The censored user: how censorship studies ignore user experience

Ksenia Ermoshina
CIS CNRS / Citizen Lab / eQualitie

From STS to usability studies… and back

Can Johnny Build a Protocol? Co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols

Ksenia Ermoshina
CNRS
Paris, France
ksenia.ermoshina@cnrs.fr

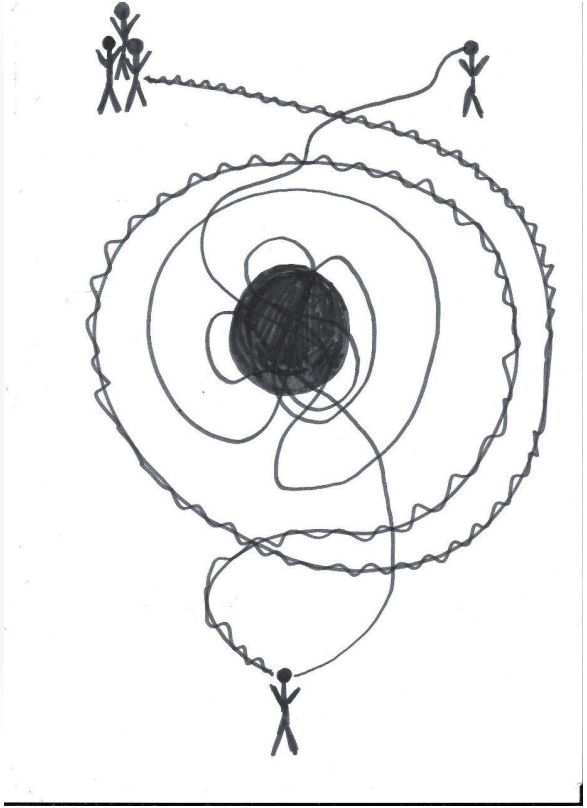
Harry Halpin
Inria
Paris, France
harry.halpin@inria.fr

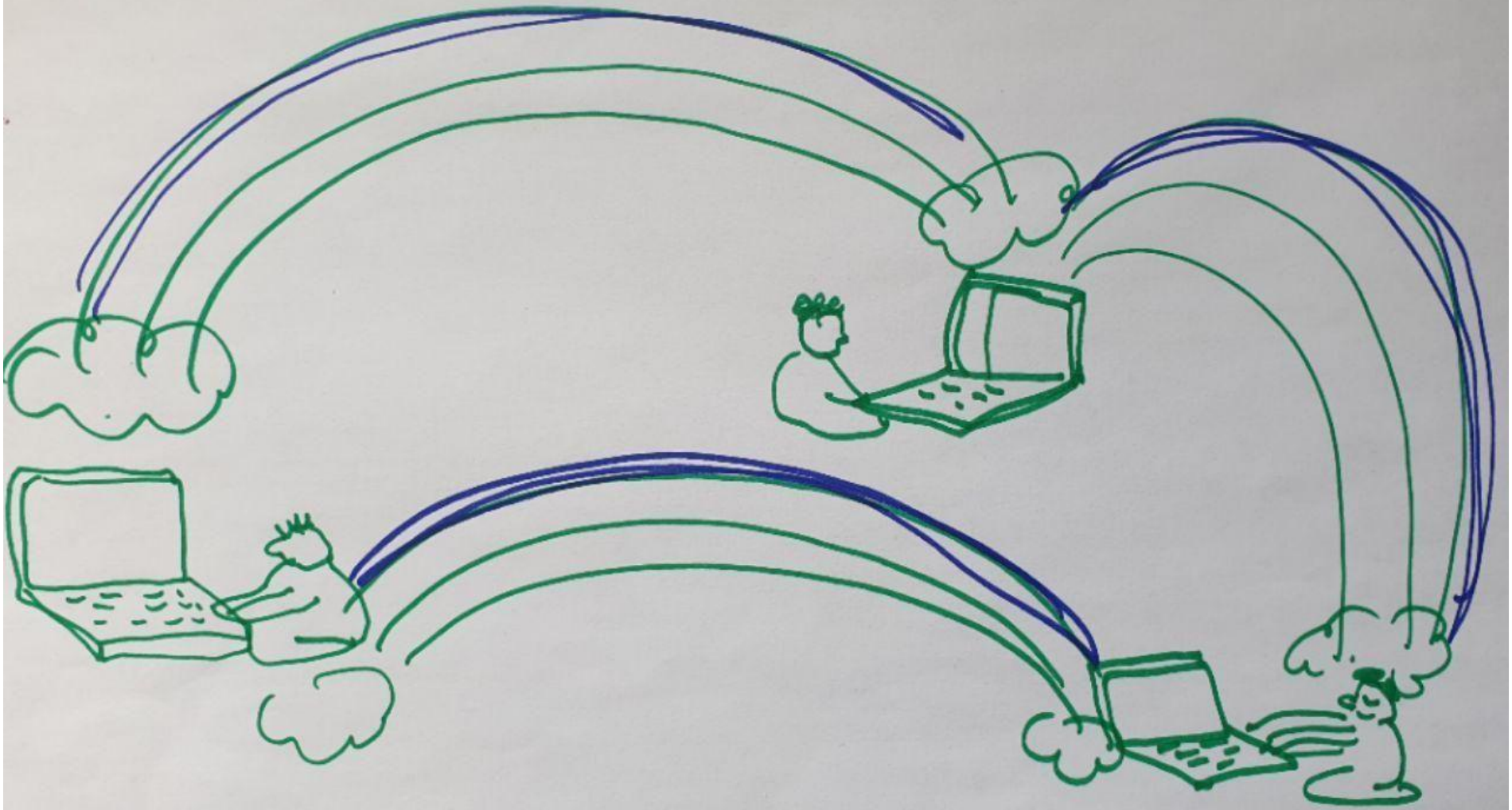
Francesca Musiani
CNRS
Paris, France
francesca.musiani@cnrs.fr

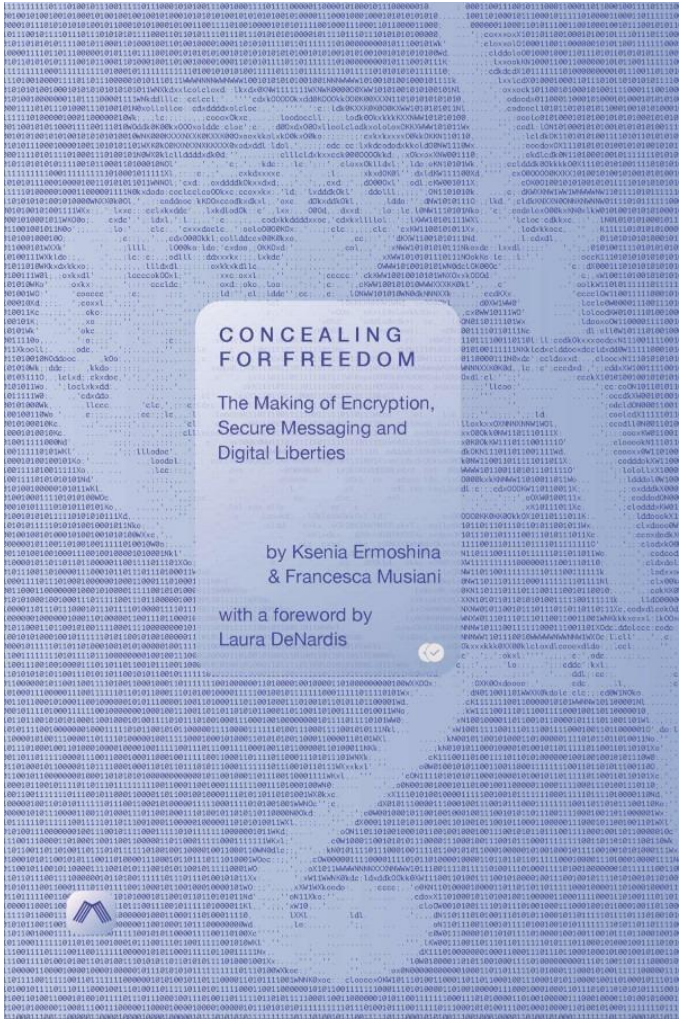
***Abstract*—As secure messaging protocols face increasingly widespread deployment, differences between what developers "believe" about user needs and the actual needs of real-existing users could have an impact on the design of future technologies. In the domain of secure messaging, the sometimes subtle choices made by protocol designers tend to elude the understanding of users, including high-risk activists. We'll overview some common protocol design questions facing developers of secure messaging protocols and test the competing understandings of these questions using STS-inspired interviews with the designers of popular secure messaging protocols ranging from older protocols like PGP and XMPP+OTR to newer unstandardized protocols used in Signal and Briar. Far from taking users as a homogeneous and undifferentiated mass, we distinguish between the low-risk users that appear in most usability studies (such as university students in the USA and Europe) and high-risk activist user-bases in countries such as Ukraine and Egypt where securing messages can be a matter of life or death.**

dozens of "silos" that are completely unable to interoperate with each other: WhatsApp users cannot chat with Signal users, Cryptocat users cannot communicate with ChatSecure users, and so on. This is in stark contrast to older federated, standardized, and freely licensed technologies such as XMPP with Off-the-Record (OTR) messaging or e-mail with PGP. For example, any email service can openly communicate with another (Gmail to Outlook, etc.) in a federated fashion. To summarize, the properties for new protocols and applications can be classified into six broad categories:

- Security Properties
- Group Support
- Privacy Properties
- Decentralization
- Standardization





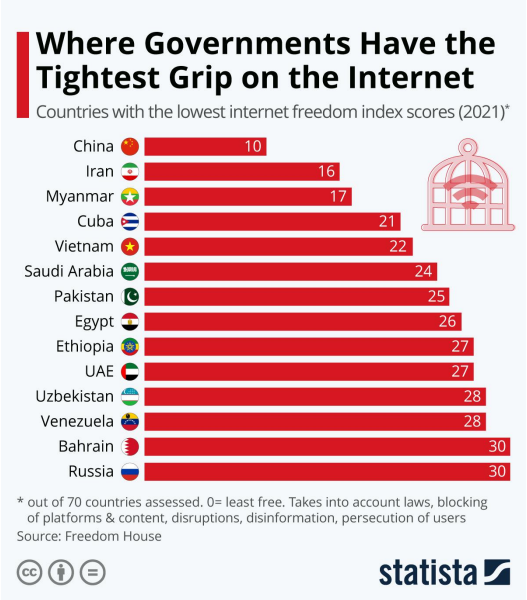


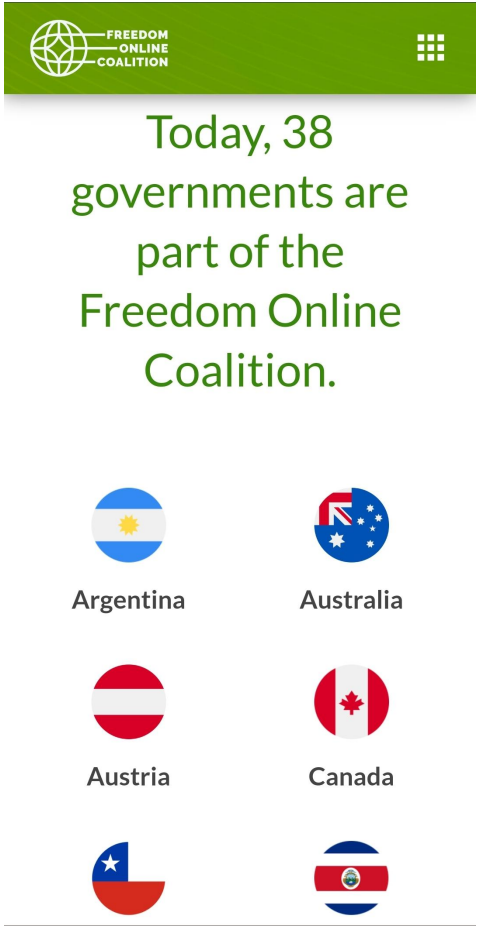
Delta Chat

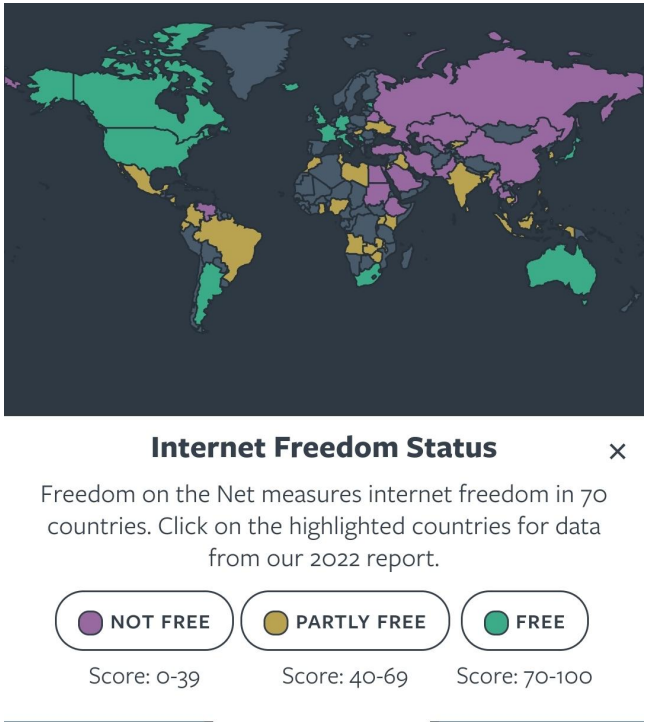
Ceno

Ouisync

Internet freedom?







How do we measure freedom of the net?

- Network measurements: monitoring trafic anomalies
- Remote measurements vs client-side approach (OONI probe)
- Analyzing BGP routing (IODA, Radar (QRator Labs)
- Multi-protocol analysis: Cloudflare Radar, M-Lab, ICLab
- Censored planet: collects and analyzes measurements from ongoing deployments of four remote measurement techniques (Augur, Satellite/Iris, Quack, and Hyperquack)
- Legal/policy analysis

Case of Crimea

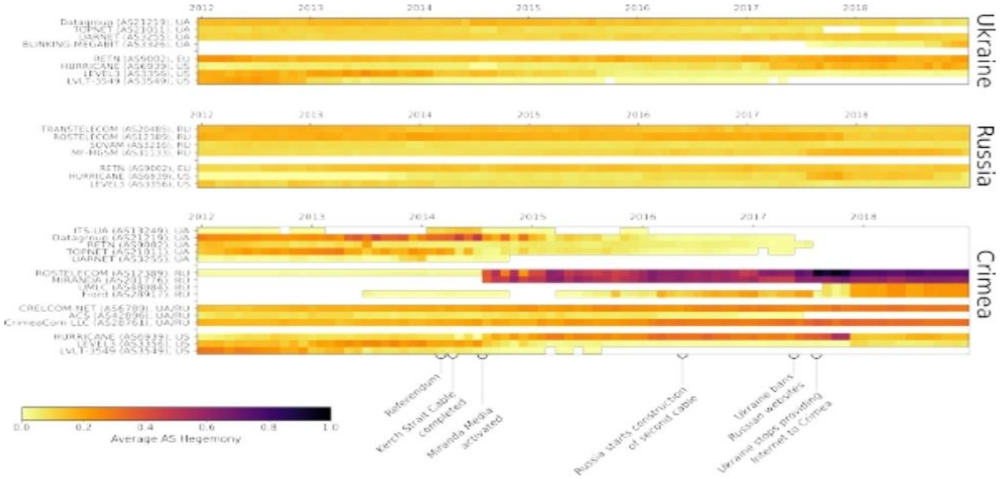


Figure 1: Average AS Hegemony for networks located in Ukraine, Russia, and Crimea. High AS Hegemony scores reveal networks that are central to reach a region.

Case of Crimea

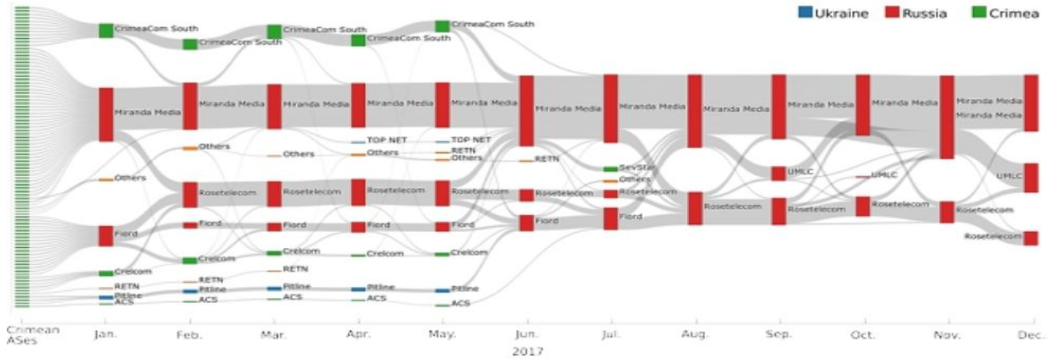
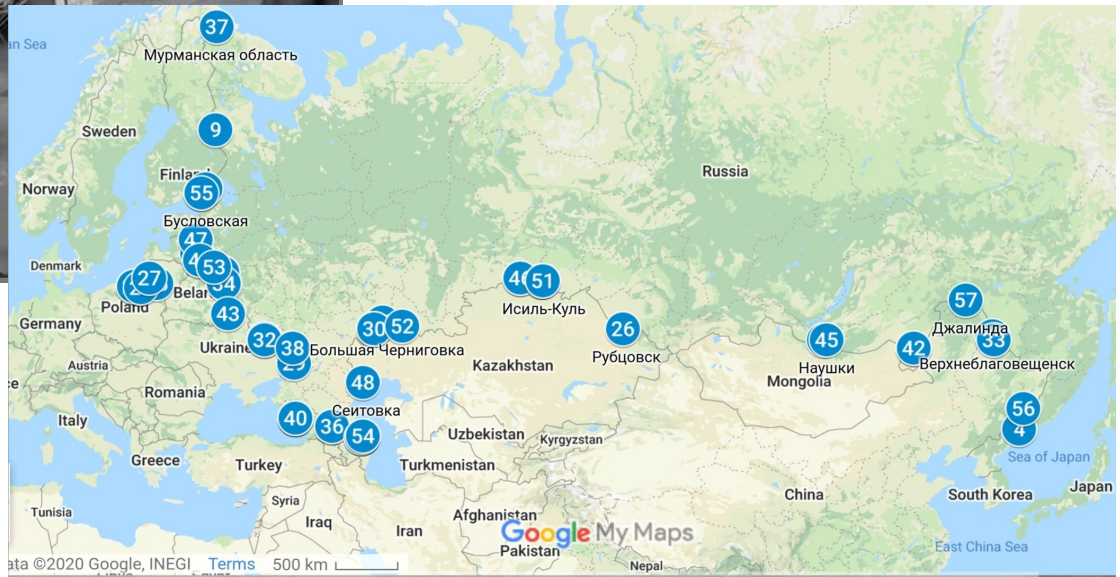


Figure 3: *End of the Transition.* Main dependencies of Crimean ASes in 2017. Left nodes represent Crimean ASes, other nodes are the main dependencies of Crimean ASes at different points in time. Only the highest dependencies are shown, in the case of a tie the closest AS to Crimea in the AS paths is selected.

One activist said that [they] could not open certain websites. We looked at it, and saw that [the access to] it was different everywhere.[7] *It all looks DIY. ISPs behave in different ways. Sometimes there are explanations and blockpages, sometimes nothing at all, some websites are partly blocked, for example Krym.Realii – just some urls and some articles are blocked* [A3].

The legend of “Runet”



6183 AS -- qrator labs (2019)

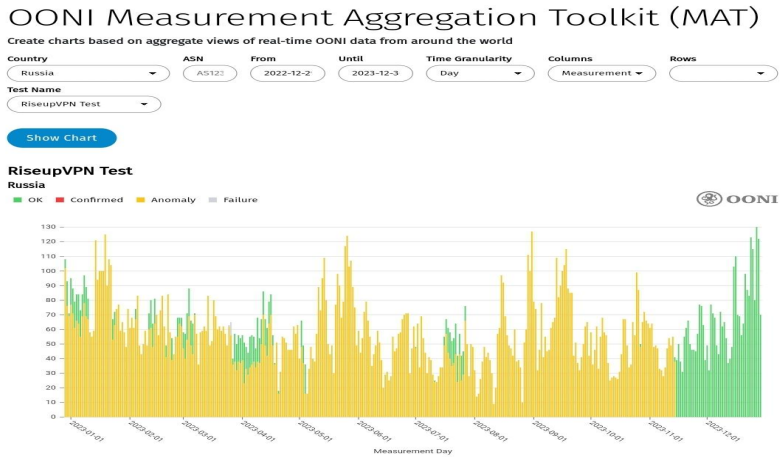
The death of “Runet”

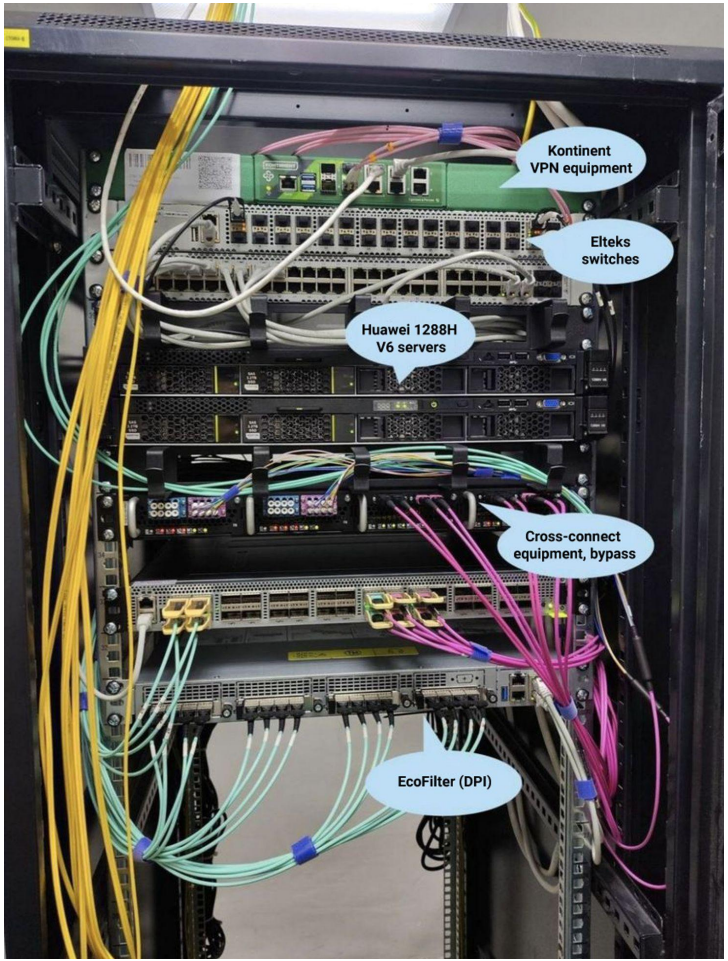
- Slow death of the runet (interviews with ISPs…)
- Waiting for the Sovereign Runet since 2016/2019
- Feb 2022:
    + Annexation of Ukrainian infrastructures, SORMification and russification of Ukrainian trafic on the ToTs
    + Influence on neighboring countries (selling SORM and DPI equipment; sanction circumvention

“runet” has no borders?

War on VPN

- War VPNs (aug-oct 2023: 167 VPN services blocked)
- Advanced usage of DPI device called TSPU for protocol-based blocking (Wireguard, OpenVPN,
- Cat and mouse game





Source: The Insider, 10.10.2023

Приложение № 2

Список технологических процессов организации

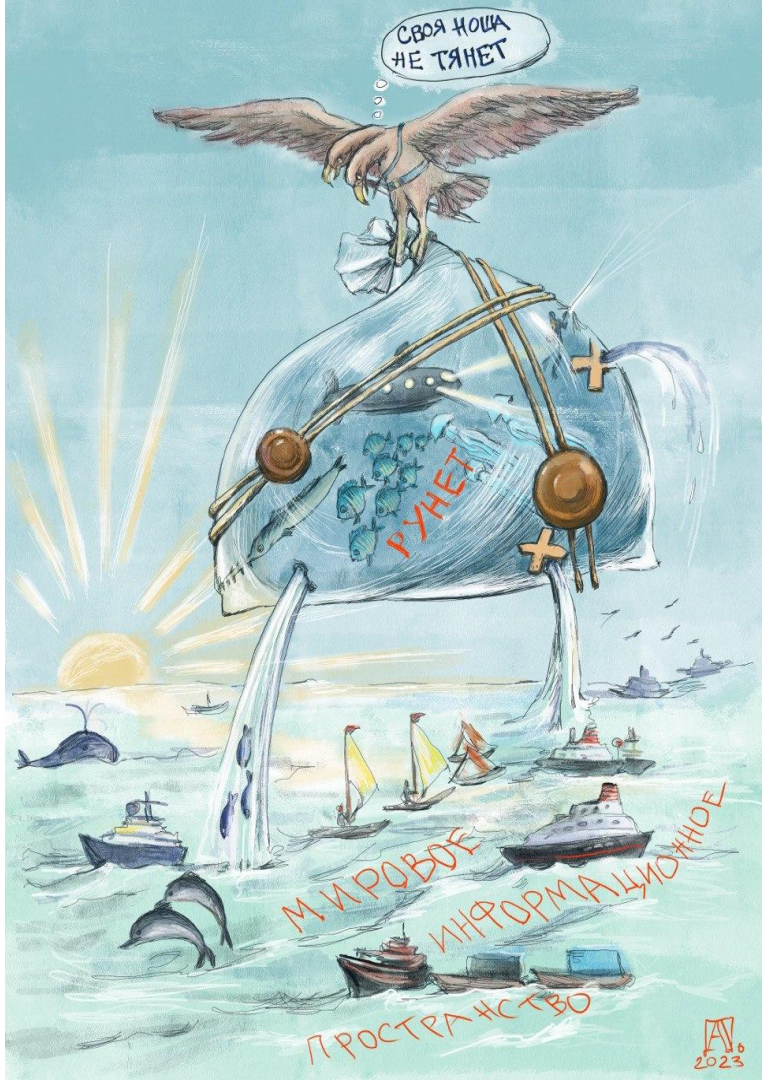
Наименование организации	Технологический процесс	Публичные IP-адрес(а) серверов, обеспечивающих VPN соединение	Контактная информация технического специалиста (ФИО, телефон, адрес электронной почты)

Source: [leak from Ministry of transportation on VPN blocking]

Приложение № 1

Список сервисов и протоколов, подлежащих ограничению

№ п/п	Наименование	№ п/п	Наименование
1.	Private Internet Access VPN	36.	WhileHat VPN Free vpn
2.	VPN Area	37.	YellowFlash VPN
3.	PIA VPN: смена IP	38.	INDIA VPN – Secure VPN
4.	Altvpn	39.	VPN – Невидимка Онлайн
5.	BullVPN – VPN Proxy Protect	40.	CheatVPN
6.	ItHelper	41.	Lets VPN
7.	Ivacy Private VPN	42.	Rez Tunnel VPN
8.	Ninja VPN	43.	Swing VPN
9.	Panda VPN	44.	Upnet VPN
10.	Planet free VPN	45.	Veee+ VPN – Fast & Stable VPN
11.	VPN by FireVPN	46.	HideMyIP VPN – быстрый ВПН
12.	Goat VPN	47.	4ebur.net VPN – Fast VPN
13.	Larva VPN	48.	PureVPN: Fast and Secure VPN
14.	Mayi VPN	49.	Протокол Shadowsocks на трансграничных узлах связи
15.	PrivadoVPN		
16.	Stark VPN Reloaded		
17.	Stark VPN Unlimited Free VPN		
18.	VPN Master – fast proxy VPN		
19.	Wirevpn – Fast Unlimited Proxy		
20.	Asia VPN – 4 UAE, Saudi, Oman		
21.	Secure VPN Proxy: Super Safe		
22.	Cool VPN Pro: безопасный VPN		
23.	VPN сервера в России		
24.	CloudVPN – впн прокси мастер		
25.	Vava VPN		
26.	BeastVPN: Secure and Fast VPN		
27.	Kiwi VPN Connection IP Changer		
28.	Blue Speed VPN: Secure & Fast		
29.	Droid VPN-Secure Proxy Premium		
30.	GABBY VPN-PRO		
31.	i2VPN – Secure VPN Proxy		
32.	ItsVpn: vpn v2ray Fast Proxy		
33.	Nolog VPN – Fast Secure Proxy		
34.	VPN Vault – Super Proxy VPN		
35.	VPN99		



Source: OrderCom

But… censorship is an experience!

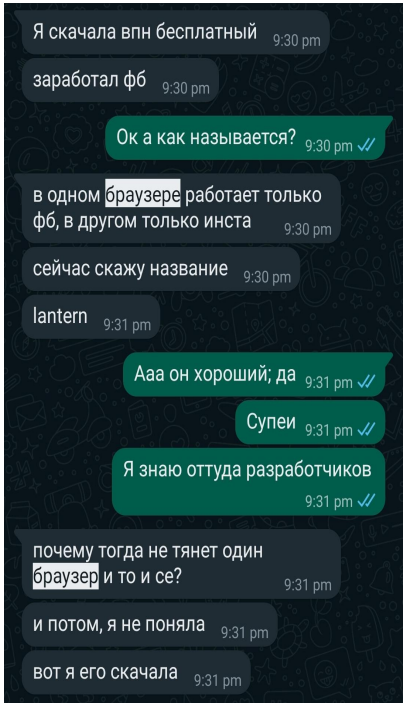
What people see / how do they feel about connectivity?

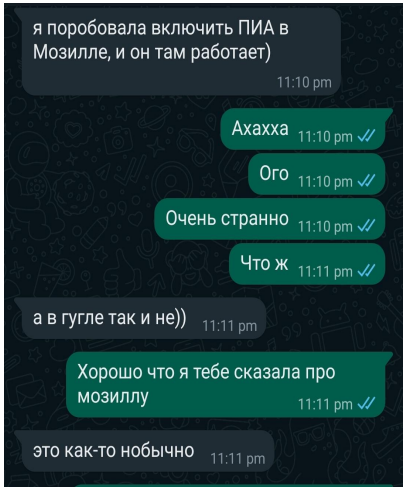
Can we actually measure the **experience of network interferences**?

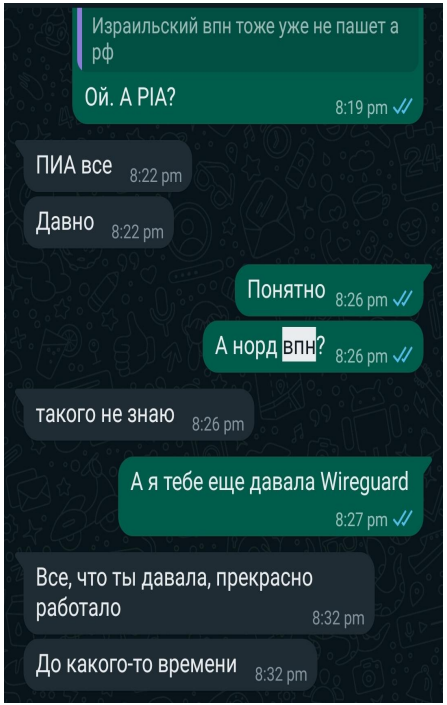
How does it affect work and life of people?

What does it mean a VPN that **works**

At which point does it become unbearable for the user?







VPN measurements… undone!

"All of them claim to be the best": Multi-perspective study of VPN users and VPN providers

Reethika Ramesh
University of Michigan

Anjali Vyas
Cornell Tech

Roya Ensafi
University of Michigan

Abstract

As more users adopt VPNs for a variety of reasons, it is important to develop empirical knowledge of their needs and mental models of what a VPN offers. Moreover, studying VPN users alone is not enough because, by using a VPN, a user essentially transfers trust, say from their network provider, onto the VPN provider. To that end, we are the first to study the VPN ecosystem from both the users' and the providers' perspectives. In this paper, we conduct a quantitative survey of 1,252 VPN users in the U.S. and qualitative interviews of nine providers to answer several research questions regarding the motivations, needs, threat model, and mental model of users, and the key challenges and insights from VPN providers. We

Only limited prior work has delved into the human factors of VPN use: factors that contribute to retention of VPNs [29,55], attitudes of university students and corporate users towards VPNs [3,10,11], and the widespread misconceptions of how privacy-enhancing tools work [45].

However, no study has combined both the users and VPN providers perspectives to answer fundamental questions about the VPN ecosystem. For instance, users using VPNs are essentially transferring trust from their network provider onto the VPN provider, but it is unclear as to what VPN features encourages them to make this shift? On the other hand, the VPN industry has been known to employ various marketing tactics [1] and dark patterns around discounts [21,48], but it is yet unknown if these practices are bound to have any sig-

Russian censorship studies… still lack on-the-ground reports!

TSPU: Russia's Decentralized Censorship System

Diwen Xue
University of Michigan

Benjamin Mixon-Baca
ASU/Breakpointing Bad

ValdikSS
Independent

Anna Ablove
University of Michigan

Beau Kujath
ASU/Breakpointing Bad

Jedidiah R. Crandall
ASU/Breakpointing Bad

Roya Ensafi
University of Michigan

ABSTRACT

Russia's Sovereign RuNet was designed to build a Russian national firewall. Previous anecdotes and isolated events in the past two years reflected centrally coordinated censorship behaviors across multiple ISPs, suggesting the deployment of "special equipment" in networks, colloquially known as "TSPU". Despite the TSPU comprising a critical part of the technical stack of RuNet, very little is known about its design, its capabilities, or the extent of its deployment.

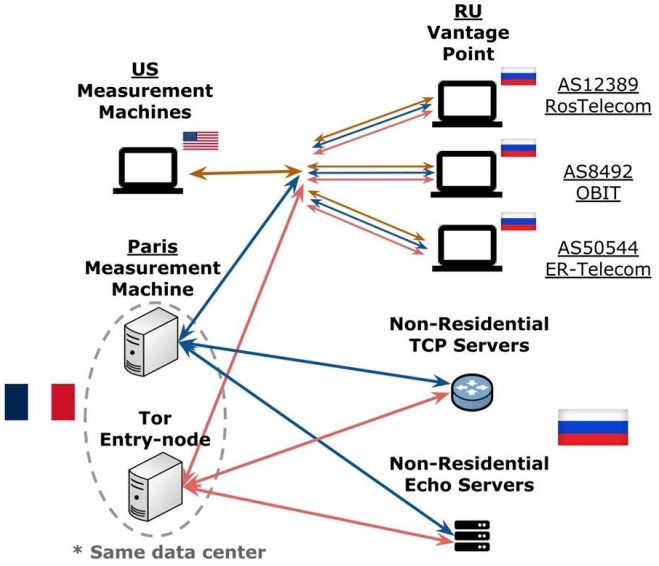
In this paper, we develop novel techniques and run in-country and remote measurements to discover the *how*, *what*, and *where* of TSPU's interference with users' Internet traffic. We identify different types of blocking mechanisms triggered by SNI, IP, and QUIC, and we find the TSPU to be in-path and stateful, and possesses unique state-management characteristics. Using fragmentation behaviors as fingerprints, we identify over one million endpoints in Russia from 650 ASes that are behind TSPU devices and find that 70% of them are at most two hops away from the end IP. Considering that TSPU devices progressed from ideation to deployment in three years, we fear that the emerging TSPU architecture may become a blueprint for other countries with similar network topology.

1 INTRODUCTION

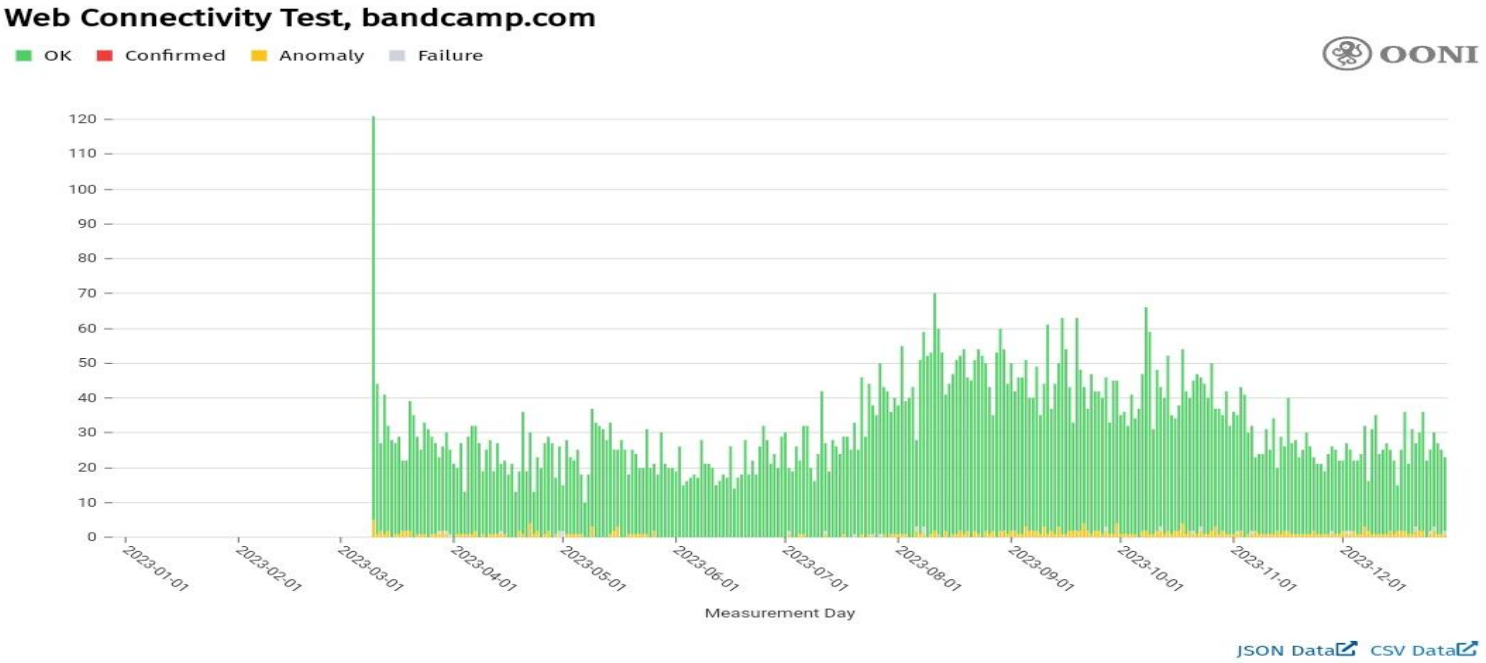
Since 2012, the Russian government has been developing both legal and technical frameworks to construct its censorship apparatus [17]. In May 2019, the "Sovereign RuNet" law was signed, requiring telecom operators to install a home-grown DPI system, colloquially known as "TSPU", on their networks free of charge [20]. This provides the government with an extraordinary ability to centrally and unilaterally control the traffic passing through thousands of privately-owned, distributed ISPs. This centralized control was established to isolate Russia's internal Internet ecosystem from the rest of the world to "protect" Russia in the face of foreign threats [27].

Previous studies independently point to the deployment of the TSPU. In March 2021, Russia pressured Twitter to comply with its content removal requests with targeted throttling and threats of outright blocking [29]. Xue *et al.* showed that throttling behaviors demonstrated a high degree of uniformity and coordination across a range of ISPs [98]. Subsequently, Roskomnadzor, Russia's communication agency, publicly confirmed that the TSPU, which comprises the technical stack of RuNet, was used for throttling [28]. In March 2022, censorship observatory OONI reported that many news and social media sites promoting narratives critical of the

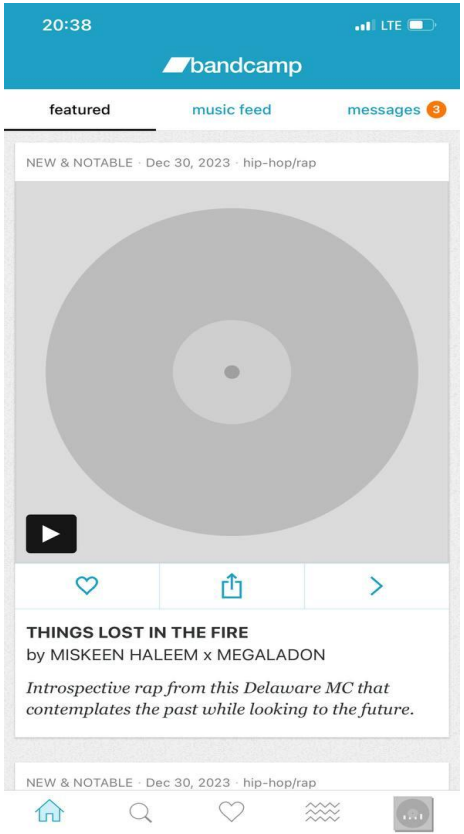
TSPU: Russia's Decentralized Censorship System

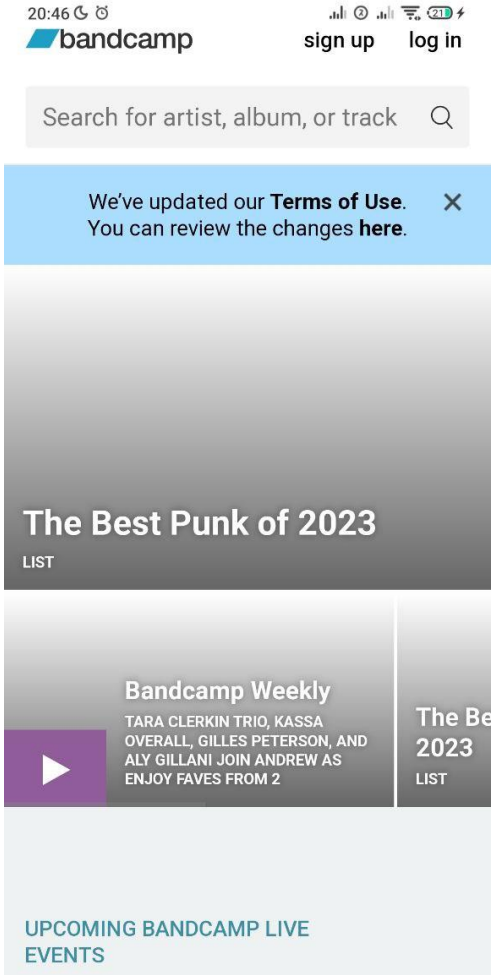


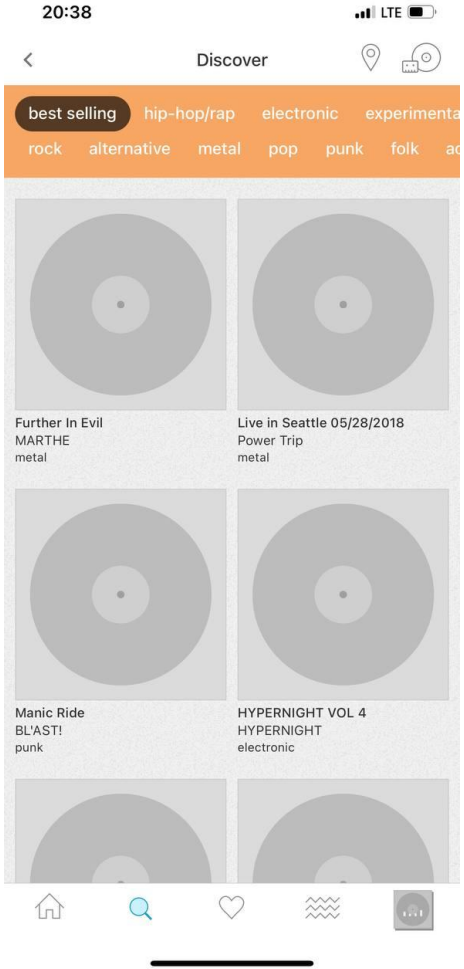
What OONI sees?



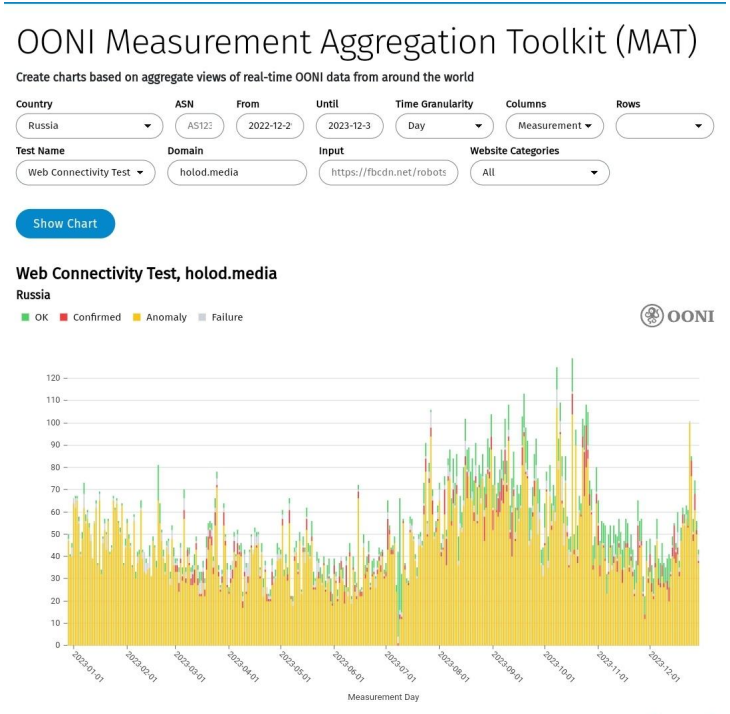
What user sees?

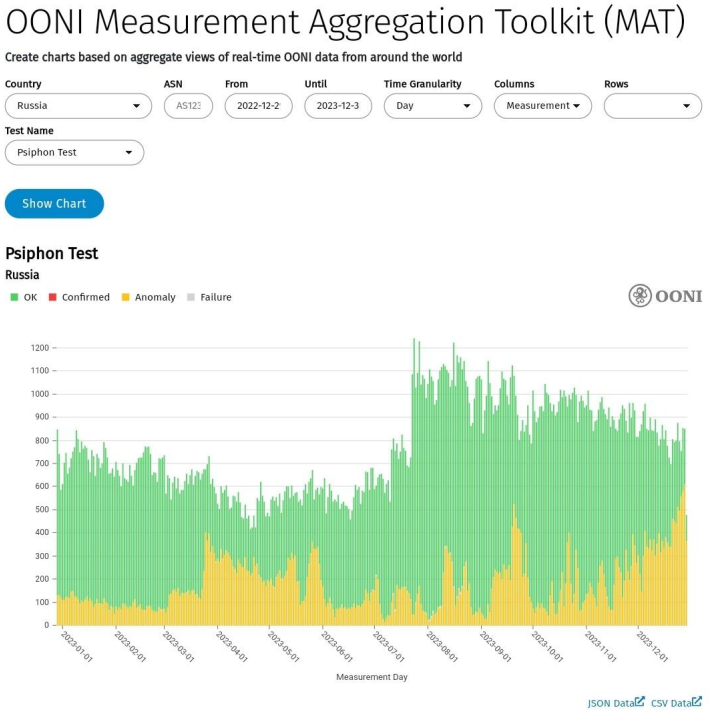




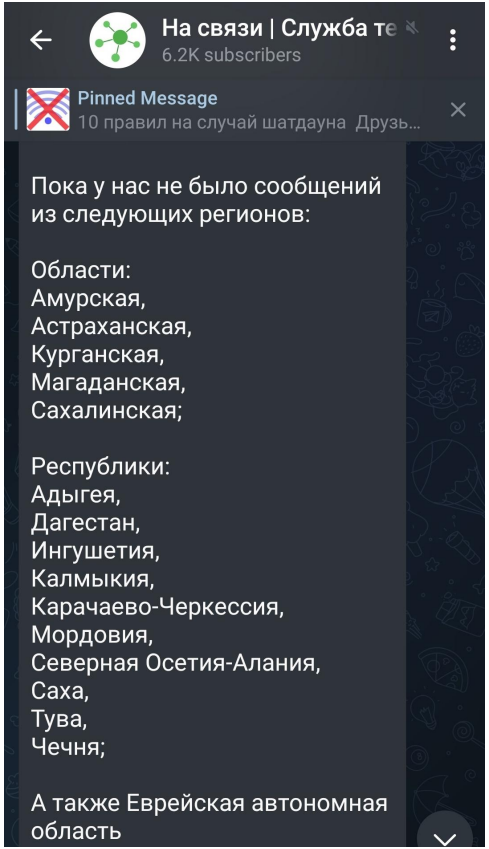


Censorship still inconsistent across the country

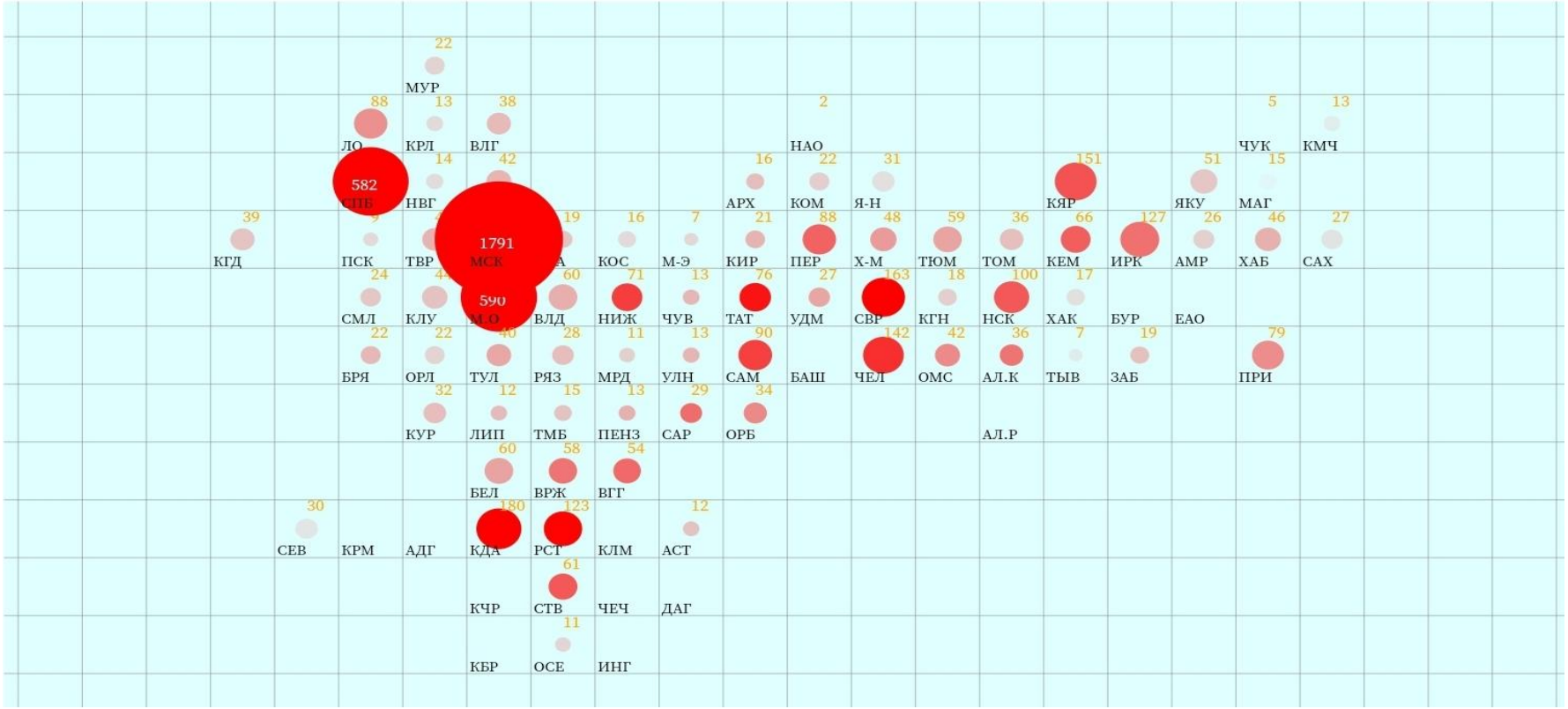




Censorship is a complex **experience**!



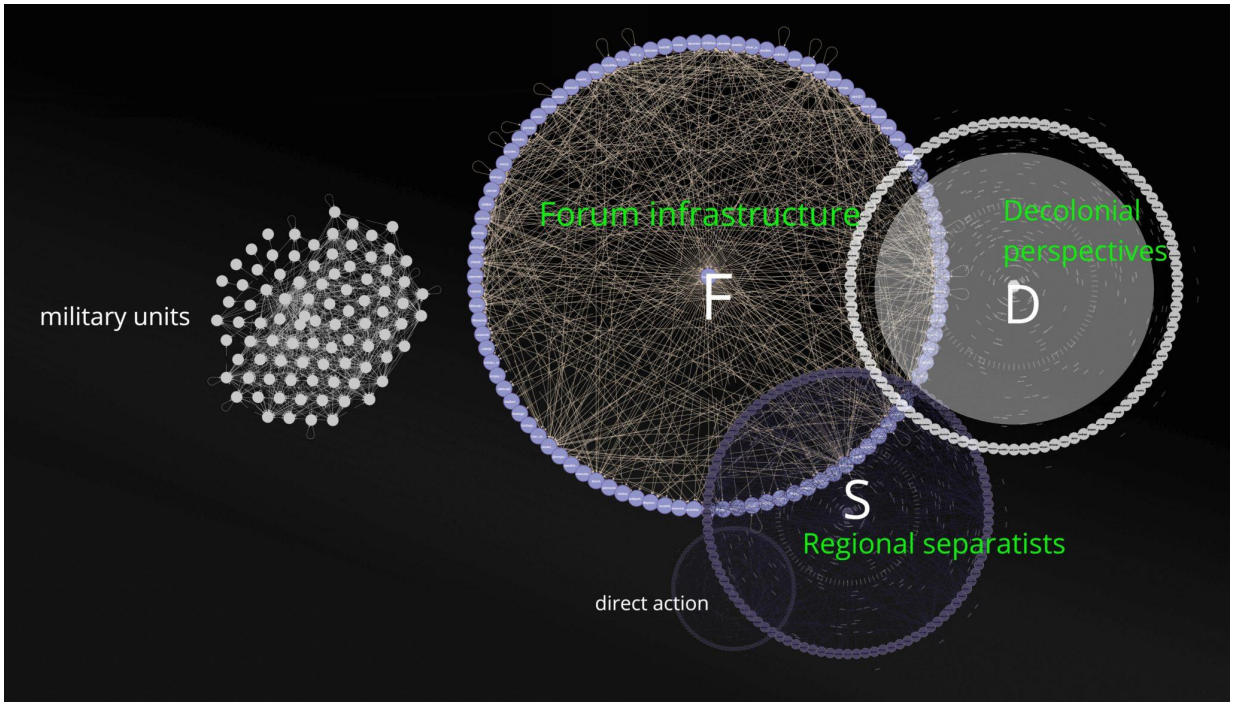
Source: [NaSvyazi digital helpline]



Moscow: 1791 ISPs
Saint-Petersburg: 582 ISPs
Mari-El: 7 ISPs
Tyva: 7 ISPs

ISPs by region: ifreedomlab.net

Raspad.network



https://gitlab.com/raspad-network/sources

Regional shutdowns

Source: IODA, BGP global prefix visibility for Ingushetia, Oct 2018

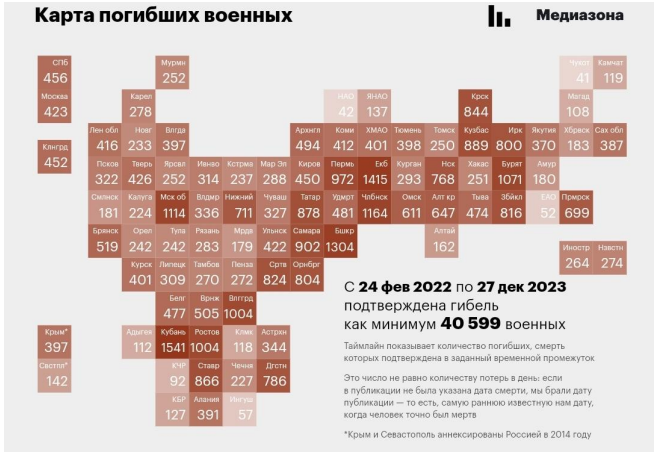
Регионы, где отсутствуют зонды RIPE Atlas.

#	Субъект РФ
1	Республика Бурятия
2	Республика Северная Осетия – Алания
3	Республика Адыгея
4	Республика Саха (Якутия)
5	Республика Коми
6	Тамбовская область
7	Республика Ингушетия
8	Кабардино-Балкарская Республика
9	Республика Калмыкия
10	Еврейская автономная область
11	Республика Марий Эл
12	Камчатский край
13	Чукотский автономный округ
14	Республика Тыва
15	Ненецкий автономный округ

Топ-10 лучших регионов по количеству зондов RIPE Atlas.

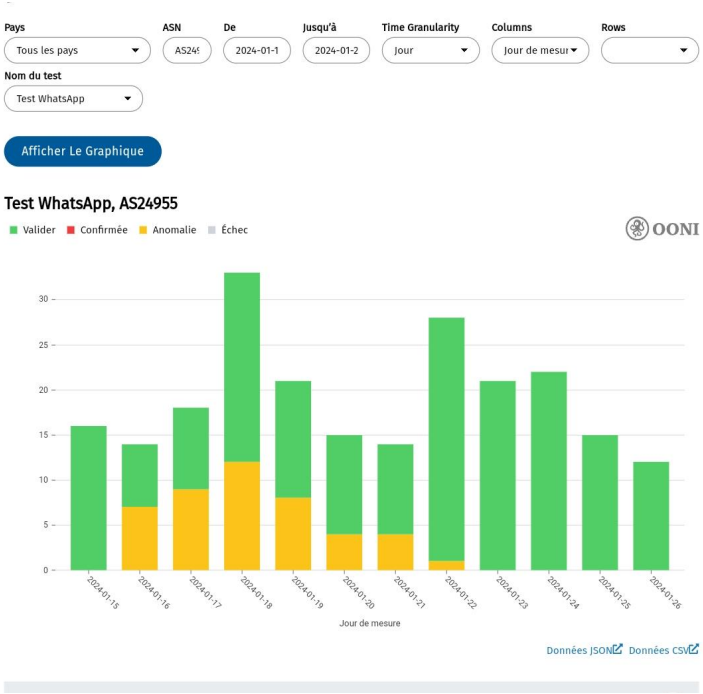
#	Субъект РФ	Значение частного показателя
1	г. Москва	25,55
2	г. Санкт-Петербург	10,92
3	Московская область	6,85
4	Новосибирская область	2,67
5	Омская область	1,63
6	Краснодарский край	1,63
7	Воронежская область	1,63
8	Свердловская область	1,51
9	Республика Татарстан	1,51
10	Ленинградская область	1,51

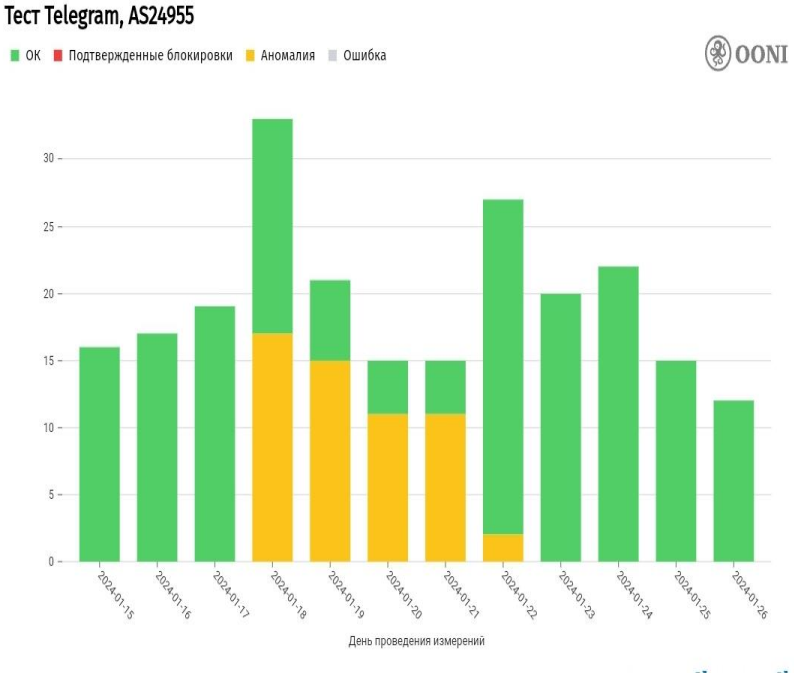
[Source: OZI report on connectivity of RU regions]



[Source: Meduza investigation on n of ru soldiers died in UA]

Telegram & WhatsApp blocking in Bashqortostan





Telegram & WhatsApp blocking in Yakutia

Анонимно 1 день назад

Якутия, ничего не работает, ни Ватсап, ни телега, ни ютуб, ни гугл нихрена вообще

5 Ответить

Екатерина 1 день назад

Якутия, ничего не работает!

3 Ответить

Анонимно 1 день назад

Якутск, вотсапп, телеграм лежат с утра. Ни с впн, ни без впн не работают. «Подключение» и «обновление» — вот и все, что я вижу. А, еще ютубчик тоже ничего не грузит. МТС.

3 Ответить

Гражданин. 1 день назад

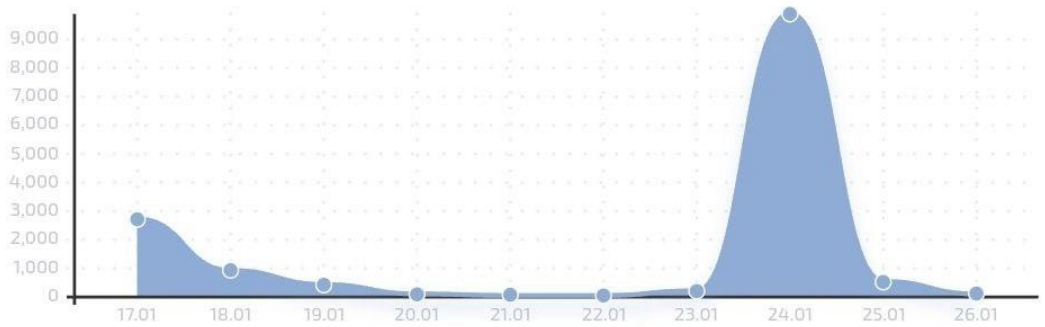
Якутия. Ютуб, телега, вотсапп не работают. Похоже идёт подготовка к отключению навсегда, подарок от власти гражданам к выборам. Северо-Корейский вариант.

3 Ответить

Reports on blocking of Whatsapp and Telegram

Что сегодня с WhatsApp*

График наглядно показывает динамику проблем за последние 10 дней.
Если на графике виден сильный отрыв от предыдущих значений, значит сбой носит массовый характер.

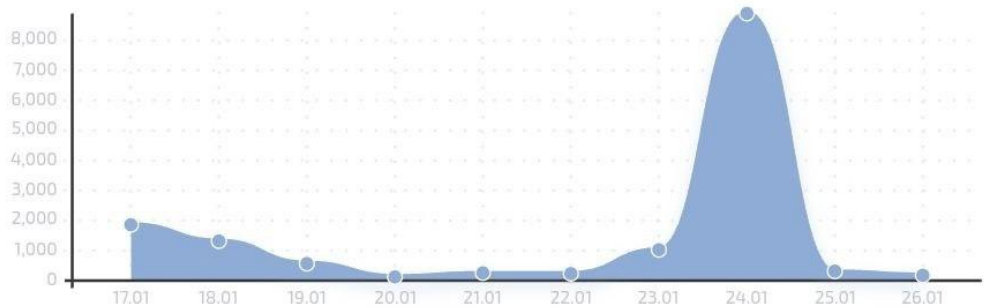


Source: сбой.рф

Reports on blocking of Whatsapp and Telegram

Что сегодня с Telegram

График наглядно показывает динамику проблем за последние 10 дней.
Если на графике виден сильный отрыв от предыдущих значений, значит сбой носит массовый характер.



Ниже на графике количество жалоб за последние 24 часа на Telegram

Source: сбой.рф

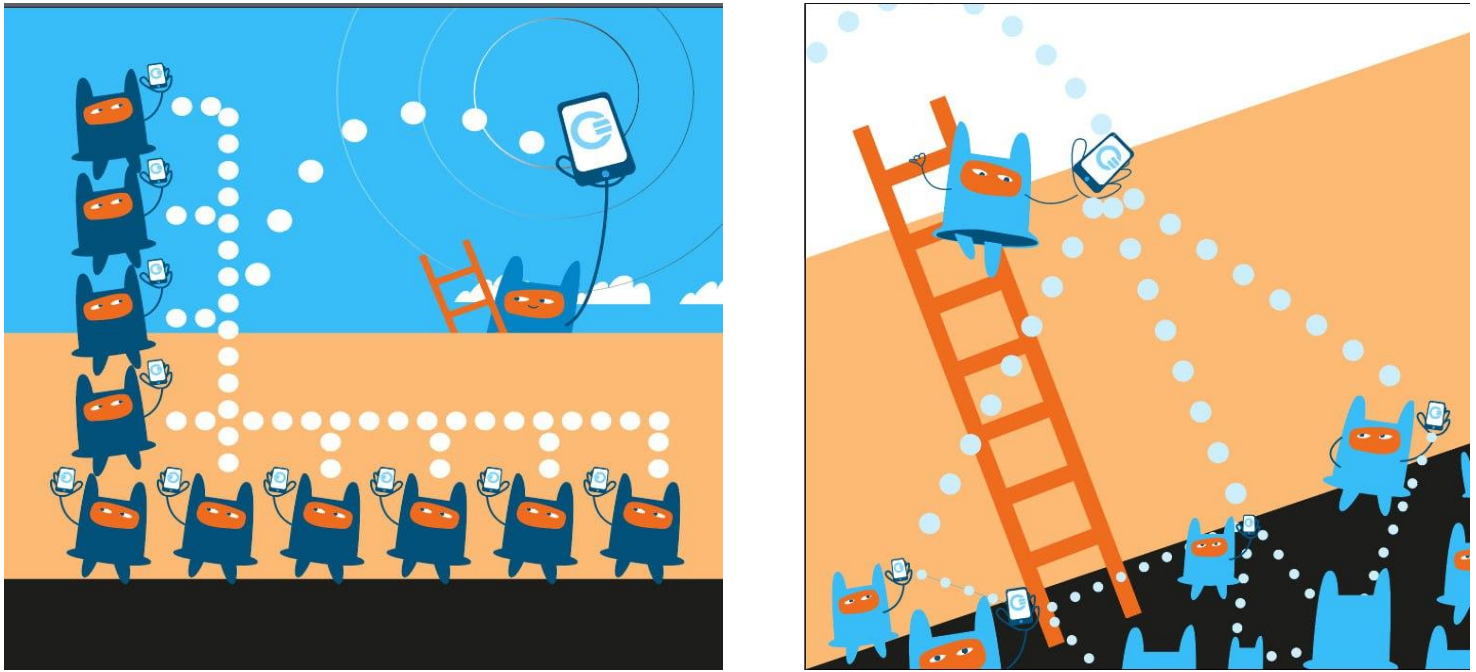
Methodological challenges

- Regional/local blocking is hard to prove (OONI data unequally distributed, lack of probes in remote regions, most probes in bigger central cities)
- Big ASNs → hard to geolocate
- Patchworked censorship, inconsistent across networks and even across browsers
- Measuring from outside… not accurate! Censorship is best measured from inside out

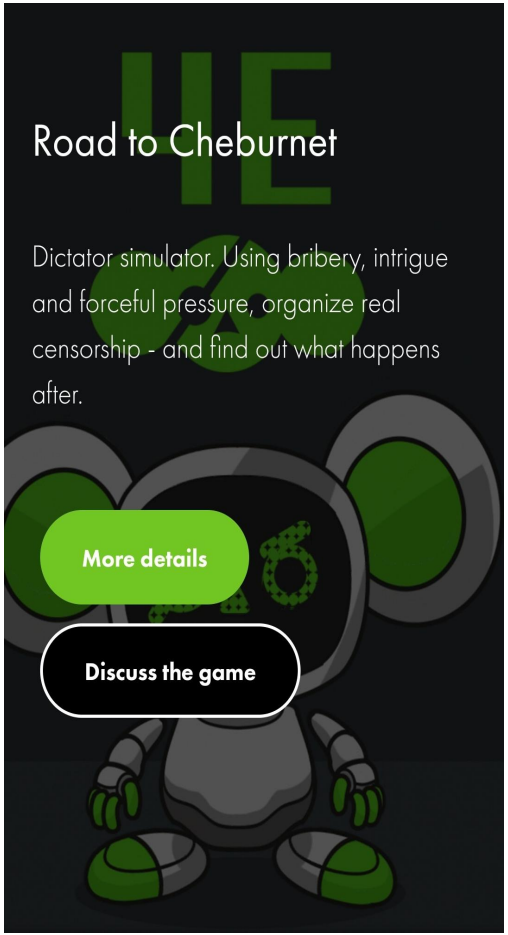
Bringing users in

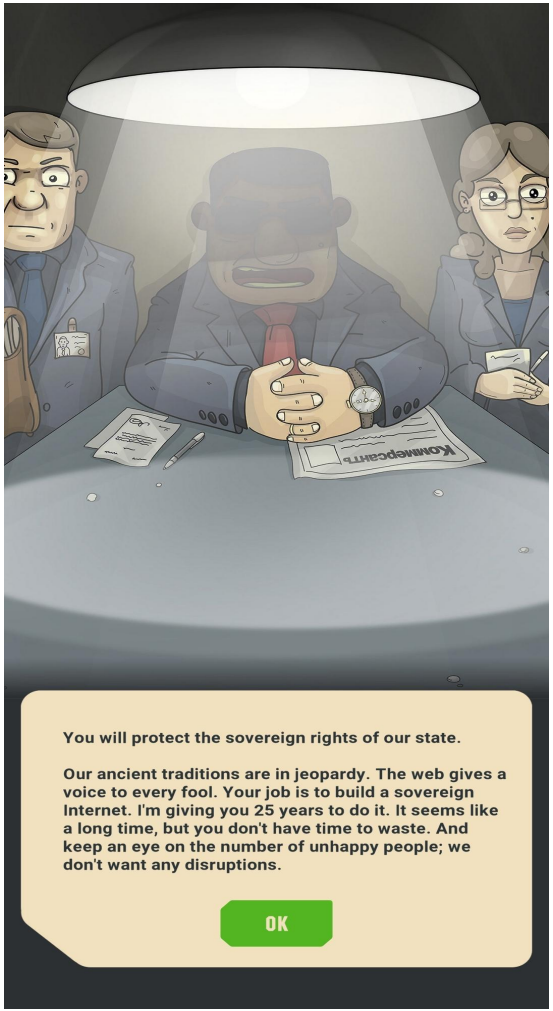
- No “runet” but “runets”
- Organizing w indigenous activists to popularize OONI probe across regions
- Developing a secure protocol to enroll testers and collect data
- Collecting qualitative descriptions of “experiences of censorship”
- Opening up “censorship” → information control
- Partnering with RiseUp/LEAP project to conduct fine-grain connectivity tests for a variety of circumvention protocols and bring new tests to OONI

“Silicon curtain”



Source: Ceno browser -- censorship.no





“The Road to Cheburnet” —
a game by eQualit.ie
and Noesis games

DONATE!!!