RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Protecting the “Core”

Challenges coming from legislative developments

Marco Hogewoning | 22 February 2022 | Roundtable Meeting for Governments (Europe)

High-Level Properties

- The Internet should be (EU position):
  - Single
  - Open
  - Neutral
  - Free
  - Unfragmented
  - Global

- Some of these properties easily translate into technology
  - Others elements rely on the need for political consensus

Different Perspectives

- “Free” can mean many different things
  - Without monetary compensation
  - Without restraint
- Regional differences make the term “free” contentious
- The technology view: “Permissionless innovation”
  - Freedom to develop new protocols and applications
  - Freedom to connect applications and devices to the underlying transport network
  - Requires independence between layers and protocols
  - **Requires some constraint from and with the Internet core!**

A Single Network?

- The Internet is a “network of networks”
  - The technical community refers to those as “autonomous networks”
  - The Barlowesque view: “My network, my rules”
- Those networks have to act in unison to a large degree
  - Requires (technical) standardisation and interoperability
  - Requires some constraint to protect the permissionless (open) properties
- Interdomain routing and connections need to be very liberal
  - It is fundamental to the resilience of the Internet as a whole
  - A routing decision made by a single network can have consequences far away
    - Also signifies the need for “routing hygiene” (security)

The Need To Be Unique

- Fundamental to the Internet being a “single” network
- There can not be any confusion about a resource
  - A name, an address, a URL can only point to a single thing or person
  - You can discuss about reachability (blocking), which is a political decision
    - Firewalls have been around for a while
- The global registry system ensures this uniqueness
  - Need an open and liberal approach to retain the permissionless open nature

Diversity Provides Resilience

- Basic engineering suggests having two (or three)
- The “network of networks” very much plays into this:
  - You can spread resources and data around, eliminating single points of failure
  - If one connection or network fails, there usually is a way around
- The Domain Name System
  - Diversity, distribution and decentralisation are key factors in its resiliency
  - It is designed to distribute and replicate information (data)
  - Cryptography (DNSSEC) guarantees the information is genuine and reliable
  - Root servers operated by 12 independent and diverse parties

Core Properties of the Internet

- Names, numbers and addresses need to be unique
  - Support and provide a single global name and address space
- Need to be easily and universally accessible
  - Support a global system that allows for and supports innovation
- Needs to be as neutral (agnostic) as possible on content
  - Support an open system that provides a large degree of freedom
- Almost all of the infrastructure is privately owned
  - Subject to market forces, which sometimes is a challenge
  - Often subject to a particular single jurisdiction

Friction Points

Risks for the Internet's core

What Does “Protect” Mean?

- We use the word all the time
- Context matters a lot
- There is a spectrum of solutions

The Role of the State?

- Protect its citizens
- Protect its interests
- Protect itself

Autonomy and Sovereign Rights

- The big underlying problem to the Internet Governance debate
- The Internet is a cooperative construct:
  - You rely on other participants, the network effect is what provides the value
- From a state's perspective you rely on other states
  - Suppliers are in another country
  - Resources are in another country
  - Users/customers are in another country
- You need to be able to trust others to not harm your interests
  - Which is a very big ask

Examples

Russian “Sovereign Internet” Law

- Broader framework to implement a vision
  - Slowly more and more elements get added
- The key objective is to become independent
  - The Russian part of the Internet needs to keep working
  - Domestic services need to be self supporting
  - Even in situations where the networks get totally isolated
- The practical consequences:
  - It removes some of the diversity: puts constraints on routing
  - It introduces a single point of failure: traffic must go to mandatory filters
- Centralisation only moves the risks and make them bigger

European Union: NIS2

- Probably not the right instrument and venue
  - Governance of global resources such as the DNS root need to be discussed and developed at a global venue
- Implications for the core of the Internet
  - Risks that it reduces the diversity, it will likely enforce a certain model
  - Possible constraints on suppliers reduce your options for a “plan B”
  - Likely to increase costs for compliance, business case might fail
- It risks further centralisation
- It might inspire other countries to do the same
  - “Their network, your rules”?

European Union: DNS4EU

- Discussions with industry and community about impact
- Some do see a need or a business case
- Others see this as a risk:
  - Further centralisation of what needs to be decentralised
  - Possible spillover effects, DNS is hard to geofence
- Some concerns and questions about longevity
  - DNS is impossible to “switch off” once people start using it
  - Does it introduce long-term risks on stability
- Concerns around “free” and “open”
  - Will it be or become mandatory?

Application of Sanctions

- It does have operational implications
  - Not everybody has access to names and addresses, infrastructure
- It reduces the “open” character of the Internet’s core
- It becomes a driver for autonomy
  - Countries and affected parties need to become self-reliant
  - This introduces additional risks
    - Reduced diversity and resilience
- It undermines the trust in global Internet governance
  - It risks the multistakeholder model in favour of binding instruments

Risk of divergence

The Global Picture

- Every country defines and implements its own laws
  - 193 different versions of “My network, my rules”
- Can we maintain global interoperability?
  - Going to be extremely hard to maintain “uniqueness”
  - Disagreement on the meaning of “open” and “free”
  - Compliance requirements will harm “permissionless innovation”
- Likely results in a less robust and resilient Internet
  - More and smaller markets that might not allow access to each other

Where You Do Require Laws

- They need to be harmonised on a global level
- Always better to intervene at the edges
  - Local rules need to be applied locally
  - Reduces the risks of spillover
- Deal with content at the application level
  - Reduces the risk of unintended side effects
- Keep core functions neutral and open to everyone
- Multistakeholder model can help
  - Get the expertise you need and harmonise the solutions

Questions

marcoh@ripe.net