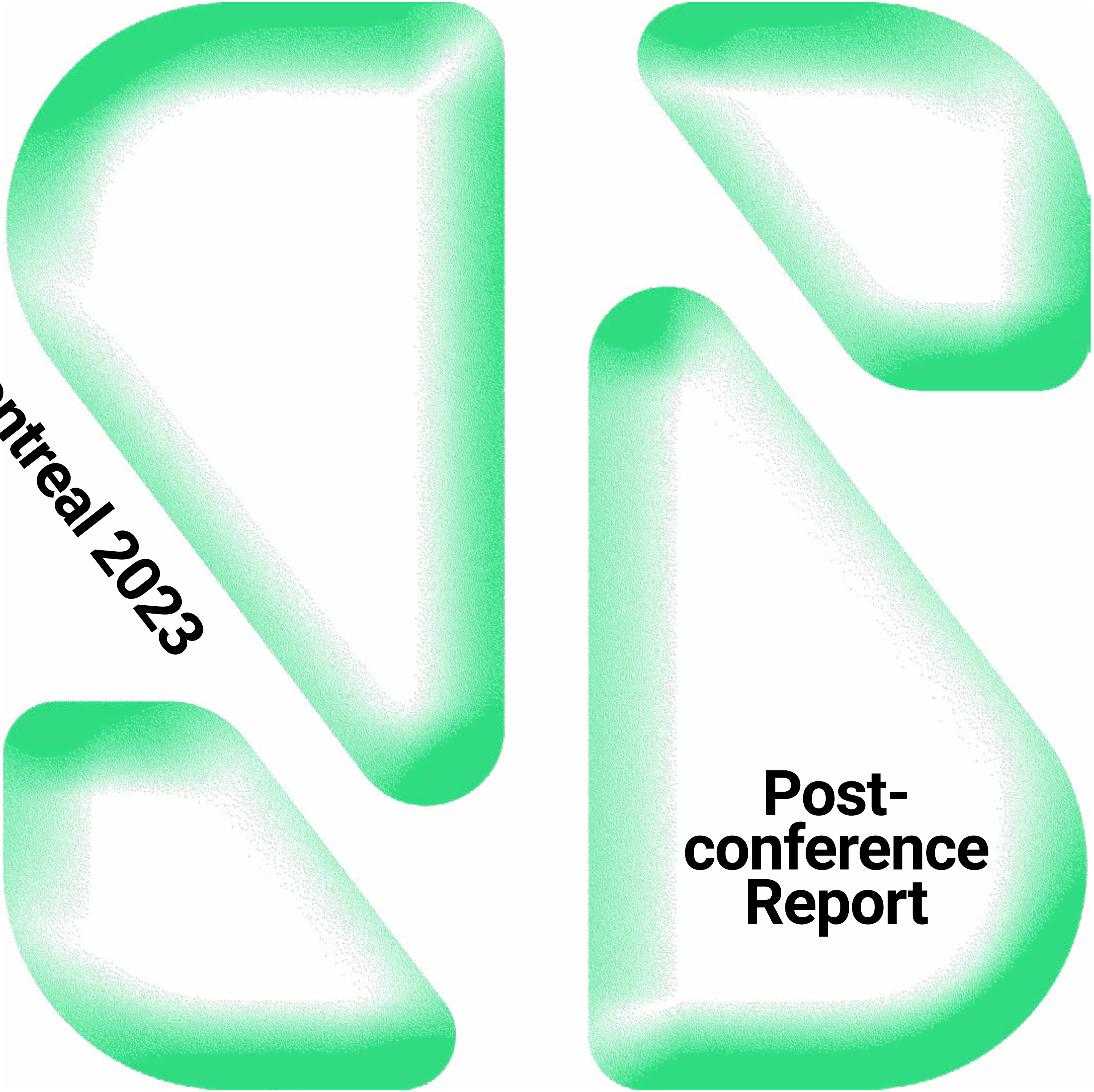
SplinterCon

Montreal 2023



Post-conference Report

eQualitie

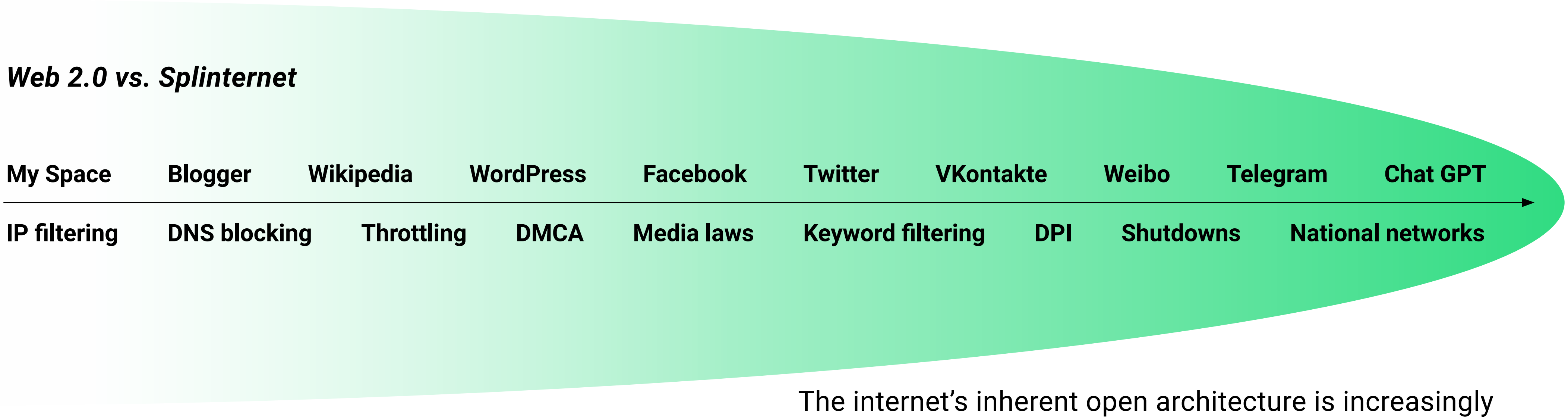
Section I

Introduction

The splinternet — what it is, where we're headed

The promise of a global digital commons has given way to an increasingly fragmented collection of closed internets with their own separate infrastructures, controlled by Big Tech and nation states, many of them autocratic or totalitarian.

Web 2.0 vs. Splinternet



The internet's inherent open architecture is increasingly weaponized as a tool for censorship and persecution. States have begun to shutdown or implement national networks, isolating citizens from the global commons. Tech companies are separating users into corporate marketplaces and digital walled gardens — **these are examples of the emergence of splinternets**.

Introducing SplinterCon

While the idea of the "Splinternet" is increasingly discussed and documented by media and advocacy organizations, SplinterCon is the first international and interdisciplinary conference to focus specifically on the technologies, processes and responses to network fragmentation.

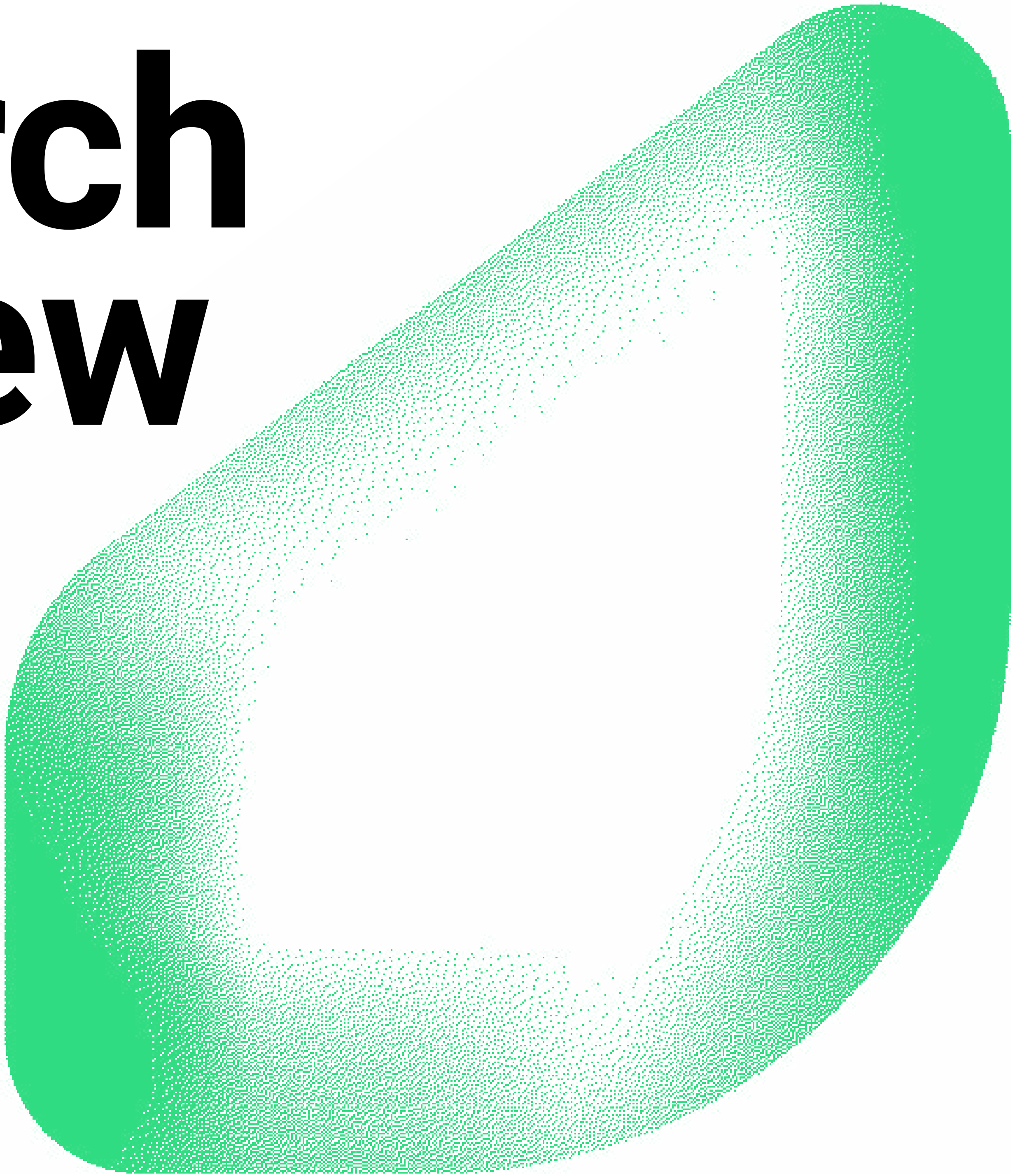
Launched by eQualitie in Montreal, December 2023, the inaugural SplinterCon brought together a hundred network researchers, technology entrepreneurs, network engineers, software developers, user experience designers, media and internet freedom advocates. Personal testimonies from a variety of countries that have suffered shutdowns enriched the discussion, along with legal and policy analysis, and incredible wireless technology demos.

SplinterCon was hosted under Chatham House Rules, and this report presents the highlights, supplemented by a selection of presentations and papers on the SplinterCon website, with explicit permission from the authors.

ABOUT EQUALITIE

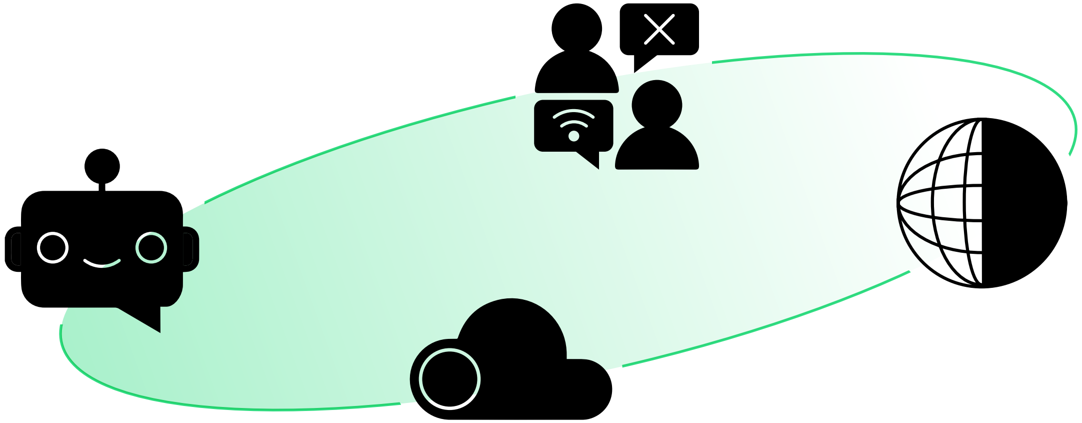
eQualitie's mission is to enable freedom of association for millions of people online, by building technologies and education programs that support a free, secure and equal internet. To that end, it supports organizations in 23 countries. Its Deflect anti-DDoS service, Ceno browser and OuiSync file sharing technologies provide private, resilient information sharing and access solutions, independent of easily blocked or restricted platforms.

Research overview



Network measurement: from censorship to shutdowns

The challenge for this SplinterCon was presented as the struggle against censorship of global connectivity. The opening keynote spoke about the corporate splinternet, where trillion dollar companies host billions of users, monetizing it through surveillance capitalism, propelled by advertising, viral marketing and cat pics; the walled gardens created by protocols and intellectual property, where human progress and achievement is fenced in walls of incompatibility and licencing; the digital divide that continues to splinter our digital world — billions still without reliable, affordable or simply any connectivity to the global network; soon, it was suggested, we'll be meeting at conferences on the splinternets of humans and machine bots.



DID YOU KNOW?
Unlike partial or full shutdowns, Splinternetization is the process of building digital or material borders, including the creation of "national Internets" — a more permanent type of network isolation. While for some regions, such as the EU, "Internet sovereignty" is a matter of economic competition with US in terms of deploying domestic alternatives for popular services, other projects of "sovereign networks", for instance the Russian "Cheburnet" or the Iranian "HalalNet", propose national cyber sovereignty via permanent disconnection from foreign cyberspace.

The territorialization and fragmentation of cyberspace

Recent events in Ukraine, Azerbaijan, Iran and other conflict areas demonstrate how states attempt to leverage foundational internet protocols as tools of political control. Research presented at Splintercon showed that:

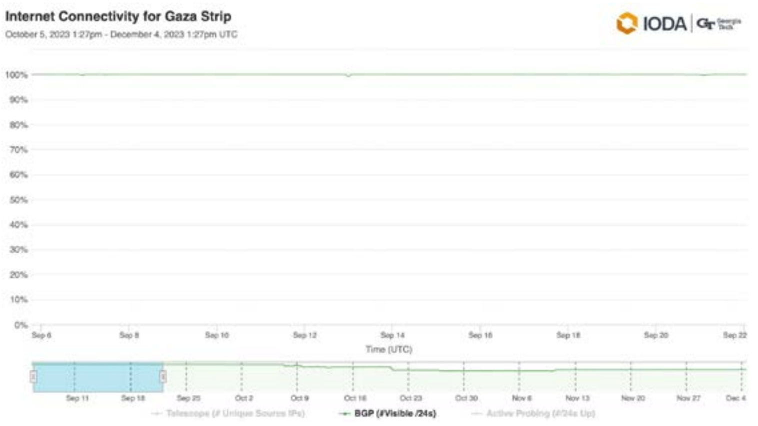
Shutdowns are 9x more likely to occur as a response to protests, 16x more likely to co-occur with coups and around election cycles.

We invited participants from a variety of network measurement initiatives such as IODA, OONI, M-Lab, and Cloudflare Radar to present their relevant research and datasets for exploration. The following pages provide an overview of their research. Here's an overview of their research...

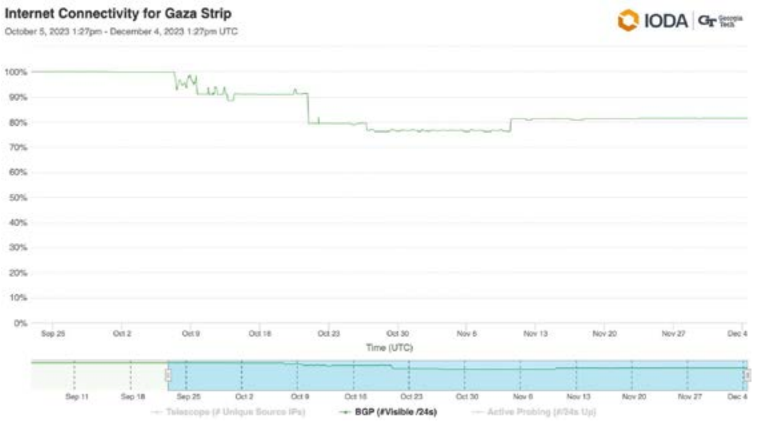
IODA (Internet Outage Detection and Analysis)

This project measures network outages rather than blockages (unlike OONI). It looks at BGP announcements, Active Probing (normal vs abnormal AP signal behaviors from continuous pings of networks at certain locales), Telescope (measures unsolicited network traffic captures through dedicated research infrastructure called a telescope). The data is available on country or regional levels; reports are published around specific events and overall outage scores are produced (see https://ioda.live).

However, the data is limited to IPv4, it has less visibility into mobile networks or countries that heavily use private IPs (NAT). IODA's insights into network disruptions helped them develop specific techniques to identify signatures of shutdowns vs spontaneous outages and to detect throttling / route changes.



Normal BGP Signal Behavior

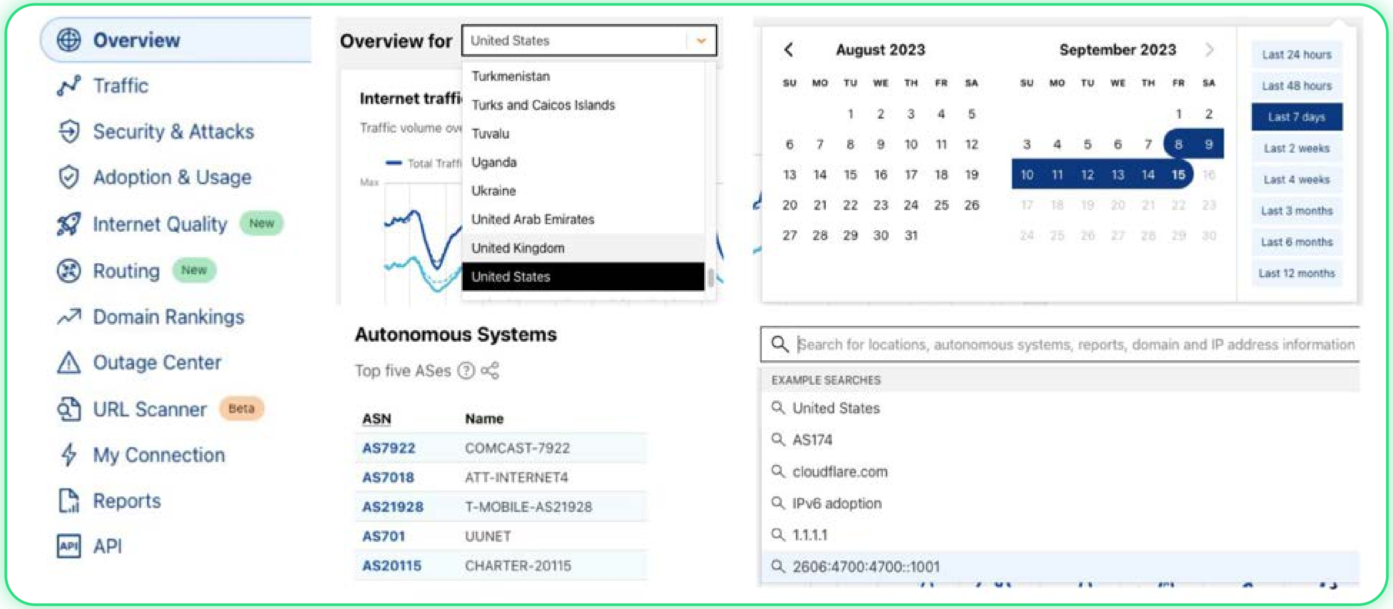


Disrupted/ Abnormal BGP Signal Behavior

Cloudflare Radar

This project helps slow down “splinternetization” by providing insights, threats and trends based on Clouflare’s aggregated data — from a security, performance and usage perspective.

Radar helps to detect and corroborate reports of Internet disruptions, providing aggregated views of traffic, outages, connection quality (bandwidth, latency, DNS, TCP connection), routing (route leaks & origin hijacks) etc. Data can be filtered by country/ASN and custom time-frames can be set.



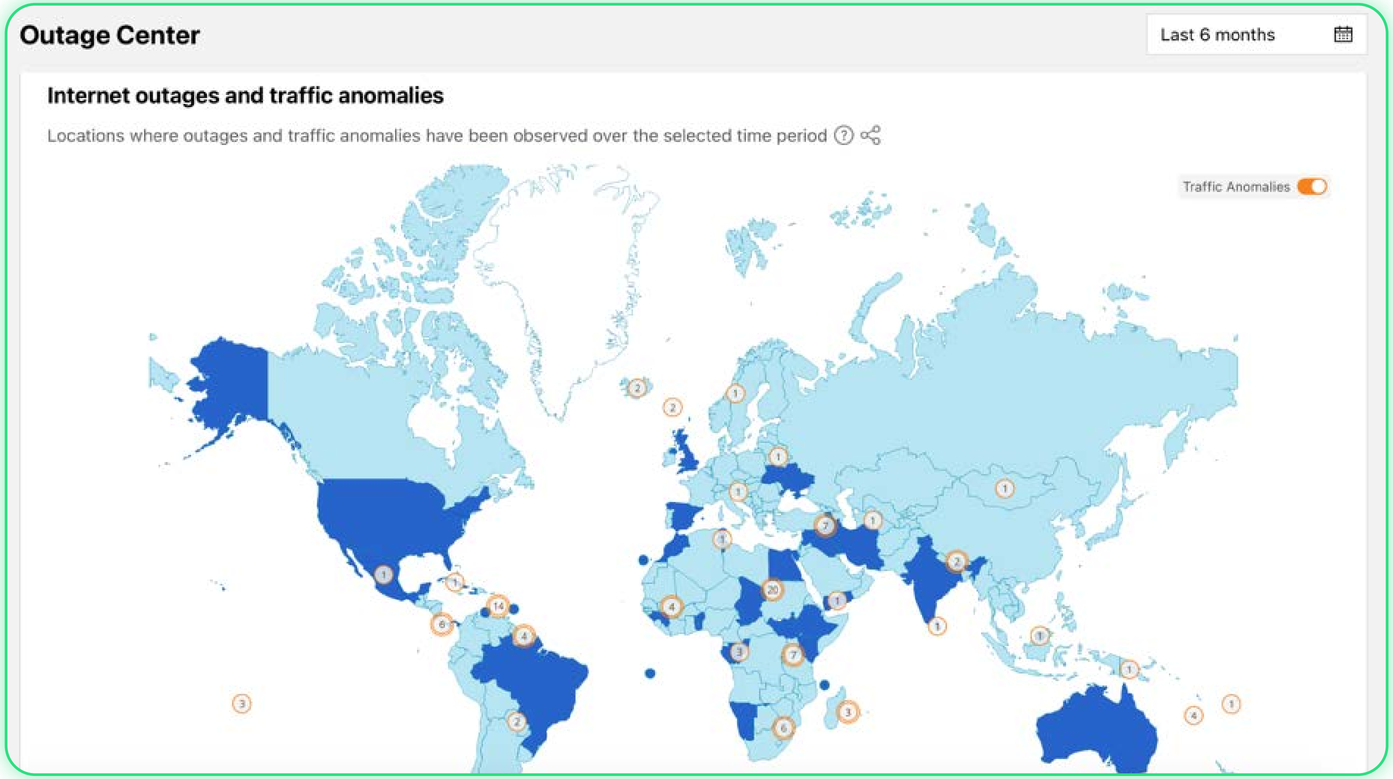
Autonomous Systems

Top five ASes

ASN	Name
AS7922	COMCAST-7922
AS7018	ATT-INTERNET4
AS21928	T-MOBILE-AS21928
AS701	UUNET
AS20115	CHARTER-20115

Cloudflare Radar

The Cloudflare Radar Outage Center (CROC) produces a curated list of observed & verified Internet outages and collects metadata about the outage or traffic anomalies. It’s also possible to manually verify the anomaly based on metrics from other projects (e.g. IODA). The adoption and usage provide metrics around the use of different technologies and protocols (HTTP version, TLS, IPv4 / IPv6).



Outage Center

Last 6 months

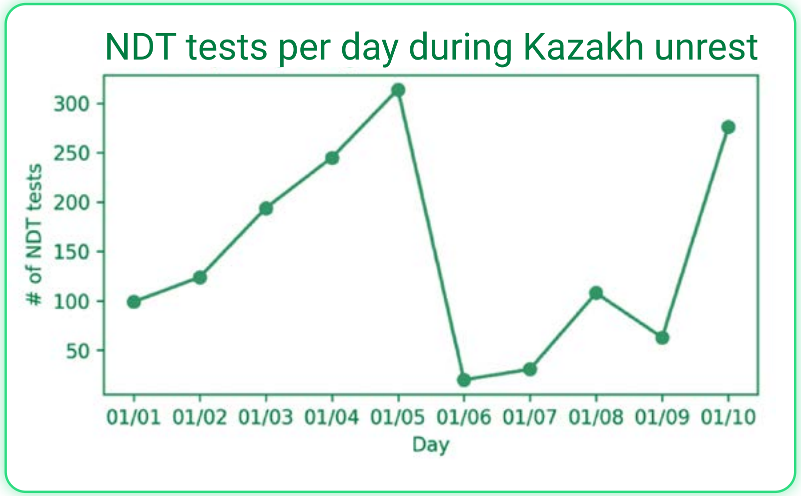
Internet outages and traffic anomalies

Locations where outages and traffic anomalies have been observed over the selected time period

Traffic Anomalies

Measurement Lab (M-Lab)

This project helps users to establish whether connectivity problems are caused by the connection itself, an application or something else. Based on one of the world's largest open internet performance datasets, it offers an open, verifiable measurement platform for global network performance — and creates visualizations and tools to help civil society and other organizations make sense of the data.



More commonly referred to as a "speed test", the project's Network Diagnostics Tool (NDT) is the most frequently run test, with over 4 million per day, on average. NDT data can be used to find evidence of throttling and/or shutdown events. The project's Wehe mobile application allows users to detect whether or not specific applications are being throttled by their ISP.

The presentation explored the possibilities of using traceroute data to find evidence of shutdowns, analysing data to see how network interference events affect the paths being taken. Suggestions around ideal server topologies to measure network interference events and internet fragmentation behaviors were also raised, along with questions around which metrics are the most useful to collect during crowd-sourced campaigns to document network interference events.

Key learnings: the challenge of network measurement

The internet is hard to measure. As one of our presenters, an expert in network measurements recommended, one should be very careful with speculations and interpretations since there are limits to what can be inferred from the data. Another challenge consists in creating visuals that can help communicate findings to social scientists and have a dialogue with them on how to analyze what we see from various data sources and tools.

The SplinterCon approach to network measurements is to combine different tools, data sources and approaches, and verify it with real-life testimonies from the field. As one of our speakers brilliantly framed,

"Censorship is best measured from inside out".

Section III

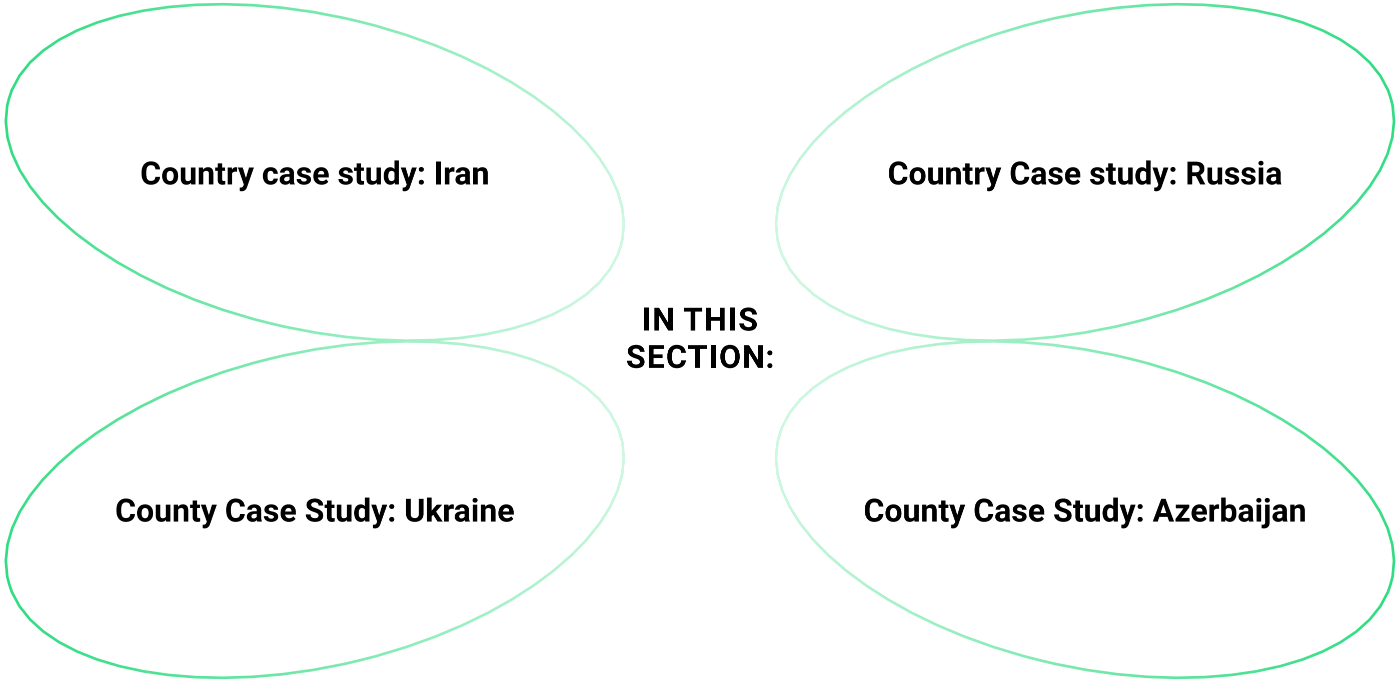
Splinternet: country case studies

Section I
Section II
Section III
Section IV
Section V
Section VI
Section VII

Splinternet: the insider’s experience

To share an “insider’s experience of a splinternet” eQualitie invited researchers who come from, or are experts in, countries where the splinternet is already “in the making”.

They compared technologies and methods used for splintertization, framing discussion around how international experiences can help us better adapt circumvention technologies and predict certain global trends in network fragmentations.



Country case study: Iran

Country Case study: Russia

IN THIS SECTION:

County Case Study: Ukraine

County Case Study: Azerbaijan

The “Arab Spring” and Internet curfews

Iran

The so-called “Arab Spring” was a bifurcation point in Internet governance globally, demonstrating the potential of organizing and mobilizing through social media while forcing authoritarian regimes to tighten their control over the internet (e.g. the series of laws adopted by the Russian government starting from 2012, marking the end of the “free Runet”).

The Arab Spring saw the beginning of government-mandated outages and shutdowns being used as a means of controlling protests (e.g. Egypt, Iraq and Syria). Rather than using a “kill switch” to shut down the internet, governments gave individual orders to major ISPs to shut connectivity down for a few hours before restoring it — making this a political rather than a technical decision.

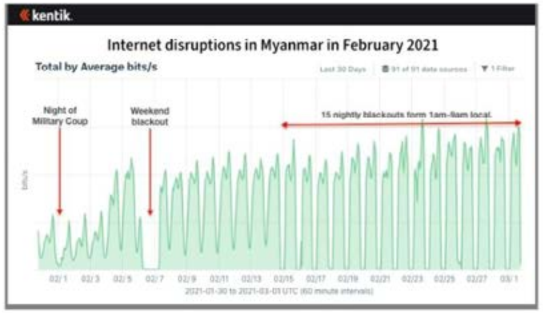
These practices have evolved in what experts call “Internet curfew” (also used in Gabon), which means a temporary, recurrent and local shutdown, instead of a complete disconnection.

Evolution of a tactic: Internet Curfew

PROBLEM
Internet shutdowns are disruptive, costly

SOLUTION
Disabling internet on a recurring basis

- First seen used in Gabon in 2016. Most recently in Myanmar, Iran, and Cuba
- By reducing the costs of these shutdowns, they become likely to continue in the future



Internet as national security threat: Iran

The Iranian government views the open internet as a national security threat. The government has employed extensive measures to block international access, shape national data usage behaviors, and compel citizens to rely on heavily controlled in-country services.

A presentation focused on Iran analyzed the key developments leading to this situation, and explored potential implications, beginning in 2009, when mass protests took place around the country, leading to a chaotic first shutdown: eGov services, banking/ATMs stopped working, embassy communications were disrupted, e-commerce platforms and private businesses went offline.
The shutdowns turned into a total communication collapse, with no IP connectivity, cellular SMS, international calls or domestic news and websites.

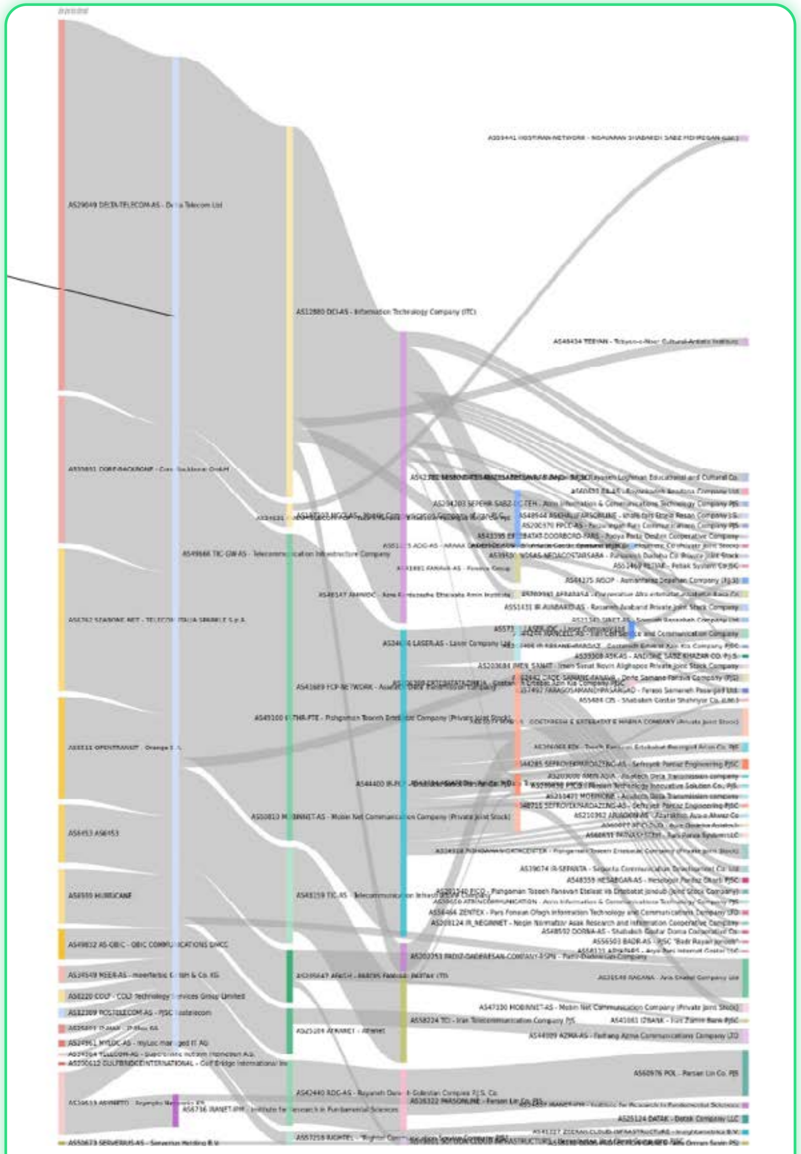
NIN and the pivot to national cyberspace

After this first experiment, circa 2013, the Iranian government began to invest in and develop a more thorough and sophisticated project called the NIN (National Information Network).

This pivot to national cyberspace required Iranian-made hardware and software. Government supported the production of domestic smartphones and a native messaging service to reach a capacity of 50 million active users. A plan to regulate VPNs and technologies that evade control was implemented. It began to continuously monitor the status of digital business services, drafted guidelines for government agencies to migrate to domestic services, and implemented a plan to secure national information network services. All equipment and services National Information Network had to be properly authenticated. National censorship was implemented, alongside with domestic security protocol certificates, including SSL.

NIN and the pivot to national cyberspace

Iran’s connection to the outside world was also affected via throttling of international IP connectivity. Pricing of international traffic was used as a basic control mechanism. Finally, companies were forced to move their infrastructure to data centers in Iran through regulation and coercion.


AS29049 DELTA-TELECOM-AS - Delta Telecom Ltd
AS33891 CORE-BACKBONE - Core-Backbone GmbH
AS6762 SEABONE-NET - TELECOM ITALIA SPARKLE S.p.A.
AS5511 OPENTRANSIT - Orange S.A.
AS6453 AS6453
AS6939 HURRICANE
AS49832 AS-OBIC - OBIC COMMUNICATIONS DMCC
AS12880 DCI-AS - Information Technology Company (ITC)
AS49666 TIC-GW-AS - Telecommunication Infrastructure Company
AS48159 TIC-AS - Telecommunication Infrastructure Company
AS50810 MOBINNET-AS - Mobin Net Communication Company (Private Joint Stock)
AS58224 TCI - Iran Telecommunication Company PJS
AS42440 RDC-AS - Rayaneh Danesh Golestan Complex P.J.S. Co.
AS6736 IRANET-IPM - Institute for Research in Fundamental Sciences
AS56402 DADEHNEGAR
AS48434 TEBYAN - Tebyan-e-Noor Cultural-Artistic Institute
AS44889 FARAHOOSH
AS47330 MOBINNET-AS - Mobin Net Communication Company (Private Joint Stock)
AS60976 POL - Persian Lin Co. PJS
AS25124 DATAK - Datak Company LLC
AS44889 AZMA-AS - Farhang Azma Communications Company LTD
AS24631 FANAPTELECOM-AS - Fanavari Pasargad Arian Co. PJS
AS50673 SERVERIUS-AS - Serverius Holding B.V.

Iran Internet Infrastructure Map — Nov 2023

Digital border control

Iran

The final step was made in July 2021, with the so-called "Users' rights and protections bill". Iran's international Internet gateways were essentially handed over to armed forces. A Digital Border Control was implemented and among other obligations, platform operators had to provide a representative in the country, and receive a special license to operate in Iran. Foreign data traffic should not exceed 30% of total network traffic and foreign mobile manufacturers have to pre-install a set of unremovable apps to receive an import license to the country.

ANATOMY OF A SPLINTERNET: IRAN

All digital platforms should respond to judiciary requests and remove any "Criminal Content" within 12 hours. All digital platforms should keep Iranian user data within the country and fully identify their Iranian users. The distribution and sale of circumvention tools, like VPNs, was criminalized. Iran is rapidly moving from a block list to an allow list type of censorship. An impossible set of regulations basically meant that all foreign digital platforms will be blocked / have been blocked, unless they comply fully with the government.

A different kind of Splinternet: Russia

Looking at the Russian “sovereign Runet” project today, we recognize many regulatory measures and techniques comparable to those deployed in Iran: localization of data inside Russia, throttling of foreign traffic, creating a registry of national software, investment in domestic smartphones and processors, VPN and social media blocking and more.

However, it would not be correct to say that Iranian and Russian splinternet models are the same: for a long time, Russia has operated a decentralized Internet topology, very well connected to the outside, and having 3500+ ISPs. Several presentations focused on the making of Sovereign Runet, from the perspective of network measurements, as well as policy angles.

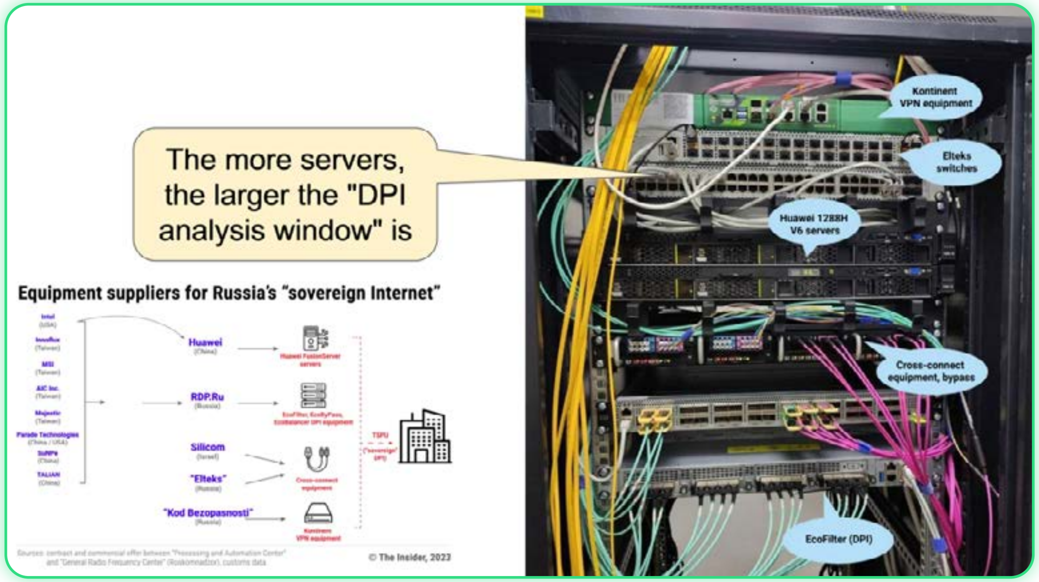
> ***The Russian case of transitioning from an open to an isolated network is an important use case, because other countries can follow the same path.***

The first blocklists appeared as early as 2007 (a list of extremist resources compiled by the Ministry of Justice), but in the wake of the Arab Spring, in 2012, control over the Runet was institutionalized and outsourced to a specific institution, Roskomnadzor, and a centralized blocklist was inaugurated, maintained and updated by a dozen different organizations.

Taming the Runet: TSPU

Russia

Initially, internet censorship in Russia was inconsistent and largely dependent on ISP filtering solutions and methods. 2019's law on sovereign Internet and the enforcement of the so-called TSPU (a DPI device), marked the beginning of efforts to tame the decentralized Runet. Twitter throttling in 2021 and 2023's "war on VPNs" showcase the capacities and willingness of the Russian state to isolate, filter and control its internet traffic.

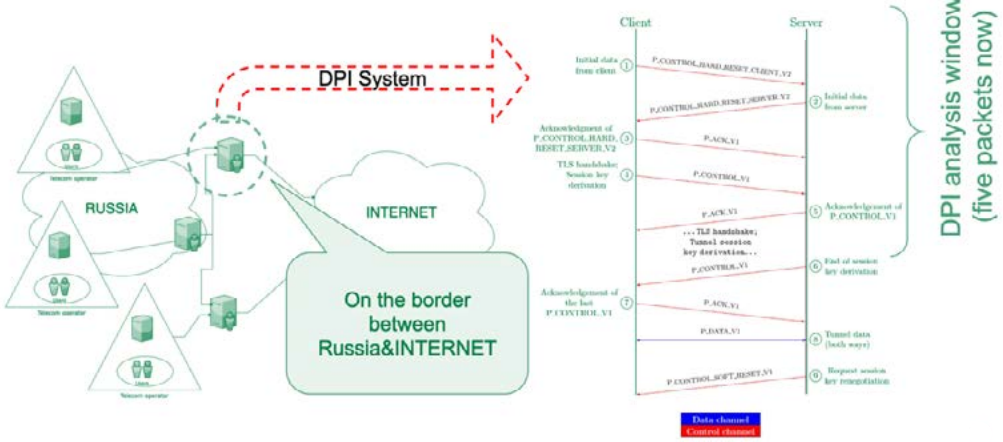

The more servers, the larger the "DPI analysis window" is
Equipment suppliers for Russia's "sovereign Internet"
Intel (USA)
Innodisk (Taiwan)
MSI (Taiwan)
AIC Inc. (Taiwan)
Majestic (Taiwan)
Parade Technologies (China / USA)
SuNPV (China)
TALIAN (China)
Huawei (China)
RDP.Ru (Russia)
Silicom (Israel)
"Elteks" (Russia)
"Kod Bezopasnosti" (Russia)
Huawei FusionServer servers
EcoFilter, EcoByPass, Ecobalancer DPI equipment
Cross-connect equipment
Kontinent VPN equipment
TSPU ("sovereign" DPI)
Sources: contract and commercial offer between "Processing and Automation Center" and "General Radio Frequency Center" (Roskomnadzor), customs data
© The Insider, 2023
Kontinent VPN equipment
Elteks switches
Huawei 1288H V6 servers
Cross-connect equipment, bypass
EcoFilter (DPI)

Taming the Runet: the war on VPNs

At the time of the report's publication, 165 VPN services and applications are blocked in Russia. Six of the most popular VPN protocols, including L2TP, IPsec, PPTP, OpenVPN UPD/TCP, and WireGuard, are partially blocked. These blockages are not accompanied by official statements from regulatory authorities and are known only from users and providers. Currently, these protocols may work intermittently, forcing users to constantly change VPN services. In general, this means that to download a VPN, you already need to have another VPN installed.

In response, the internet freedom community has shifted to protocols more resistant to blocking: OpenVPN over Cloak and AmneziaWG, a proprietary implementation of the WireGuard protocol by the Amnezia VPN service (the standard WireGuard is already blocked in some regions). Shadowsocks continues to operate for now.

How VPNs are blocked by protocols

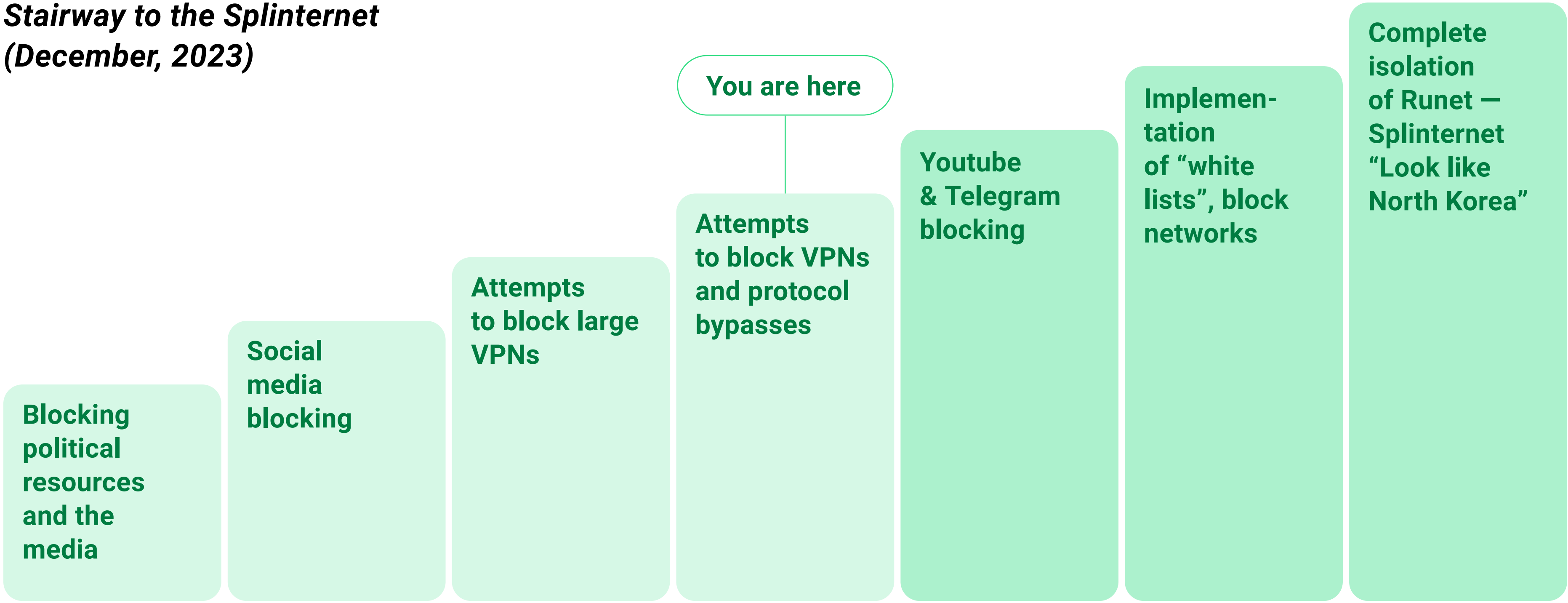

DPI System
RUSSIA
Telecom operator
INTERNET
On the border between Russia&INTERNET
Client
Server
Initial data from client
P_CONTROL_HARD_RESET_CLIENT_V2
Initial data from server
P_CONTROL_HARD_RESET_SERVER_V2
Acknowledgment of P_CONTROL_HARD_RESET_SERVER_V2
P_ACK_V1
TLS handshake; Session key derivation
P_CONTROL_V1
Acknowledgment of P_CONTROL_V1
P_ACK_V1
...TLS handshake; Tunnel session key derivation...
End of session key derivation
P_CONTROL_V1
Acknowledgment of the last P_CONTROL_V1
P_ACK_V1
P_DATA_V1
Tunnel data (both ways)
Request session key renegotiation
P_CONTROL_SOFT_RESET_V1
Data channel
Control channel
DPI analysis window (five packets now)

The making of a sovereign internet

The “making of” a Russian sovereign Internet is a long process involving complex, risky and expensive operations and a series of country-wide network tests. Experts are closely observing the progress of “sovereignization” of the Runet and several possible scenarios were discussed at SplinterCon.

Several shutdown episodes, such as in Ingushetia in 2018, Moscow in 2021, Dagestan in 2023, all happening during mass protests, illustrated the capacities and techniques of isolating specific regions.

Stairway to the Splinternet (December, 2023)



Blocking political resources and the media

Social media blocking

Attempts to block large VPNs

You are here

Attempts to block VPNs and protocol bypasses

Youtube & Telegram blocking

Implementation of “white lists”, block networks

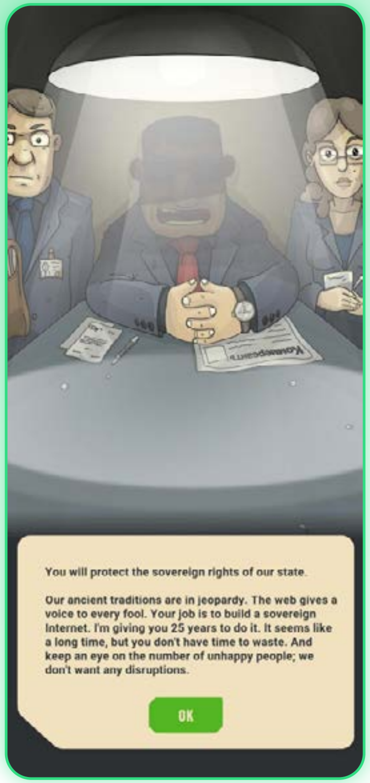
Complete isolation of Runet — Splinternet “Look like North Korea”

The making of a sovereign internet

Russia

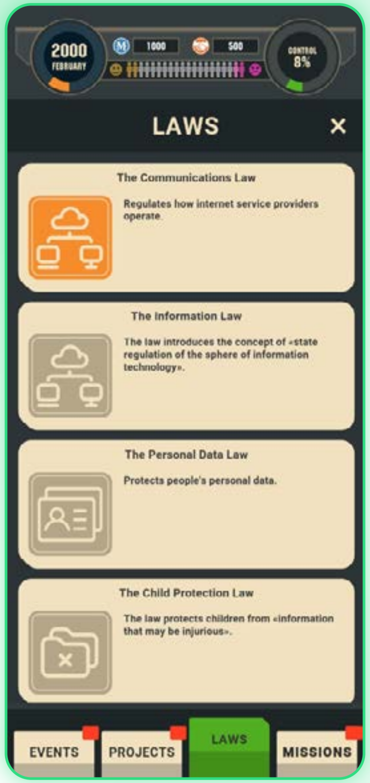
The project of Splinternet “à la russe” is estimated to be finalized by 2024 or 2025. However Russian technological capacities in this area are largely undermined by international sanctions that block or slow down the import of necessary electronic components for the DPI, SORM and other information control devices. The war in Ukraine has played an important role in questioning Russian technological sovereignty.

Road to Cheburnet



You will protect the sovereign rights of our state.

Our ancient traditions are in jeopardy. The web gives a voice to every fool. Your job is to build a sovereign Internet. I'm giving you 25 years to do it. It seems like a long time, but you don't have time to waste. And keep an eye on the number of unhappy people; we don't want any disruptions.



The Communications Law

Regulates how internet service providers operate.

The Information Law

The law introduces the concept of «state regulation of the sphere of information technology».

The Personal Data Law

Protects people's personal data.

The Child Protection Law

The law protects children from «information that may be injurious».

Mobile game focused on building the Russian Splinternet (also called “Cheburnet” by Russians) was presented at SplinterCon. The Road to Splinternet is a game developed by eQualitie and Noesis games. The goal of the game is to play for the censor, adopt laws and enforce measures to control and isolate the national network. This game was built around the Russian case but can unfortunately be applied to almost any country where governments are on their way to build a sovereign Internet.

› Download for IPhone
› Download for Android

The Crimean model: fragmentation of Ukraine’s cyberspace

Russia’s ambitions to control Internet traffic beyond its borders was manifested in 2014, following the annexation of Crimea. A mix of regulatory, economic, military and technological means were used to reroute Crimean traffic under Russian upstreams. Ukrainian mobile operators left Crimea, radio frequencies were reallocated and infrastructures seized. The ISPs that stayed have finally accepted operating under Russian licenses and Russian upstream traffic.

> ***The Crimean model served as a “laboratory for information control”, and similar strategies and actors were involved in 2022 following the full-scale invasion of Ukraine.***

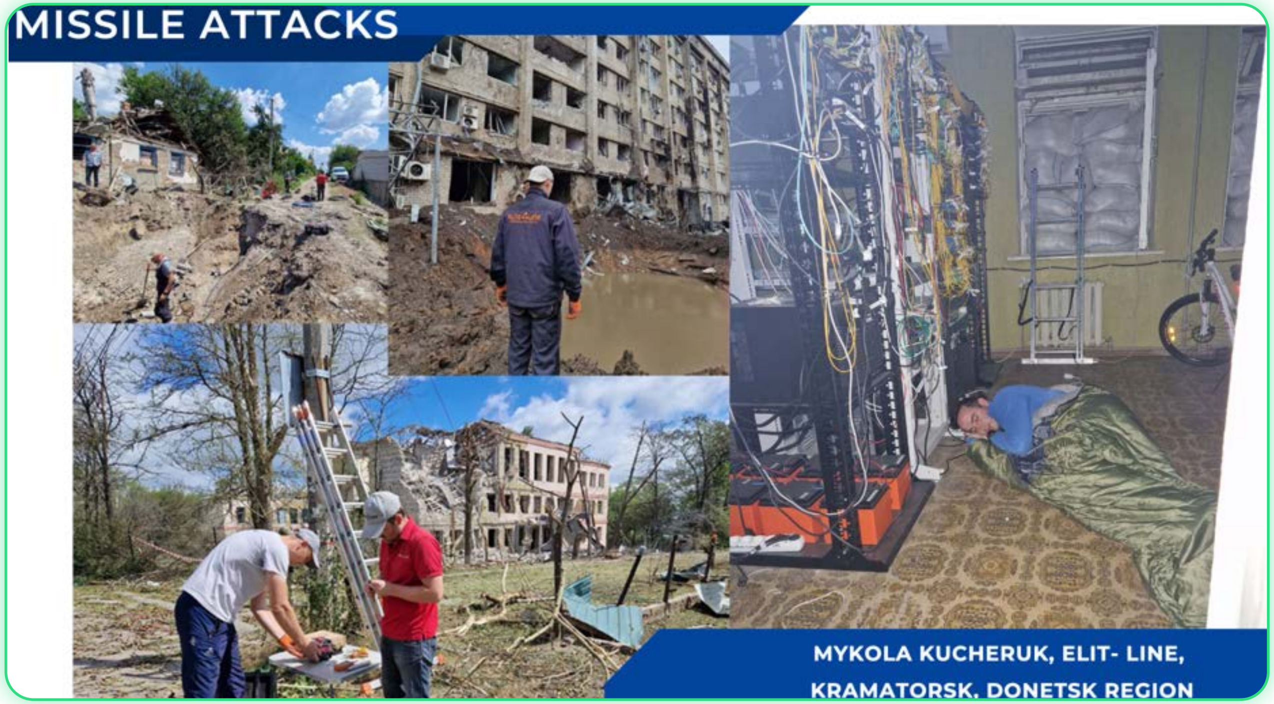
SplinterCon hosted a panel of Ukrainian speakers from the ISP community, as well as academics specializing in Ukrainian cyberspace studies, who shared their experience and powerful lessons from the Ukrainian use case.

The traffic wars, russification and fragmentation

The fragmentation of Ukraine's cyberspace is a decade-long process. After the 2014 Maidan Revolution, Russia taking control of the Crimean Peninsula, and backing separatist forces in Eastern Ukraine, Ukrainian Internet was fragmented, some of its parts were forcibly “russified” and marginalized (such as Donetsk and Luhansk regions where TV and radio infrastructures were seized) and existed in a “routing interregnum” for several years.

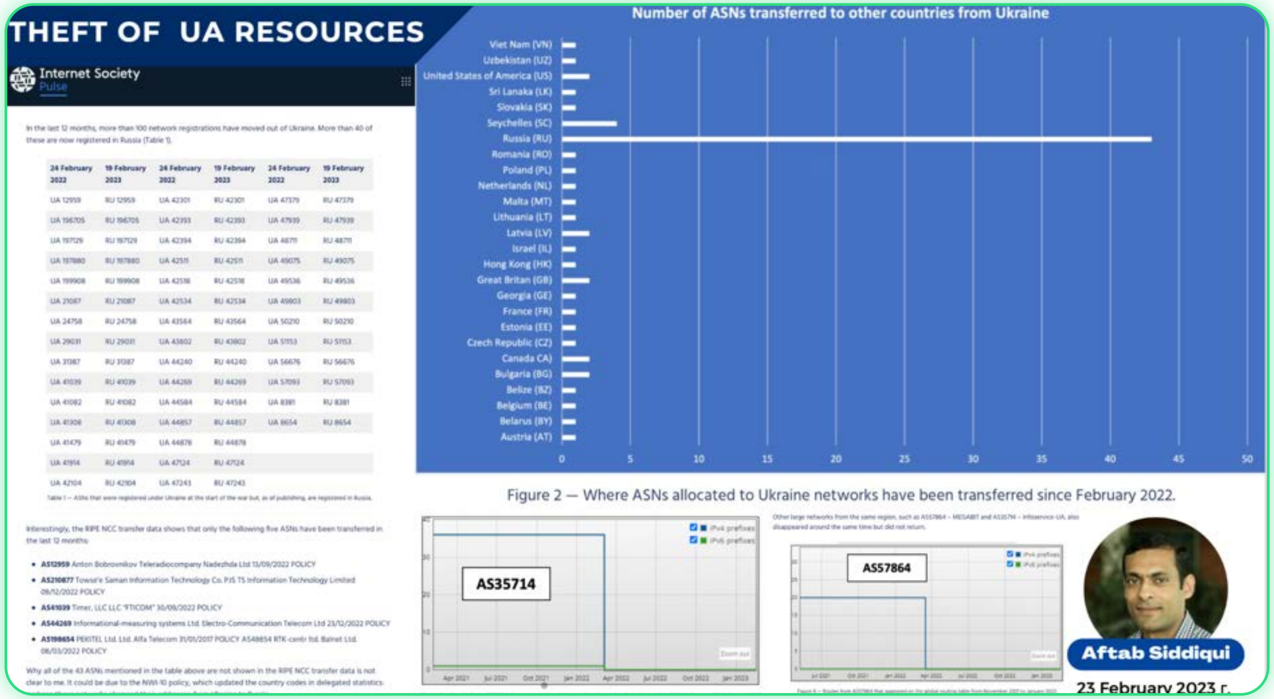
Russian and Ukrainian networks were closely connected before 2014 — with many direct links, peering agreements and sometimes even shared infrastructure. Following the annexation of Crimea, this cooperation began to decrease, accelerating even more after the full scale invasion on February 24, 2022. Over 1,880 cyber attacks were conducted by Russian against the Ukrainian government, military, media and critical civic infrastructure.

The traffic wars, russification and fragmentation



One of the iconic cases of "traffic wars" is the occupation of Kherson between May and November 2022, when Internet traffic was forcibly rerouted via the Russian-controlled operator Miranda-Media in Crimea, forcing Russian network censorship and surveillance on Khersonians. Since the beginning of the war, over 8,000 ASNs switched to 'located in Russia', with hundreds of thousands of Ukrainian IPs stolen.

The traffic wars, russification and fragmentation



THEFT OF UA RESOURCES

In the last 12 months, more than 100 network registrations have moved out of Ukraine. More than 40 of these are now registered in Russia (Table 1).

24 February 2022	19 February 2023	24 February 2022	19 February 2023	24 February 2022	19 February 2023
UA 12959	RU 12959	UA 42301	RU 42301	UA 47379	RU 47379
UA 196705	RU 196705	UA 42393	RU 42393	UA 47939	RU 47939
UA 197129	RU 197129	UA 42394	RU 42394	UA 48711	RU 48711
UA 197880	RU 197880	UA 42511	RU 42511	UA 49075	RU 49075
UA 199908	RU 199908	UA 42518	RU 42518	UA 49536	RU 49536
UA 21087	RU 21087	UA 42534	RU 42534	UA 49803	RU 49803
UA 24758	RU 24758	UA 43564	RU 43564	UA 50210	RU 50210
UA 29031	RU 29031	UA 43802	RU 43802	UA 51153	RU 51153
UA 31387	RU 31387	UA 44240	RU 44240	UA 56676	RU 56676
UA 41039	RU 41039	UA 44269	RU 44269	UA 57093	RU 57093
UA 41082	RU 41082	UA 44584	RU 44584	UA 8381	RU 8381
UA 41308	RU 41308	UA 44857	RU 44857	UA 8654	RU 8654
UA 41479	RU 41479	UA 44878	RU 44878		
UA 41914	RU 41914	UA 47124	RU 47124		
UA 42104	RU 42104	UA 47243	RU 47243		

Table 1 — ASNs that were registered under Ukraine at the start of the war but, as of publishing, are registered in Russia.

Interestingly, the RIPE NCC transfer data shows that only the following five ASNs have been transferred in the last 12 months:

- **AS12959** Anton Bobrovnikov Teleradiocompany Nadezhda Ltd 13/09/2022 POLICY
- **AS210877** Towsa'e Saman Information Technology Co. PJS TS Information Technology Limited 09/12/2022 POLICY
- **AS41039** Timer, LLC LLC "FTICOM" 30/09/2022 POLICY
- **AS44269** Informational-measuring systems Ltd. Electro-Communication Telecom Ltd 23/12/2022 POLICY
- **AS198654** PEXITEL Ltd. Ltd. Alfa Telecom 31/01/2017 POLICY AS48654 RTK-centr ltd. Balnet Ltd. 08/03/2022 POLICY

Why all of the 43 ASNs mentioned in the table above are not shown in the RIPE NCC transfer data is not clear to me. It could be due to the NWI-10 policy, which updated the country codes in delegated statistics.

Number of ASNs transferred to other countries from Ukraine

Figure 2 — Where ASNs allocated to Ukraine networks have been transferred since February 2022.

Other large networks from the same region, such as AS57864 – MEGABIT and AS35714 – Infoservice-UA, also disappeared around the same time but did not return.

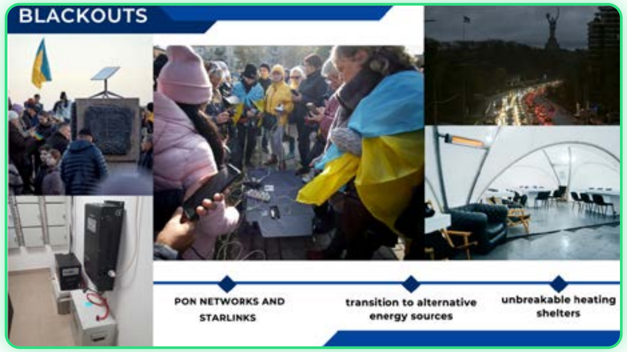
Aftab Siddiqui

23 February 2023 г.

Russia has also begun degrading Ukrainian physical internet infrastructures via explosive ordinance. In times of war, connectivity saves lives. A study by AccessNow has shown that Ukrainian territories that were cut from the Internet showed the highest number of civilian victims and cases of human rights violation.

Keeping Ukraine connected

The presentation "The state of digital infrastructure in Ukraine and the challenges and successes of those on the ground addressing it" focused on technologies used by Ukrainians to keep their country connected.

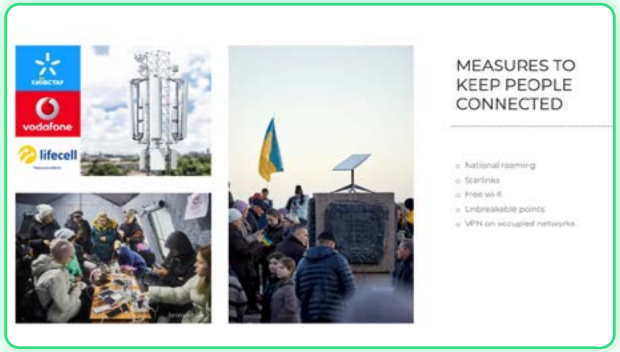


BLACKOUTS

PON NETWORKS AND STARLINKS

transition to alternative energy sources

unbreakable heating shelters



vodafone
lifecell

MEASURES TO KEEP PEOPLE CONNECTED

- National roaming
- Starlinks
- Free wi-fi
- Unbreakable points
- VPN on occupied networks

During electricity blackouts, passive optical networks (PONs) became a backup solution and alternative energy sources were introduced by the ISPs. More than 70 thousand Starlink terminals were brought into Ukraine. Anti-bomb shelters were already equipped with WiFi in 2022. Today, Ukraine has over 4000 ISPs, whose engineers are constantly risking their lives when going out to repair damaged infrastructure.

Keep Ukraine Connected launched by the Ministry of Digital Transformation of Ukraine and supported by eQualitie and SplinterCon helps ISPs get the necessary equipment to rebuild their networks and customer connectivity.

Pulling the plug: internet shutdown in Azerbaijan

The keynote “Pulling the Plug: How Azerbaijan’s government combines technology and fear to control the internet” focused on another armed conflict, and subsequent network control, in the Armenia-Azerbaijan crisis. On September 27, 2020 citizens of the border regions of Azerbaijan were notified that internet access would be shut down to prevent “Armenian provocation”, without any information on the timeline. After a few days people realized how the shutdown affected them; coupled with the effect of the COVID-19 pandemic, it became impossible to access news, social media and other online information sources.

The ISPs and mobile operators gave no explanation to customers, saying that there was a “government order”, or just ignoring their questions. Naturally, citizens started using circumvention tools, but the authorities circulated news that VPNs were bad for privacy, stating that their use was illegal (despite the lack of any law to support this).Due to monopoly infrastructure — the main ISP being government-aligned — network segmentation filtering was easy to implement. This shutdown cost $243 million.

During the “44 day war”, and later in 2022, Tiktok was blocked to “protect the kids”, .az and .tr domain names blocked, other well known sources blocked too, (1.1.1.1 resolver was tampered with in some provider networks — blocking was done on a DNS level mostly. The government also warned Starlink to abide by local laws.

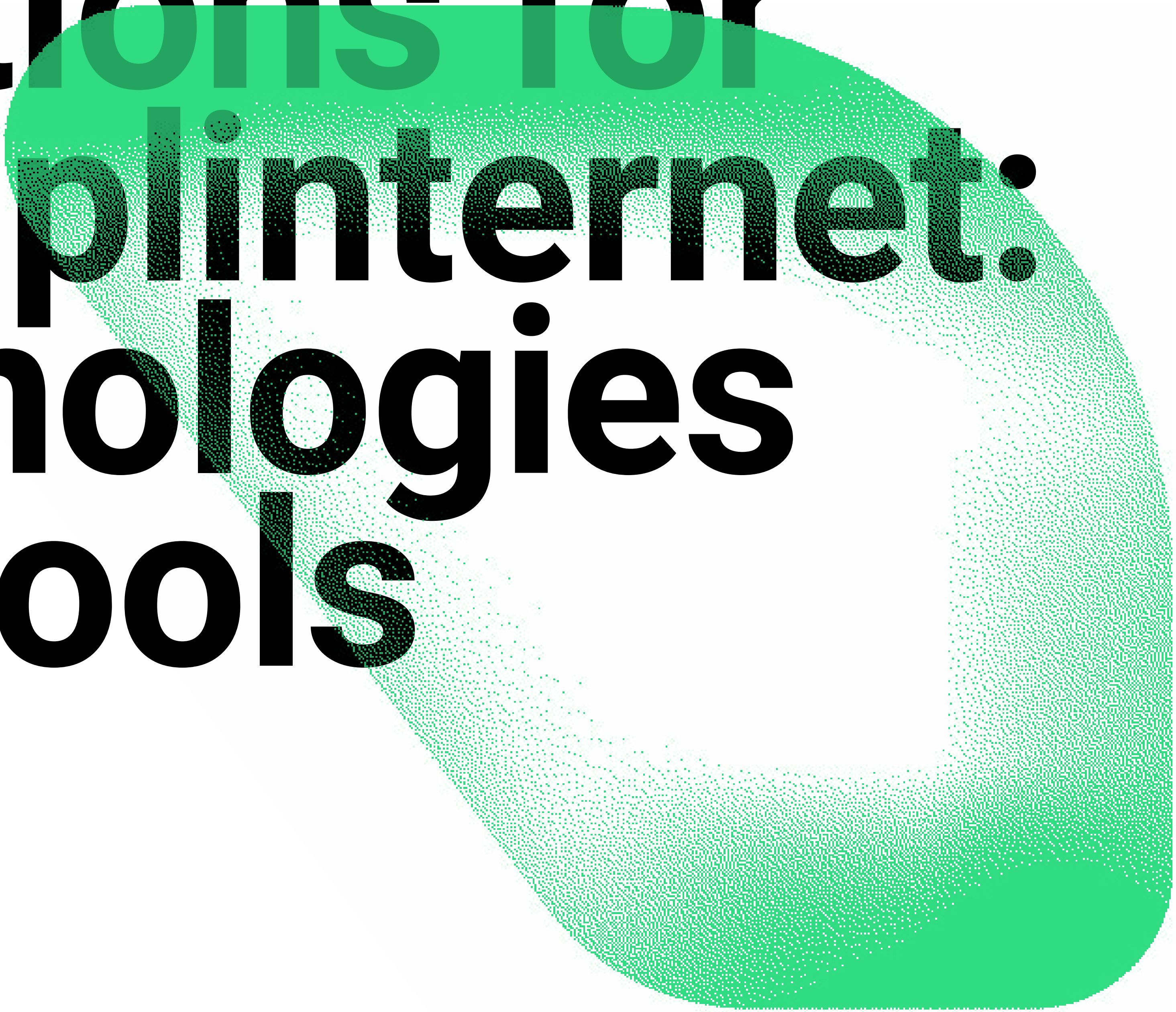
Preparing for the Splinternet

The country case-studies presented at SplinterCon also included examples from the Gulf region, where significant foreign policy changes impact digital routes and borders in the Middle East. The presentation about the US policy on blackouts was an outstanding example of a democratic regime controlling its connectivity, showing that Splinternetization is a global trend that also includes the European Union (see the Splinternets report for the European Commission published in 2022). The discussions at SplinterCon raised several examples of sparks of splinternet in the so-called Global North: the EU's demand to decrypt TLS certificates and new French regulation of end-to-end encryption being two examples.

Countries appear to be mimicking one another with regard to censorship and shutdowns, and their responses are becoming more similar over time. Moreover, there is a growing international market of technologies for connectivity control, for example Russia selling its DPI technologies to Afghanistan, Iran, Kazakhstan, Cuba and many other regions. In this context of global Splinternetization, the time is right for preparing technologically and socially. SplinterCon's practical sessions from Day 2 focused exactly on this "getting ready for the splinternets." Two big challenges were addressed: how do we communicate with those inside splintered networks? And how do we communicate when we are already inside a splintered net?

Section IV

Solutions for the Splinternet: technologies and tools



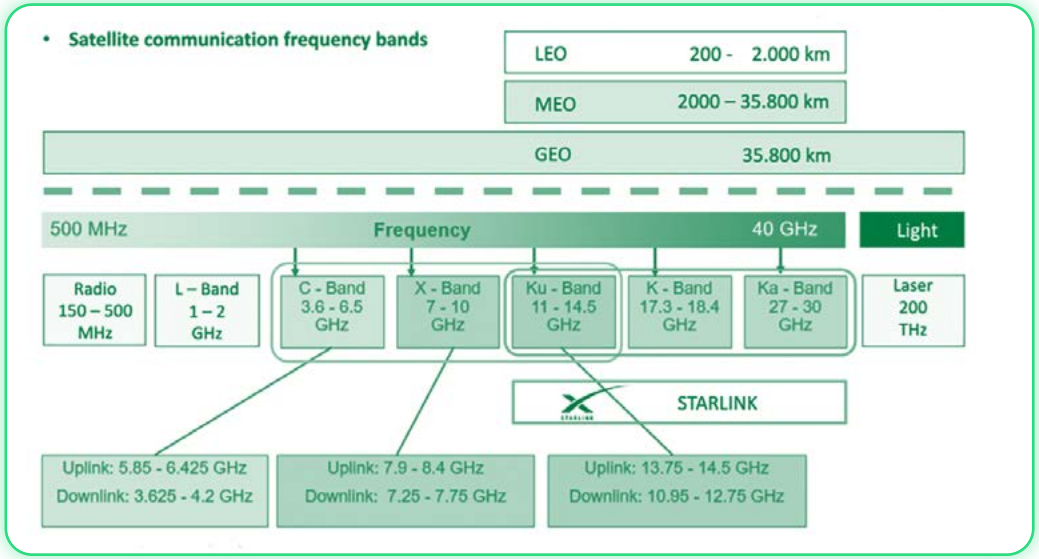
Reaching users in a splintered network

The second day of SplinterCon was focused on reviewing and imagining solutions for two distinct scenarios: connecting to users in a splintered network from the “outside”, and tools for those who find themselves inside an isolated network. Several cutting-edge technology projects presented their solutions; rotating sessions were dedicated to in-depth discussions of various approaches identifying their advantages and limitations.

The solutions for reaching out to sovereign networks were mainly grouped around two approaches: exploring the potential of **wireless technologies** and building more advanced and harder to trace **VPN solutions**.

The sky's the limit: wireless technologies for splintered networks

Satellite technologies play an important role in delivering news and information to censored networks, bypassing the terrestrial controls and censorship mechanisms that governments impose on traditional media and the internet. They can be used for news delivery in censored countries using satellite TV Direct-to-Home (DTH) services, satellite radio, Internet Satellite Constellations (e.g. Starlink or OneWeb), satellite phones (e.g. 5G via satellite).



One SplinterCon presentation focused on the traceability of satcom ground stations with existing radio location finders used by border control missions. While satellite technologies provide a means of delivering uncensored news and information, they are not entirely immune to interference or geo-tracking.

Section I
Section II
Section III
Section IV
Section V
Section VI
Section VII

Counteracting satellite jamming

Governments can often jam satellite signals or disrupt access to outside news sources. To counteract these efforts, news organizations often use encryption and other security measures to protect the transmission of information.

Starlink was cited as an example (already deployed and tested in Ukraine), the main advantage being that it's not under control of local governments or operators. Before Starlink, there were other attempts to deploy an accessible satellite Internet service, such as Project Loon or Aquila.

Electromagnetic signals transmitted and received by internet satellite constellation user terminals (e.g. Starlink), ground stations and satellites, have distinct signatures. Radio direction finder equipment can detect these signals, making it possible for authorities to geo-locate users according to their device's uplink transmission.

Nowadays these detection technologies work in real-time. In a one-way satellite data distribution network, data flows in only one direction, typically from a centralized source to multiple receivers. One-way satellite service signals can be detected from the ground, similar to TV broadcast channels, but it is difficult to detect the receivers as they are not emitting an uplink signal.

- Portable & mobile radio direction finder

portable radio direction finder equipment

mobile radio direction finder equipment

Two-way satellite: challenges

To mitigate the traceability of two-way satellite links, solutions included moving user terminals away from the roads (detectors are usually installed on mobile vehicles).

Two-way satellite solutions have distinct obstacles — ground terminals may be difficult and sometimes illegal to acquire and may be dangerous to operate. Moreover, satellite based service won't have the capacity to replace lost fiber-optic bandwidth. Largely, this service requires spectrum authorization and sometimes even a license to operate.

Section IV

Shutdown-resilient connectivity: eQSat

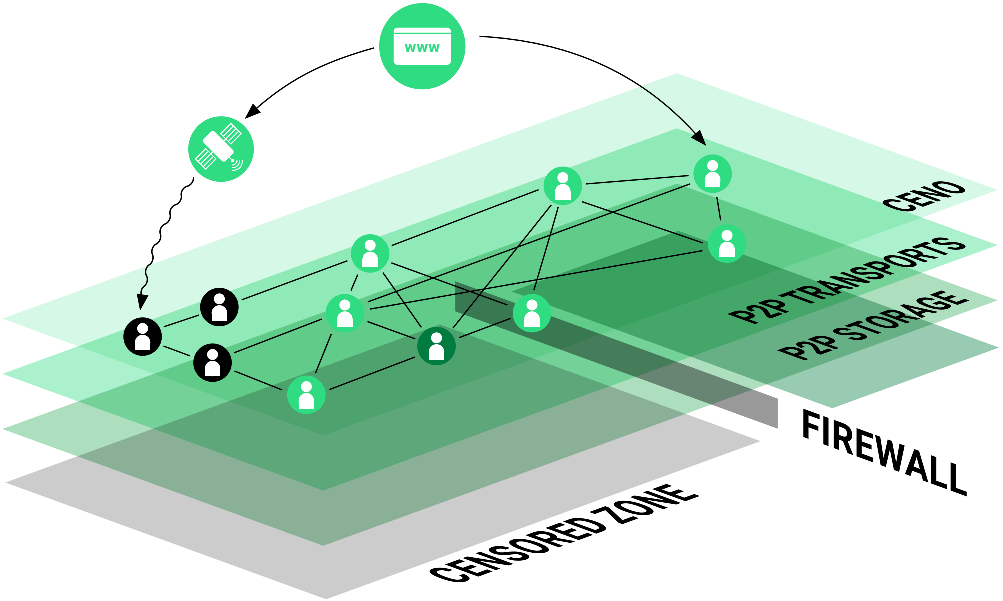
eQualitie presented their innovative eQSat solution, that rebuilds important web platforms inside an isolated network by juxtaposing various technologies, including web scraping, satellite datacasting and the Bittorrent-powered Ceno browser. eQSat helps package, deliver and propagate static resources inside censored networks. It is already used and tested in several regions including Ukraine, Russia and the Middle East. Project libraries can be used to empower other efforts with shutdown resilient connectivity. For instance, eQSat was recently implemented to support Paskoocheh — a Farsi software marketplace for privacy and circumvention tools.

OuiService → eQSat

Two-way Internet
- Near-border LTE coverage
- Satellite Internet

One-way content delivery
- Just a few injection nodes
- TS-MPEG / DVB-S
- Large geographic coverage

Propagation
- Ouinit / Ouisync
- Fediverse
- Decentralized networks
- Sneakernets

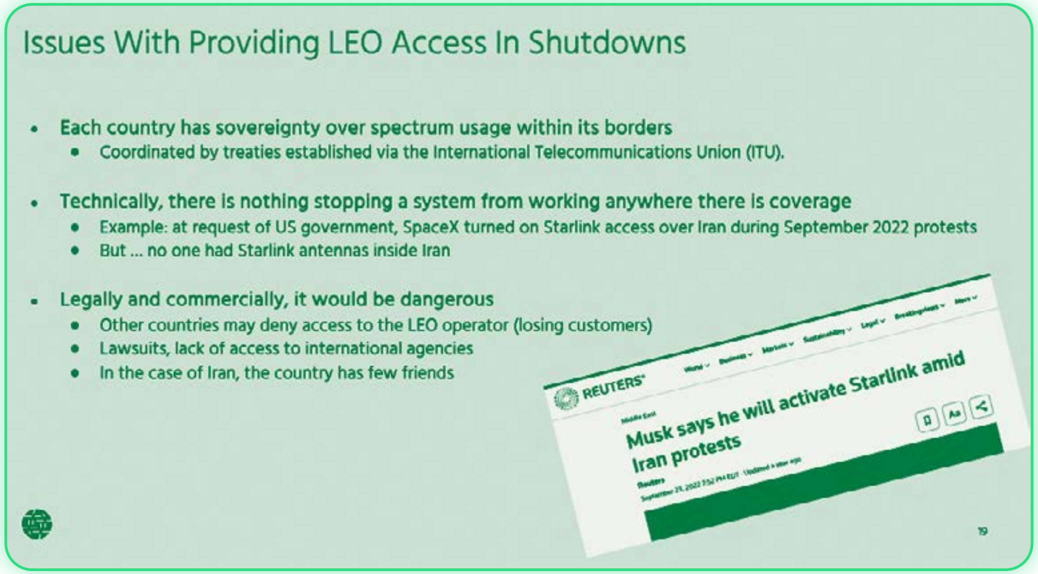


Avoiding a splinternet of satellites

An important takeaway for SplinterCon participants was that we cannot completely rely on LEO satellite commercial solutions, otherwise we might end up with an Elon-splinternet or a Bezos-splinternet.

> ***The war in Ukraine has demonstrated how satellite internet provision can become a marketing and political tool.***

And therefore to guarantee neutrality and availability of services, we need to provide alternative free software solutions, some of which were presented at SplinterCon.



Issues With Providing LEO Access In Shutdowns

- Each country has sovereignty over spectrum usage within its borders
  - Coordinated by treaties established via the International Telecommunications Union (ITU).
- Technically, there is nothing stopping a system from working anywhere there is coverage
  - Example: at request of US government, SpaceX turned on Starlink access over Iran during September 2022 protests
  - But ... no one had Starlink antennas inside Iran
- Legally and commercially, it would be dangerous
  - Other countries may deny access to the LEO operator (losing customers)
  - Lawsuits, lack of access to international agencies
  - In the case of Iran, the country has few friends

REUTERS
World
Business
Markets
Sustainability
Legal
Breakingviews
More
Middle East
Musk says he will activate Starlink amid Iran protests
Reuters
September 23, 2022 7:52 PM EUT · Updated a year ago
Aa
19

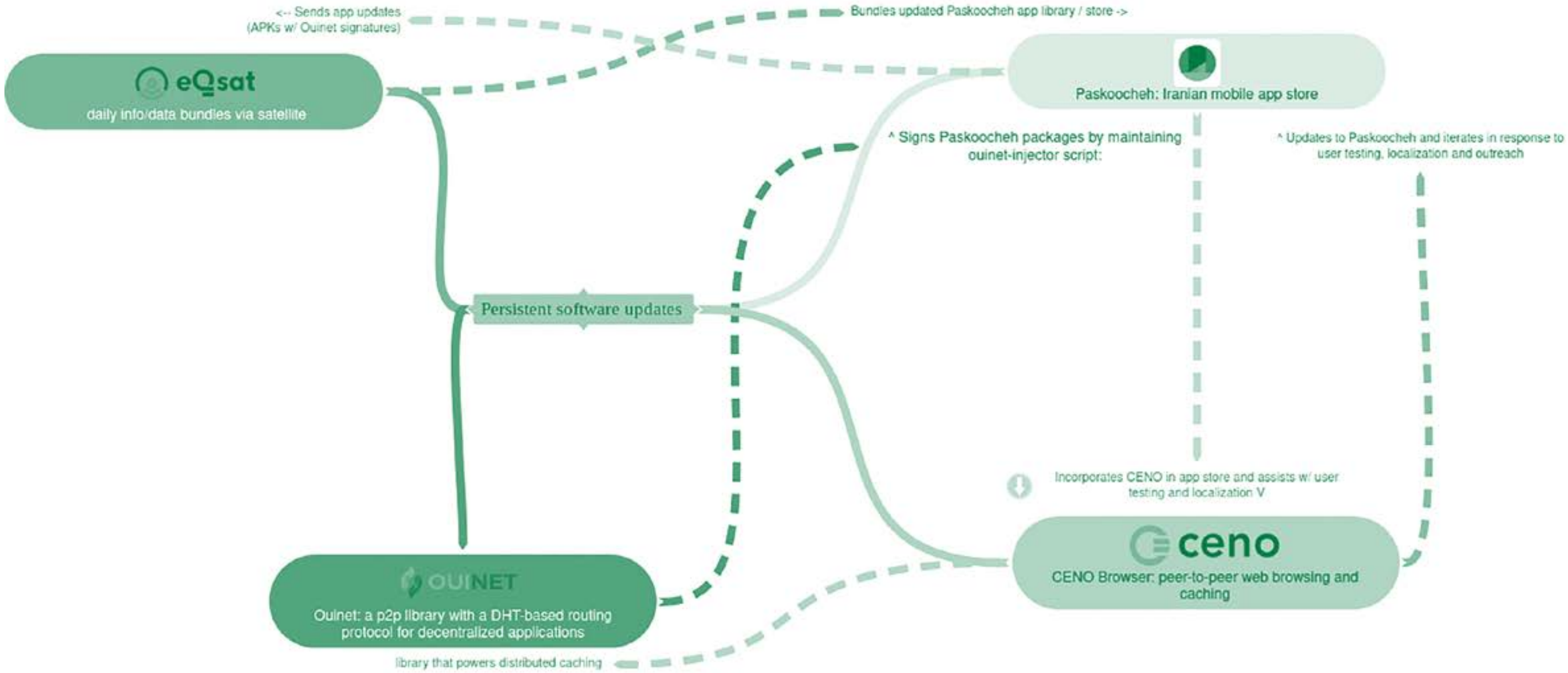
Section IV

Circumvention technologies

Other kinds of technical solutions helping to reach out to isolated networks included new kinds of VPN tools, and especially libraries, since one of SplinterCon's main missions is to build a technological open knowledge database that can be further developed and reused by communities in need of breaking informational isolation.

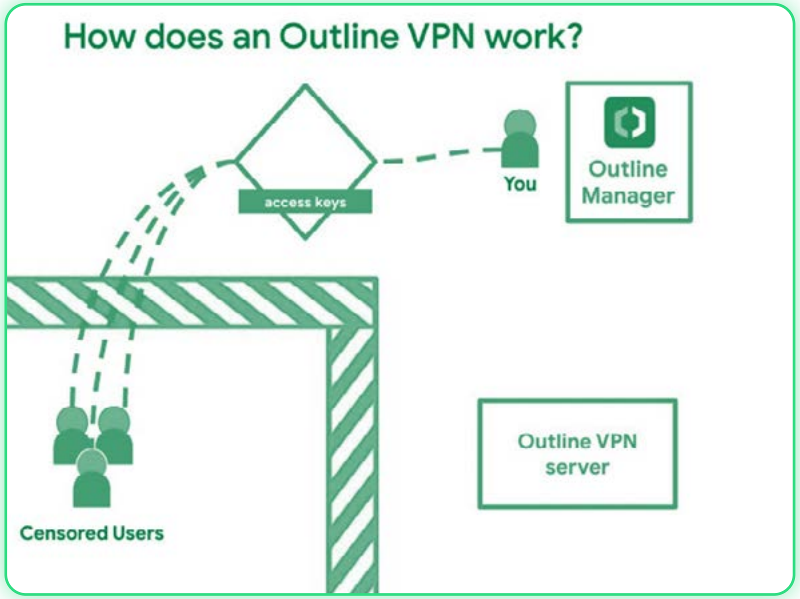
Paskoocheh: integrating with Ouinet P2P

A presentation was focused on the Paskoocheh Technology Stack, with a specific emphasis on the integration of Ouinet peer-to-peer technology, a library developed by eQualit.ie. This talk was also an opportunity to inspire other community organizations present at SplinterCon to think through this network stack for their own user communities in Russia, China, Myanmar etc.


<-- Sends app updates
(APKs w/ Ouinet signatures)
Bundles updated Paskoocheh app library / store ->
eQsat
daily info/data bundles via satellite
Paskoocheh: Iranian mobile app store
^ Signs Paskoocheh packages by maintaining ouinet-injector script:
^ Updates to Paskoocheh and iterates in response to user testing, localization and outreach
Persistent software updates
Incorporates CENO in app store and assists w/ user testing and localization V
ceno
CENO Browser: peer-to-peer web browsing and caching
OUINET
Ouinet: a p2p library with a DHT-based routing protocol for decentralized applications
library that powers distributed caching

Outline SDK: censorship-resistant apps

Outline SDK was presented as a versatile library that empowers developers to build censorship-resistant apps with Outline's networking techniques. Outline SDK is designed for researching splinternet scenarios, building new anti-censorship tools, or even innovating with multi-hop routing like onion routing. The approach chosen by Outline is suited for splinternet, as anyone can become a VPN provider ("Outline manager") and help others inside the censored area to access restricted content by distributing access keys. This approach has already proven its efficacy in countries such as Russia where the censor is attentively analyzing the traffic and quickly blocking what they consider as being VPN-related infrastructures.



Outline SDK is fully customizable and supports different protocols and techniques:

Multiple built-in transports

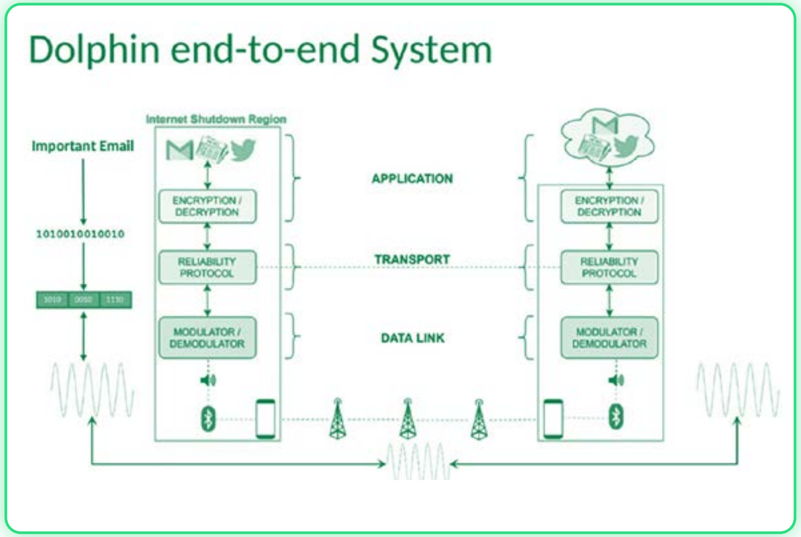
- *TLS*
- *HTTP CONNECT*

Multiple built-in protocols

- *Shadowsock*
- *SOCKS5*

Dolphin: access during shutdowns

Dolphin is a first-of-its-kind system enabling access to lightweight internet applications during shutdowns utilizing the cellular voice channel to transmit data bits by encoding them into audio during a voice call.



The general assumption is: cellular services are working during shutdowns, this has been observed in multiple recent shutdowns. For Dolphin to work, users need to dial another user over cellular network to access content. Overcoming challenges of bandwidth constraints, unreliability, and eavesdropping, Dolphin prioritizes usability for regular users with basic devices.

Dolphin was tested during actual internet shutdown, and access to the internet was possible. Successful lab and real-world tests demonstrated its efficiency in accessing emails, tweets, and news snippets during shutdowns.

Affordable digital telecoms: Hermes

The High-frequency Emergency and Rural Multimedia Exchange System, better known by its acronym, HERMES, provides affordable digital telecommunications over High Frequency (HF) band using a simplified visual interface accessed via smartphone or computer. It allows for the transmission and reception of data (email, text, audio, documents, photos, GPS coordinates, etc). For security, this information can be easily encrypted and password-protected by the sender. HERMES, both architecture designs and software, is free and open-source.

Hermes began in the Amazon rainforest, given the struggle to provide telecom access there. HF is typically the last resort, it allows very wide coverage, thanks to ionosphere skywave propagation.

Affordable digital telecoms: Hermes

In 2015 HERMES started with off- the-shelf hardware and raspi 2 or 3. By 2018–2020 **HERMESv1** was out, built on their own custom hardware. It relied on Airdrop or VARA modem and UCCP for transfer, using about 15 watts of power. By 2019–2023 HERMESv1.x was deployed in Amazons.

In 2023 — **HERMESv2** was out, as an open source wideband HF transceiver. It uses a radio called sBitx, reduced the size a lot, has native voice support (mic+ptt+speaker). HERMES's Web interface provides a wifi landing page with email, news, a bbs-inspired message board, and configuration screens. Images are compressed to 10KB or less using h.266 image encoder before being sent and an lpcnet for audio encoding compression.

For email **Delta Chat** is the recommended client and is bundled along with roundcube (postfix + dovecot). Currently 10 KBps can be transferred to a gateway when the signal is good.

The radio costs $500 without batteries, and the same equipment can be used for the gateway and endpoint. It uses P2P connections and multicast to transmit Future developments include support for realtime messaging, DRM broadcast, digital telephony.

Section V

Solutions for the Splinternet: communicating within splintered networks

Section V

Solutions for the Splinternet: communicating within splintered networks

One of SplinterCon’s biggest challenges was to identify solutions for people already living within splintered networks. How do we keep people connected — at least locally? How can we provide at least some security and privacy to those existing inside highly surveilled and censored networks? Several projects were presented that could be grouped around three main approaches: federated self-hosted alternatives, mesh-based or p2p solutions and new projects that creatively reuse older technologies.

Federated solutions: dComms

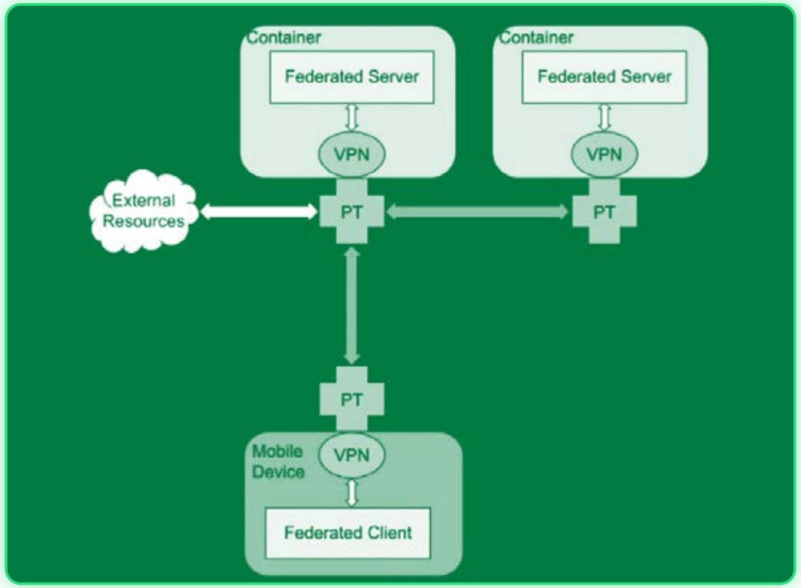
Salvation does not necessarily lie on the other side of the firewall. To bring back secure and efficient communications to those inside a splinterned net, we need to re-focus on community networks and the protocols that underpin them. The dComms project is a growing assembly of tools and services for re-building decentralized and independent networks. Obvious use cases are war or natural disaster, but there are other examples outside emergencies, if we want more open, equitable and community-led internet services.

Centralized platforms such as Signal, Telegram or Whatsapp don't work in a shutdown context, while federated self-hosted services such as Matrix, Mattermost, Jitsi, Delta Chat might work on splinternets — if protected.

The dComms project set up nine servers in Ukraine during the first months of the full-scale invasion. It was hard to find locations for hosting outside major urban hubs, since the hosting market is more centralized than the ISP market. Unfortunately, the project served its purpose only in four of the nine locations due to bombs destroying infrastructure. However, after the connection was restored, the conversations that happened while area was disconnected were seen. The challenges include moderation and administration, network metadata profiling, honeypot use-case (if deployed on an adversarial network), node seizure. Some of these challenges are addressed by another federated project presented at SplinterCon.

Federated solutions: Sunbeam

Sunbeam is a proposal for a general-purpose architecture for adding censorship resistance to existing federated services so that they can run on splinternets. It is designed from the ground up for the specific needs of adversarial networks. All connections are encrypted to provide privacy and obfuscated to provide censorship resistance in order to protect the federated services from discovery and censorship. Sunbeam is also service-agnostic — it's designed to work generally with federated services that are normally designed to function over the Internet, without modification to those services.



Sunbeam is reminiscient of Tor hidden services, but the architecture is different. It is a Virtual Private Network that provides private communications between federated services, servers, clients. The novel part is putting the federated server inside of a container that connects it directly into VPN and pluggable transports. In case of not full shutdown, plugganle transport will work as normal. The IPs of federated servers are hidden through one hop and through pluggable transport which uses a different protocol that makes traffic look completely innocuous.

P2P, Mesh & Near-field communication solutions (NFC): Briar

Over the last year, Briar Project has conducted research towards building a public mesh transport layer. This work mainly covered nearby-device advertisement and p2p connections using Bluetooth, p2p WiFi and WLAN physical layers. At SplinterCon Briar Project presented its initial findings and topics for future work in this area, and this work's connection to bigger themes in distributed computing, like local-first software and the actor model of computation.

Briar uses peer-to-peer connections over Wi-Fi LAN, Bluetooth, Tor, and sneakernet (eg SD cards). Briar Mailbox is a newly-deployed project enabling creation of a personal server for sending and receiving messages asynchronously, based on the Bramble library.

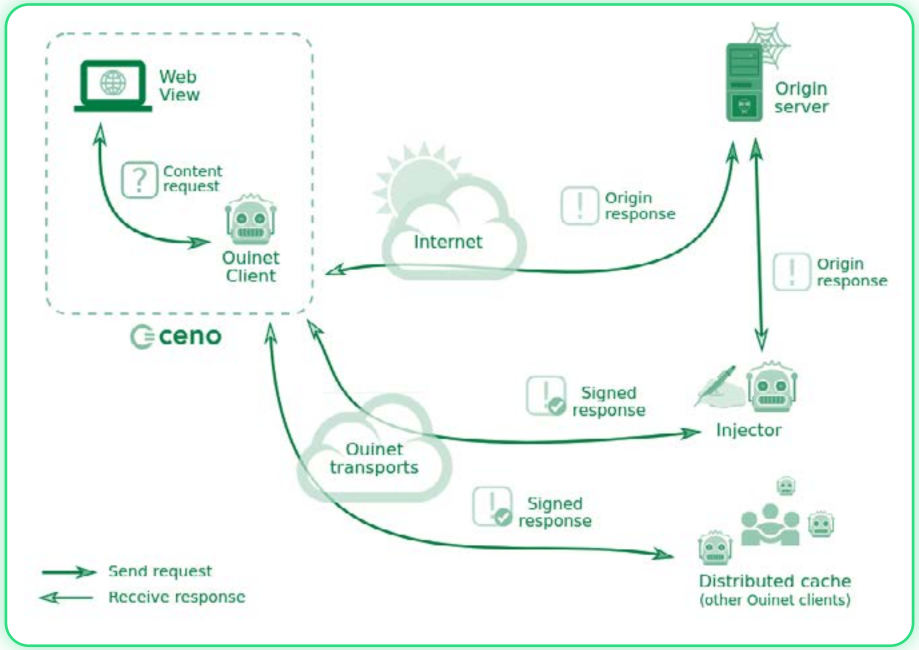
Two unfamiliar contacts can establish connections via announcements over BTLE GATT system. A device advertises a service id hardcoded to whatever service you're running for the public service. Interesting research coming out of the rise of Covid contact tracing apps using BTLE. The “Allocator Characteristic” can be used as a sort of socket that can support up to 6–7 devices simultaneously.

Section V

P2P, Mesh & NFC: Ouisync

Securely backing up, sharing and transporting data has been a challenge for as long as recorded media has existed. Ouisync, eQualitie's newest project, endeavors to rise to the challenge. Utilizing established peer-to-peer technologies and latest encryption techniques, Ouisync is a free and open source cross-platform app enabling people to securely store and share files even in unreliable network conditions.

The Ouisync presentation focused on use-cases for this new tool inside a splintered network. One scenario included a “digital emergency suitcase” with a set of pre-downloaded apps that can work inside a shutdown area or help bypass censorship (including Ceno, Outline, Briar and other tools presented at SplinterCon). Another scenario was developed for media organizations inside censored areas that can distribute their content using Ouisync and circumvent blocking of their websites. Finally, because Ouisync can work on a local network, it can also help organizations to maintain collaborative work on common projects even during shutdowns.



P2P, Mesh & NFC: Xochiteopan Community Internet System

Xochiteopan is a cooperative that supports indigenous communities and organizations in the use of communication and technology to defend the territory. Together with communities from Mexico and Ecuador, it has developed a model for training and community management of digital communication infrastructures that have the capacity to be economically self-sustaining.

These processes are now building their own communication and archiving platforms to store all the information generated during the environmental monitoring they carry out. It is a necessity for these territorial defense processes to have control of the data that will be used to judicially prosecute those who pollute their territories. We believe that this model of community management and administration of infrastructure and services can be very useful in the context of massive repression, with internet blackouts or blocking of social networks.

P2P, Mesh & NFC: Butterbox

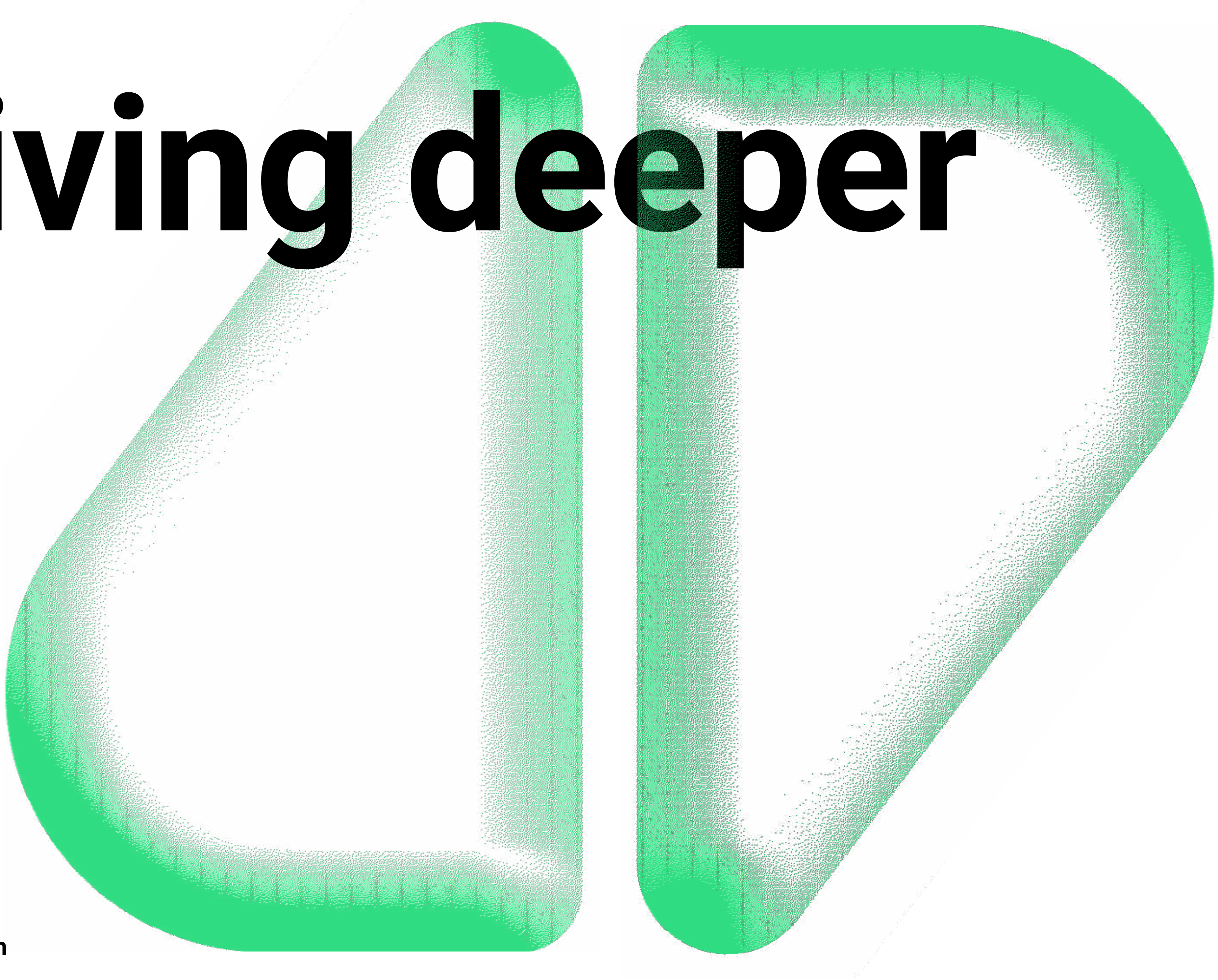
A butterbox deployment includes digital tools for monitoring, collecting evidence and circumventing censorship in high risk areas. A mini computer powered by a portable battery or solar panel, it works as a hotspot that people connect to via WiFi when there is no local access to the Internet.

A butterbox deployment features an ad-free, curated collection of apps from partners that can be shared offline and work on low-end devices. The apps are very small so users don't have to remove data on their phone to install it.

It also features a local encrypted Matrix chat that can be joined anonymously to chat and share images or videos. Butterbox works with journalists, activists, indigenous communities and NGOs. It has been deployed in many areas with limited Internet connectivity and electricity. It is possible to add software and content locally with some technical background using custom butterbox runners. The concept is intended to be deployed before a disaster event so users are familiar with it.

Section VI

Diving deeper



Diving deeper

Many of the technological ideas were further explored and tested on the Day 3 of SplinterCon, planned as an un-conference with sessions proposed by participants, including:

- *Hands-on workshops where participants could learn to deploy a mesh network, experiment with Briar or HERMES.*
- *Network measurements with a hands-on workshop by OONI about running measurements from within a splintered net or developing a shutdown rapid response protocol. Another sessionexplored challenges of visualizing internet routes.*
- *Regional gatherings focused on shutdowns in Senegal and Iran.*
- *A collaborative session between tech experts and human rights activists.*

Section VII

Conclusion — what's next…

Conclusion — what's next...

The inaugural Splintercon created a unique opportunity to gather a hybrid community of technologists, researchers, activists, media professionals around an urgent techno-social challenge: informational isolation and global communication fragmentation.

While many still take the "world wide web" for granted, Splintercon experts showed how entire countries are already experiencing these scenarios, and proposed tools to measure the impacts of splinternetization and solutions to mitigate them.

Key learnings

SplinterCon's interdisciplinary approach demonstrated that solutions are more likely to succeed in a splintered area when they:

- ***Are hybrid and rely on several protocols and communication channels (see eQSat, that uses satellite tv infrastructures in combination with Ouinet library and Ceno browser; or the dComms project that proposes "containers" with several federated services that can ensure communication inside the country's national web or even locally, or Butterbox that can come equipped with tools like Ouisync, Matrix or Delta Chat and so on).***
- ***Rely on active users / relays "on the ground" who can propagate information inside an isolated network.***

There is a strong interest in mesh, p2p and near-field communication solutions but we have seen that, security-wise, these local solutions still lack robust end-to-end encryption. Reusing older technologies such as HF radios seems promising, but requires a rather high learning curve and relies on power-users, those tech-savvy activists who can ensure maintenance, popularization and functioning of those tools.

Section VII

The importance of community — and the next SplinterCon(s)

All these challenges bring us to the idea that technological solutions on their own are not enough and need to be carried out by a community. A strong community of experts in touch with active users on the ground, who have the capacity to iterate and improve from field tests and real-life experiences inside fragmented networks.

With this in mind, we will bring more SplinterCon gatherings in 2024 and onward to foster these communities, creating an accessible base for developers and researchers working on breaking informational isolation.

Subscribe to our newsletter

Stay informed about upcoming SplinterCon events and be part of the community driving change. Join us in shaping the future of internet resilience.

Produced in Canada, Province of Quebec, December 2023

This document reflects the information and insights gathered during the SplinterCon conference and is current as of the date of its initial publication. eQualitie reserves the right to update this report at any time to reflect new findings or changes in our understanding of digital equality and security. The examples and case studies included herein are provided to illustrate how various organizations and communities are impacted by the “splinternet” and how they have implemented strategies for digital security and resilience, and the outcomes of such initiatives. It is important to note that the effectiveness of these strategies can vary significantly based on specific situational factors and operational contexts.

The results discussed in this report are specific to the entities involved and cannot be generalized or expected in all cases. Each organization's or community's results will depend on their unique circumstances, including their technical infrastructure, operational practices, and the specific challenges they face. As such, it is crucial for readers to critically assess the relevance and applicability of the strategies and outcomes described in this report to their own situations.

Statement of Good Security Practices:
In the realm of information technology and cybersecurity, no system or solution can be deemed entirely secure, nor can any single measure guarantee complete protection against unauthorized access or malicious activities. eQualitie does not claim that the approaches discussed in this report will render any organization or system invulnerable to cyber threats.

Responsibility for legal and regulatory compliance remains with each organization. While eQualitie provides insights and recommendations based on our expertise in digital security and resilience, we do not offer legal advice or assurances that adherence to our recommendations will ensure compliance with all applicable laws and regulations. Where possible or appropriate, organizations are encouraged to consult with legal and compliance professionals to ensure their operations align with regulatory requirements and best practices in cybersecurity.

eQualitie