RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Sovereignty as Regulatory Trend in Russia

Maxim Burtikov

External Relations Officer
RIPE NCC

RIPE 81 I 28 October 2020

Recent Initiatives and Proposals

- Data collection and storage of all electronic communications
- “Sovereign Internet” law
- Proposed ban of TLS 1.3.,DoT, DoH
- Other - instant messengers’ user registration, taxation of e-services…

Data Collection and Storage (June 2016)

- Operators must store metadata for three years
- All electronic communications must be stored for six months - all voice, images, texts, audio, video and any other type of information
- Data needs to be stored using locally certified data storage equipment; capacity must be increased by 15% every year
- LEAs are granted direct access to this data
- Decryption keys must be provided to LEAs

“Sovereign Internet” Law (May 2019)

- ASNs, IP blocks, routing policies, network infrastructure must be registered with the regulator
- IXPs must register, ISPs need to peer only with registered IXPs or via direct peering, which has to be reported
- In case of a threat to RUnet, the regulator is authorised to manage traffic routing directly or via obligatory routing policies
- Special equipment, provided by the regulator, must be installed on the ISPs network and needs to be used to block illegal content

Ban of TLS 1.3., DoT, DoH (Sep 2020)

- A proposal to ban encryption protocols that mask DNS queries
- Reason: inability to prevent users from accessing content that is blocked in RU via these protocols
- Any resource to be confirmed using such protocols to be banned within one working day after such discovery
- Industry is voicing security concerns, because if implemented directly, encrypted traffic might have to be filtered out whatsoever

Is Russia alone?

- This is a global trend - digital sovereignty
- The Internet’s “trust model” is under scrutiny
  - Trust is not a legally sufficient term anymore
  - Even in US vs EU - anti-trust, privacy and tax legislation issues
- Current examples of demand for local control and sovereignty:
  - EU’s GDPR & Digital Services Act
  - US vs. TikTok/WeChat
  - China is sucessfully exporting its technical approaches on Internet regulation

What Does This Mean?

- “Borderism” vs. distributed nature of the network
- More sovereignty/control over information flow, user data, infrastructure, usage, finances
- Governments apply existing analogue approaches to digital world
  - Logistics, transportation, mail and telegraph, taxation of physical goods, citizen registrations… new technologies inherit old regulatory approaches
- This is a vicious circle
- What responsibility does industry bear?

Questions ?

mburtikov@ripe.net