The market of black boxes:
Russian industry of censorship and surveillance

Ksenia ERMOSHINA (ISCC/CNRS; Citizen Lab)
Benjamin LOVELUCK (i3-SES, Télécom ParisTech)
Francesca MUSIANI (ISCC/CNRS)
Introduction: Russian ISPs, a market to domesticate?

- Initially a dynamic sector:
  - 6000 ISPs with a license
  - From local networks (*domovaya set*) to small ISPs
  - Competition, low prices, good quality of networks
  - Specific topology: connections with foreign cable infrastructures

- But growing surveillance and censorship constraints
  - The “golden age” of the RuNet has gone (Konradova and Schmidt 2014)
  - Towards “Sovereign Internet” (Nocetti 2015)
  - The technologies of control must also be “made in Russia”
The law, the code and the market

- Digital innovation sector in Russia – **under the “rule of law”**
  - Russian paradox: technologies are “behind” the law
  - e.g.: no working technical solution for the Yarovaya law

- The regulation of the RuNet creates an industry / a market of surveillance and censorship, and **shapes “competition”**
  - Many vendors appear to propose technological solutions for the FAIs to comply with the law...
  - ...non-standardized, expensive and complicated to implement

- This market can be approached by a study of “**middleboxes**”
The “middleboxes”: distributed and opaque objects

- 2 kinds of devices
  - SORM – *lawful interception* (surveillance and traffic storage)
  - “RKN-compliant” – *filtering* and blocking of websites

- In reality – multitude of *distributed technical objects*
  - Software / proxies / cloud-based services
  - Legal and semi-legal ad hoc arrangements
  - Middleboxes: storage buffers, commutators, servers...

- “Black boxes”
  - Supposed technical complexity
  - Surveillance and censorship functions
  - Connections with military innovation sector
Challenges of this research

- Study **configurations** of sociotechnical actants in their relations with the **tactics** of regulatory and economic agents
  - Combine the study of “dispositifs” (Akrich, 1989, 1991) and conventionnalist approach to markets (Dupuy et al. 1989 ; Eymard-Duvernoy 2006)

- Grasp the “**market agencements**” (Callon 2013) and “**market agencing**” (Cochoy et al, 2015) between these technical devices, regulators, vendors, ISPs
  - Study the heterogenous processes and activities in-the-making, and power relations that traverse them
  - Study how this “market agencing” creates “concerned groups and publics and opens new spaces for political controversies” (Geiger et al. 2014) in the governance of Russian IT market

- Understand how the constraints to block, filter and survey **shape resistances and foster “politicisation”** of Russian IT professionals
Methodology

- Mixed-methods
  - **Interviews** with ISPs and telecom workers, lawyers specialized in Internet regulation, vendors of filtering equipment, activists of various associations “for Internet freedom”;
  - **Technical analysis** of fingerprints of the middleboxes (Citizen Lab – Jakub Dalek);
  - **Analysis of websites and commercial materials** produced by the vendors of censorship and surveillance equipment; secondary materials from specialized conferences (e.g. SORM conferences);
  - **Web-ethnography** of dedicated forums and chats of ISPs;
SORM = System for Operative Investigative Activities (lawful interception)

Coommutators, switches, servers, software, storage buffers, remote control (at the local FSB office)

Directly controlled by the FSB

On-demand access: tax police, border police, customs, police
SORM (surveillance)

- An **old – but actively evolving** – system:
  - SORM-1: 1996 – wiretapping, phone surveillance;
  - SORM-2: 2000 – Internet
  - SORM-3: 2014 – metadata + multimedia files + long-term storage
  - Loi “Yarovaya” 374-FZ — suggested in 2016; enforced on July 1, 2018: 30 days storage of the whole traffic – for ISPs; 6 months – for telcos; metadata – 3 years.

- Important **costs** of implementation and maintenance:
  - Analysis of public procurement for “SORM”: minimum **105K** rub (RGGU) – maximum **91 383 000** rub (Rostelecom)

- Long and complex **certification** → techno-legal vacuum
  - "The legalisation of SORM-2 took 10 years, the ISPs managed to defend themselves in courts because the equipment was not certified" [Lawyer, OrderCom]
  - The certifications for SORM-3-Yarovaya will not be published until 2021
The surveillance market

- **Political ambitions and business opportunities**
  - "There are 2 kinds of people in the SORM and censorship industry. The first one thinks that we need to block everything because they are afraid of Americans. The second approaches surveillance and blocking pragmatically, because one can earn money with it. Since 2016 the SORM market grew 1,8 times. The yearly turnover for SORM is around 26 billions of rubles" [Klimarev, director of the Society for Defense of the Internet, author of ZaTelecom blog (17K readers), telecommunication engineer]

- "Import substitution" and national vendors:
  - Market leaders: (5-6 billion rub/year) : MFI-Soft (leader of public procurements), Specialnyie Technologii, Vasexpert, Norsi Trans;
  - + 8 smaller vendors
Between constraints and tinkering

- Growing techno-legal constraints...
  - “The ISP is between the FSB and the SORM vendor. In order to access clients’ data, the extractor has to be able to receive commands from the remote control station, that’s located in the local FSB office. Earlier, every local office had a remote control station from a specific vendor, that was bought via public procurements on the internal military market. For example, FSB in Nizhniy Novgorod was using Norsitrans, in Saint-Petersburg it was Specialnye Technologii, and so on. Since December 2016, when the certifications for SORM-2 were published, the FSB asked for a universal remote control, that will be compatible with SORM equipment of all vendors” [Lawyer, OrderCom]

- ...but still some room left for maneuvering and tinkering
  - “Adopt parts of your existing systems, because when they finally publish the certs, we will have to spend lots of money again, and we will have to do so, because it’s law” [an ISP - forum Nag.ru, 4 novembre 2015]
The regime of risk

- **Distributed responsibilities**
  - “We record the traffic, but who will be responsible in case of a leak? Everything is distributed. Every ISP has its own equipment. The ISP buys it from a vendor, but there’s also the person who will install this equipment, and the end-user, the FSB agent. So. There are like 3 parts involved in the process. Who will be responsible in case of a leak? Who will appear in court?” [SORM conference, November 2017]

- **Arrangements between ISPs** according to their budget and size:
  - Small ISPs: **ad hoc demands** (“When it’s needed, the FSB calls us or contacts us over email and asks to make a tcpdump of traffic for a specific IP, and share it over ftp or something like that” [https://habr.com/post/65924/];
  - “**Shared SORM**” - 20 to 25% savings (according to OrderCom);
  - “**OutSORMing**” (agreement between a small and a big ISP);
  - “**SORM race**”: ephemeral ISPs → creating new legal entities in case of problems with SORM;
  - When the ISP is big enough, it has to install the equipment;
SORM is inefficient?

- SORM equipment is absent or badly configured at around 70% of ISPs
- 450 cases for violation of SORM regulation in 2017 (RBC study)
- What are the reasons?
  - Economic: easier to pay fines (30K-50K rub) than to buy SORM (100K minimum);
  - Infrastructural: “Pre-existing infrastructures are sometimes incompatible with new equipment that “very competent institutions” would like to make ISPs implement. In order to install this equipment, the ISP has to fundamentally change the network architectures, and replace very expensive installations” [Klimarev, Director of the Society for Defense of the Internet]
  - Technical: recording and storing encrypted traffic (TLS 1.3) is inefficient for lawful interception goals;
  - Legal/operational: in most of cases when an investigation is ongoing, FSB uses other ways to gather information [e.g. manual tapping; device seizure; hacking into accounts and so on].
Filter traffic according to the blacklist compiled and published by the RosKomNadzor (Federal Service for Supervision of Communications, Information technologies and mass-media)

### Blocked websites:

<table>
<thead>
<tr>
<th>Institution</th>
<th>Blocked since the beginning</th>
<th>Blocked now</th>
<th>Unblocked</th>
<th>Illegally blocked now</th>
<th>Illegally blocked since the beginning (by IP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drug Control Service</td>
<td>27,225</td>
<td>1,586</td>
<td>25,639</td>
<td>104,295</td>
<td>892,692</td>
</tr>
<tr>
<td>Persecutor General</td>
<td>32,476</td>
<td>16,885</td>
<td>15,591</td>
<td>250,786</td>
<td>502,712</td>
</tr>
<tr>
<td>RosPotrebNadzor</td>
<td>1,710</td>
<td>376</td>
<td>1,334</td>
<td>1,341</td>
<td>68,046</td>
</tr>
<tr>
<td>Moscow Court</td>
<td>23,351</td>
<td>5,869</td>
<td>17,482</td>
<td>48,218</td>
<td>168,488</td>
</tr>
<tr>
<td>Court</td>
<td>79,545</td>
<td>27,548</td>
<td>51,997</td>
<td>1,846,174</td>
<td>4,261,575</td>
</tr>
<tr>
<td>RosComNadzor</td>
<td>26,423</td>
<td>9,577</td>
<td>16,846</td>
<td>100,071</td>
<td>319,629</td>
</tr>
<tr>
<td>Ministry of Interior</td>
<td>19,555</td>
<td>10,575</td>
<td>8,980</td>
<td>445,913</td>
<td>1,040,068</td>
</tr>
<tr>
<td>Alcohol Control Service</td>
<td>935</td>
<td>655</td>
<td>280</td>
<td>4,121</td>
<td>4,914</td>
</tr>
<tr>
<td>Taxe Control Service</td>
<td>101,208</td>
<td>54,012</td>
<td>47,196</td>
<td>801,316</td>
<td>1,699,873</td>
</tr>
<tr>
<td>Ministry of Communications</td>
<td>3,947</td>
<td>3,897</td>
<td>50</td>
<td>47,680</td>
<td>47,711</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>316,375</strong></td>
<td><strong>130,980</strong></td>
<td><strong>185,395</strong></td>
<td><strong>3,649,915</strong></td>
<td><strong>9,105,808</strong></td>
</tr>
</tbody>
</table>
Website blocking: methods and vendors

Methods

Forum Nag.ru: survey among ISPs – (511 voted);
Interpreting the constraints

- **Complex certification and standardization** process:
  - Internet censorship implemented - 2012
  - First laws – on “protection of children”: reorientation of the market (“parental control” solutions → middleboxes for censorship)
  - First tests to certify equipment: Autumn 2017
  - 7 certified vendors (but more than 14 exist)
  - Only in March 2018: Law 149-FZ, alinea 10 – to standardize technical methods of blocking and parameters for blockpages

- **Legal gaps and breaches → possibilities for tinkering and circumvention**
  - “Some were blocking by IP, others by DNS. There was a kind of technological vacuum – block as you can. RosKomNadzor could not recommend any solutions to the ISPs, because they could fall under the law against monopolies. But very quickly there were lots of complaints from website owners, whose websites were accidentally blocked. So now they are recommending us to block by URL. Before, the ISPs were writing their own scripts DIY, but now it’s much less frequent, as they really risk to be fined”
    [CTO, SkyDNS, filtering equipment vendor]
The introduction of a middlebox for "control of control"

- System AS Revizor – introduced in 2016, implemented since 2017
  - Automatic control of ISP compliance: no exceptions – even for very small
  - Exists as a middlebox and as software;
  - Obscure, not open source (attempts of ‘reverse-engineering’ by some ISPs)

- Survey 2018 (source: Nag.ru), out of 279 ISPs
  - 238 installed Revizor (192 – the box, 46 – the software);
  - 241 did not get any fines, 38 got one or several fines (from 50K to 100K rub)
The market of censorship

- Costs for ISPs
  - Fines - 50-100K rub + cost of equipment up to 1M+ rub

- Possibility to purchase pre-filtered traffic ("upstream filtering") - but conflicts of legal responsibility:
  - "Imagine I’m a small ISP and I buy pre-filtered traffic from, say, Rostelecom. I install Revizor, but something is not blocked. Who will pay the fine? Me or Rostelecom? Rostelecom will say that we’ve badly configured our equipment on the local level" [Klimarev, Director of the Society for Defense of the Internet]

- Competition between vendors
  - New offers: insurance against RKN fines, or ad hoc arrangements between vendors and their clients – ISPs;
  - Recent trend: “non-compliance as a feature” - response to overblocking;

- Competition among ISP
  - Small ISPs are more repressed;
  - Bigger ones do not always block;
Techno-legal resistances

- **Technical tricks** of the ISPs
  - “Some ISPs apply censorship on a separate subnetwork where they implement Revizor. For end-users they have another network, without or with much less censorship” [CTO, SkyDNS]

- **Blockpages** used as means of contention

- **Hacktivism** based on the breaches of the controlling equipment

- **Legal resistance:**
  - OrderCom : helps ISPs to appeal against decisions and fines by RKN (around 15% of court decisions canceled in 2016);
  - The Association for Alternative Internet Service Providers – launched inquiry for “antitrust law violation” against SORM vendors;
Effects on the Russian Internet Service market

- **Consolidation/centralization**
  - “We can observe consolidation among ISPs. We have around 300 ISPs who use our filtering solutions and we see a trend – bigger ISPs like Dom.ru are absorbing smaller ones. If you have 2 to 3K clients, you can be next in line for acquisition” [CTO, SkyDNS]

- **Rise** of Internet service costs for end-users
  - “Yarovaya [law] had a big impact on our association. The cost of equipment equals annual revenue of an ISP, without counting the costs of certification” [A. Lomakin, Director of the Association of Alternative ISPs]
  - According to a study among 100 ISPs conducted on November 21, 2018, **52 % ISPs** envision to **increase costs of their services** for end-users. The increase has already started (Rostelecom, Dom.ru and others – between 5% and 10%);

- **Threat of “balkanization”**: 
  - Centralization of the ISP market impacts the AS Hegemony Index;
  - The number of ISPs having agreements for transnational peering is decreasing;
  - The project of law on “autonomous Russian Internet” - proposed on December 13, 2018;
Conclusion

- Simplistic image of **state-level regulator** who has only to deploy a certain technological solution to achieve goals of political control has to be **deconstructed**

- Legal framework **generates a market** of surveillance and censorship, that is **embedded** in a bigger ecosystem of Internet services, but is deeply **reshaping** it
  - From the infrastructure layer (peering agreements) to the application layer (website and app accessibility)

- The economic rationality is dependent on **interpretations of the techno-legal norm**, and the capacity of actors to negotiate, circumvent or adapt to this norm

- **Resistance**, if it exists, is profoundly shaped by technical and legal characteristics of controlling equipment

- New **“concerned publics”** emerge and frame their participation more and more in political terms (e.g. small IT-entrepreneurs; ISP associations...)