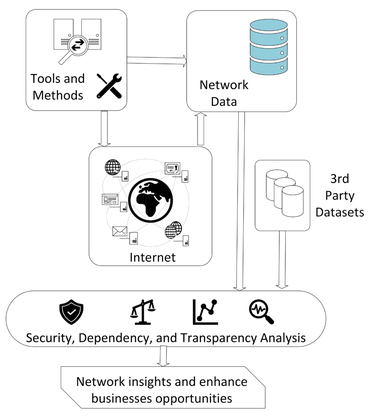
Series of annual workshops since 2021:
"Transparency, accountability, and user control for a Responsible Internet"

Internet transparency to increase trust in the digital world – insights into services and operations

UNIVERSITY OF TWENTE.

Goals:
- Transparency via continuing, global-scale network measurements
- Accountability via logging infrastructure
- Detect dependencies between and on operators, routing infrastructure, middleboxes, …
- Provide means for security-property aware routing

Lessons learned:
- Must strengthen collaboration between operators and ISPs to enable deeper understanding of infrastructure
- CERT notifications for weaknesses (that we found) are largely ineffective – case for accountability.
- Evidence that secure paths exist, and operators can use them – if appropriate business models exist



Overview of our measurement approach.

Designing for transparency and controllability in a Responsible Internet

waag technology & society

Goals:
- Align prototypes with values the public associates with a Responsible Internet
- Inform design of prototypes by testing them with members of the public

Actions:
- Engage public with participatory methods, e.g., focus groups, testing sessions
- Inform design of prototypes by testing them with members of the public

Left: testing session at Public Spaces conference in 2024.

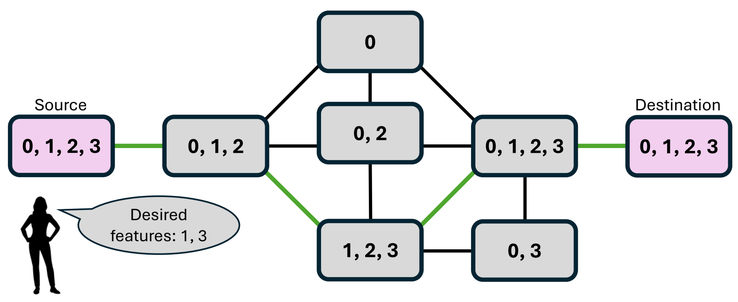
Visitors were asked to make routing choices in a fictitious scenario. This allowed us to provide directions for the prototype's user interface.

Lessons learned:
- Decisions based on factors such as energy, distance, jurisdiction crossed
- Need comparable, summarized info; users realize risks (greenwashing, surveillance)
- Favoured independent oversight body to decide on routing

Path selection based on desired properties

TU Delft

Goal:
Enable control over the route one's data takes through the Internet



Idea: iteratively explore all possible paths such that ignored paths can only lead to worse solution.

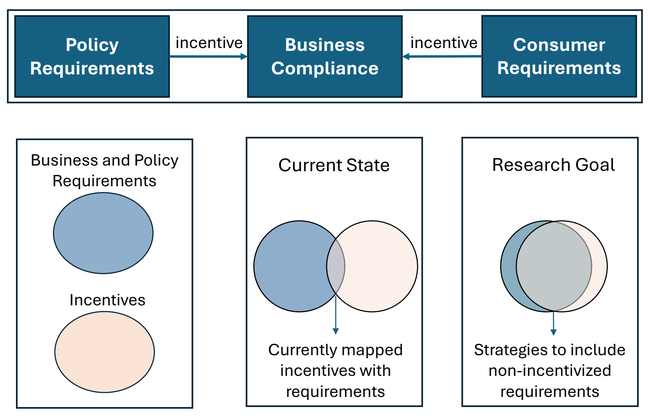
Novel path selection algorithm **quickly** selects the path through the Internet that fulfills as many of the user's **desiderata** (e.g., security level) as possible

Lesson learned:
Economic incentives needed to achieve support by network operators.

Investigation of ways to enable adoption

UNIVERSITY OF TWENTE.

Goal:
Alignment of policy and business requirements with incentives for stakeholder adoption of the Responsible Internet



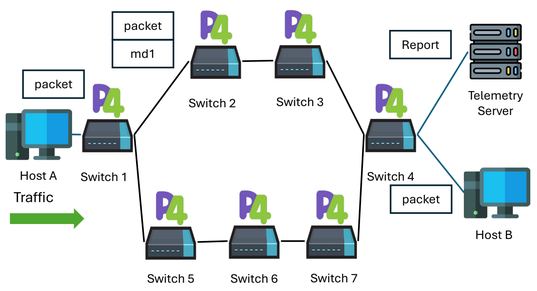
Lesson learned:
Business strategies need to align with digital governance policies

Transparency and Controllability through programmable data planes

University of Amsterdam

Goals:
- In-band network telemetry: transferring information of networking devices through traffic
  Light-weight: distribute desired information and optimize data transmission
- Utilise P4 programming language (high-level, open source)

Features:
- Path tracing: devices are identified, end-users informed about active path
- Trust: devices are evaluated, insight into network state
- Congestion estimates to avoid service interruption

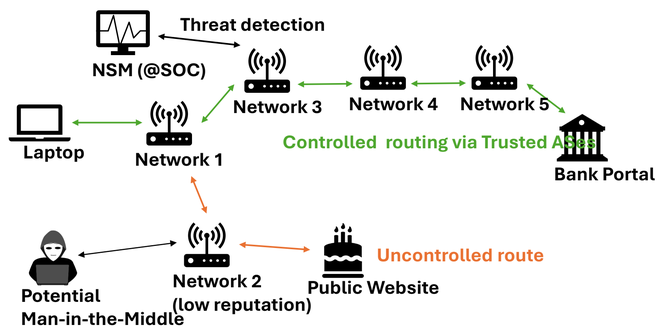


Lessons learned:
- Amount of information to be provided is decided by operator/programmer
- Capabilities of network devices (e.g, operations to enhance privacy) are bound by available resources

Enhancing Network Security Monitoring in the context of Security Operations Centres

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Goals:
- Monitoring as a feature: select route based on desired security properties
- Data enrichment: improved alert interpretability and analysis
- Enhanced monitoring rules: design principles to reduce workload



Lesson learned:
Rule-based methods are not fully developed – much potential left

Contact us: https://www.catrin.nl