



OOONI

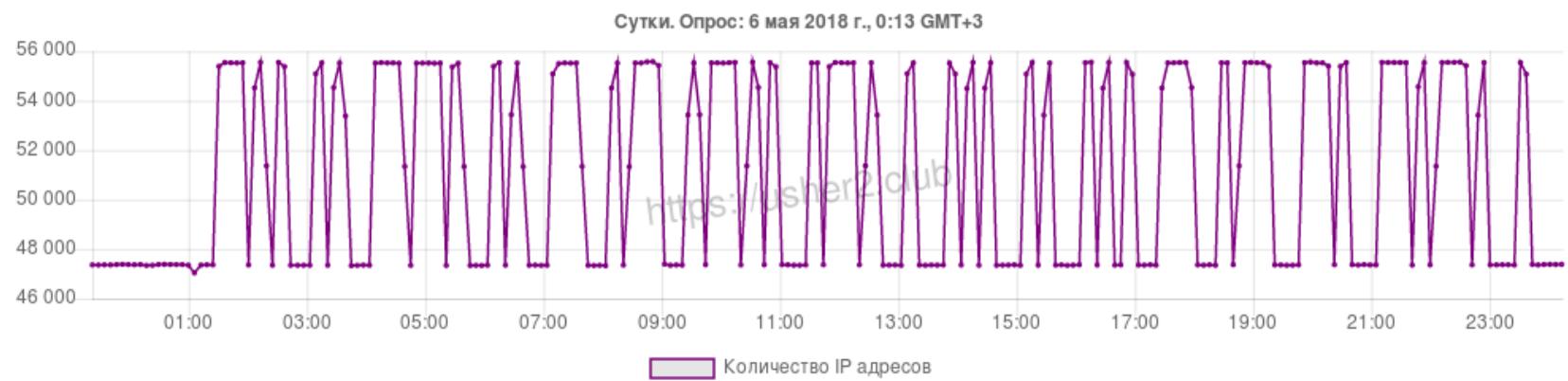
РКН-тян

болячки и побочки

Леонид Евдокимов
CryptoInstallFest 5
Москва, 22 сентября 2018
slides.ooni.io/2018/CIF

Бывший darkk@yandex-team.ru

Ныне darkk@torproject.org



Почётный клоун usher2.club.



OONI

The Open Observatory of Network Interference



Memo leaked last year from State Department policy chief reveals US human rights playbook currently active in its Iran (but not Saudi) discourse. politico.com/f/?id=00000160 ...

One useful guideline for a realistic and successful foreign policy is that allies should be treated differently -- and better -- than adversaries. Otherwise, we end up with more adversaries, and fewer allies. The classic dilemma of balancing ideals and interests is with regard to America's *allies*. In relation to our competitors, there is far less of a dilemma. We do not look to bolster America's adversaries overseas; we look to pressure, compete with, and outmaneuver them. For this reason, we should consider human rights as an important issue in regard to US relations with China, Russia, North Korea, and Iran. And this is not only because of moral concern for practices inside those countries. It is also because pressing those regimes on human rights is one way to impose costs, apply counter-pressure, and regain the initiative from them strategically.

2:30 PM - 2 Jan 2018

[twitter/wikileaks](#)

**БУДЕТ
ХУЖЕ**

В 2016 — временный запрет HTTPS, SSH.
В 2018 — OpenVPN.

Каскадное нагромождение разных фильтров.
По-разному работающего, по-разному настроенного.
Эшелонированная оборона от контента?

Врезка рекламных редиректов, в т.ч. раздающих малварь.
Прекратилась после публикации отчёта CitizenLab.

Состояние Интернет-цензуры в Египте

Июль 2018

ooni.io/post/egypt-internet-censorship



автор: @aquam1ne

ping: 38ms → 61ms

Квартили "дополнительных" задержек (25/50/75%):

Омск, Дом.ру: -0.9 / +0.4 / +1.5 ms

СПб, Ростелеком: -2 / +5 / +18 ms

Yota vs. VPN

19 мая 2014, "Об ограничениях p2p-трафика"
... p2p и VPN ограничиваются в 32 кбит/с ...

26 сентября 2014, "VPN в мобильном интернете от Yota"
... VPN-трафик никак не ограничивается ... VPN также
относится к высокоприоритетным сервисам ...

17 сентября 2015, "Уже год создаём оператора вместе"
... изначально мы не планировали внедрять такой
функционал, но выяснилось, что VPN на смартфонах очень
востребован ...

Как же начинает надоедать. Сейчас клиент 10 минут жаловался коллеге, что не может играть в world of trucks. Ещё и извинений требует от нас лично!

У нас клиенты воют! Гугл не работает, ютуб не работает, инстаграм не работает, твич не работает, стим не работает. на некоторых сайтах просто белый экран.

Слушайте, а что там про инстаграм?

Yota vs. Telegram

Тормозит?

Видимо, MTProtoProxy классифицируется DPI как p2p.
Скорость ~21 кбит/с

Видимо, Socks5 классифицируются DPI как "белый" VPN.
Скорость ~7500 кбит/с ^_(ツ)_/^-

Socks5 не шифрован! При подключении к Wi-Fi СОРМ *будет* знать, что это тот же пользователь Socks5, что и в мобильной сети!

Yota vs. Tor

Видимо, Speedtest получает приоритет.
Скорость ~57 мбит/с

Видимо, Speedtest через Tor красится DPI как "белый" VPN.
Скорость ~7 мбит/с

Видимо, Speedtest через Tor + obfs4 красится DPI как p2p.
Скорость неизвестна, Tor зависает на bootstrap 10%
-＼(ツ)_/-

GoVPN: готовимся к Великому Российскому Firewall

```
cat /dev/urandom | nc host port ?
```

```
cat radiotelescope.raw | nc host port ?
```

```
govpn -iface tap3 ... -remote host:port ?
```

CIF3 – Сергей Матвеев – GoVPN



00:13

```
$ curl https://yandex.ru/internet/api/v0/ip
WARNING: linker: Unsupported flags DT_FLAGS_1=0x8
WARNING: linker: Unsupported flags DT_FLAGS_1=0x8
"94.25.171.5"
$ nc brie.darkk.net.ru 42042 | pv >/dev/null
 500KiB 0:02:36 [3.20KiB/s] [=>          ]          ]
$ curl -ksS https://brie.darkk.net.ru/500k | pv >
/dev/null
WARNING: linker: Unsupported flags DT_FLAGS_1=0x8
WARNING: linker: Unsupported flags DT_FLAGS_1=0x8
 500KiB 0:00:02 [ 213KiB/s] [<=>          ]
$ curl -ksS https://brie.darkk.net.ru/10m | pv >/dev/null
WARNING: linker: Unsupported flags DT_FLAGS_1=0x8
WARNING: linker: Unsupported flags DT_FLAGS_1=0x8
10.0MiB 0:00:05 [1.95MiB/s] [ <=>          ]
$
```

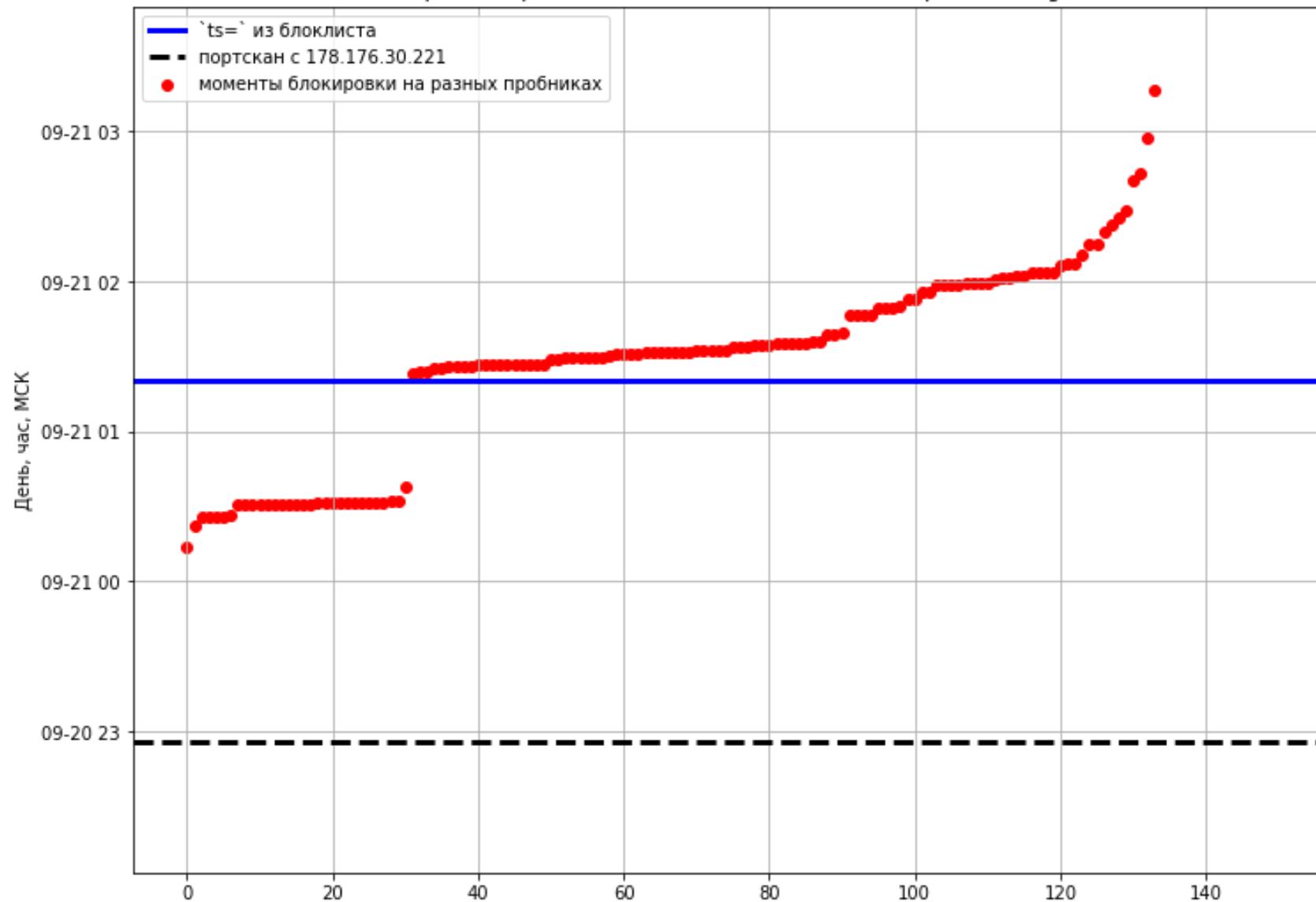
Poor man's MTProto

О том, как Ростовский Ростелеком MTProto блокировал.

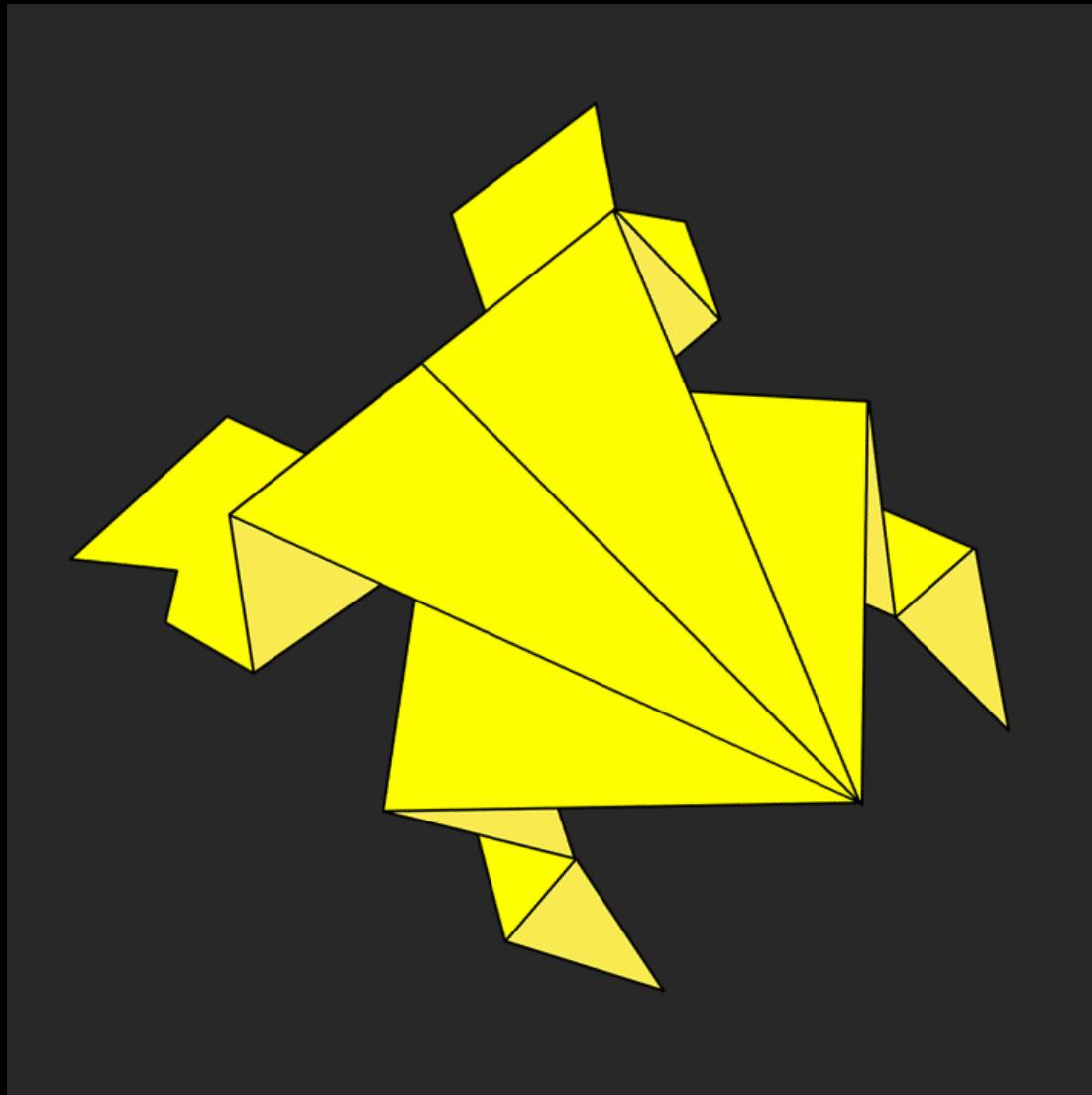
[github/poormansmtproto](https://github.com/poormansmtproto)



Блокировка сервиса 173.255.215.241:24914, эксперимент s5tg-05



github/rkn-git-flow



medium/@cyberlabukraine

Образование, РКН, неравенство

stepik :-(

Coursera :-(

SkyEng :-(

TED :-(

AS Name	Rostelecom
AS Number	8997
<u>Cloudflare Data Center</u>	ARN

Connectivity to Resolver IP Addresses

1.1.1.1	No
1.0.0.1	Yes
2606:4700:4700::1111	No
2606:4700:4700::1001	No

[1.1.1.1/help](#)



bobuk
@bobuk

Follow



Слушайте, а вот если вы живете на AWS,
как вы избегаете попадания на сети,
которые заблокированы РКНом?

2:42 am - 24 Aug 2018

1 Retweet 7 Likes



16

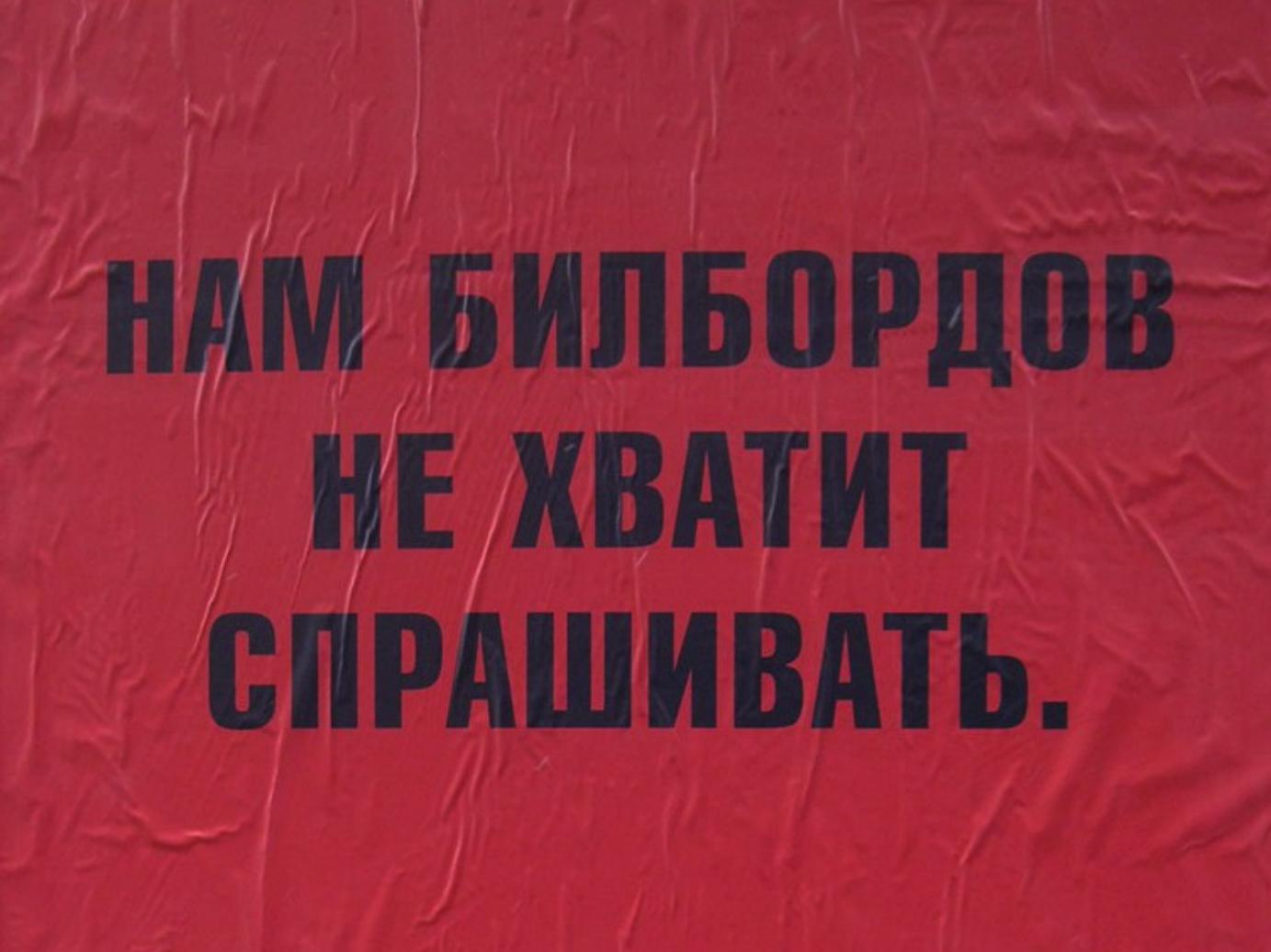
1

7

[twitter/bobuk](#)

Блокировка anus.com

Открытое письмо об избыточных блокировках



**НАМ БИЛБОРДОВ
НЕ ХВАТИТ
СПРАШИВАТЬ.**

Открытое письмо об избыточных блокировках

Я люблю АС "Ревизор", а ещё больше Яровую

767 members



Pinned message

Правила общения в группе: Политика, оскорблений, ...



OV

Олег Вераксич

Комrades, добрый день, подскажите плиз ресурс со списком доменов попавших под РКНовские ковровые блокировки сетями

10:56 AM



Vladislav Minakov

admin

Олег Вераксич

Комrades, добрый день, подскажите плиз ресурс со спис...

После драки кулаками не машут. Реально единицы подтвердили сбои на своих сетях

11:04 AM

@i_love_auditor

Заказ 500

ПОКУПАТЕЛЬ

Фамилия: Евдокимов

Имя: Леонид

Телефон: +79816800702

Тип заказа: Физическое лицо

ДОСТАВКА

Тип: СДЭК

Адрес доставки: Санкт-Петербург, Санкт-Петербург Санкт-Петербург ул.
Одоевского, 28

Стоимость: 170,00 ₽

ОПЛАТА

Тип: Банковская карта

СОСТАВ ЗАКАЗА

Артикул	Товар	Цена	Скидка	Кол-во	Стоймость
00037	Футболка Будет хуже - L	2 500,00 ₽	--	1	2 500,00 ₽

Диалоги - Mozilla Firefox

Диалоги +

https://vk.com/im?sel=-142153191

Search

VK Поиск

Леонид

Моя Страница
Новости
Сообщения 1
Друзья
Группы 3
Фотографии 14
Музыка
Видео
Игры
Товары
Закладки
Документы

СДЭК доставка

Сообщение от официального сообщества.

Подробнее Отписаться

СДЭК доставка 18:00
Поступил заказ 1090194604 от Kul'trab. Адрес выдачи: ul. Odoevskogo, 28 рп-пт 09:00-21:00, sb-vs, 10:00-19:00, +78127080027. Сумм. 0,00. Хранение до 06.09.2018. Наличие паспорта обязательно.

Леонид 18:04
Клааааас!

Напишите сообщение...

Search

СДЭК доставка

Осторожно, ВКонтакте! Вас посадят

ВК выстроила бизнес-процесс помогающий спецслужбам сажать пользователей за лайки и репосты.

Количество дел по 282 статье возбуждённых на пользователей за посты:

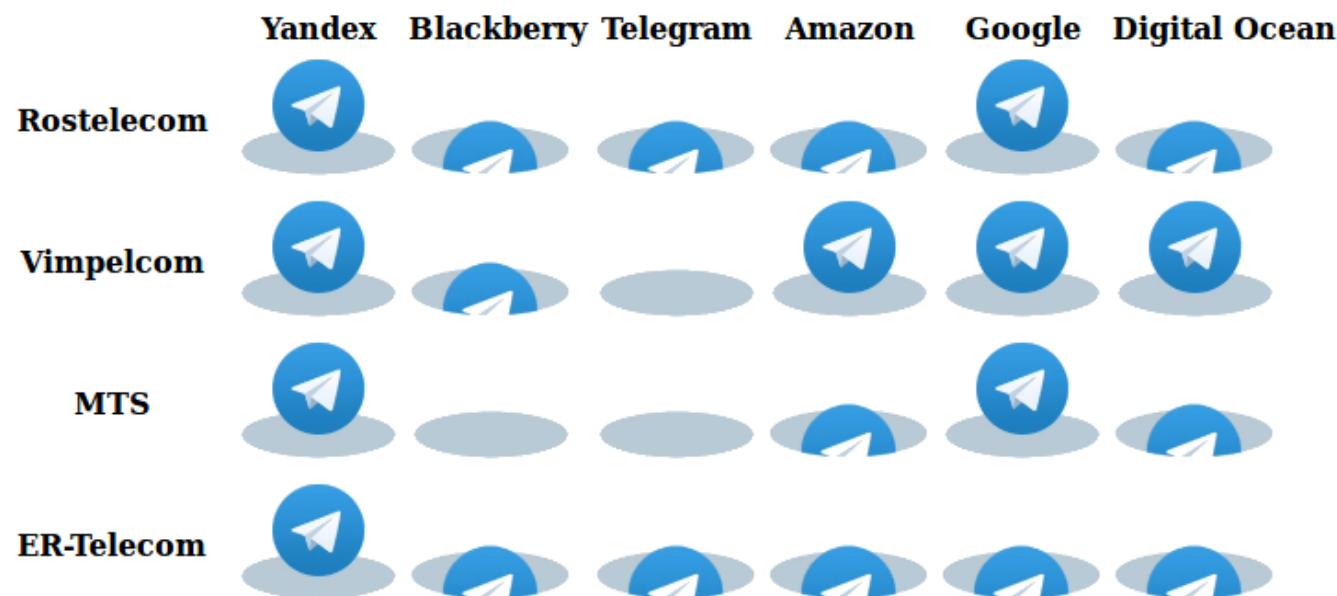
ВКонтакте	OK	FB
603	14	4

Если вы знакомы с сотрудником ВК, пожалуйста, спросите у него что он об этом думает

Источник: Информационно-аналитический центр «СОВА»

автор: [@max_katz](#)

А примерно так ISP (не) блокируют облака:



Увы, без подробностей



TWO DJS DEFY THE ISLAMIC REGIME

RAVING IRAN

A FILM BY SUSANNE REGINA MEURES

Что делать?

donate.zona.media

roskomsvoboda.org/donate

usher2.club

*Спаси тебя Иисус,
спаси тебя Аллах
от центра «Э»
и перегибов на местах.*

... и гнева Роскомнадзора

slides.ooni.io/2018/CIF