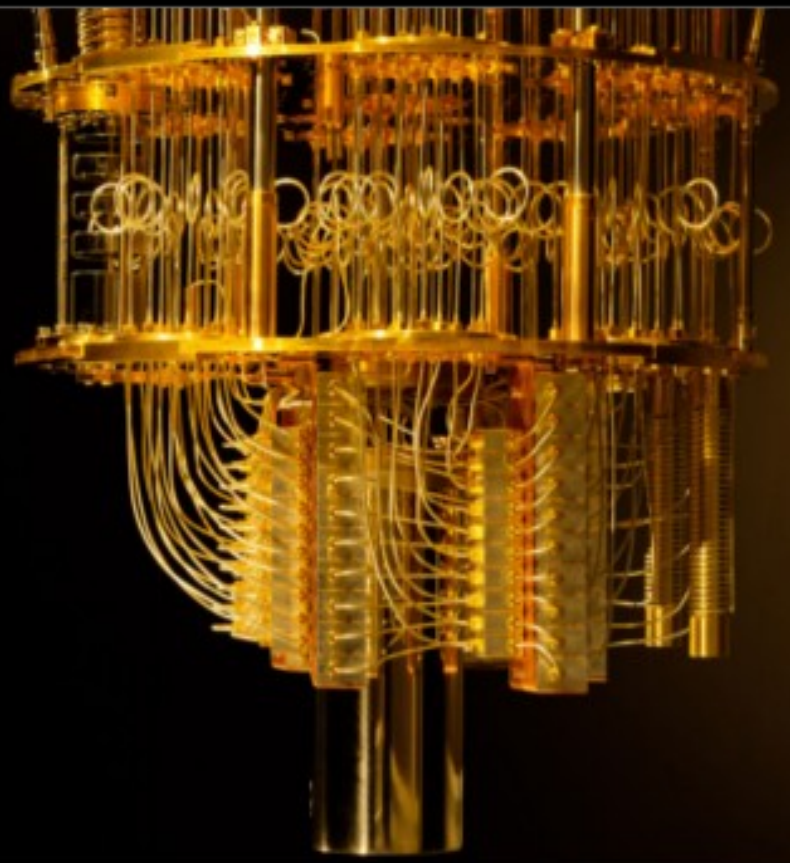
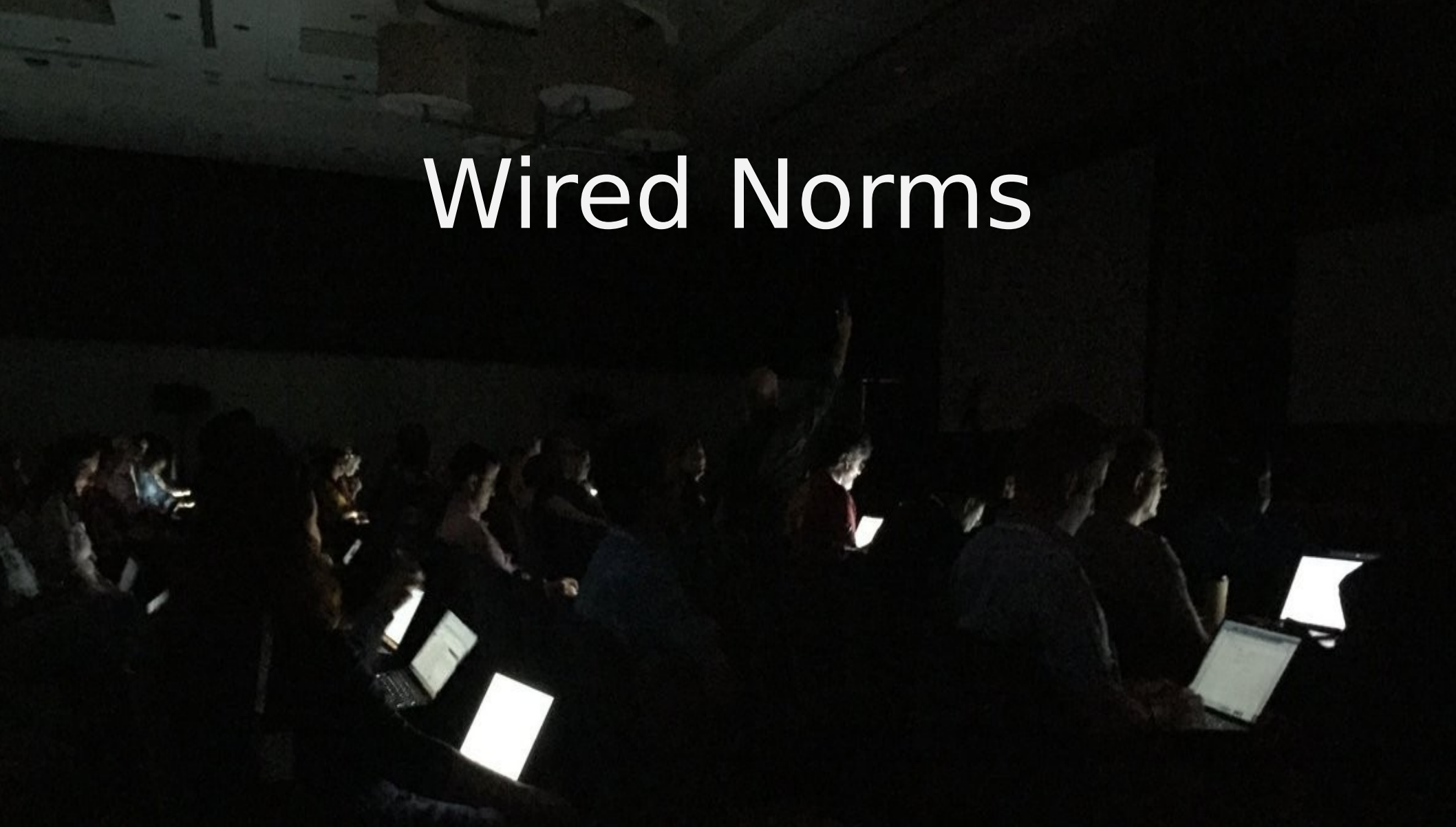
Niels ten Oever, PhD
Postdoctoral Researcher

University of Amsterdam
Texas A&M University

mail@nielstenoever.net
https://nielstenoever.net
@nielstenoever



Wired Norms



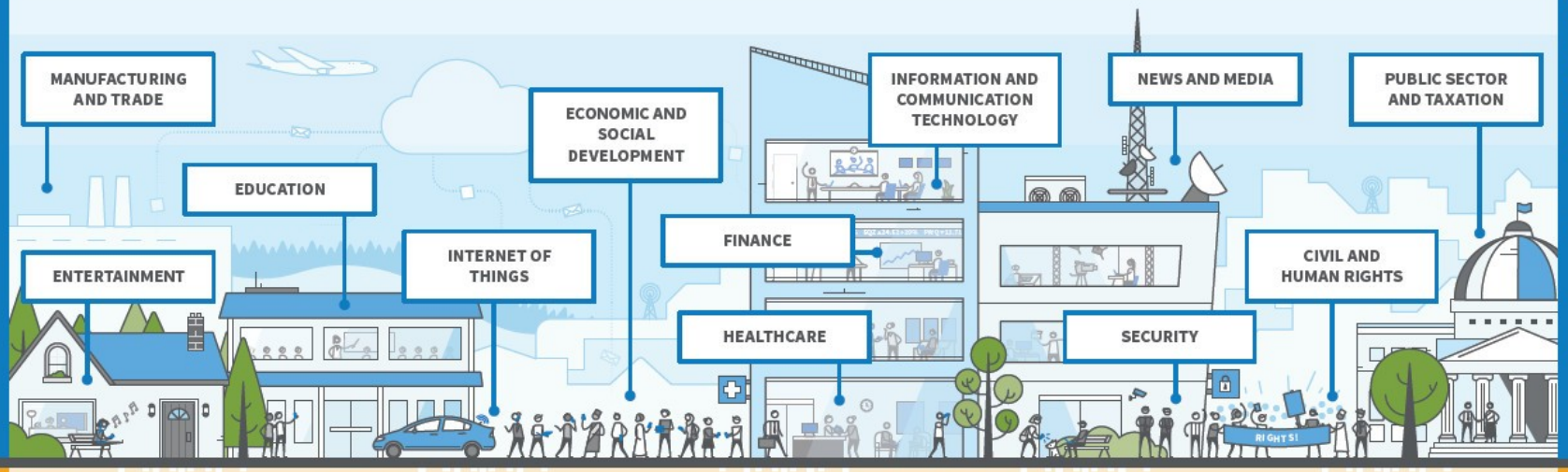
Inscription, resistance, and subversion in the governance of the Internet infrastructure

THE THREE LAYERS OF DIGITAL GOVERNANCE

No one person, government, organization, or company governs the digital space. Digital Governance may be stratified into the three layers depicted here: Infrastructure, Logical, Economic and Societal. Solutions to issues in each layer include policies, best practices, standards, specifications, and tools developed by the collaborations of stakeholders and experts from actors in business, government, academia, technical, and civil society. For a map of Digital Governance Issues and Solutions across all three layers, visit https://map.netmundial.org.

DIGITAL GOVERNANCE ACTORS

ECONOMIC AND SOCIETAL LAYER



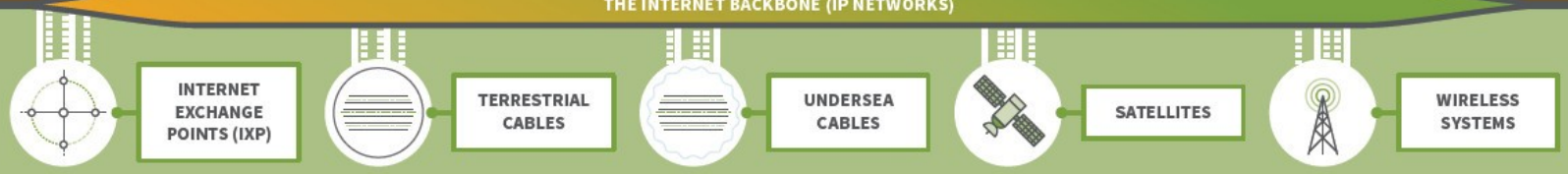
- IGF
- World Economic Forum
- NETmundial Initiative
- W3C
- Industrial Internet Consortium
- ISOC
- National Governments
- Private Sector (ex.: Facebook, Google, Sony, Alibaba)
- Inter-governmental Organizations (ex.: OECD, UNESCO, WTO, WIPO)
- Civil Society (ex.: Human Rights Watch, APC)
- Academia
- Law Enforcement Agencies (ex.: INTERPOL, FBI)

LOGICAL LAYER

- ICANN / IANA
- IETF
- NRO / RIRs
- ISO
- ETSI
- TLD Operators
- Domain Name Registrars
- IEEE
- W3C

INFRASTRUCTURE LAYER

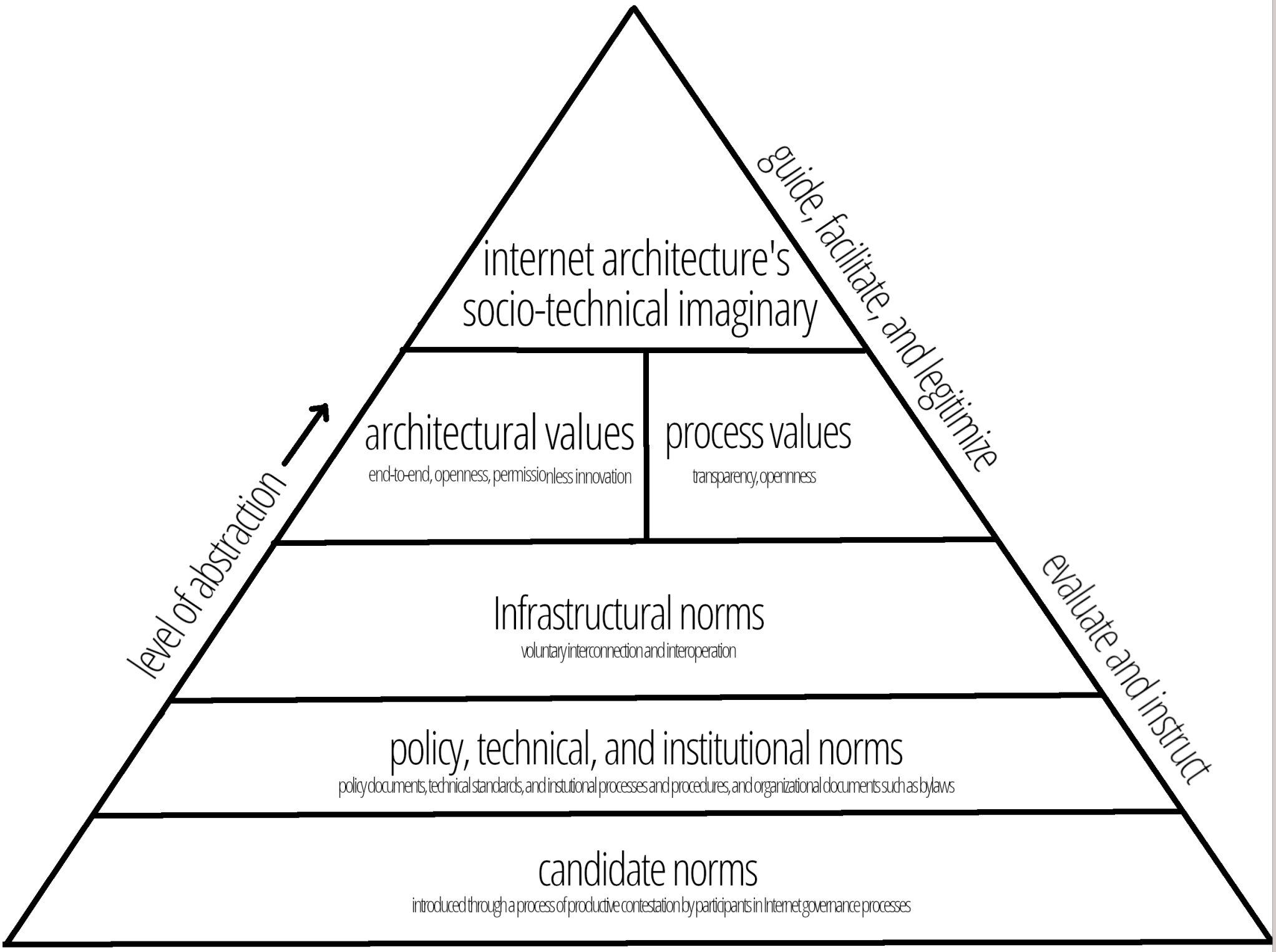
THE INTERNET BACKBONE (IP NETWORKS)



- GSMA
- IEEE
- IETF
- ITU
- National ICT Ministries
- National Regulators
- Network Operators

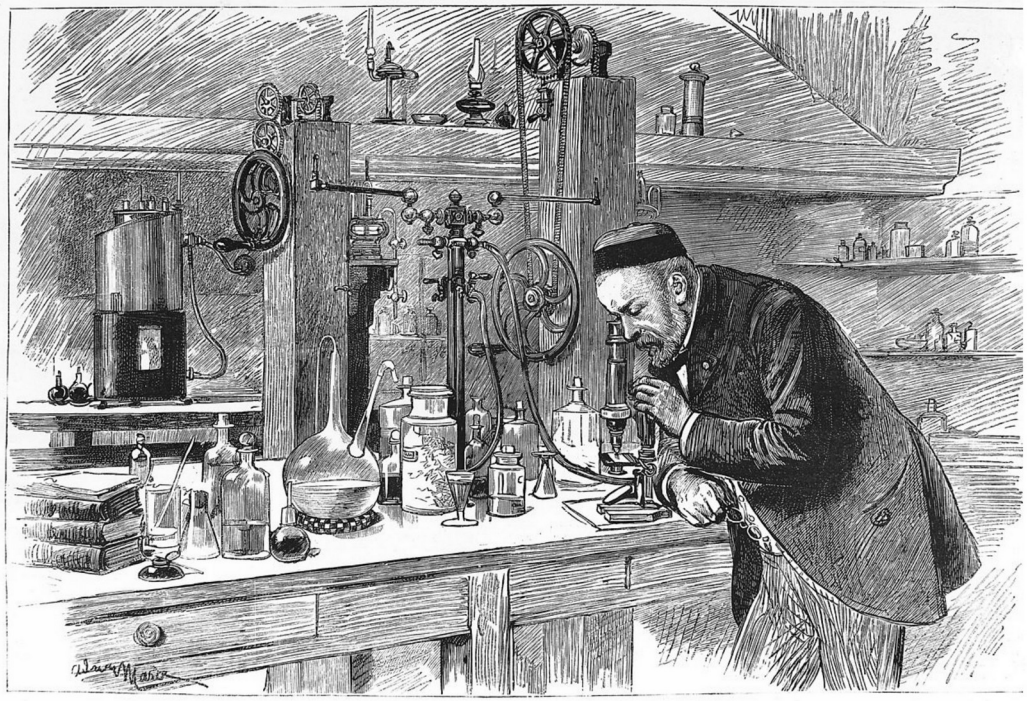
For public use. Designed by XPLANE, in assignment by ICANN. v2.1 • 16 December 2015

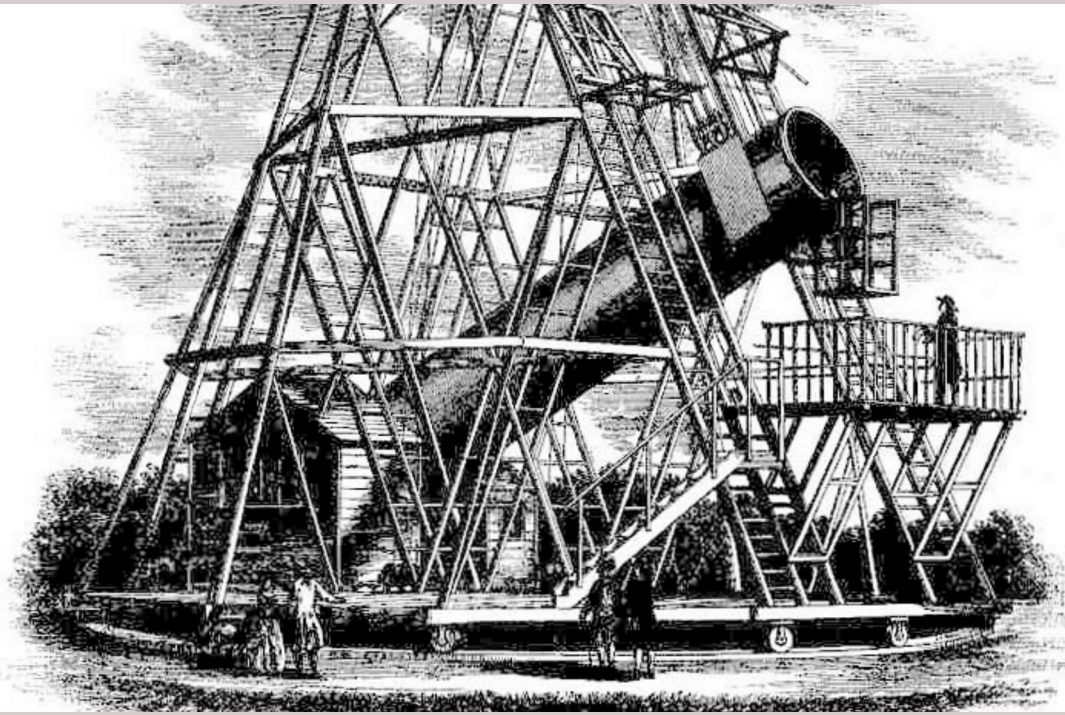
2015 | Creative Commons Attribution - NonCommercial


internet architecture's
socio-technical imaginary
architectural values
end-to-end, openness, permissionless innovation
process values
transparency, openness
Infrastructural norms
voluntary interconnection and interoperation
policy, technical, and institutional norms
policy documents, technical standards, and instutional processes and procedures, and organizational documents such as bylaws
candidate norms
introduced through a process of productive contestation by participants in Internet governance processes
level of abstraction
guide, facilitate, and legitimize
evaluate and instruct

‘This is not how we imagined it’

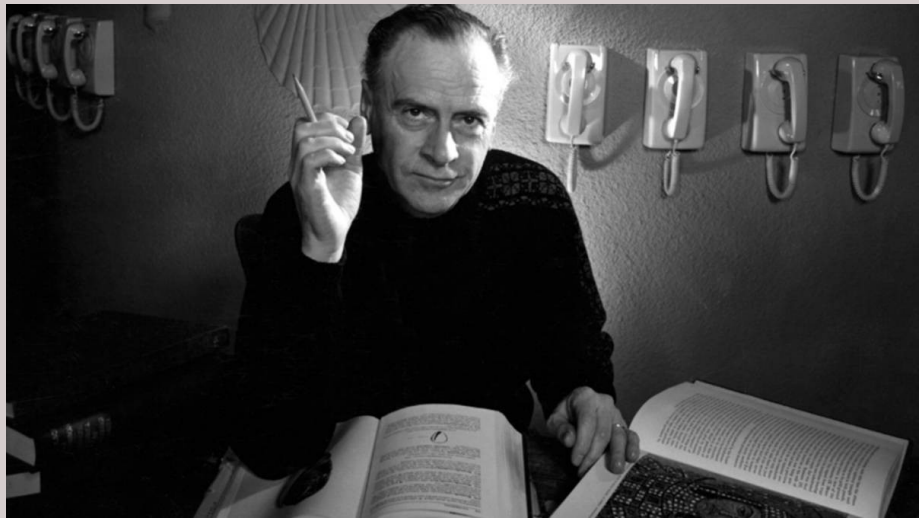
the
Inscription and Subversion
of Values in
Transnational Internet
Infrastructure Governance





The medium is the message

– Marshall McLuhan



‘Infrastructure sets the invisible rules that govern the spaces of our everyday lives’

‘changes to the globalising world are being written, not in the language of law and diplomacy, but rather in the language of infrastructure’

– Keller Easterling

The uses made of technology are largely determined by the structure of the technology itself

– Neil Postman

We shape our tools
and thereafter they shape us.

–John Culkin

Infrastructure is both relational and ecological

– Susan Leigh Star

Affordances

- Constraining as well as enabling features
- ‘functional and relational aspects which frame, while not determining, the possibilities’

– Ian Hutchby

A sociotechnical imaginary:

- visions,
- symbols,
- futures

that exist in groups and society which influence:

- behavior, individual and collective identity,
- development of narratives,
- policy,
- Technology,
- institutions

Co-production: the simultaneous processes through which modern societies form their epistemic and normative understandings of the world

– Sheila Jasanoff

[Docs] [txt|pdf] [draft-iab-princ...] [Tracker] [Diff1] [Diff2]

Updated by: 3439 INFORMATIONAL

Network Working Group B. Carpenter, Editor
Request for Comments: 1958 IAB
Category: Informational June 1996

Architectural Principles of the Internet

Status of This Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

The Internet and its architecture have grown in evolutionary fashion from modest beginnings, rather than from a Grand Plan. While this process of evolution is one of the main reasons for the technology's success, it nevertheless seems useful to record a snapshot of the current principles of the Internet architecture. This is intended for general guidance and general interest, and is in no way intended to be a formal or invariant reference model.

Table of Contents

1. Constant Change

In searching for Internet architectural principles, we must remember that technical change is continuous in the information technology industry. The Internet reflects this. Over the 25 years since the ARPANET started, various measures of the size of the Internet have increased by factors between 1000 (backbone speed) and 1000000 (number of hosts). In this environment, some architectural principles inevitably change. Principles that seemed inviolable a few years ago are deprecated today. Principles that seem sacred today will be deprecated tomorrow. The principle of constant change is perhaps the

Technology is a very human activity
– and so is the history of
technology.

– Melvin Kranzberg

Standard setting is a wild mix of politics and economics

– Shapiro and Varian

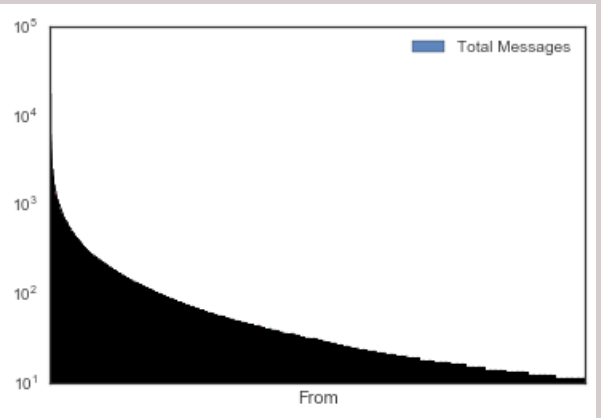
Theoretical framework

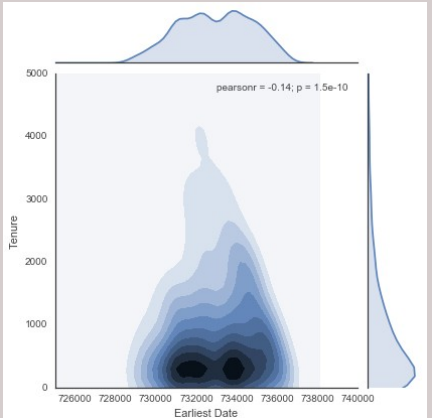
- Science and Technology Studies
  - Technological materiality
  - Co-production
  - Socio-technical imaginaries

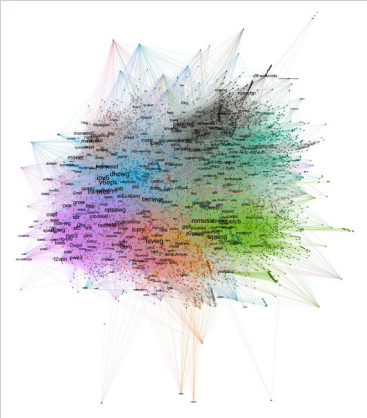
- International Political Economy
  - Consolidation / Market concentration
  - Self-regulation
  - Commercialization

Methods

- 25 interviews
- Quantitative analysis of all RFCs
- Qualitative analysis of 25 RFCs
- Quantitative and qualitative mailinglist analysis (35 GB, 1.944.019 e-mails, 955 lists)
- Participant observation during four years (11 meetings)



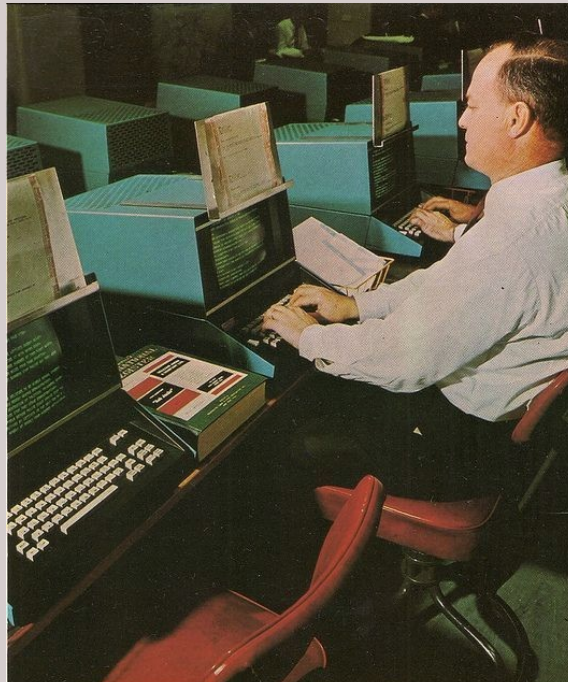




Internet Architecture Imaginary (1)

- End-to-end principle
  - Intelligence at the edges
  - Network only provides datagram transport
  - Low complexity
  - High robustness

  But...



The purpose of this document is not, therefore, to lay down dogma about how Internet protocols should be designed, or even about how they should fit together. Rather, it is to convey various guidelines that have been found useful in the past, and that may be useful to those designing new protocols or evaluating such designs.

A good analogy for the development of the Internet is that of constantly renewing the individual streets and buildings of a city, rather than razing the city and rebuilding it. The architectural principles therefore aim to provide a framework for creating cooperation and standards, as a small "spanning set" of rules that generates a large, varied and evolving space of technology.

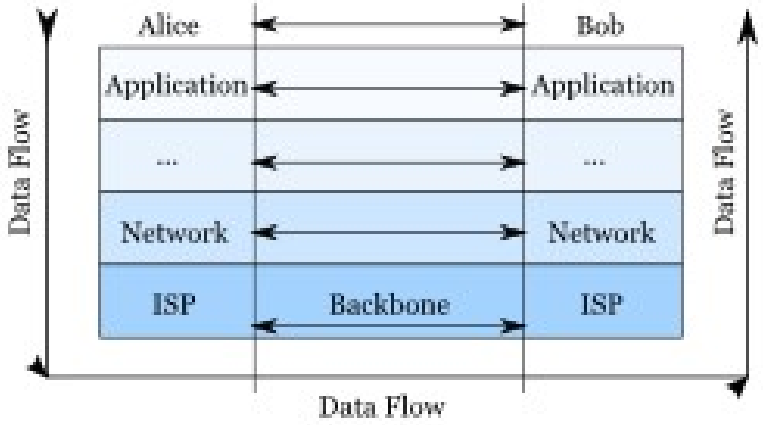
Some current technical triggers for change include the limits to the scaling of IPv4, the fact that gigabit/second networks and multimedia present fundamentally new challenges, and the need for quality of service and security guarantees in the commercial Internet.

As Lord Kelvin stated in 1895, "Heavier-than-air flying machines are impossible." We would be foolish to imagine that the principles listed below are more than a snapshot of our current understanding.

2. Is there an Internet Architecture?

2.1 Many members of the Internet community would argue that there is no architecture, but only a tradition, which was not written down for the first 25 years (or at least not by the IAB). However, in very general terms, the community believes that the goal is connectivity, the tool is the Internet Protocol, and the intelligence is end to end rather than hidden in the network.

End-to-end principle



(Another step is to choose leaders that we trust to exercise their good judgement and do the right thing. But we're already trying to do that.)

4. Issues with Scoping the IETF's Mission

4.1. The Scope of the Internet

A very difficult issue in discussing the IETF's mission has been the scope of the term "for the Internet". The Internet is used for many things, many of which the IETF community has neither interest nor competence in making standards for.

The Internet isn't value-neutral, and neither is the IETF. We want the Internet to be useful for communities that share our commitment to openness and fairness. We embrace technical concepts such as decentralized control, edge-user empowerment and sharing of resources, because those concepts resonate with the core values of the IETF community. These concepts have little to do with the technology that's possible, and much to do with the technology that we choose to create.

Internet Architecture Imaginary (2)

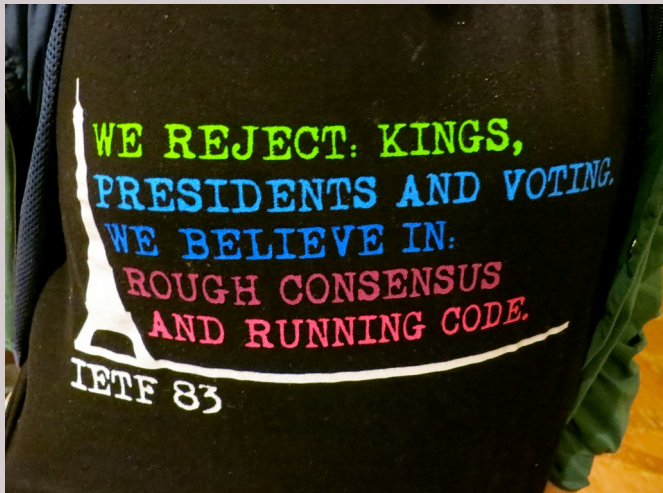
- Permissionless innovation
  - No barriers for deployment of new protocols
  - No need to negotiate with entities in the middle of the network
  - Response to Telco era (and perhaps Acceptible Use Policy of ARPANET & NSFnet)

Internet Architecture Imaginary (3)

- Openness (network)
  - Reach any endpoint on the Internet without being hampered, altered or stopped
  - Ability to add new endpoints to the network
- Open standards
  - Voluntary
  - Freely accessible
- Open governance
  - Transparent
  - Open participation
  - Open archives

We reject: kings,
presidents and voting.
We believe in: rough consensus
and running code.

- Quote from Dave Clarke in the Tao of the IETF



Explicit discussions about rights and freedoms, as well as social impact of technology have featured in RFCs since their beginnings

-Sandra Braman

Commercialization & Privatization (end 80s, early 90s)

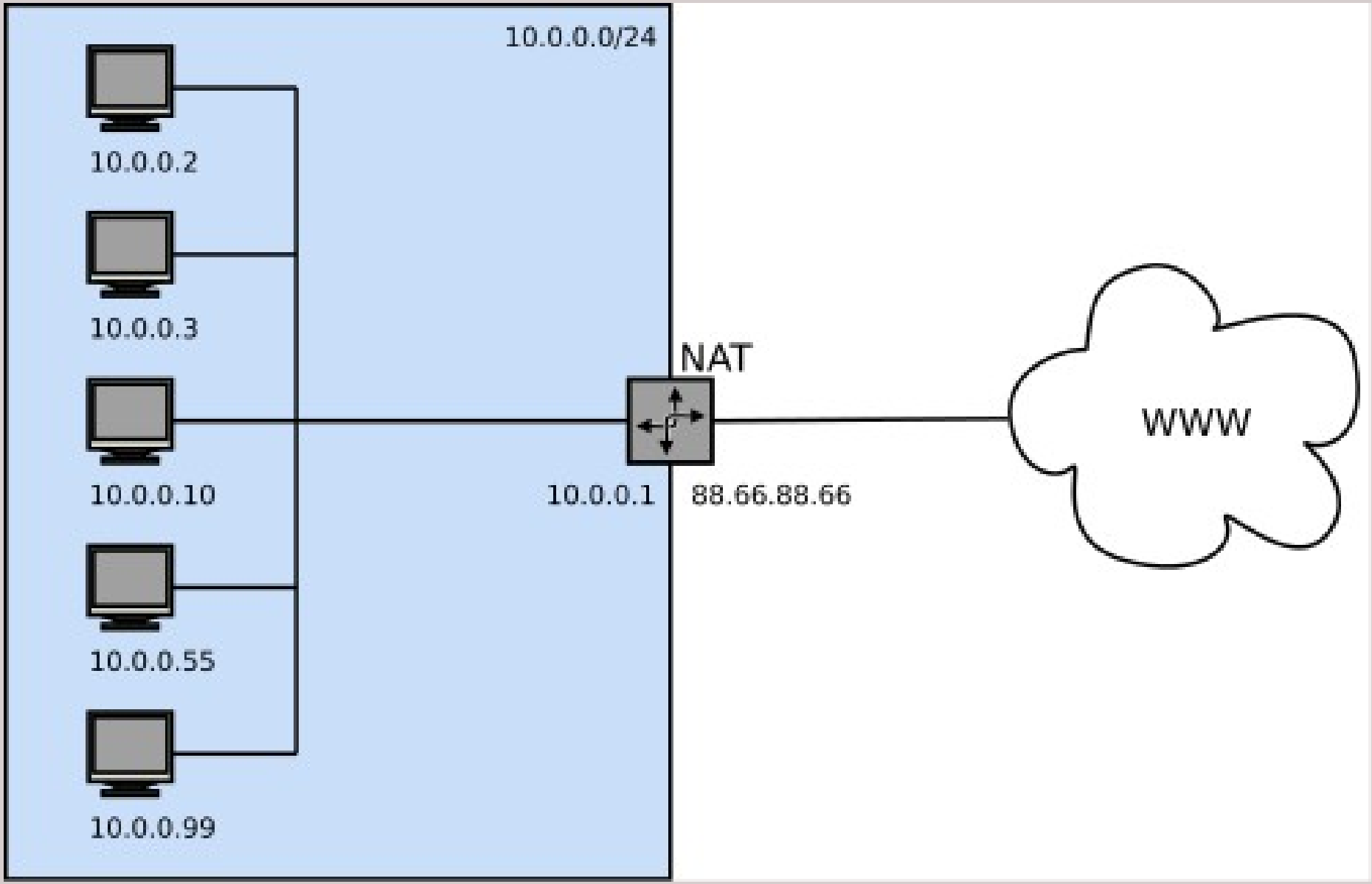
- US government cedes direct control:
  - ARAPNET (Dept of Defense)
  - NSFNET (Dept of Education)
  - ESNET (Dept of Energy)
- Establishment of Commercial Internet Exchanges
- Formal institutionalization of:
  - Internet Engineering Taskforce
  - Internet Society
  - Regional Internet Registries

Crack in the imaginary: Rise of the Middlebox

- IPv4 running out
  - ‘only’ 4.3 billion IP addresses
  - No replacement done yet
- Security considerations
  - Internet was no longer comprised of trusted actors
- Perceived need from network operators differentiate business models

(RFC3725)

Network Address Translation

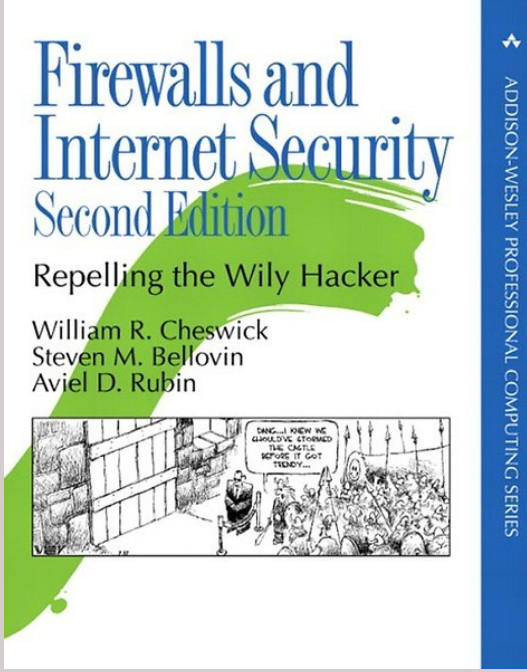


Firewalls

- Security
- Administrative control

‘a lot of networks do a lot of bad things to peer-to-peer traffic’

‘firewalls didn't serve only a security purpose, they also served an administrative control purpose, that's a third party in the midst of the peers who are talking to each other. So it's been difficult for Internet peer to peer things to take off. ‘

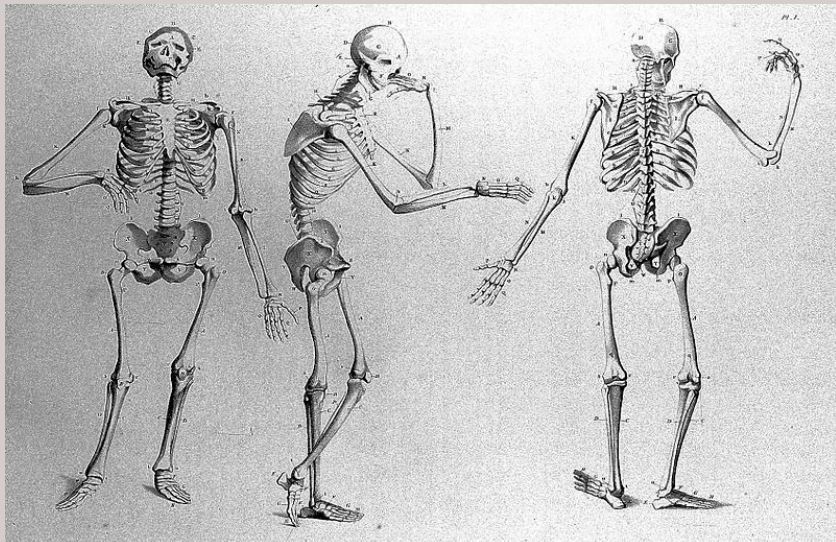


Network management

- Quality of service
- Caching
- Prioritization of services

Rise of the Middlebox (4)

- Added functionality to the network
- Not at the edges, but in the network
- This led to ‘ossification’
- Introduced directionality, created users and producers
- Created a new **affordance structure** in the Internet architecture



Example 1 : TLS1.3

```
If a server established a TLS connection with a previous version of
TLS and receives a TLS 1.3 ClientHello in a renegotiation, it MUST
retain the previous protocol version.  In particular, it MUST NOT
negotiate TLS 1.3.

Structure of this message:

   uint16 ProtocolVersion;
   opaque Random[32];

   uint8 CipherSuite[2];    /* Cryptographic suite selector */

   struct {
       ProtocolVersion legacy_version = 0x0303;    /* TLS v1.2 */
       Random random;
       opaque legacy_session_id<0..32>;
       CipherSuite cipher_suites<2..2^16-2>;
       opaque legacy_compression_methods<1..2^8-1>;
       Extension extensions<8..2^16-1>;
   } ClientHello;
```

Example 2: Stream Control Transmission Protocol

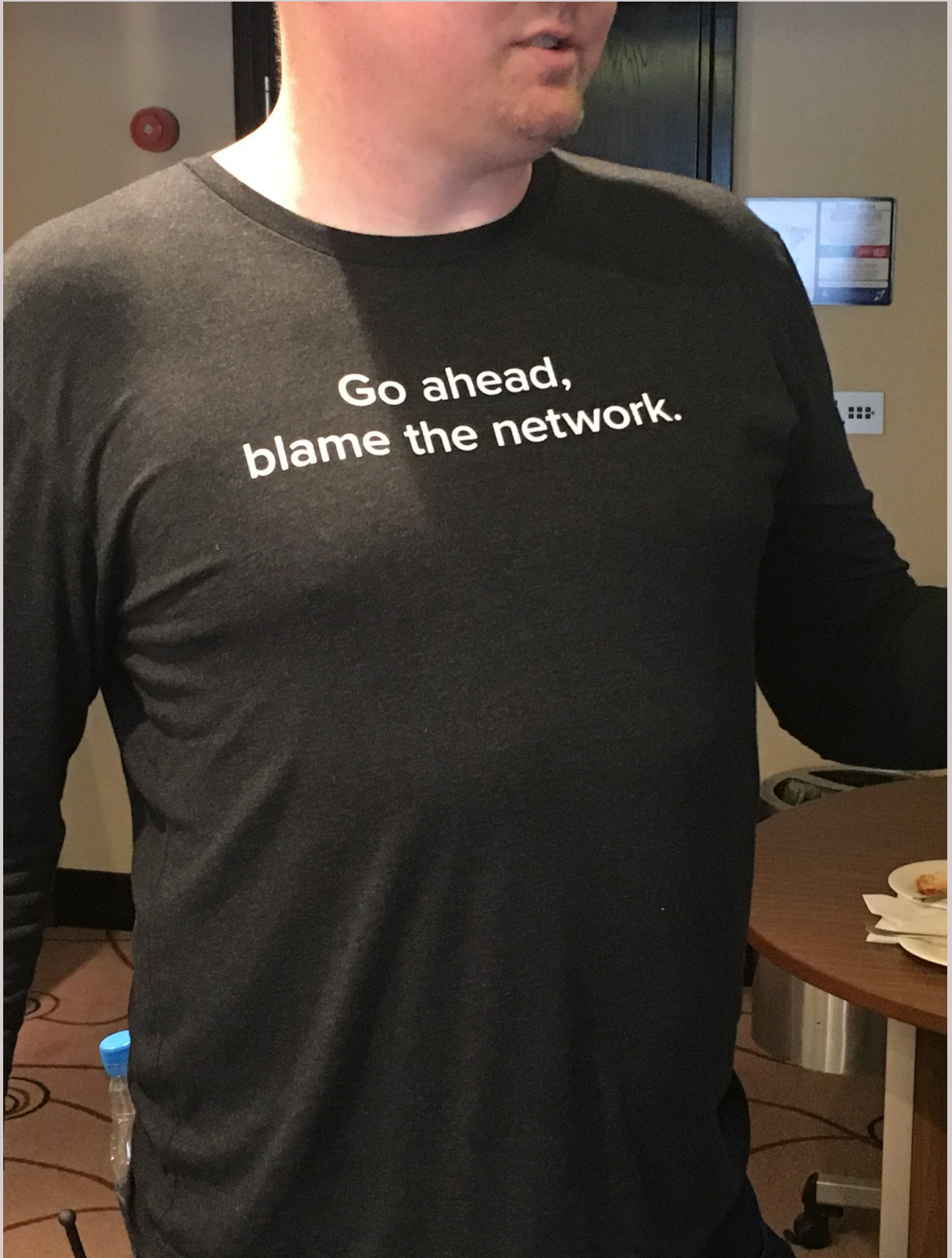
- Transport layer replacement for TCP
- Multiple streams
- Multiple transmission paths
- No head of line blocking
- Described in 39 (!) RFCs
- Worked perfectly in the lab
- Blocked by many NATs
- Never reliably worked on the Internet
- Because of reordered affordances

First RFC:
April 2002

Last RFC:
November 2017

Protocol
Failure

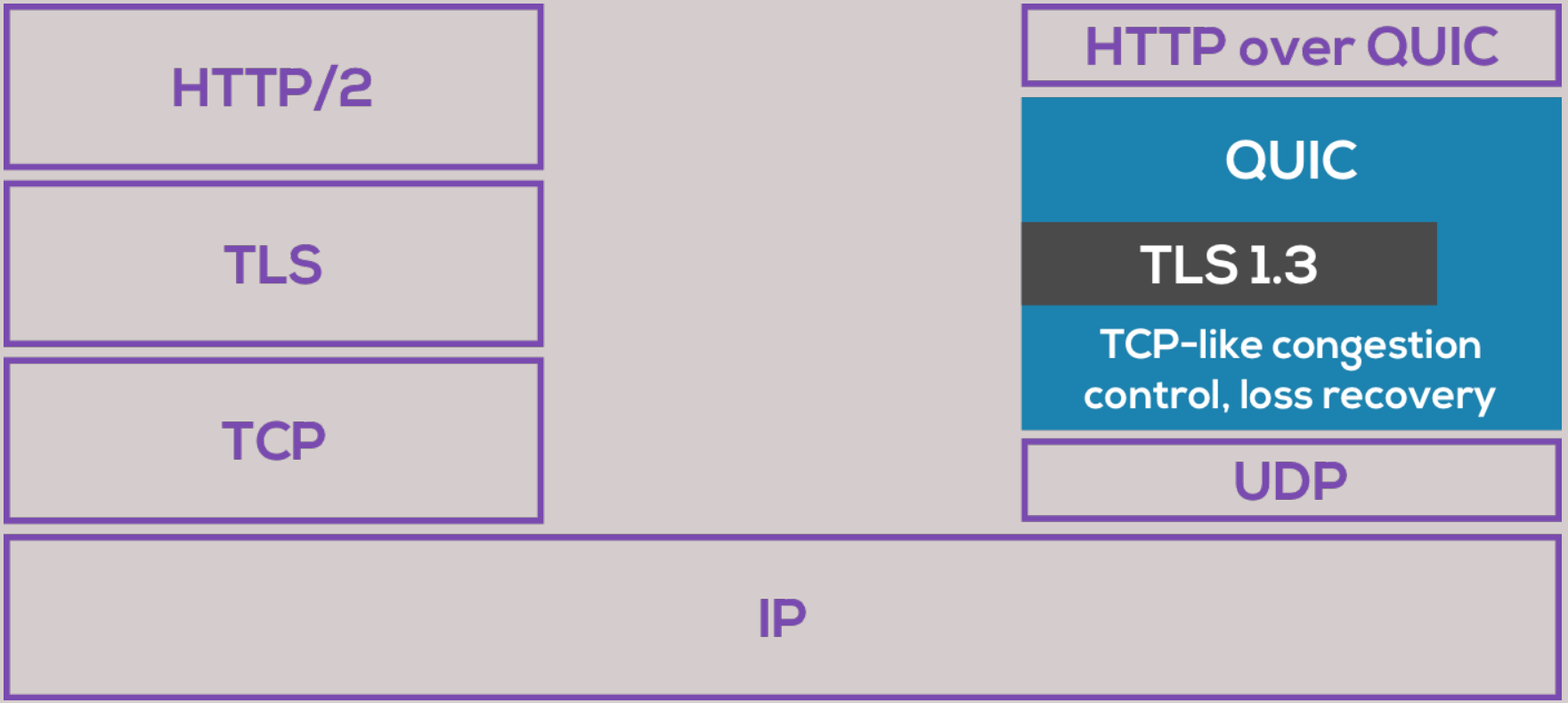
- RFC8261: Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets
- RFC8087: The Benefits of Using Explicit Congestion Notification (ECN) informational
- RFC7829: SCTP-PF: A Quick Failover Algorithm for the Stream Control Transmission Protocol
- RFC7765: TCP and Stream Control Transmission Protocol (SCTP) RTO Restart experimental
- RFC7605: Recommendations on Using Assigned Transport Port Numbers bcp
- RFC6951: UDP Encapsulation of Stream Control Transmission Protocol (SCTP) Packets for End-Host to End-Host Communication
- RFC6633: Deprecation of ICMP Source Quench Messages
- RFC6526: IP Flow Information Export (IPFIX) Per Stream Control Transmission Protocol (SCTP) Stream
- RFC6525: Stream Control Transmission Protocol (SCTP) Stream Reconfiguration
- RFC6458: Sockets API Extensions for the Stream Control Transmission Protocol (SCTP) informational
- RFC6096: Stream Control Transmission Protocol (SCTP) Chunk Flags Registration
- RFC6084: General Internet Signaling Transport (GIST) over Stream Control Transmission Protocol (SCTP) and Datagram Transport Layer Security (DTLS) experimental
- RFC6083: Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)
- RFC6053: Implementation Report for Forwarding and Control Element Separation (ForCES) informational
- RFC5923: Connection Reuse in the Session Initiation Protocol (SIP)
- RFC5827: Early Retransmit for TCP and Stream Control Transmission Protocol (SCTP) experimental
- RFC5811: SCTP-Based Transport Mapping Layer (TML) for the Forwarding and Control Element Separation (ForCES) Protocol
- RFC5062: Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures informational
- RFC5061: Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration
- RFC5043: Stream Control Transmission Protocol (SCTP) Direct Data Placement (DDP) Adaptation
- RFC4960: Stream Control Transmission Protocol
- RFC4895: Authenticated Chunks for the Stream Control Transmission Protocol (SCTP)
- RFC4820: Padding Chunk and Parameter for the Stream Control Transmission Protocol (SCTP)
- RFC4666: Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)
- RFC4460: Stream Control Transmission Protocol (SCTP) Specification Errata and Issues informational
- RFC4233: Integrated Services Digital Network (ISDN) Q.921-User Adaptation Layer
- RFC4168: The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)
- RFC4166: Telephony Signalling Transport over Stream Control Transmission Protocol (SCTP) Applicability Statement informational
- RFC4138: Forward RTO-Recovery (F-RTO): An Algorithm for Detecting Spurious Retransmission Timeouts with TCP and the Stream Control Transmission Protocol (SCTP) experimental
- RFC3873: Stream Control Transmission Protocol (SCTP) Management Information Base (MIB)
- RFC3868: Signalling Connection Control Part User Adaptation Layer (SUA)
- RFC3807: V5.2-User Adaptation Layer (V5UA)
- RFC3758: Stream Control Transmission Protocol (SCTP) Partial Reliability Extension
- RFC3708: Using TCP Duplicate Selective Acknowledgement (DSACKs) and Stream Control Transmission Protocol (SCTP) Duplicate Transmission Sequence Numbers (TSNs) to Detect Spurious Retransmissions experimental
- RFC3554: On the Use of Stream Control Transmission Protocol (SCTP) with IPsec
- RFC3436: Transport Layer Security over Stream Control Transmission Protocol
- RFC3331: Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer
- RFC3286: An Introduction to the Stream Control Transmission Protocol (SCTP) informational
- RFC3257: Stream Control Transmission Protocol Applicability Statement informational


Go ahead,
blame the network.

The return of the strong endpoints: The Rise of QUIC

- Quick UDP Internet Protocol (QUIC)
- Stream-based protocol
- Similar to SCTP, but..
  - Developed by Google
    - Communicate between Google servers (CDNs) and browsers (mainly Chrome)
    - Experimental A/B testing
- Fallback to TCP

Includes encryption by default...

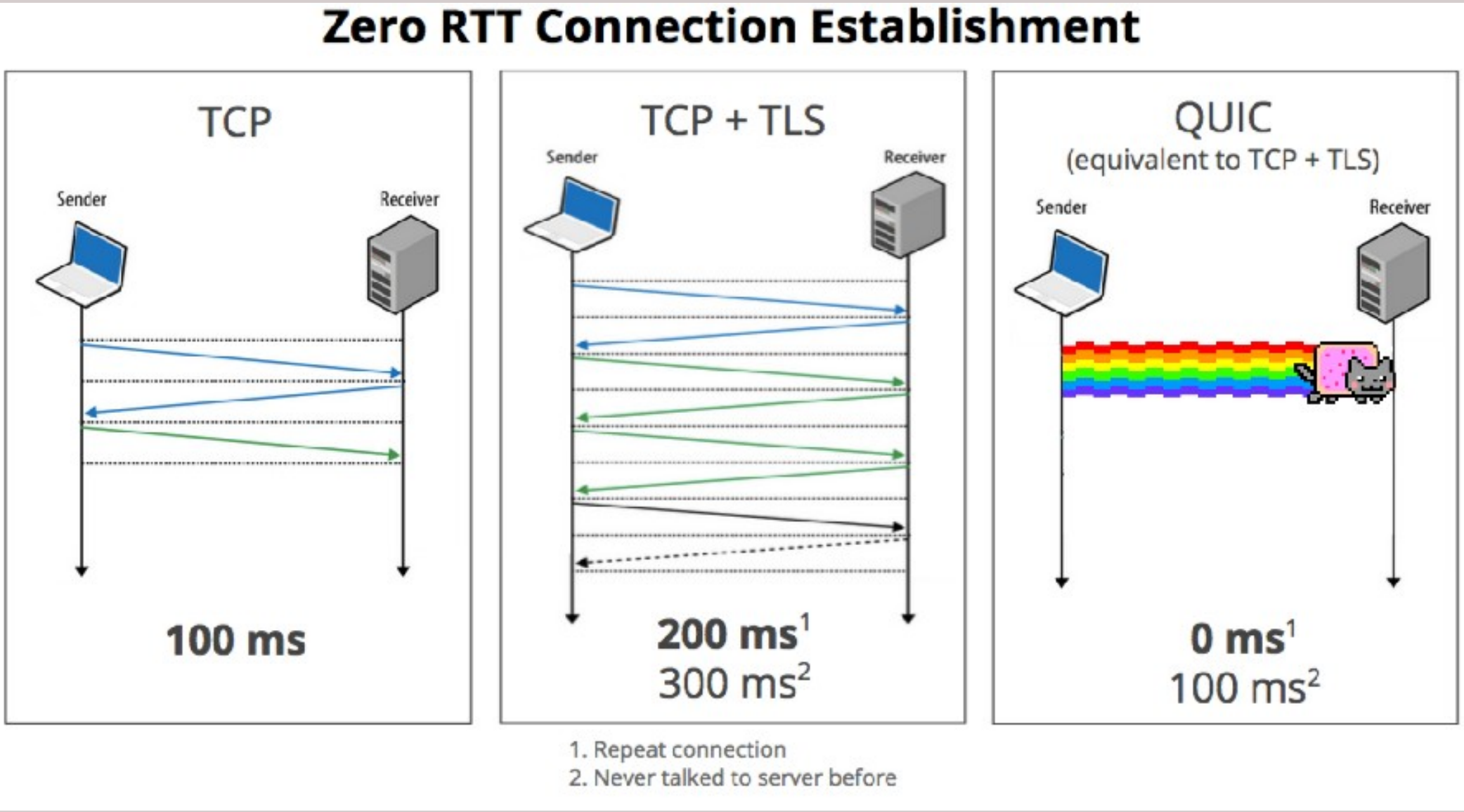


...as much as possible

“Let’s not share anything [with the network] unless we really need to because I don't care whether it’s ossified or whether it’s not. We’ve tried this in the past and we’ve failed because people ossify whatever is visible. I don't care what they can and cannot use it for. I just don't want to share it unless there is…

The burden of proof, in my opinion, is on the operators to say we really, really, really can’t run our networks unless we see this one bit. And if they can prove that, then maybe it’s fine at that point.”

Latency wins

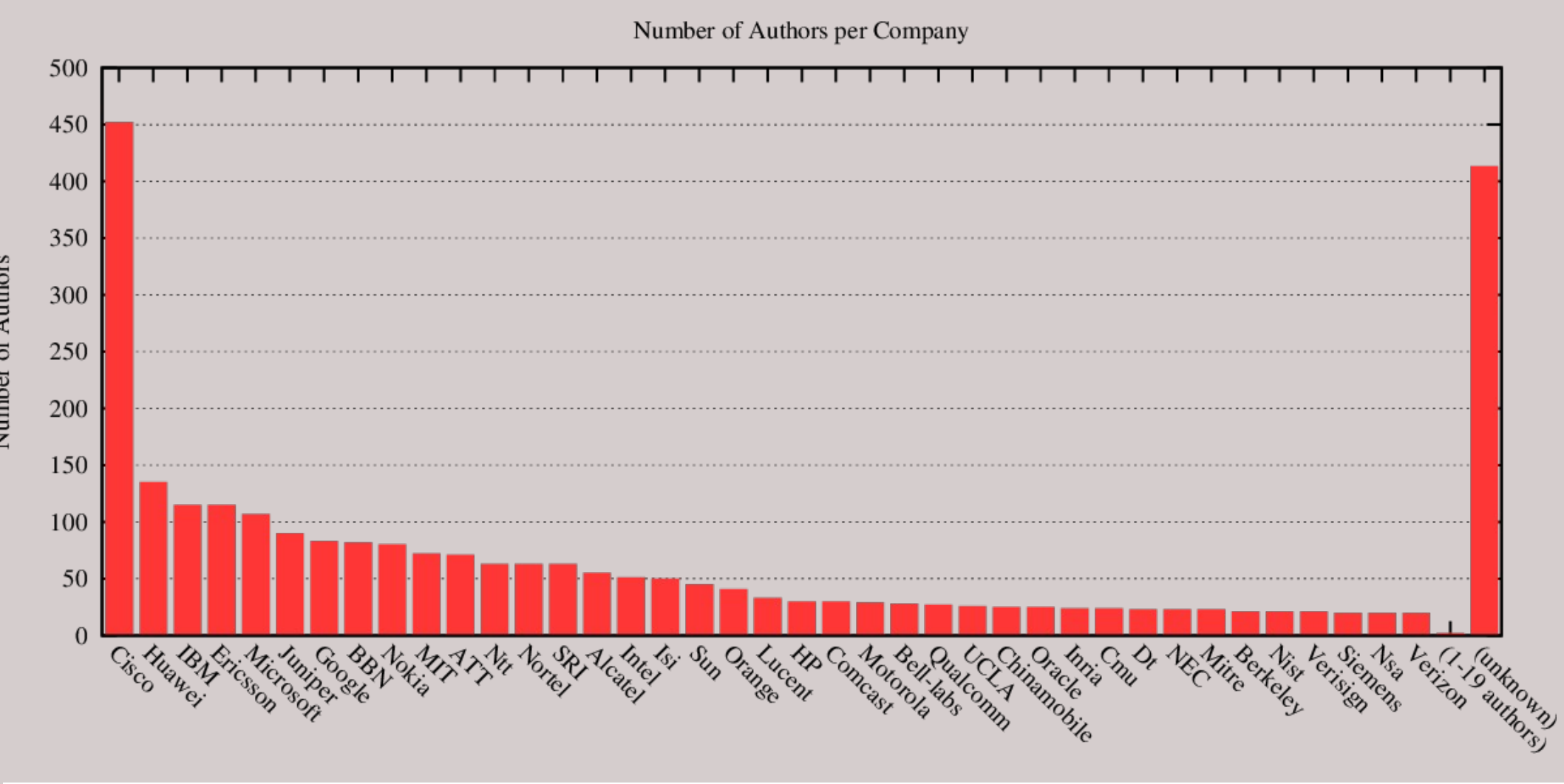


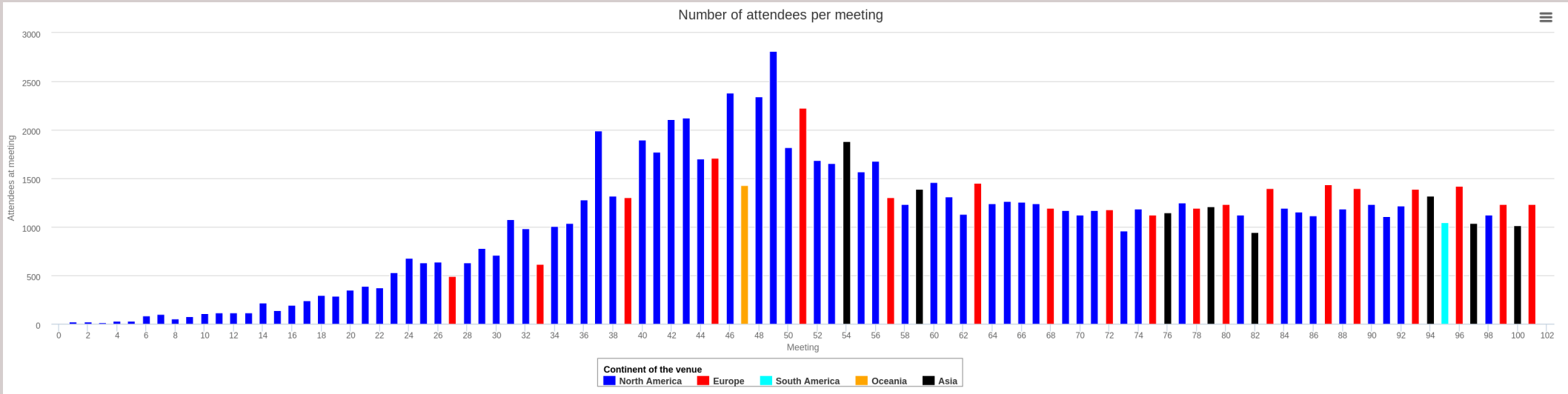
All's well that end(-to-end)s well?

- Only large effort by a transnational corporation with significant control of the network could make this evolution, and change affordance structure
- QUIC tooling not readily available (yet)
- QUIC deployment will arguably strengthen consolidation
- NAT directionality is still in place, equality of nodes is by no means restores
- With ubiquitous encryption it is harder to analyze on the network (for researchers as well)
- Network operators are not pleased

Imaginaries They Are A-Changin’

‘you need to play in some of the operators or vendors earning models in order to get something deployed’


Number of Authors per Company
Number of Authors
500
450
400
350
300
250
200
150
100
50
0
Cisco
Huawei
IBM
Ericsson
Microsoft
Juniper
Google
BBN
Nokia
MIT
ATT
Ntt
Nortel
SRI
Alcatel
Intel
Isi
Sun
Orange
Lucent
HP
Comcast
Motorola
Bell-labs
Qualcomm
UCLA
Chinamobile
Oracle
Inria
Cmu
Dt
NEC
Mitre
Berkeley
Nist
Verisign
Siemens
Nsa
Verizon
(1-19 authors)
(unknown)


Number of attendees per meeting
Attendees at meeting
3000
2500
2000
1500
1000
500
0
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64 66 68 70 72 74 76 78 80 82 84 86 88 90 92 94 96 98 100 102
Meeting
Continent of the venue
North America
Europe
South America
Oceania
Asia

‘[m]yths are important for what they reveal (including a genuine desire for community and democracy) and for what they conceal (including the growing concentration of communication power in a handful of transnational media businesses)’

– Vincent Mosco

intermediary conclusion (1)

The sociotechnical Internet architecture imaginary and its self-regulatory governance model have **not been able to safeguard freedom and equality** of researchers, small companies or individuals to innovate on the Internet protocol level.

Permissionless innovation, for the purpose of retaining openness, has undermined itself and the end-to-end principle.

Intermediary conclusion (2)

Corporate interests have become a first-order consideration for protocols to be adopted and implemented

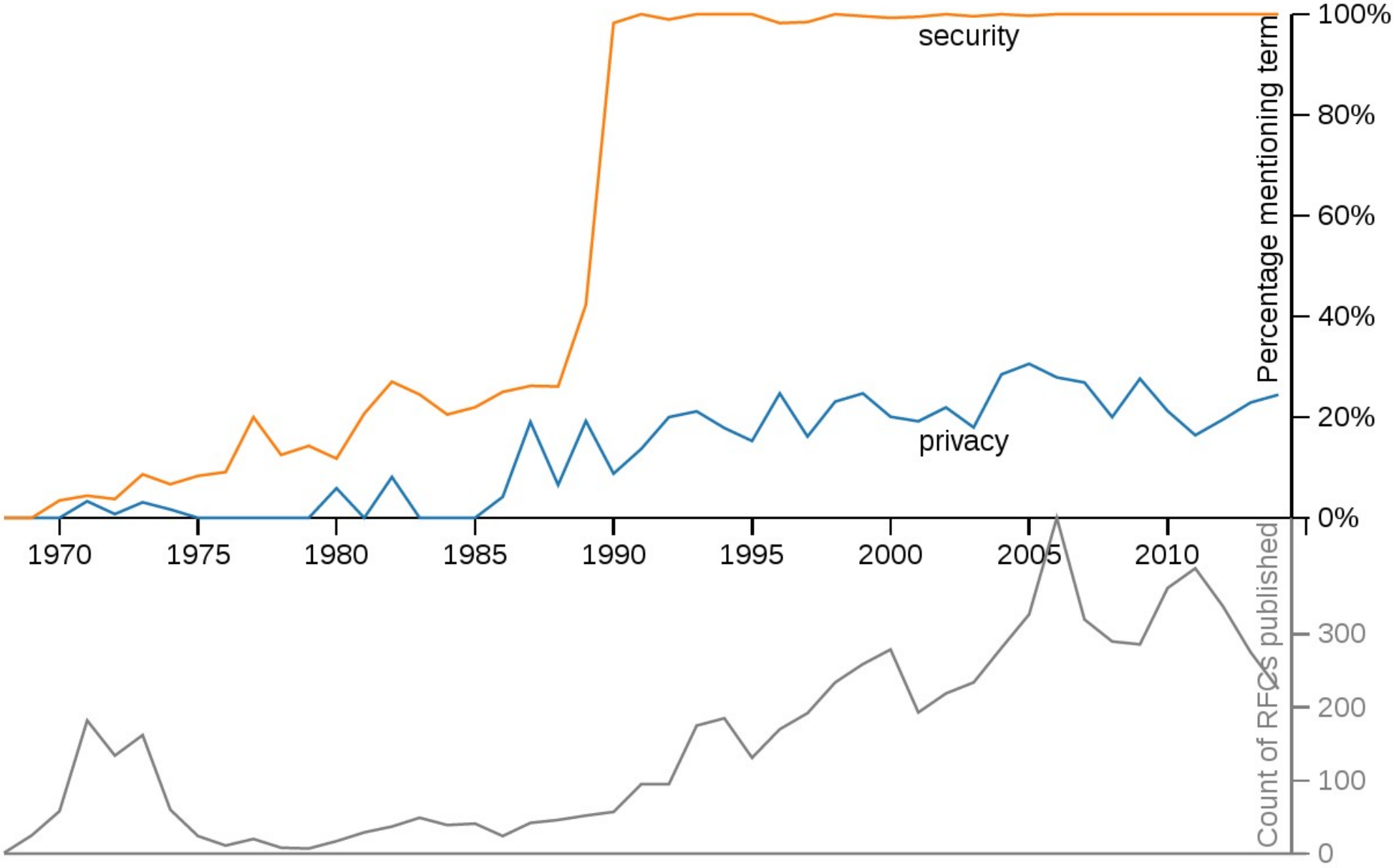
Political conceptions of the architectural imaginary are fading into the background.

Intermediary conclusion (3)

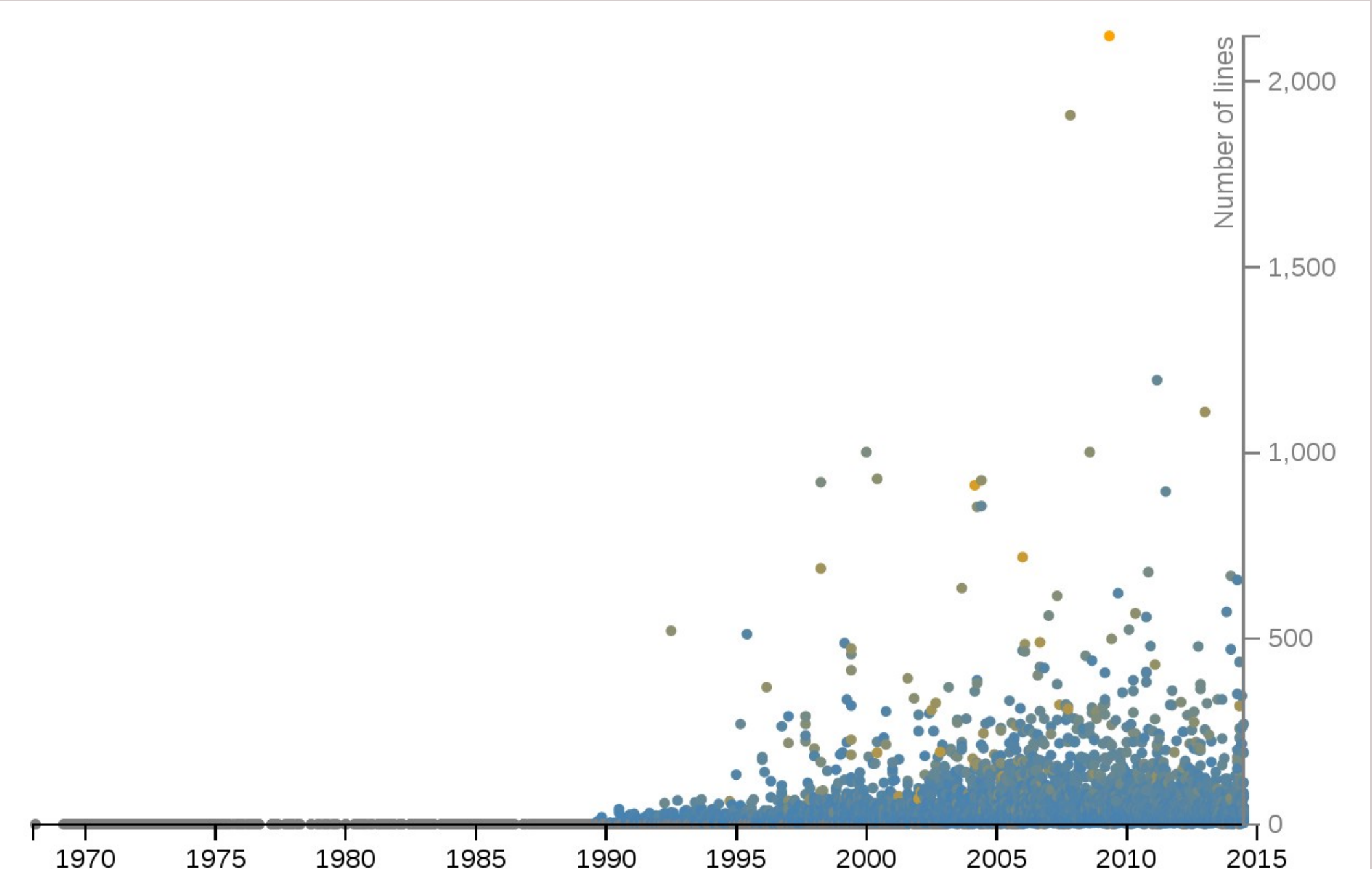
The importance and size of the Internet architecture has only grown, and with it its societal implications.

Societal implications are not structurally considered.

Increased work on security



Length of security considerations



Internet Research Task Force (IRTF)
Request for Comments: 8280
Category: Informational
ISSN: 2070-1721

N. ten Oever
ARTICLE 19
C. Cath
Oxford Internet Institute

October 2017

Research into Human Rights Protocol Considerations

Abstract

This document aims to propose guidelines for human rights considerations, similar to the work done on the guidelines for privacy considerations (RFC 6973). The other parts of this document explain the background of the guidelines and how they were developed.

This document is the first milestone in a longer-term research effort. It has been reviewed by the Human Rights Protocol Considerations (HRPC) Research Group and also by individuals from outside the research group.

8. Human Rights Considerations

At the time of publication of this document, there was a growing interest in considering the impacts that IETF (and IRTF) work can have on human rights; some related research is discussed in [RFC8280]. As such, the human rights considerations of TLS-PWD are presented here.

The key exchange underlying TLS-PWD uses public key cryptography to perform authentication and authenticated key exchange. The keys it produces can be used to establish secure connections between two people to protect their communication. Implementations of TLS-PWD, like implementations of other TLS ciphersuites that perform authentication and authenticated key establishment, are considered "armaments" or "munitions" by many governments around the world.

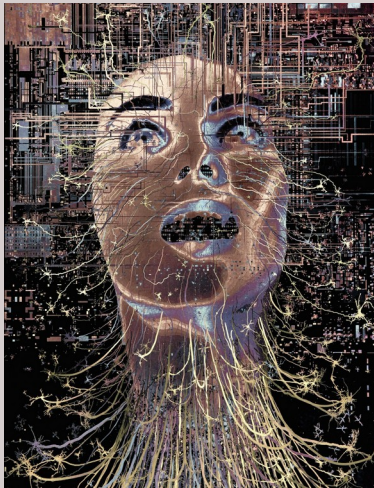
The most fundamental of human rights is the right to protect oneself. The right to keep and bear arms is an example of this right. Implementations of TLS-PWD can be used as arms, kept and borne, to defend oneself against all manner of attackers -- criminals, governments, lawyers, etc. TLS-PWD is a powerful tool in the promotion and defense of universal human rights.

Norm conflict in the governance of transnational and distributed infrastructures:

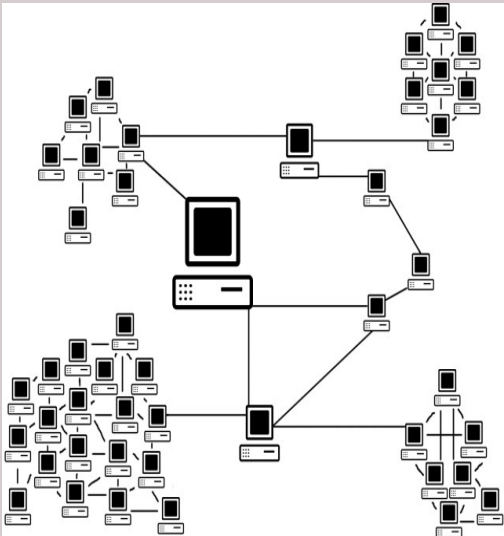
the case of Internet routing

Why routing infrastructure?

- Platforms are overstudied
- Internet infrastructure is understudied (in social sciences)
- It is very researchable (still)
- Internet infrastructure is idealized or forgotten
- Commonly used for censorship and surveillance

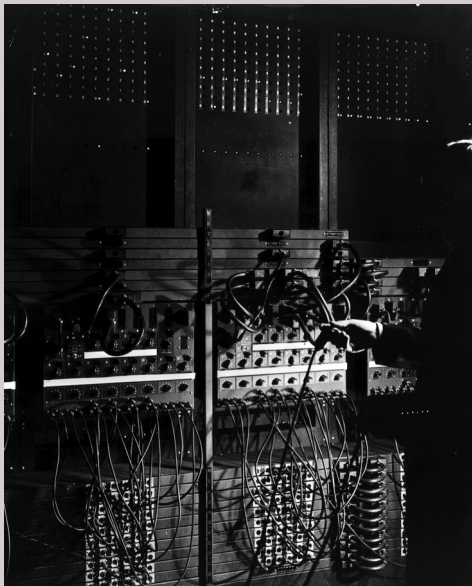


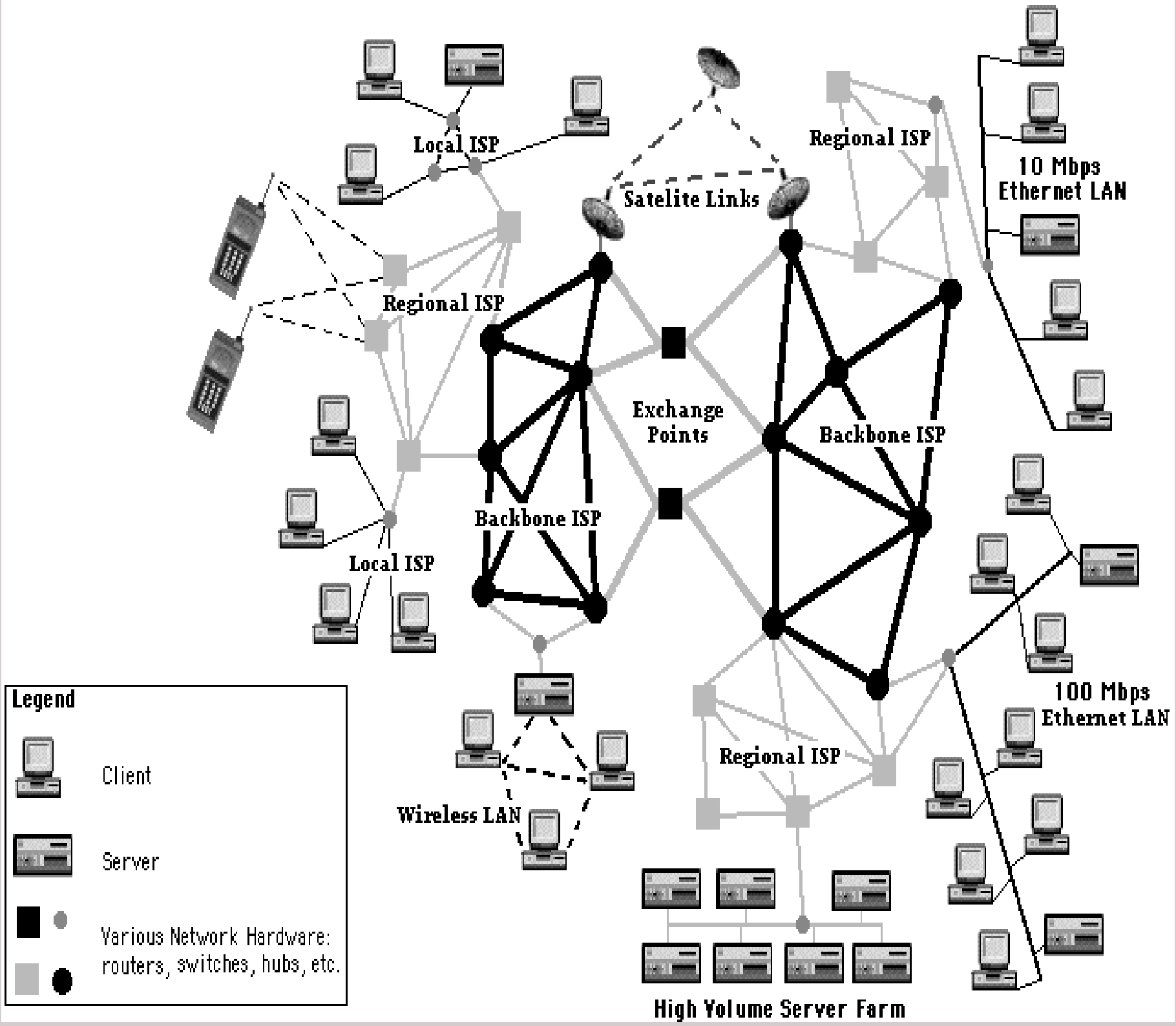
How does norm setting and norm conflict work in a distributed complex and transnational infrastructure, such as Internet routing?

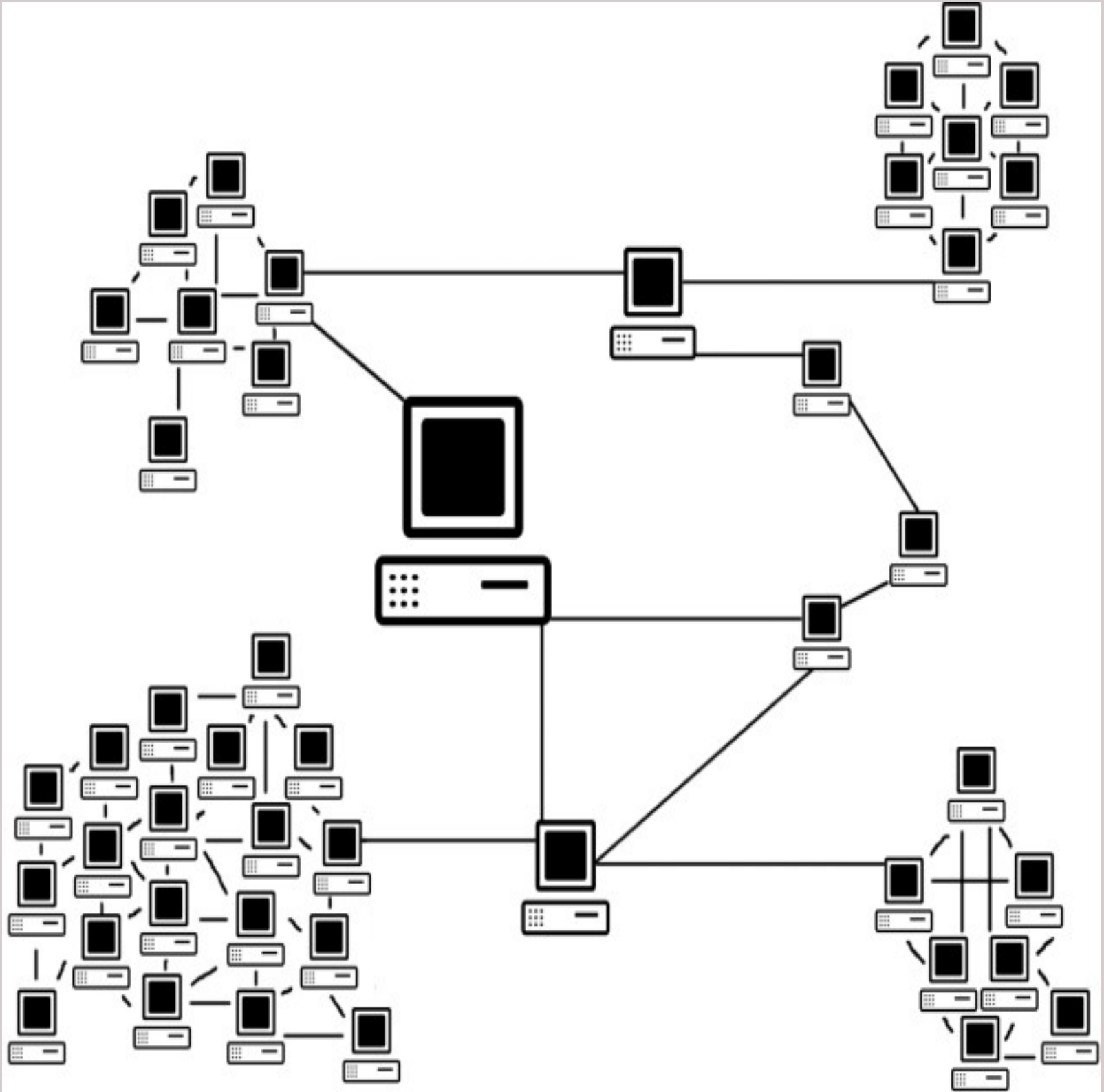


Routing concepts

- Autonomous Systems
- Autonomous System Numbers (assigned by RIRs)
- Blocks of IP addresses (assigned by RIRs)
- Border Gateway Protocol (BGP)
  - Gossip
  - Announcements
  - Filtering
  - RPKI or BGPSEC




Local ISP
Satelite Links
Regional ISP
10 Mbps
Ethernet LAN
Regional ISP
Exchange
Points
Backbone ISP
Backbone ISP
Local ISP
100 Mbps
Ethernet LAN
Regional ISP
Wireless LAN
High Volume Server Farm
Legend
Client
Server
Various Network Hardware:
routers, switches, hubs, etc.



The Tussle

different stakeholders that are part of the Internet milieu have interests that may be adverse

[...]

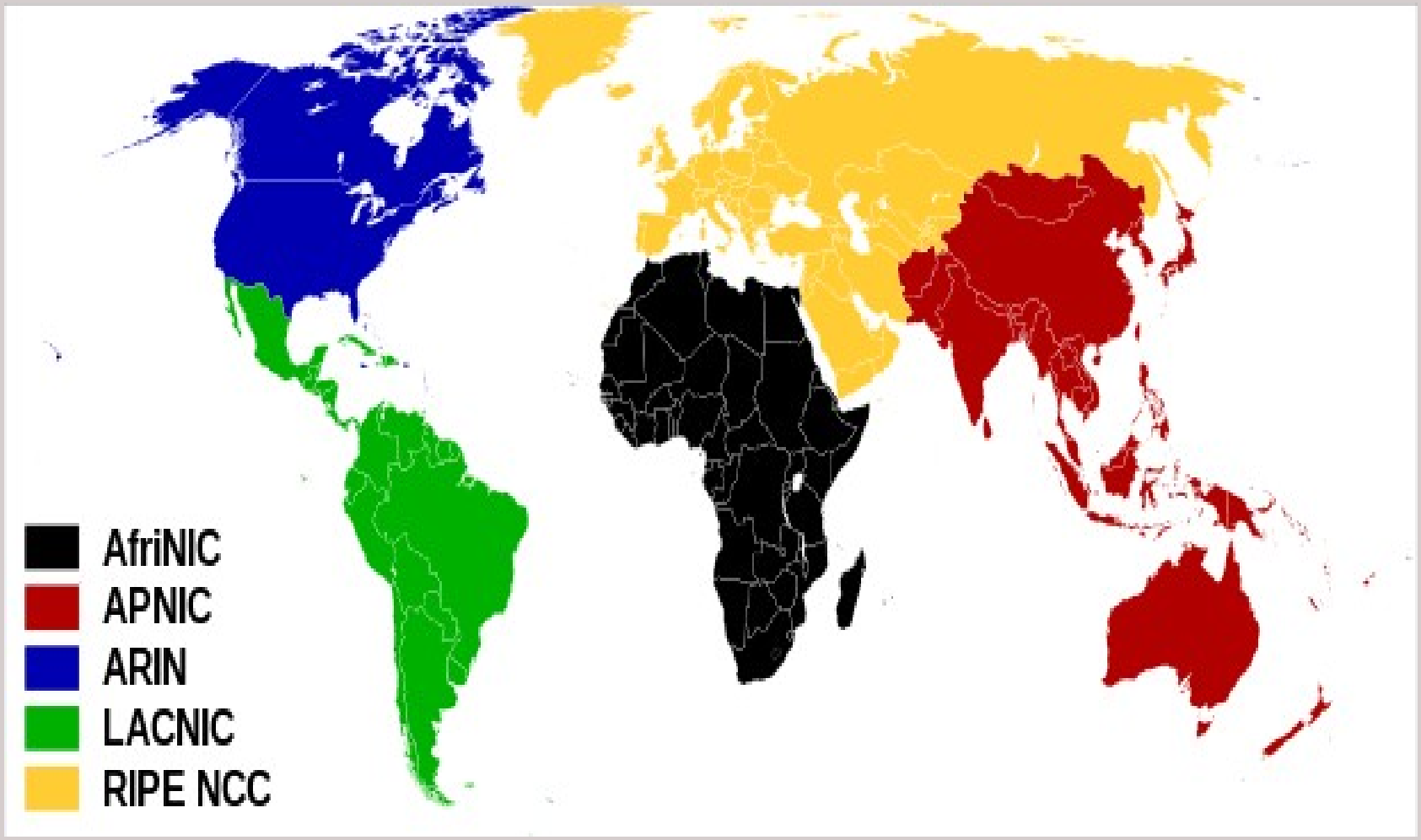
accommodating this tussle is crucial to the evolution of the network's technical architecture.

– Clarke, Wroclawski, Sollins, Braden (2005)




Routing decisions are currently made based on a mixture of efficiency, trust, and economics

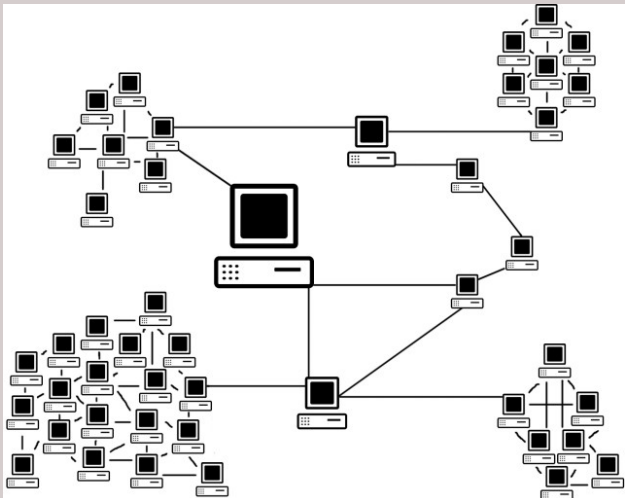
-Ashwin Mathew


AfriNIC
APNIC
ARIN
LACNIC
RIPE NCC

Designing an experiment

What values to express?

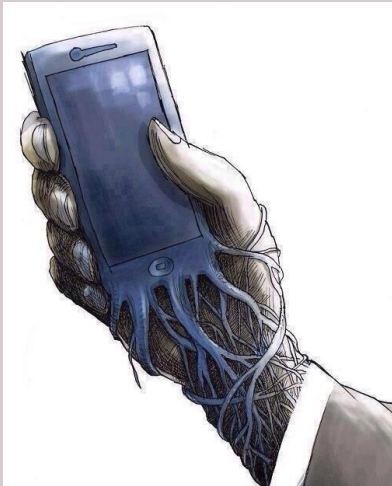
- Relevant
- Applicable
- Existing framework
- Transnational




General Data
Protection Regulation

General Data Protection Regulation

- EU law on data protection and privacy
- Unifies data regulation across the EU
- Applicable for inhabitants of the EU and EU citizens
- Addresses export of personal data outside of the EU and EEA



UNITED NATIONS GUIDING PRINCIPLES ON BUSINESS & HUMAN RIGHTS

UN Guiding Principles for Business and Human Rights

- Human rights: globally most accepted norm, since 1947
- For companies: responsibility to respect human rights
- Outlines a full framework which addresses policies, assessment, mitigations, and redress

Proposal: introduction of two objects to RIPE database

as-set: AS-GDPR

remarks: members of this set declare to be compliant with the General Data Protection Regulation of the European Union

mbrs-by-ref: ANY

as-set: AS-UNGP

remarks: members of this set declare to have adopted and implemented the United Nations Guiding Principles on Business and Human Rights

mbrs-by-ref: ANY

Proposal: introduction of two objects to RIPE database

REJECTED

as-set: AS-GDPR

remarks: members of this set declare to be compliant with the General Data Protection Regulation of the European Union

mbrs-by-ref: ANY

as-set: AS-UNGP

remarks: members of this set declare to have adopted and implemented the United Nations Guiding Principles on Business and Human Rights

mbrs-by-ref: ANY


WHY?

Infrastructural normativity (1)

Infrastructural power:

‘the capacity of the state to actually penetrate civil society, and to implement logistically political decisions’ (Mann 1984, 189)

‘If the state then loses control of its resources they diffuse into civil society, decentering and de-territorialising it’ (Mann 1984, 210).

Infrastructural normativity (2)

Norms:

'the common values of society' (Bicchieri, Muldoon, and Sontuoso 2018)

'collective expectations for the proper behavior of actors with a given identity' (Katzenstein 1996)

Four aspects:

- (a) Identity
- (b) Behavior
- (c) Propriety
- (d) Collective expectation (Finnemore and Hollis 2016)

Interconnection norm

- Identity:
  - Network operators
- Behavior
  - Produce interconnection
- Propriety:
  - Voluntary, bottom-up, collaboration, trust
- Collective exceptions:
  - Networks facilitate and engage in interconnection through the BGP protocol
  - RIPE coordinates and facilitates interconnection through the RIPE database
  - Everyone has control over their own networks
  - Interconnection is based on 'incentive structures' and 'enlightened self-interest'

Enforcing interconnection

- Technology:
  - ‘the routers do now allow for that’ (vendors!)
- Institutions
  - ‘the database is not meant for that’
- Identities
  - ‘this is not how it is done’
- Economy
  - ‘there is no incentive to do this’
  -

What norms get resisted?

Everything that complicates, or hampers, interconnection:

- Laws (GDPR)
- Ethical frameworks (UNGP)
- Jurisdictions (Schengen routing)
-
- Security measures ?
-
-
-

Intermediary conclusion (4)

The voluntary interconnection norm instructs the epistemic community of network operators in RIPE to create more interconnection between and among networks, and resist any norm or value that could hamper that.

Conclusion (1)

Internet governance is guided by the Internet's socio-technical imaginary, anchored in architectural values and process values such as openness and transparency.

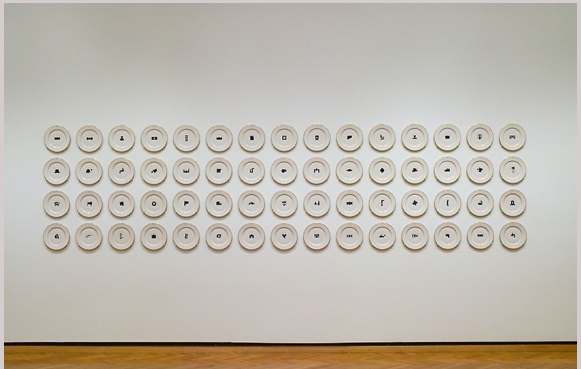
The socio-technical Internet architecture imaginary serves to guide and facilitate the process of norm development, and legitimize the current institutional ordering, even if they are concretely subverted in practice.

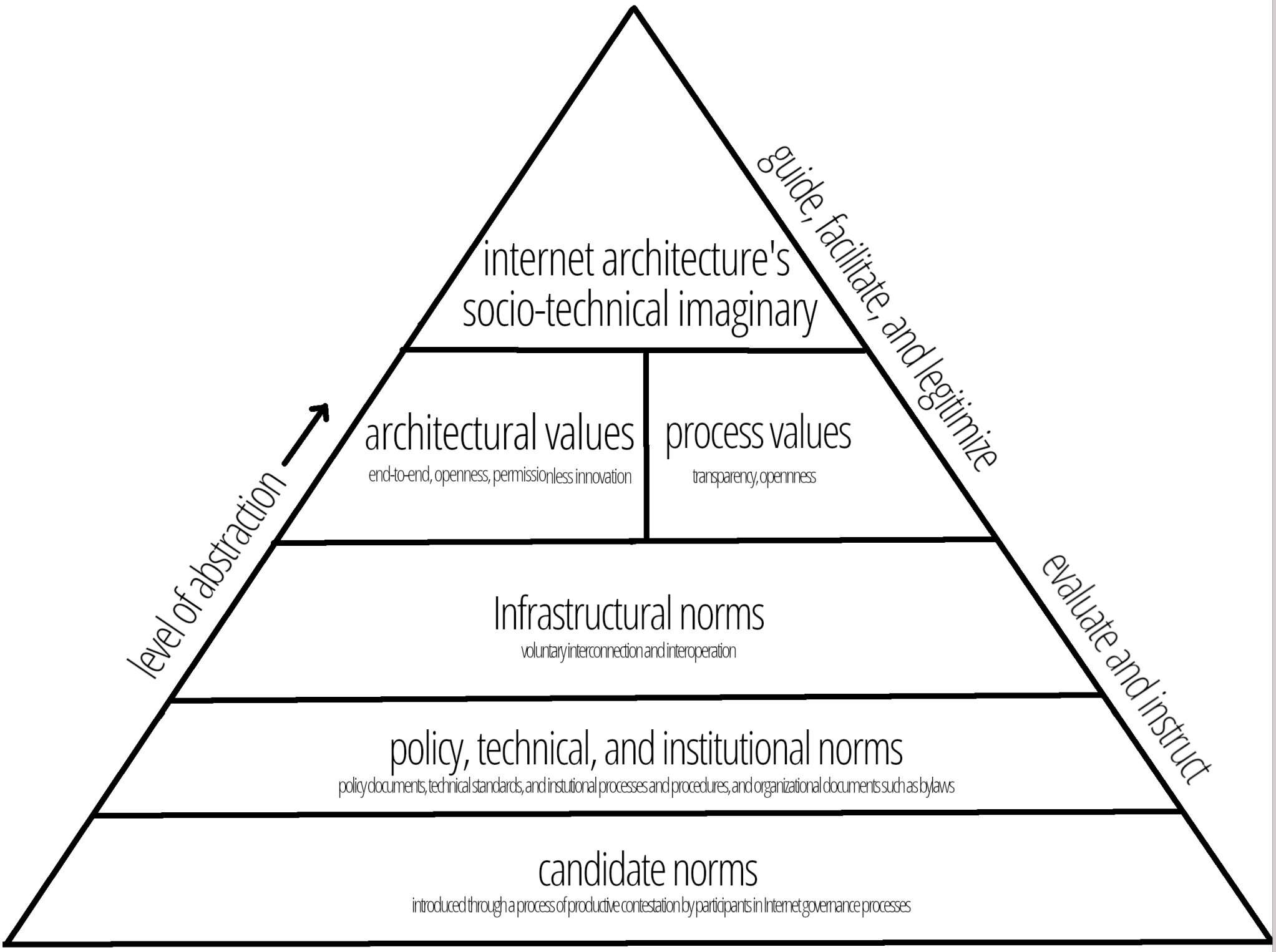
Conclusion (2)

Infrastructural norms exist to instruct new norm development and evaluate norms that are being introduced.

The introduction of norms is successful

- if the candidate norm serves the interests of these significantly represented groups
- the new norms are not in conflict with the overarching infrastructural norms of voluntary inter-connection and inter-operation.

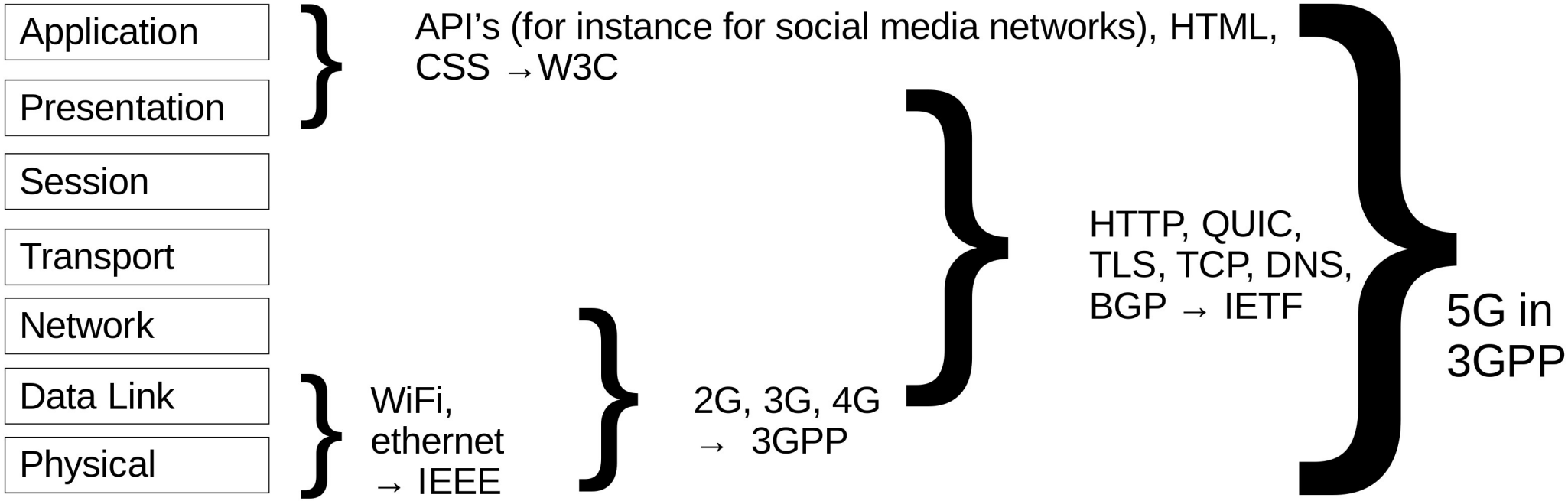



internet architecture's
socio-technical imaginary
architectural values
end-to-end, openness, permissionless innovation
process values
transparency, openness
Infrastructural norms
voluntary interconnection and interoperation
policy, technical, and institutional norms
policy documents, technical standards, and instutional processes and procedures, and organizational documents such as bylaws
candidate norms
introduced through a process of productive contestation by participants in Internet governance processes
level of abstraction
guide, facilitate, and legitimize
evaluate and instruct

Impact

The Internet governance regime undermines its own authority, scope, and legitimacy because it resists norms that are in the interest of nation states

Bonus: alternative norm regimes



5G: new networking paradigm

- The network that never was
- (re-)empowerment of consolidated network operators
- Software Defined Networking
- Network Function Virtualization
- The end of IP?

Back to the Future?

National laws and norms?

- Sovereign Internet
- Regulates “(licensed) network operators, owners of communication networks, Autonomous System Number holders” (“сети связи операторов связи, собственников или владельцев технологических сетей связи, а также иных лиц, имеющих номер автономной системы”)
- Approves creation and gives authority to “Public Network Monitoring and Control Center (“центр мониторинга и управления сетью связи общего пользования”)

National laws and norms?

1) follow rules of routing set up by regulator (RosKomNadzor)

2) apply corrections to routing, issued by regulator

3) resolve domain names using approved by regulator equipment

4) follow continuity rules set up by regulator

5) execute orders issued by Control Center

6) use only registered IXPs

7) report to regulator (ASN, routing policy, DNS resolution and network infrastructure equipment)

8) set up SORM and “technical equipment enforcing restrictions set by laws”

9) Participate in “security stability, continuity”,“trainings” (if enlisted to participate)

competing norms & metagovernance

Interconnection market // Multistakeholder Internet governance regime

1. Networking effects (more networks, more value)
2. Individual network sovereignty
3. Voluntary adoption
4. Trust

Telecoms // Multilateral telecommuncations regime

1. Consolidate
2. Converge
3. Harmonize policies, laws, and technology
4. Organized and incorporated in specific jurisdictions (billing!)
5. Combine access and identification