Internet Abuse by Russian LEAs

RIPE76, Marselle 17.05.2018

ОБЩЕСТВО ЗАЩИТЫ ИНТЕРНЕТА

Abuse

Internet was not designed to comply LEAs requirements and complete LEA tasks

Forms of LEA abuse:

- mass surveillance
- content blocking
- imitation of activity
- misuse of powers
- provocation of crime and offences

LEAs motivation (official)

- youth protection
- fight against terrorism and crimes
- difficulties in cooperation with other countries and international LEAs

Mass surveillance

SORM - System for operative search activities. “blackbox” connected to the network, operated without any possible control by operator and civil society, purchased on account of operators.

- SORM1 - bulk telephone wiretapping
- SORM2 - bulk internet data wiretapping
  - 24 hour traffic storage added
- SORM3 - bulk internet data wiretapping with automatic transfer of user identification
- “Yarovaya package” - storage of all telecommunication messages (=all traffic) for up 6 month.

Is it effective?

No.

Nearly 1 million of wiretapping orders issued by the courts per year

Abuses:

- sales of recorded calls to competitors (regular criminal cases)
- blackmails by LEAs
- effective for fight and comprometation of political opposition

User identification

- WiFi by passport
- SIM cards sales by passport (doesn’t work at all)
- Data retention for all corporate users.

Communicatios secrecy violations

New definition by Supreme court:

“LEAs doesn’t require additional search order, in case they already have smartphone in hands”

Imitation of Law Enforcement activities

Punishments for likes, posts, reposts - “Mind crimes”.

Much easier to find, no risks.

Collaborating companies (like VKontacte) easily provide used identification to LEAs.

Is this NAZI propaganda?

Bogatov case

TOR exit node operator accused in “terrorism propaganda” crime.

Having alibi - was arrested.

Actual author of “terrorist posts” have been identified by community, but investigators was not interested.

Mr. Bogatov saved from jail by mr. Putin - “IP address means nothing” (in reply to American elections accusations).

Case is still not decided by court

Content blocking

“We need to protect youth”

“ONLY and ONLY 3 kinds of information to be blocked”

- child abuse images
- drug production and sales
- suicide propaganda and methods

Procedures: Decision by LEA, takedown notice from RosKomNadzor to resource owner and hoster, if unsuccesful transition to “blocking list” offloaded to ISPs.

Content blocking - development

- any information considered illegal by court
- counterfeit content
- Federal list of extremist material
- “personal data”
- terrorist and extremist propagands
- gambling and tax avoidance methods
- ways to avoid and dodge content blockings
- to be continued

Content blocking - imitation of activities

Wiki pages related to drugs

Humor pages (“to commit suicide just stop breathing”)

LinkedIn - for personal data law violation (not localized to Russia)

lurkmore.to (kind of absurdopedia) - also personal data violation

Content blocking

1) All traffic to IP/subnet
2) Whole domain name
3) Selected page on a website

At the begiining there was no strict recommendations and onrol methods.
Now blocking recommendations doesn’t match supervision procedures leading to fines (~1500 per unblocked resource).

Not enough clean way to remove blocked resource from the list.

Updated recommendation: install DPI for the whole bandwidth of uplinks.

Content blocking - development

“Critical Internet Infrastructure” law. (still in discussion)

- national TLDs (now GONGO)
- national Internet Exchange (now owned by Rostelecom)
- Enforced Routing Registry (under cover of safe government controlled copy of RIPE Database)

“BGP Blackholing” blocking method. (leaked documents on experiments)

Content blocking - damage to technical infrastructure

1) additional CAPEX and OPEX
2) additional points of failure
3) access slowdown
4) Internet fragmentation and connectivity breakage
5) collateral blockings
6) malicious abuse of content blocking infrastructure

Content blocking - success?

No.

- No official data on decreased terrorism activities
- No data on decreased number of suicides (sustained)
- Number of criminal cases related to drug sales increased

Yes.

- political censorship works (and noone feels responsible for it)

Telegram Messenger case

Internet Intermediaries must provide decryption keys. (whatever it means)

Telegram refused, appealed in court. (Case close to San-Bernardino iPhone)

Court decided to block telegram.

RKN blocked Telegram llc. resources and started chase for proxies.

Huge ranges of major hosters fell into blockinglists. With all possible collateral damage. “Rubber” General Prosecution Office from 2015 used to motivate bloking of that ranges.

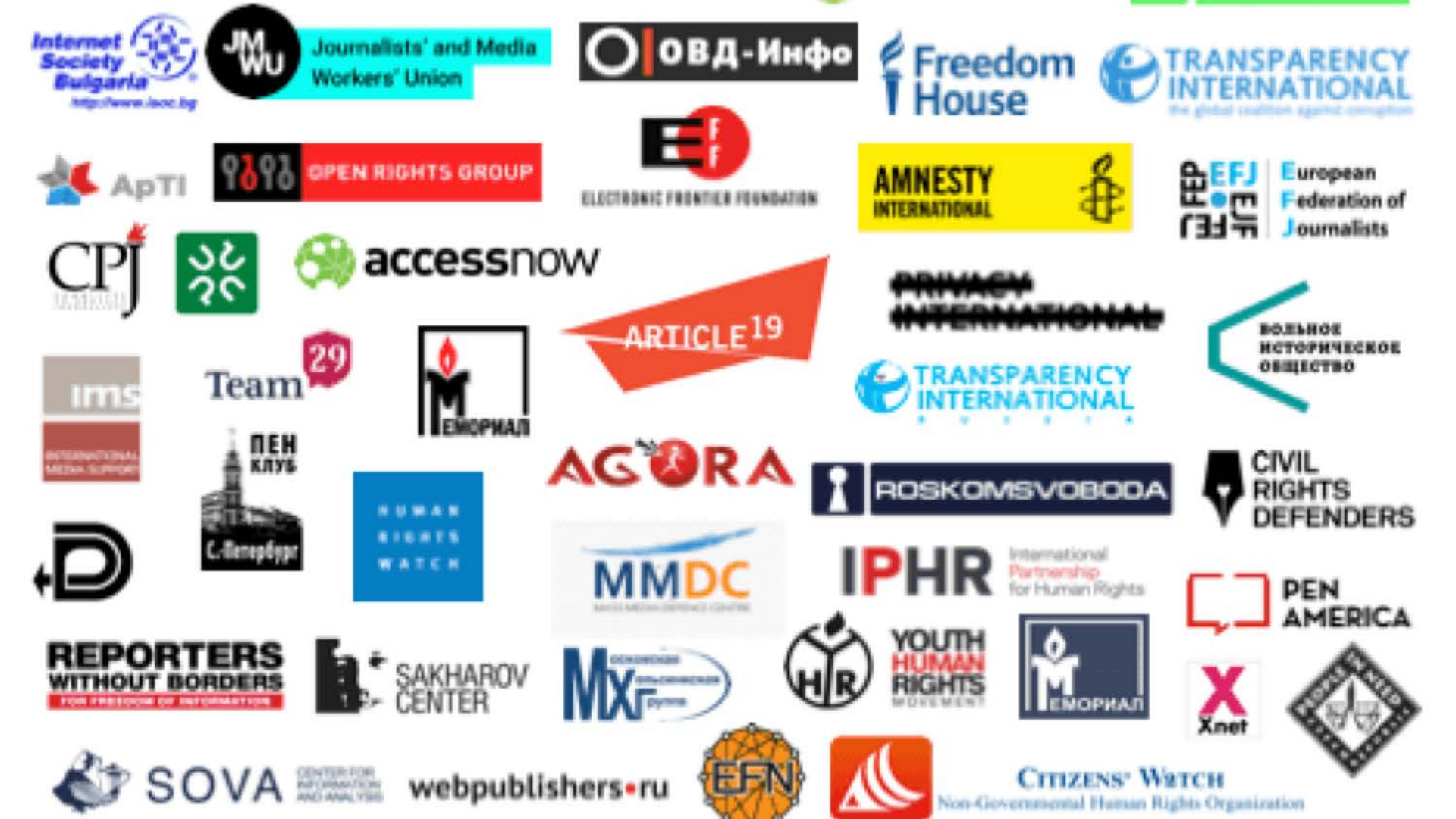
Telegram messenger case

IPv6 is not affected!!!

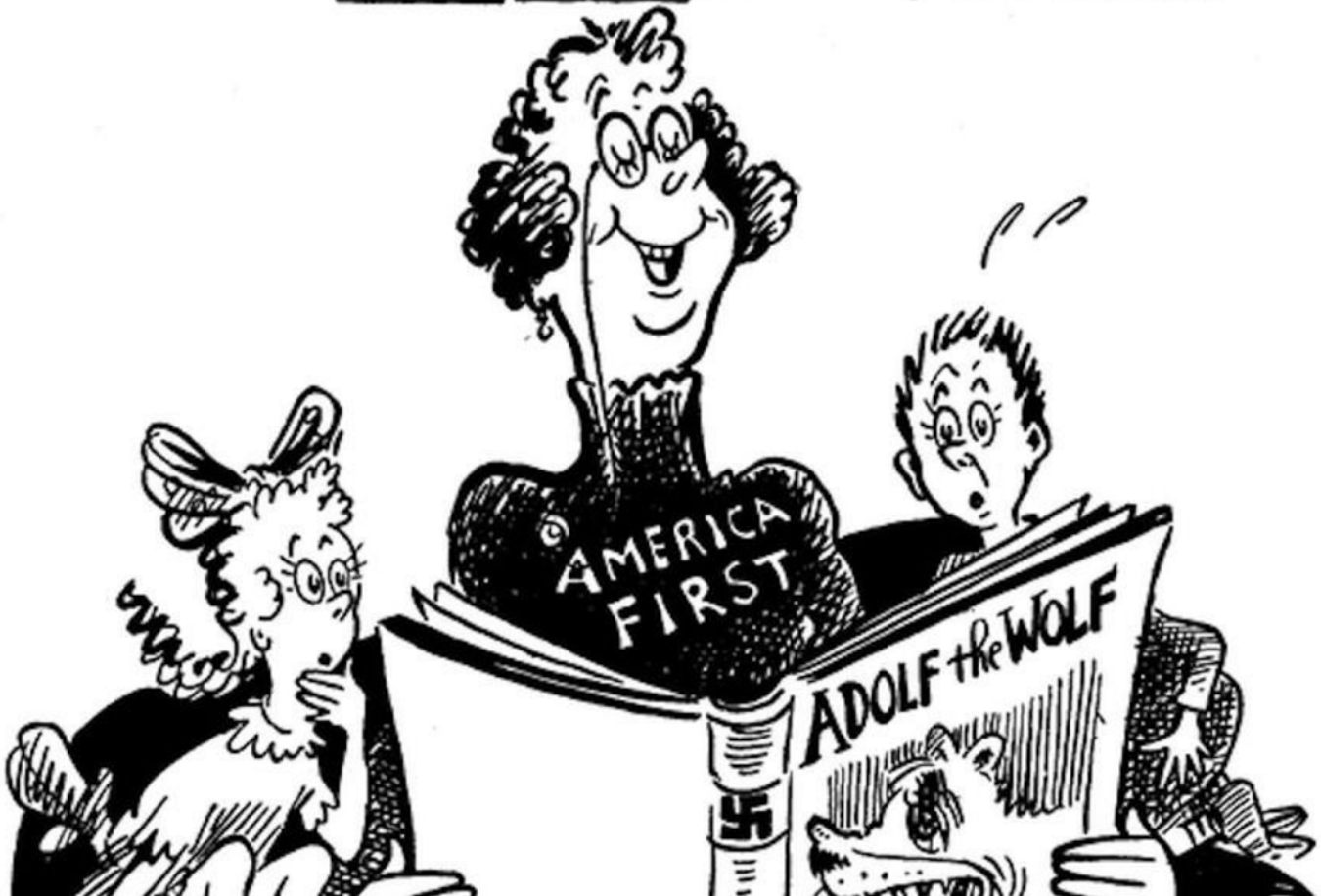
Some ranges were released. Some hosters decided to collaborate with RKN, kicking customers running VPNs and proxies.

Messenger Telegram still works

UPD: 15 May 2018 Court announced, that decision to block Telegram doesn’t actually came into the power.


Internet Society Bulgaria
Journalists' and Media Workers' Union
ОВД-Инфо
Freedom House
TRANSPARENCY INTERNATIONAL
ApTI
OPEN RIGHTS GROUP
ELECTRONIC FRONTIER FOUNDATION
AMNESTY INTERNATIONAL
EFJ European Federation of Journalists
CPJ
accessnow
ARTICLE 19
PRIVACY INTERNATIONAL
ВОЛЬНОЕ ИСТОРИЧЕСКОЕ ОБЩЕСТВО
ims
Team 29
МЕМОРИАЛ
TRANSPARENCY INTERNATIONAL RUSSIA
ПЕН КЛУБ С.-Петербург
AGORA
ROSKOMSVOBODA
CIVIL RIGHTS DEFENDERS
HUMAN RIGHTS WATCH
MMDC
IPHR International Partnership for Human Rights
PEN AMERICA
REPORTERS WITHOUT BORDERS
SAKHAROV CENTER
YOUTH HUMAN RIGHTS MOVEMENT
МЕМОРИАЛ
Xnet
SOVA CENTER FOR INFORMATION AND ANALYSIS
webpublishers.ru
EFN
CITIZENS' WATCH Non-Governmental Human Rights Organization

. . . and the Wolf chewed up the children and spit out their bones . . .
But those were Foreign Children and it really didn't matter."



Conclusion

Internet related LEA activities brings to them false feeling of infinite powers

Do not say “We are just technical community, let’s follow laws”

Make everything transparent

Try to keep governments away from Internet regulations

Общество Защиты Интернета - Internet Protection Society

To make internet freedoms part of Agenda

Our projects:

1) Internet Freedom Index
2) Internet Connectivity Index
3) Internet Repressions mapping
4) Making caveats of Russian Internet regulations public.

Questions?

RosComSvoboda.org

ozi-ru.org

isavnin@gmail.com