INTERNET GOVERNANCE IN RUSSIA TREND ON SOVEREIGNIZATION

ILONA STADNIK

SAINT-PETERSBURG STATE UNIVERSITY, RUSSIA

Cyberspace alignment to national borders instead of Internet fragmentation (Mueller 2017)

THEORETICAL FRAMEWORK

Methods to implement alignment

1. **National securitization**
   - Reframing Cybersecurity as a national security issue
   - Militarization of cyberspace
   - Nationalization of threat intelligence
   - Reliance on national standards and technologies
   - Reassertion of legal authority for network kill switches
2. **Territorialization of information flows**
   - Content filtering
   - Data localization
3. **Efforts to structure control of critical Internet resources along national lines**

National Securitization

Reframing cybersecurity as a national security issue	→	2000, 2016 *Doctrine on information security*
Militarization of cyberspace	→	*"information operations troops" since 2013*
Nationalization of threat intelligence	→	GOSSOPKA, NCCCI, and public/private CERTs
Reliance on national standards and technologies	→	Import substitution program for software 2015
Reassertion of legal authority for network kill switches	→	Discourse of ***external* kill switch** local shutdowns of mobile Internet in Ingushetia Republic and Moscow

Territorialization of information flows

- Content filtering →

filtering practices since 2012 through adoption of specific laws.
child pornography, information promoting drugs and suicide, calls for mass riots, extremist activities, participation in mass public events that violate the established procedure, unlicensed content – buy a court decision or by request of federal executive agency

"Blacklist" is maintained by Roskomnadzor
system "Revizor" checks the operator's compliance to block the banned Internet resources

search engines must connect to the federal "blacklist" to automatically filter search results
Google fined for incompliance in December 2018

- Data localization →

Localization of personal data storage and processing (FZ-242) in 2016
LinkedIn is the first victim
Civil proceedings against Facebook and Twitter in 2019, fines + new draft law on higher fines

Control over critical Internet resources along national lines (1)

General distrust in ICANN's work among the Russian leadership

Cyber drills tested the external shutdown in 2014

- **Draft law** (2016-2017) on the basic elements of the critical infrastructure of the Internet in Russia and its regulation introduced by the Ministry of Communication

State Information System aimed to ensure the integrity, stability and security of the Russian national segment of the Internet, called "**GIS Svyaz**":

- Traffic exchange points, including telecom operators and organizers of information distribution
- Network addresses and information on individuals who own these network addresses
- Numbers of autonomous systems of the Internet, and also data on persons/entities to whom such identifiers are provided, and date of their providing
- Routing policies for Internet packets

Control over critical Internet resources along national lines (2)

Second draft law (December 2018) on “sovereign Runet”

“to protect RUnet from external shutdown by hostile actors”

6 (!!!) months later it was signed as a Law FZ-90, will come into force on 1 Nov 2019

- The law gives unprecedented powers to Roskomnadzor, initially a supervising agency

- Failure to make Telegram messenger to comply with the anti-terrorist law and inability to block it for the Russian users - one of the main reasons for Roskomnadzor to take a big stake in the law enforcement

Control over critical Internet resources along national lines (2)

It is a set of amendments to two existing laws "on Communications" and "on Information":

- The main subjects responsible for stable operation of the Internet in Russia are **telecom operators** and **owners** and/or proprietors of: (1) **technical communication networks** (used for operations of transport/energy and other infrastructures, not connected to the public communication network), (2) **traffic exchange points**, (3) **communication lines crossing the state border** and (4) **autonomous system numbers** (ASN). Roskomnadzor will keep registries for the last three categories. All subjects must participate in the regular exercises for testing the stability of Runet.
- **Roskomnadzor** will execute the **centralized management of communication networks in the event of threats** to the stability and security of the Runet, by **defining routing policies for telecom operators and other subjects and coordinating their connections.**
- Telecom operators are required to ensure the installation in their networks of **technical means for countering threats** to the stability, security and integrity of Internet operation on the territory of Russia ("black boxes" with deep packet inspection functions). These technical means **will also serve the purpose of traffic filtering and blocking access** to prohibited Internet resources.
- The law creates a **Center for monitoring and control of public communication networks** under the Roskomnadzor supervision.
- The law creates a **National Domain Name System**

Control over critical Internet resources along national lines (2)

What is going on until November 1?

~ 40 regulatory acts to fill executive gaps:

- present a list of threats to the Runet
- present principles of centralized traffic management
- define technical parameters and rules for governing the "black boxes”
- define how the registry of traffic exchange points will be formed
- define rules for providing information from operators and owners of ASN for maintaining various information systems,
- figure out how the national DNS will be formed and used by providers
- establish a Center for monitoring and control of the public communications network and define its powers

Control over critical Internet resources along national lines (2)

Up to date:

- only 5 regulatory acts passed approval
- Out of 28 prepared for consideration 17 violated the procedure of introducing new regulatory acts for public discussion, got a negative evaluation for its regulative power.
- Tests of filtering capacity of “technical means for countering threats” in the Ural region

CONCLUSIONS

- The political intention to align Internet with the state borders of Russia is very strong.
- The most important technical part is still under consideration
- Unique discourse – keep Internet accessible despite the external shutdown, but make it independent from the current Internet governance system created around ICANN and other related organizations
- Despite this, filtering of traffic is a priority
- In case of success, an example for other states with similar internet infrastructure composition?

QUESTIONS?

Ilona.st94@gmail.com