



**RIPE NCC**

RIPE NETWORK COORDINATION CENTRE

# The Ground Beneath Our Feet

Recent (and Upcoming)  
Developments in Internet Governance

Chris Buckridge | November 2021 | UKNOF 48

# What are we talking about?



- **“Internet governance”** a (growing) umbrella term
  - National legislation and regulation
  - International law (UN conventions etc.)
  - “Soft law” (internationally-agreed regulatory frameworks, norms)
  - Ad hoc arrangements between government and industry
  - Technical standardisation processes and outputs
  - Community policy development
  - **The complex interplay of all of the above**

# What's changed?



- The Internet has grown ever more crucial to how societies operate
- Legislation and regulation specifically targeting Internet use and operations becoming common
- Increasing politicisation of Internet standards
- Shifting political window of what is considered “acceptable” regulatory impact
- Increasingly active efforts at UN/global-level policymaking

# What's driving this?



- **Safety(/crime)**
  - Of individuals (*COVID a factor - more people online, more people at risk*)
  - Of business/companies
- **Privacy**
- **Intellectual property protection**
- **Cybersecurity** (*especially national security*)
- **Political control**
- **Internet development and access** (*COVID again a factor*)
- **Structural imperatives** (*...regulators gonna regulate!*)

# National developments: Russia



- An active advocate and implementer of Internet controls
- ‘Sovereign Internet Bill’ (Federal Law #90) introduced in May 2019, includes multiple measures:
  - Requiring operators to install specific equipment (provided by regulator) on their networks to block forbidden or illegal content
  - Network operators must register all number resources, routing policies, network infrastructure with the regulator
  - IXPs must be registered and abide by specific rules re. connections, resilience and stability
  - A “National Domain Name System” has been established, introducing a local proxy DNS resolver to be used by Russian operators
  - Platforms required to register local presence, and fined for hosting “illegal content”



# National developments: Germany



- Germany a strong advocate of multistakeholder approach (and host of IGF 2019)
- New Online Copyright Clearance System (CUII) employs DNS blocking [launched February 2021]
  - An example of private-public cooperation and development of new models (as alternative to hard regulation)
  - Initiative of the copyright industry, support from German federal agencies
- Not the only German example of strong copyright-related legal action relating to Internet services
  - Quad9 case

CircleID



Quad9



# National developments: UK

- Online Safety Bill
  - Places a “duty of care” on Internet service providers
  - Would ban end-to-end encrypted communications
  - Scope: “user-to-user services” and “search engines” with “links to the UK”

“...no administration has ever tried to regulate the online world as comprehensively as the Online Safety Bill. It really is a mammoth piece of legislation.”

*Caroline Dinenage, former UK Minister of State for Digital and Culture*

- With Brexit, UK regulatory efforts being compared to developments in the EU



Slate



Lawfare



# Beyond national: European Union



- The EU a pioneer and innovator in digital regulation
- Currently several major pieces of legislation moving through the system:
  - Directive on measures for a high common level of cybersecurity across the Union (NIS 2)
  - Digital Services Act (DSA)
  - Digital Markets Act (DSM)
  - Data Governance Act (DGA)
  - E-privacy Regulation
- Also...
  - DNS4EU; Cyber Resilience Act (2022); cyber defence a priority





# A world tour of Internet governance



- These are just four examples
- Many, many other countries are enacting legal, regulatory efforts in the Internet space
  - United States, China, Brazil, Australia, Canada, etc. etc.

Bert Hubert's recent talk at NANOG has lots more if you're interested...



# Going global



- UN Member States are getting more active
  - Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security 2021-2025 will kick off in December
  - A joint Russia-China proposal for a Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
- ITU developments
  - Next year's Plenipotentiary sees a race for Secretary-General position between American and Russian candidates
  - "New IP" proposal was shut down in 2020; but expect similar proposals to come, attempting to standardise more top-down control models
- Standardisation high on the agenda at the G7, the OECD

# Meanwhile, at the IGF...



- IGF continues to evolve
- Currently in process of forming an “IGF Leadership Panel”
  - “...a strategic, empowered, and multistakeholder body, to address strategic and urgent issues, and to highlight Forum discussions and possible follow-up actions, in order to promote greater impact and dissemination of IGF discussions.”
- The Secretary-General’s Roadmap for Digital Cooperation
  - Establishment of a UN Envoy on Technology
- Digital issues also featured in the recent Common Agenda
  - Leading to a UN Digital Compact as part of a Summit of the Future, to which the IGF will contribute

# The takeaway



- The impacts of Internet governance are getting very real
- The complexity of global Internet governance is rapidly increasing
- Many governments reference the principle of maintaining an “unfragmented Internet” ...
  - But a fragmented approach to governance risks a fragmented Internet
- Multistakeholder models may still be our best defence against that fragmented approach
  - **But multistakeholder models require multistakeholder engagement!**



# Questions



chrisb@ripe.net  
@\_buckr

Internet Governance Forum 2021  
6-10 December

