SplinterCon

Building resilience for a fragmented future

2023 - 2025

MONTREAL, BRUSSELS, BERLIN

eQualitie

SplinterCon is an international and interdisciplinary conference that focuses specifically on internet fragmentation and its consequences on contemporary societies and online liberties. The inaugural event was launched by eQualitie in Montreal, December 2023. Since then, we've hosted SplinterCon to Brussels, Estoril, Berlin and now, Taipei. These gatherings assembled hundreds of creative minds from communities encompassing network researchers, technology entrepreneurs, network engineers and software developers, user experience designers, media and internet freedom advocates, in order to:

- Analyze the practices and impacts of network isolation and shutdowns;
- Evaluate existing and future technology solutions for communicating with and within sovereign networks;
- Invest in practical and user-oriented solutions for connectivity and content distribution across digital barriers.

SplinterCon is normally held under Chatham House rule, and we have sought explicit permission from presenters to share their materials for post-conference reporting. This collation presents highlights from three events and summarizes the 'state of the splinternet' as a point of reflection and in order to strategize from hereon.

splintercon.net equalit.ie

Acknowledgments

Dmitri Vitaliev
Founding Director,
eQualitie

Mallory Knodel
CTO,
Center for Democracy
and Technology

Ksenia Yermoshina
Researcher,
eQualitie, Ecole
nationale Superieure
des Mines de Paris

Lai Yi Ohlsen
Direclor
M-Lab

Nicolas Diaz
Head of Digital Security,
Reporters Without Borders

Ethan Zukerman
Associate Professor,
the University of
Massachusetts

Alena Epifanova
Research Fellow,
The German Council
on Foreign Relations

Hammer
Founder and Director,
Project Ainita

Isabella Bargueros
Executive Director
Tor Project

We're deeply grateful to the SplinterCon Advisory Council members, whose guidance and support have shaped this project from the very beginning. Your guidance and dedication have been key to making SplinterCon happen.

Mart van Santen
Co-Founder & Director,
Greenhost

Roya Ensafi
Associate Professor,
the University of
Michigan

Marion Mareau
Technology Journalist

Timothy Ball

Alexey Sidorenko
Director,
Teplitsa.Technologies
for Social Good.

Jean-Philippe Décarie-Mathieu
Co-founder,
Crypto.Québec

Nick Sullivan
Cryptography and
System Security Advisor

Aurang
Director of Technology,
and Innovation,
ASL 19

Amir Rashidi
Director of Digital
Rights and Security,
The Miaan Group

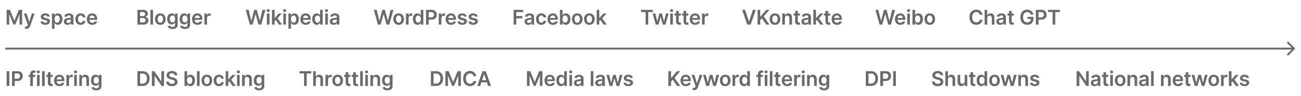
Contents

Introduction

Introduction

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. The Internet's inherent open architecture is increasingly weaponized as a tool for surveillance capitalism, censorship and priorities driven by speculative hype and bubble-like trends. Multiple autocratic and totalitarian states are increasingly turning to network shutdowns in order to control the narrative and making progress on defining and implementing national networks, isolating their citizens from the global commons. Tech companies are separating users into corporate marketplaces and digital walled gardens — these are all prima facie examples of the emergence of **splinternets**.

From Web 2.0 to Splinternets



My space Blogger Wikipedia WordPress Facebook Twitter VKontakte Weibo Chat GPT

IP filtering DNS blocking Throttling DMCA Media laws Keyword filtering DPI Shutdowns National networks

SplinterFact

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 or China 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.

Section 1

Splinternets in progress

Recent events in Iran, Russia, Ukraine, Myanmar and other conflict areas demonstrate how states attempt to leverage foundational internet protocols as tools of political control. To share an “insider’s experience of a splinternet” SplinterCon gathered researchers who come from, or are experts in, countries where the splinternet is already “in the making”.

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

Halalnet

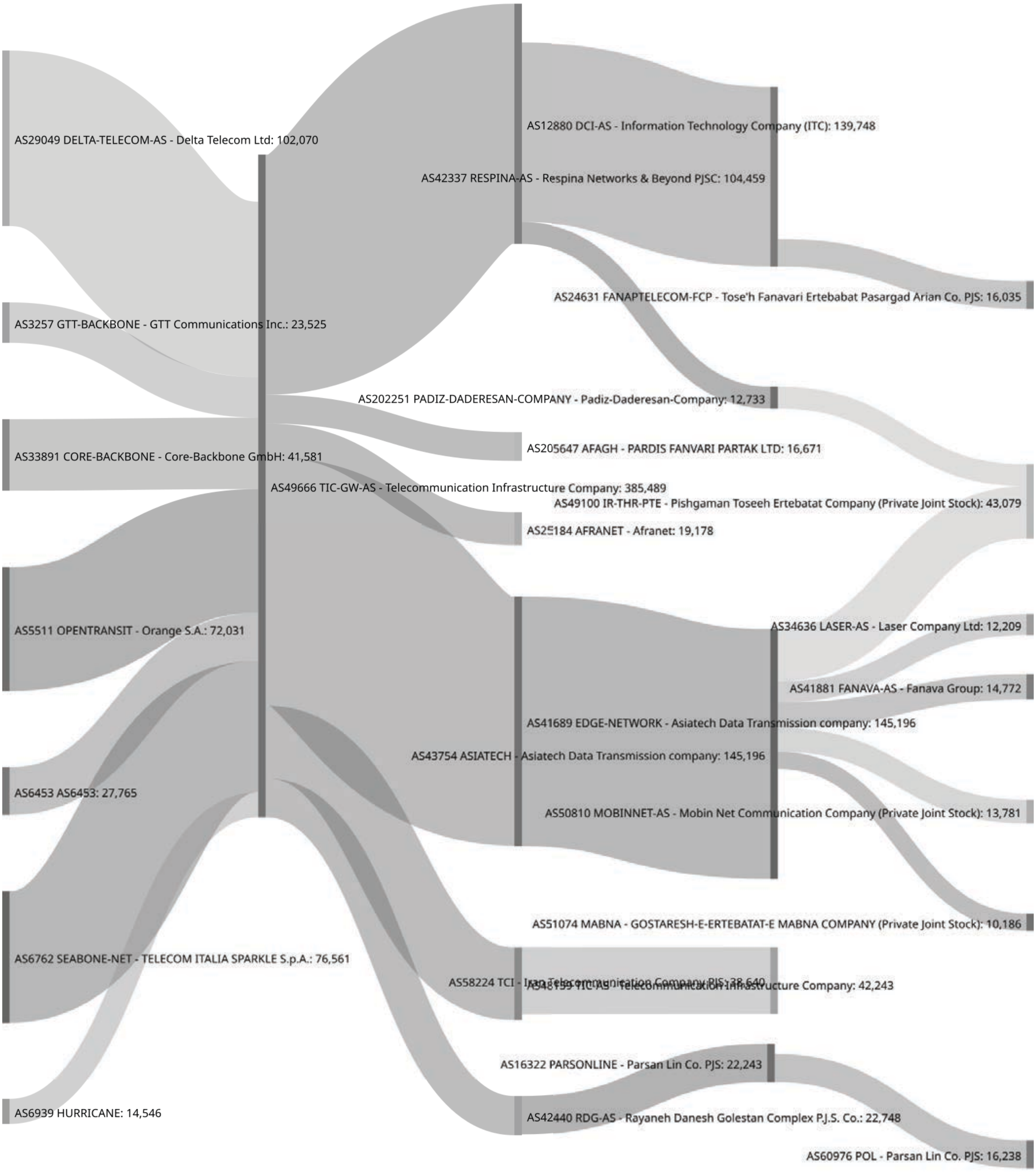
Internet As A National Security Threat

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: eGovernment 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.

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. 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.

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.


AS29049 DELTA-TELECOM-AS - Delta Telecom Ltd: 102,070
AS3257 GTT-BACKBONE - GTT Communications Inc.: 23,525
AS33891 CORE-BACKBONE - Core-Backbone GmbH: 41,581
AS5511 OPENTRANSIT - Orange S.A.: 72,031
AS6453 AS6453: 27,765
AS6762 SEABONE-NET - TELECOM ITALIA SPARKLE S.p.A.: 76,561
AS6939 HURRICANE: 14,546
AS49666 TIC-GW-AS - Telecommunication Infrastructure Company: 385,489
AS12880 DCI-AS - Information Technology Company (ITC): 139,748
AS42337 RESPINA-AS - Respina Networks & Beyond PJSC: 104,459
AS24631 FANAPTELECOM-FCP - Tose'h Fanavari Ertebabat Pasargad Arian Co. PJS: 16,035
AS202251 PADIZ-DADERESAN-COMPANY - Padiz-Daderesan-Company: 12,733
AS205647 AFAGH - PARDIS FANVARI PARTAK LTD: 16,671
AS49100 IR-THR-PTE - Pishgaman Toseeh Ertebatat Company (Private Joint Stock): 43,079
AS25184 AFRANET - Afranet: 19,178
AS34636 LASER-AS - Laser Company Ltd: 12,209
AS41881 FANAVA-AS - Fanava Group: 14,772
AS41689 EDGE-NETWORK - Asiatech Data Transmission company: 145,196
AS43754 ASIATECH - Asiatech Data Transmission company: 145,196
AS50810 MOBINNET-AS - Mobin Net Communication Company (Private Joint Stock): 13,781
AS51074 MABNA - GOSTARESH-E-ERTEBATAT-E MABNA COMPANY (Private Joint Stock): 10,186
AS58224 TCI - Iran Telecommunication Company PJS: 38,640
AS48159 TIC-AS - Telecommunication Infrastructure Company: 42,243
AS16322 PARSONLINE - Parsan Lin Co. PJS: 22,243
AS42440 RDG-AS - Rayaneh Danesh Golestan Complex P.J.S. Co.: 22,748
AS60976 POL - Parsan Lin Co. PJS: 16,238

Iran Internet Infrastructure
Map. Nov. 2023

Mobile Internet And Surveillance In Iran

The Iranian model of the splinternet is largely defined by the predominance of mobile Internet that is usually more centralized and easier to control. In Iran, mobile Internet subscribers outnumber fixed-line users ten to one. While only 15% of households have wired internet, there are 1.7 SIM cards per person.

In 2009, after the Iranian Green Movement, it turned out that In those years, monitoring involved triangulation of user metadata between mobile and landline phones. The organizer and manager of this system was the state-owned **Communications Regulatory Authority of Iran (CRA)**. Mobile control and surveillance have only become more intense since then.

Iran already had a mobile monitoring and surveillance system built by **Nokia Siemens**. In 2014, anonymous SIM cards were banned, and in 2015, a universal digital transaction identification platform, **Shaahkar**, was launched. Shaahkar tracked all digital transactions, linking them to mobile numbers and social security numbers via an API that all digital service providers had to connect to. Internet providers were obliged to store information about static and dynamic IP addresses assigned to users.

Splinternet In Action: Methods Of Iranian Censorship

How is Iranian censorship organized in a technical sense? Let us turn to the protocol level:

HTTPS-blocking (leveraging a TLS extension called Server Name Indication or the SNI). Imagine Google with one server that hosts multiple services, such as website hosting, Google Drive, Gmail, etc., Server Name Indication contains the name of the service user wants to connect. Even though HTTPS is encrypted, this element is in plain text and can tell your Internet service provider what website you're trying to visit. And this is monitored. Moreover, in older versions of TLS, server certificates are in plain text. So, these are all the sorts of information that the ISP can see and try to block access to certain services.

IP address censorship. The censor detects that you are trying to connect to a specific address and blocks it directly or through DNS, essentially cutting off certain domains.

Research presented at the SplinterCon has measured these censorship tactics at the core of Iran’s national firewall — IP-based censorship, **DNS-based censorship**, and both **HTTP and HTTPS-based censorship**. A temporary workaround has been to run HTTPS traffic on nonstandard ports, evading detection until the authorities catch on. However, a more robust solution needs to meet several critical criteria: it shouldn’t involve traffic masking, require user actions, or rely on a special architecture that authorities can easily detect. Several methods meet these criteria:

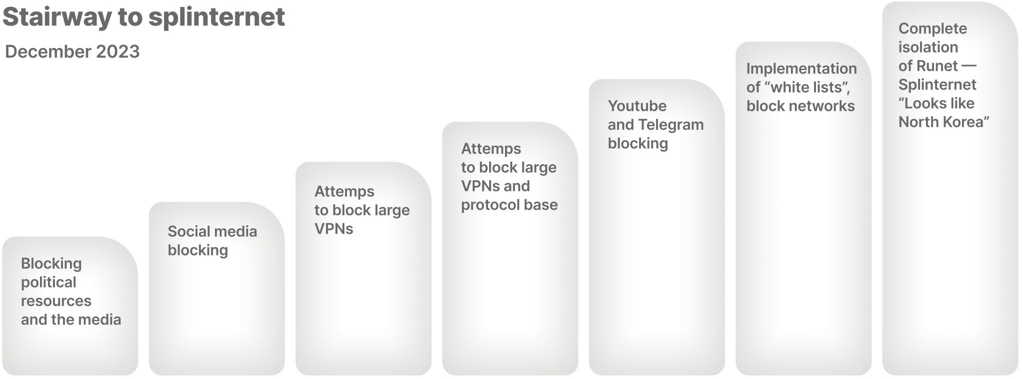
QUIC, a transport layer network protocol based on HTTP/3. It is encrypted by default, and Server Name Indication obfuscates. While it can be monitored, but requires a lotof effort, blocking the protocol entirely — or accepting that they can't censor specific services.

Encrypted Client Hello, masks Server Name Indication used to negotiate a TLS handshake. However, such traffic is different from normal HTTPS, and authorities can still censor all traffic of this type

Cheburnet

Stairway to splinternet

December 2023



Blocking political resources and the media

Social media blocking

Attemps to block large VPNs

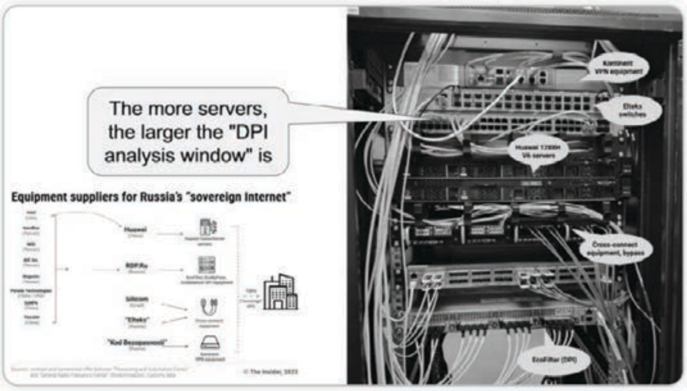
Attemps to block large VPNs and protocol base

Youtube and Telegram blocking

Implementation of “white lists”, block networks

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

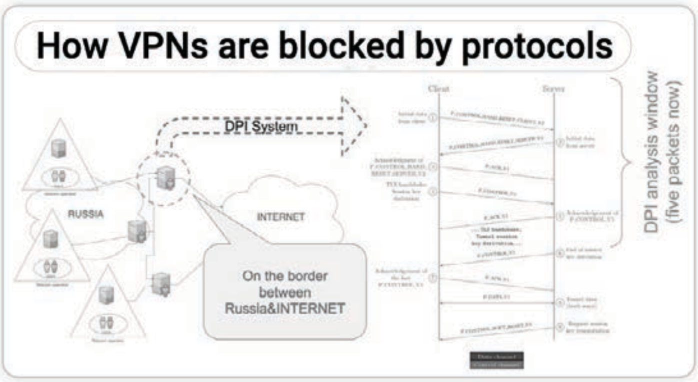
The Russian case significantly differs from the Case of Iran, and is described as a “decentralized control” model. The Russian case of transitioning from an open to an isolated network is an important use case, because other countries can follow the same path. There are about 3,500 ISPs in the country, and with this diversity of players the state has moved to a hybrid model of information control. It combines a national blocklist implemented at each ISP’s network using various techniques (more than 15 vendors exist that offer filtering solutions) and a new generation DPI equipment called **TSPU** (that is remotely controlled by the authorities). These two methods coexist, and this complexity contributes to a very peculiar and not always consistent censorship pattern.


The more servers, the larger the "DPI analysis window" is
Equipment suppliers for Russia's "sovereign Internet"
Huawei
RDP.Ru
Silicom
"Elteks"
"Kod Bezopasnosti"
Kontinent VPN equipment
Elteks switches
Huawei 1288H V6 servers
Cross-connect equipment, bypass
EcoFilter (DPI)
© The Insider, 2023

However, there are also similarities between splinternets. As in the case of Iran, Russian restrictions are driven mainly by political events. Following mass protests "for fair elections" (2011-2012) control over the **Runet** was institutionalized and delegated to a specific institution, **Roskomnadzor**. In 2014, when Russia annexed Crimea and following international sanctions, the discourse of the sovereign Internet emerged.

This project was rectified in a relevant law in 2019, and the implementation of the **Sovereign Runet** accelerated considerably after the full-scale invasion of Ukraine in 2022. According to **Roskomsvoboda**, over 1,699,000 domains are blocked in Russia, including almost all independent media websites, anti-war activists, human rights organizations, and services like Grammarly, Patreon, SoundCloud, etc.

The "war on VPNs'' continues as this report is being written, with over 197 VPN services and other circumvention apps being blocked inside the Runet and/or removed from app stores. In the latter half of 2023, Russian authorities turned from website blocking to applications and protocol blocking. In 2023, regulators blocked the six most popular VPN protocols without official statements. Currently, these protocols may or may not work intermittently depending on the region and ISP, forcing users to change VPN services constantly. In particular regions, especially those where indigenous movements are active, such as Yakutia or Bashkortostan, regulators block Telegram and WhatsApp.


How VPNs are blocked by protocols
DPI System
RUSSIA
INTERNET
On the border between Russia&INTERNET
Client
Server
DPI analysis window (five packets now)

Measuring Sovereignty: Hybrid Approach To Analyzing Russian Splinternet

While censorship in Russia is escalating with more advanced blocking tactics and legal suppression, international monitoring, measurements, advocacy, and tech innovation remain critical in countering digital repression. A panel uniting the members of **OONI (Open Observatory of Network Interferences)**, **OZI (Internet Protection Society)** and **Digital Security Helpline NaSvyazi** focused on sharing techniques of network measurements and discussing methodological challenges faced by researchers and technologies who try to understand the growing splinternization of Russia. From a remote analysis based on open source data from RIPE or CAIDA to crowdsourced user-generated data and personal accounts of censorship and shutdowns, the panel offered a diverse overview of the state of the art approaches to censorship studies.

Nasvyazi presented their Runet Monitor 2024 report, a comprehensive review of internet censorship, network disruptions, and digital repression in Russia. The report detailed shutdown patterns, legislative changes, Roskomnadzor’s (RKN) expanding censorship efforts, and predictions for 2025.

Key Numbers From A Runet Monitor

According to the analysis of Nasvyazi, the control on Runet will only tighten, including more targeted censorship with messengers, social networks, and streaming platforms facing increased protocol-based filtering; independent bloggers and registered media outlets will be forced to comply with state-imposed rules or face bans. Finally, we must expect more regional blackouts and localized network manipulations, particularly during politically sensitive events.

According to the analysis of Nasvyazi, the control on Runet will only tighten, including more targeted censorship with messengers, social networks, and streaming platforms facing increased protocol-based filtering; independent bloggers and registered media outlets will be forced to comply with state-imposed rules or face bans. Finally, we must expect more regional blackouts and localized network manipulations, particularly during politically sensitive events.

1,984 outage reports throughout 2024.

36 network anomalies affecting access to foreign services.

7 types of internet shutdowns, including regional blackouts, localized mobile downgrades, and selective censorship techniques.

Major Internet Shutdowns in 2024

January – Total Blackout in Rural Areas
Entire villages experienced complete communication shutdowns, cutting off access to the outside world.

March – Alexey Navalny's Funeral Restrictions
Authorities downgraded mobile networks from LTE to 3G to disrupt livestreaming and real-time reporting.

August – "Antimessenger" Mode in Volgograd
During a rebellion in one of the prisons, messaging services were blocked locally to prevent coordination or news leaks.

December – South Russia Network Isolation
Three regions were cut off from the global internet under the pretense of "military exercises."

New legal initiatives scheduled for 2025

January 2025 – Russian websites will no longer allow logins via foreign services (Google, Apple, etc.).

January 2025 – Foreign cybersecurity services will be banned for government use.

September 2025 – Moscow will legalize biometric data collection without user consent, further increasing state surveillance.

Myanmar

Myanmar's military coup on February 1, 2021, led to the arrest of Aung San Suu Kyi and National League for Democracy (NLD) officials. As mass protests erupted, the junta responded with brutal crackdowns, killing over 4,000 civilians. The military sought to silence dissent by controlling the internet, introducing censorship, surveillance, and infrastructure shutdowns. By 2024, the situation had worsened, with Myanmar's economy collapsing, civil war escalating, and the exiled National Unity Government (NUG) challenging military rule.

The junta's censorship infrastructure is modeled after China's Great Firewall, with direct technical assistance from Chinese entities. The key players in the project included Fang Binxing (architect of China's Great Firewall) who provided advisory support and the Geedge Networks that developed Tiangou Secure Gateway (TSG), enabling Deep Packet Inspection (DPI) and SSL/TLS decryption; while the China National Electronics Import & Export Corporation (CEIEC) assisted in location tracking and internet control systems.

By 2024, the junta had expanded its censorship capabilities, deploying real-time monitoring, keyword detection, and mass VPN blocking. The state is also shifting toward a whitelist model, where only approved government-controlled websites are accessible.

Social Media Monitoring – The military employs Russian-trained supervisors to infiltrate opposition networks, spread disinformation campaigns, and manipulate online discourse.

Beyond digital tactics, the military engages in physical repression including checkpoint Inspections, where people's devices are searched for VPNs, opposition content, and encrypted messaging apps. Independent reporters face arrests, media closures, and targeted intimidation. The military also embeds informants in local communities to track dissent.

Besides, Myanmar's military has criminalized digital transactions as a tool for repression. The junta has frozen accounts suspected of funding resistance movements. The government flags keywords and transaction patterns to disrupt dissent financing. Activists increasingly rely on Bitcoin and alternative financial networks to bypass financial surveillance.

List of blocked resources in Myanmar by 2024

Social Media – Facebook, Instagram, and X (formerly Twitter) have been blocked.

News Websites – Independent media, including BBC, RFA, Myanmar Now, and Irrawaddy, have been restricted.

VPNs and Circumvention Tools – Wireguard, Psiphon, Riseup, and Tor are aggressively blocked.

Educational Platforms – Wikipedia and local academic resources are inaccessible.

Encrypted Messaging Apps – Signal, Viber, Facebook Messenger, and WhatsApp are banned, though Telegram remains accessible.

Myanmar surveillance apparatus:

Biometric Data & SIM Registration – Internet activity is tied to national ID systems, enabling targeted crackdowns.

Smart City CCTV & Facial Recognition – Surveillance cameras powered by HIK Vision (China) track movements in urban areas.

Mobile Data Extraction – Forensic tools from Cellebrite (Israel), MSAB (Sweden), and BlackBag (US) are used to unlock and extract personal data from confiscated devices.

Financial Surveillance – Over 18,000 mobile money accounts have been frozen since 2021, disrupting opposition funding.

Alternative Communications: the Fight for Connectivity

With the internet increasingly restricted, Myanmar's people have developed offline and alternative communication methods:

Walkie-Talkies – Due to rising demand, prices for transceivers have increased tenfold since 2021.

Mesh Networking – Low-bandwidth, decentralized communication tools are used in medical and emergency situations.

GEO & LEO Satellites – Internet via Thuraya, IPStar, and Inmarsat costs about $100 per 60GB, making it expensive but viable.

Starlink Internet Cafés – Starlink terminals are being used in bomb shelters to avoid military airstrikes. However, the junta has threatened to block Starlink services.

Myanmar's digital landscape is a high-stakes battleground, where the military uses censorship, surveillance, and financial repression to control society. However, resistance efforts continue through alternative communication methods, decentralized networks, and innovative circumvention strategies.

Global support by digital rights activists, developers, and organizations is required to assist in building more resilient circumvention tools to help Myanmar's people stay connected. The fight for digital rights in Myanmar is far from over, but the resilience of its people continues to challenge the junta's efforts to silence them.

Ukraine

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. 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 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.

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. 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.

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.

Missle Attacks
Source: Mykola Kucheruk, ELIT-LINE, Kramatorsk, Donetsk Region

Missle Attacks
Source: Mykola Kucheruk, ELIT-LINE, Kramatorsk, Donetsk Region

Missle Attacks
Source: Mykola Kucheruk, ELIT-LINE, Kramatorsk, Donetsk Region

Missle Attacks
Source: Mykola Kucheruk, ELIT-LINE, Kramatorsk, Donetsk Region

Today, Ukraine has over 4000 ISPs, whose engineers are constantly risking their lives when going out to repair damaged infrastructure.

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.

The European Union, with its new legislative initiatives such as DMA and DSA, as well as the EUID project (European Digital ID), and the pervasive DNS blocking are advancing towards a “EUnet” version of a splinternet. The current political crisis in the US, including deletion of strategically important databases and websites and major reforms of technological platforms such as Meta, are threatening global connectivity worldwide.

In this context of global splinternetization, the time is right for preparing technologically and socially. SplinterCon’s major focus is on “getting ready for the splinternets.” We address two major challenges: how do we communicate with users inside splintered networks? And, how do users inside a severed network continue independent and importantly secure communications with each other?

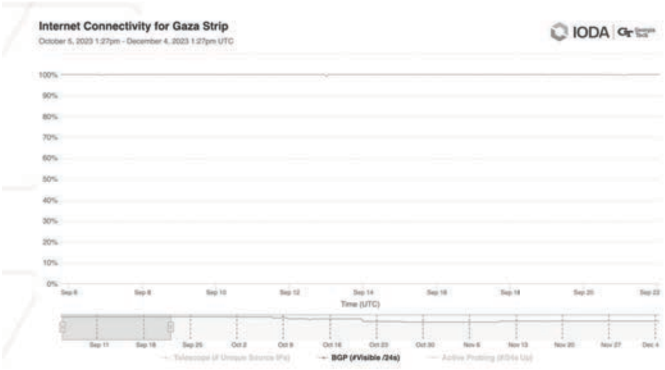
Section 2

Researching censorship and isolation

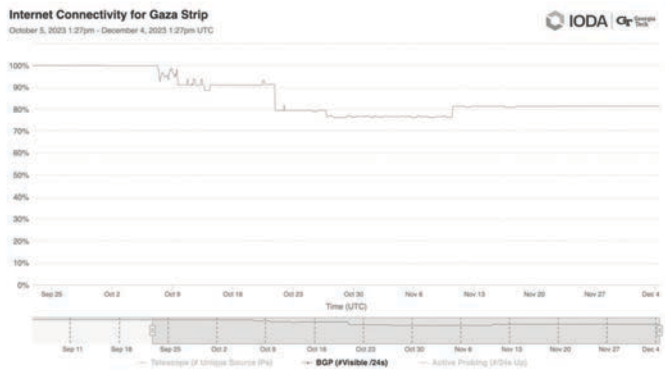
SplinterCon gathered major participants from a variety of network measurement initiatives such as IODA, OONI, M-Lab, Cloudflare Radar, OZI, Lab IV, Critical Infrastructure Lab and others to present their research on network measurements. The following pages provide key insights of their research.

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.

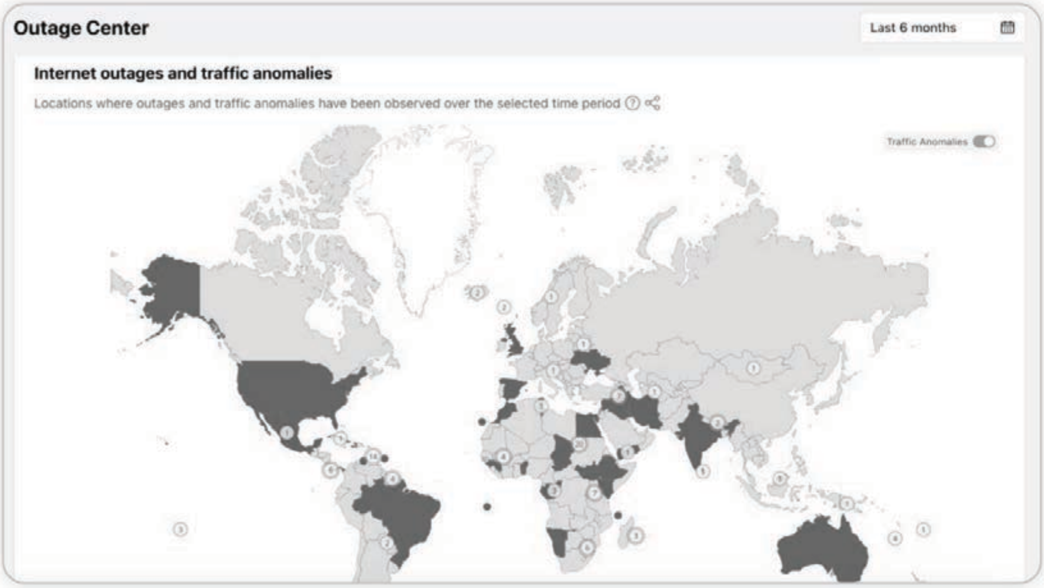
The Cloudflare Radar Outage Center (CROC) produces a curated list of observed & verified Internet outages and collects metadata about the outage or traffic anomalies. It's also possible to manually verify the anomaly based on metrics from other projects (e.g. IODA). The adoption and usage provide metrics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

M-Lab (Measurement 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.

M-Lab uses traceroute data to find evidence of shutdowns, analysing data to see how network interference events affect the paths being taken. However, the ideal server topologies to measure network interference events and internet fragmentation behaviors are still discussed, along with questions around which metrics are the most useful to collect during crowd-sourced campaigns to document network interference events.



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

Assessing Shutdown Risks: Connectivity And Reliability Indexes For A Free And Stable Internet

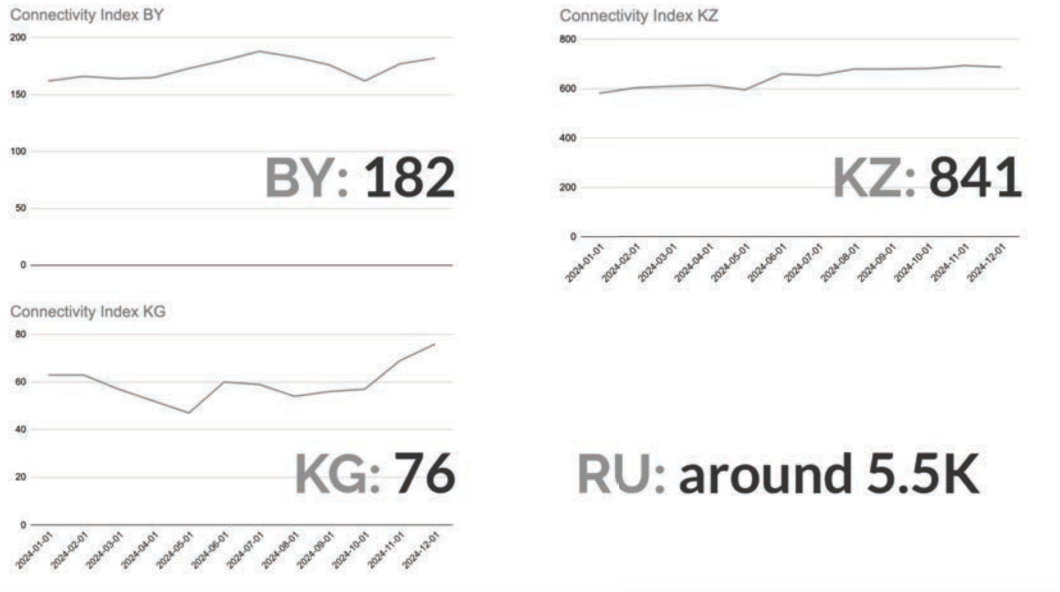
A research conducted by the Internet Protection Society (OZI) in collaboration with Lab IV (Data Engineering Consulting, Berlin) to analyze internet shutdown risks using Connectivity and Dependency Indexes. The study focuses on the ability of countries to maintain stable access to global internet infrastructure, assessing their resilience to network disruptions.

The research team gathered data from leading internet measurement platforms, including: RIPE NCC , Cloudflare, CAIDA and IODA. The datasets from these sources allowed the team to analyze real-time and historical internet connectivity data to assess stability, dependency, and resilience.

To quantify the risk of internet shutdowns, two key metrics were developed:

Connectivity Index which measures the total number of active connections between local networks and foreign networks in a country. A higher index indicates a more stable and decentralized internet presence

Dependency Index: A developing metric that aims to measure how reliant a country is on specific providers, routes, or geopolitical influences for external connectivity.



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 3

Reaching out to isolated networks

In this section of the report, we look closely at tools and infrastructures presented at SplinterCon, which can help maintain connectivity with and within isolated networks. These tools often rely on older, well established protocols and standards. Still, they all need some ingenuity to hide from censors' gaze and successfully navigate the growing complexity of filtering and censorship.

While some of these solutions already have a solid user base, others are innovative and still in the testing phase. As a laboratory of circumvention, SplinterCon offered a place for all these tools to gather feedback and involve participants in testing and tinkering.

A splintered network such as the NIN may be seen and perceived as a "thing in itself," a sovereign ecosystem that locks users into a specific set of whitelisted protocols, IPs, websites, and apps. That is why at SplinterCon, we aim at developing a "counter-splinternet" ecosystem to build a community of tool makers and protocol designers working on various levels, from wireless and satellite tech to network architectures, network measurement kits and new messaging apps.

The solutions for reaching out to sovereign networks presented at SplinterCon are grouped around two approaches: exploring the potential of satellites and wireless technologies and building more advanced and harder to trace traffic obfuscation 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).

While satellite technologies provide a means of delivering uncensored news and information, they are not entirely immune to interference or geo-tracking. 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.

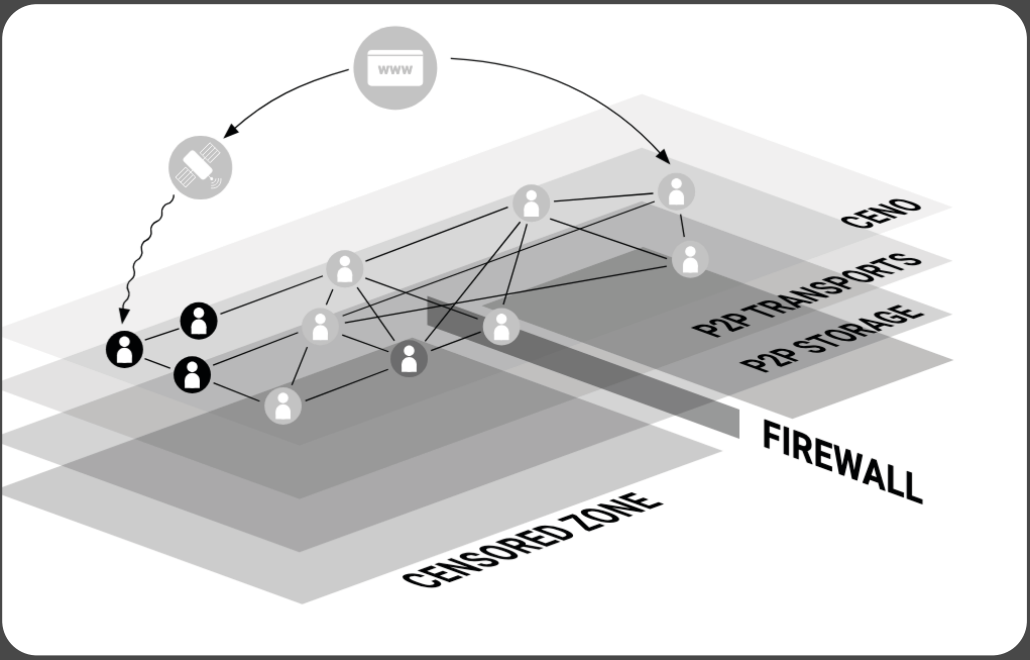
The security and privacy of Starlink solution, that has been previously used in many at-risk countries, such as Ukraine, is now questionable due to its controversial ownership. was cited as an example (already deployed and tested in Ukraine). Before Starlink, there were other attempts to deploy an accessible 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.

An important takeaway for SplinterCon participants is that we cannot completely rely on LEO satellite commercial solutions, otherwise we might end up with an Elon-splinternet or a Bezos-splinternet. And therefore to guarantee neutrality and availability of services, we need to provide alternative free software solutions, some of which were presented at SplinterCon.

Shutdown-Resilient Connectivity: Ouisuite



OuiSuite by eQuailitie is a comprehensive strategy for countering internet censorship and ensuring decentralized access to information. It is a set of tools designed to maintain open access to information even in heavily censored environments. OuiSuite 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, it was recently implemented to support Paskoocheh — a Farsi software marketplace for privacy and circumvention tools.

Decentralization, resilience, accessibility, privacy, and security are critical to maintaining an open internet. However, achieving this comes with significant challenges, including censorship blockades, infrastructure limitations, and surveillance risks. Addressing these issues requires breaking dependence on centralized systems, which can be easily co-opted or shut down by state actors.

The OuiSuite ecosystem includes several key technologies that work together to bypass censorship and ensure access to restricted content:

1. Ceno Browser – A collaborative web browser that enables users to share cached content peer-to-peer, ensuring that once a page is retrieved, it remains available to others within the network. This systemreduces reliance on traditional infrastructure and allows users to access censored content without needing constant internet connectivity.

2. OuiSync – A file synchronization and caching system that enables content distribution without a central server. Files can be imported, shared, and synchronized across decentralized networks, making it possible to maintain access to important information even during internet shutdowns.

3. Satellite and Alternative Networks – The data can be transmitted using satellite internet, HF radio, DVB-S(2) satellite broadcasts, and point-to-point WiFi networks. These alternative communication channels provide ways to distribute information beyond the reach of traditional internet restrictions.

4. TV and Digital Broadcasting – Existing digital television infrastructure (DVB-T2 and DVB-S2) can be repurposed for data transmission, allowing users to receive censored content through traditional broadcast signals. This method is particularly useful in regions where the internet is heavily controlled but broadcast media remain accessible.

OuiSuite's approach focuses on preparing for extreme censorship scenarios, such as complete internet shutdowns. The proposed solutions ensure that even in the worst conditions, users can still access information through offline caching, peer-to-peer sharing, and satellite communication. Additionally, OuiSuite aims to normalize decentralized access by integrating these tools into existing systems and improving usability. However, a need remains for simplified interfaces, interoperability standards, localized support, and community-driven development to make censorship-resistant technologies accessible to a broader audience.

By leveraging decentralization, peer-to-peer networks, and alternative communication channels, Ouisuite provides a robust defense against censorship.

Svoboda Satellite: Using Satellite to Penetrate Media Firewalls

Svoboda Satellite project, backed by Reporters Without Borders (RSF), uses satellite television as a tool for bypassing media censorship in Russia. Svoboda Satellite offers an alternative way to deliver independent journalism directly to audiences—without relying on the internet.

The Svoboda Satellite project operates through a contract with Eutelsat, utilizing a transponder on the Hotbird 13E satellite, one of the most widely used free-to-air satellite positions in Russia and Europe. This allows them to broadcast up to 25 independent TV channels, accessible without encryption to anyone with a standard satellite dish. The coverage area extends across Europe, the Middle East, and 4.5 million households in Russia, offering an uninterrupted way for audiences to access alternative perspectives.

Unlike internet-based platforms, satellite broadcasting is a one-way transmission, meaning that users can receive content without the risk of their viewing habits being tracked by Russian authorities. This feature makes it a secure and effective method for circumventing state censorship.

The Svoboda Satellite package currently includes 12 active channels, featuring a mix of independent news, investigative journalism, and cultural programming. Many of the top Russian-language alternative media outlets have joined the project, including well-known YouTube journalists such as Irina Shykhman, Pavel Kanygin, and Roman Anin, as well as organizations like Novaya Gazeta and Euroradio (Belarus). The package also includes international broadcasters like Deutsche Welle Russia, TV8 (Moldova), and Current Time, which were previously blocked in Russia.

Additionally, Svoboda Satellite has launched eQtv, a newly created channel by eQualitie. This is the first satellite channel dedicated to digital security awareness and privacy education, broadcasting content in Russian, English, and Ukrainian.

While satellite technology offers a promising workaround, it is not immune to interference. Russia has previously jammed Ukrainian satellite signals, and while Svoboda Satellite has managed to avoid direct disruption so far, the risk remains. The team has implemented countermeasures to mitigate potential jamming attempts, and recent activity suggests that Russia may be de-escalating its satellite interference operations—possibly due to diplomatic factors.

A similar satellite-based censorship circumvention model could be implemented in other authoritarian states. The feasibility of such an approach depends on three key factors:

1. Widespread use of satellite television in the targeted country.
2. Availability of major Western satellite providers that can be contracted for broadcast services.
3. A strong ecosystem of independent content creators willing to contribute to the channel lineup.

Satellites for Iran: Toosheh

To evaluate opportunities of satellite technologies for NIN, SplinterCon hosted a panel discussion among three circumvention projects that rely on satellite transmission: **eQSat**, **Toosheh**, and **Starlink**. Uplink antennas are forbidden in Iran, but in recent years, there has been a proliferation of satellite Internet usage, which has reduced the cadence of enforcement. At SplinterCon we discussed the many possible use cases for innovative wireless tech and opened pathways for further collaborations

Toosheh is the original datacasting over satellite TV project that delivers more than 7GB of daily content in bundles, accessible over a local LAN. Payload includes flattened websites, software, educational material, and audiovisual content. This content is accessible through a dashboard that shows files, packages, and available offline website. It is deployed in Iran and Middle East, and has around 5M daily users.

GEO&LEO Satellite Internet: 2-way

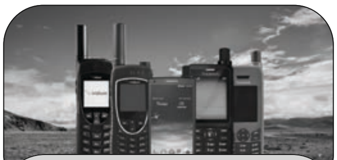
Border LTE coverage: 2-way

Data over DVB-T(2): 1-way within 100km from borders

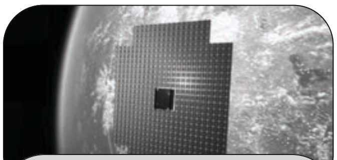
Point to Point Wifi: 2-way, (requires line of sight)

HF Radio: low bandwidth, 2-way

Data over DVB-S(2) Satellite: 1-way

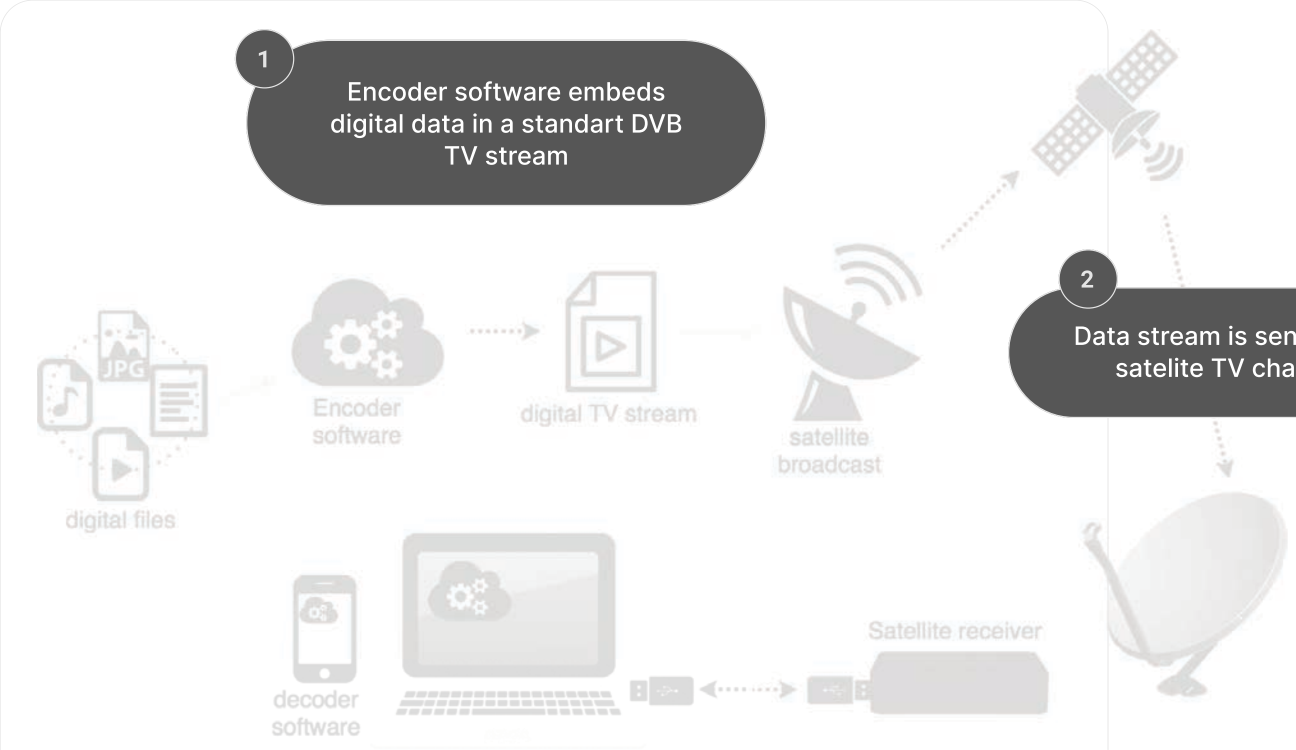


Satellite Phones: high exposure, 2-way



5G (3GPP) Broadband: Phones to LEO, 2-way

Missle Attacks
Source: Mykola Kucheruk, ELIT-LINE, Kramatorsk, Donetsk Region



1 Encoder software embeds digital data in a standart DVB TV stream

2 Data stream is sent over a satelite TV channel

3 User records TV stream using standart Satelite. Set top box receiver on USB flash

4 Extractor (decoder) software on a PC or mobile extracts encoded data from the recorded TV stream

451 Tools+Deflect: Empowering Publishers in Splinternets World

451 Tools+Deflect (projects by **Zamaneh media** and **eQualitie**) is a technological suite designed to help independent publishers and civil society organizations avoid online censorship. The integration of these two technologies enables an innovative channel that ensures information remains accessible despite network censorship and without requiring any installation or even knowledge of the underlying technologies from users.

Governments, particularly in authoritarian regimes, use a combination of legal and technical measures to block access to independent news and activist platforms. HTTP 451, the status code for content "Unavailable for Legal Reasons," has become a common reality for many websites facing state censorship. In response, 451 Tools and Deflect offer dynamic and decentralized solutions to keep online content reachable.

451 Tools, developed by Zamaneh Media, is a JavaScript-based system that integrates with a website to manage the accessibility of the platform's content across multiple mirror domains. When a primary domain is censored, 451 Tools automatically fetches up-to-date content from available mirrors, allowing users to continue accessing the website without interruptions. Additionally, it supports offline content sharing, ensuring that information can be distributed even in environments with limited or no internet access.

Deflect.ca, a service provided by eQualitie, specializes in DDoS protection and website security for independent media, human rights organizations, and non-profits. It not only protects sites from cyberattacks but also dynamically replaces blocked domain names on the fly through its mirroring technology. By integrating with 451 Tools, Deflect can offer seamless censorship circumvention without requiring users to install a VPN or configure special settings.

The core technology behind these tools involves dynamic DNS rotation, ensuring that when one domain is blocked, others remain available. Deflect's infrastructure continuously redirects users to operational mirrors while keeping them on the same website, avoiding the need for redirections that could alert censors. Unlike traditional VPNs or proxy services, this approach doesn't require users to take extra steps—access remains automatic and uninterrupted.

These technologies are Radio Zamaneh, an independent media organization that uses 451 Tools to distribute news in Iran.

By employing a mix of online mirroring and offline sharing strategies, Radio Zamaneh ensures that critical reporting reaches audiences despite government efforts to suppress it.

Independent media organizations can register for Deflect's services for free. Once onboarded, sites can integrate 451 Tools without modifying their existing code, as Deflect dynamically injects the necessary scripts. The system requires at least two mirror domains, which Deflect helps configure. Once active, the site automatically detects censorship attempts and reroutes users to accessible mirrors. As internet censorship becomes more sophisticated, so too must the tools designed to counter it. Deflect and 451 Tools provide a zero-configuration, censorship-resistant solution for publishers operating in hostile environments. By dynamically adapting to network interference and offering seamless access through mirroring, these technologies empower independent media to continue their work without fear of being silenced.

Protocol-based Solutions: Obfuscation, Proxyless and DNS-Level Circumvention

In this part we list the most interesting and novel approaches in the field of obfuscation protocols, to move beyond VPNs. While censors' capacities to detect and filter circumvention tools at the protocol level are improving, it is crucial to innovate on the level of infrastructures and protocols. Here is an overview of some of the best solutions presented at SplinterCons.

Towards "obfs5"

Obfs5 is a new successor to obfs4, which is a transport protocol designed to obscure internet traffic and circumvent censorship. Obfs4 is a popular obfuscation protocol used to prevent traffic fingerprinting, making it harder for censors to detect and block the Tor network. However, obfs4 has several limitations:

1. It uses the XSalsa20Poly1305 cipher without hardware acceleration
2. The protocol has limited obfuscation capabilities, which makes it vulnerable to advanced traffic analysis techniques.
3. The handshake process is based on the outdated NTor v1, which lacks early data support and has limitations in terms of flexibility and cryptographic strength.

The goal of obfs5 is to build on the strengths of obfs4 while addressing its weaknesses and include the following features:

1. Strong Obfuscation: Traffic is made computationally indistinguishable from random, even to adversaries who know the server's public identity.
2. Forward Secrecy: Ensures that session keys cannot be compromised even if long-term keys are exposed.
3. Replay Resistance: Protects against replay attacks by ensuring that legitimate flows cannot be replayed.
4. XChaCha20Poly1305: Replaces the outdated cipher, supporting hardware acceleration for improved performance.
5. Post-Quantum Forward Secrecy: With the advent of quantum computing, obfs5 incorporates measures to ensure that encrypted data cannot be decrypted in the future with quantum computers.

Obfs5 introduces Hybrid Key Establishment (HPKE) and Kemeleon, which combine existing cryptographic algorithms to offer robust post-quantum encryption. Early Data Support allows the protocol to send encrypted data before the handshake is complete, improving efficiency. While Granular Permissioning provides better control over which features are enabled or disabled depending on the environment.

Ongoing implementations of key cryptographic components include Elligator2 and Kemeleon, which are designed to enhance the obfuscation and security of the protocol. There is also a focus on exploring QUIC for transport features, aiming to improve the reliability and flexibility of the protocol. QUIC supports multiple independent streams over a single connection, enabling session migration, preventing external interference, and optimizing for real-time communication (RTC).

However, while obfs5 offers stronger cryptography and more features than its predecessor, it is still in an experimental phase. There is a need for hardware acceleration support and the development of reliable internal protocols for media streaming and real-time traffic.The protocol needs further testing and refinement before it can be widely deployed.

Tor Webtunnel: A New Web-Based Pluggable Transport for Bypassing Censorship

WebTunnel is a new web-based pluggable transport (PT) designed by Torproject to help users circumvent internet censorship. Tor is a critical tool for ensuring online privacy and freedom, particularly in regions where governments and ISPs aggressively block access to the network.

However, censorship techniques are becoming more sophisticated, requiring constant innovation in circumvention strategies.

The two major problems in keeping **Tor** accessible are distributing rridges (getting bridge addresses to users without detection and hiding bridges (preventing censors from identifying and blocking bridge nodes). Bridges are non-public relays that allow users to connect to the Tor network even when direct connections are blocked. However, advanced censors deploy deep packet inspection (DPI) and active probing techniques to detect and block these connections.

Pluggable Transports (PTs) are tools used by Tor to disguise its traffic.

Different PTs take different approaches to avoid detection:

- obfs4 – Makes Tor traffic appear as randomized, encrypted data, avoiding detection by DPI.
- Snowflake – Embeds Tor traffic within WebRTC connections, making it resemble peer-to-peer (P2P) traffic.

While these methods work in many scenarios, sophisticated censors continue to develop machine learning-based detection techniques that can still flag Tor traffic. Therefore, Torproject has worked on a new PT called WebTunnel, designed to make Tor traffic look like regular web traffic, blending in with the billions of normal HTTPS connections that occur every day.

How WebTunnel Works?

It mimics legitimate web traffic patterns, making it harder for censors to distinguish Tor connections from normal internet usage. Unlike obfs4, which relies on appearing as random noise, WebTunnel takes an approach similar to Snowflake by embedding itself in common protocols. The exact technical details were not covered in the presentation, but the goal is clear: WebTunnel aims to be less detectable and more resilient than existing solutions.

For users in censored regions, WebTunnel could be a game-changer, providing a more stealthy and effective way to access the open internet. For censors, this represents a new challenge, as they will need to develop even more sophisticated blocking techniques. For bridge operators and the Tor community, the challenge is to scale WebTunnel to ensure widespread adoption and resilience against censorship. The more bridges exist, the harder it becomes for censors to block access to Tor.

DNS-level Circumvention

The DNS plays a critical role in modern internet infrastructure, supporting CDN operations, cloud services, microservices, and auto-discovery configurations. As the internet grows, the scale of DNS usage becomes increasingly vast, making its security paramount. DNS is frequently used as a tool of information control and blocking. Even the democratic states, such as the EU, enforce DNS-based blocking. DNS plays in controlling internet access, monitoring behaviors, and facilitating censorship. Manipulation or interception of DNS queries is observed in various countries, where governments or entities may block, redirect, or surveil users without their knowledge. Examples include "quiet manipulation" where queries are intercepted, rewritten, or denied.

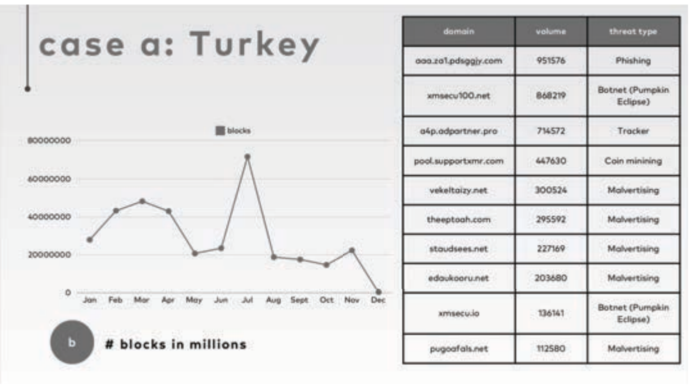
Alternative approaches to DNS are developed, offering an additional layer of resilience. At SplinterCon we held several DNS-focused sessions with technologists and policy researchers, to develop together the future of a resilient DNS.

Quad9

Quad9 is a non-profit foundation based in Switzerland, offering open and secure DNS services. The primary aim is to provide reliable and uncensored DNS resolution, with an emphasis on privacy, security, and maintaining an unmodified, consistent, and standard service for users. Quad9 operates in over 260 locations across 115 countries, reaching more than 100 million people.

Regional Challenges:

Turkey: DNS queries are often "eaten" or denied for certain VPN services, effectively preventing users from accessing VPN providers. This happens at the point between the user and the authoritative server.



case a: Turkey

blocks in millions

domain	volume	threat type
aaa.za1.pdsggiy.com	951576	Phishing
xmsecu100.net	868219	Botnet (Pumpkin Eclipse)
a4p.adpartner.pro	714572	Tracker
pool.supportxmr.com	447630	Coin minining
vekeltaizy.net	300524	Malvertising
theeptoah.com	295592	Malvertising
staudsees.net	227169	Malvertising
edaukooru.net	203680	Malvertising
xmsecu.io	136141	Botnet (Pumpkin Eclipse)
pugoafals.net	112580	Malvertising

China: Quad9 faces challenges in China, where many users cannot connect to Quad9 servers due to preemptive refusals, especially for unencrypted queries. Encrypted queries are routed to neighboring countries, though they remain vulnerable to manipulation. Malware blocking is more effective through the service, especially for command and control sites.

Malaysia: There is a growing demand for uncensored internet, and resistance against filtered DNS services has been observed. Quad9, being exempt from local DNS regulations, continues to operate while facing pressure from local authorities and international threats.

The types of threats blocked by Quad9 include phishing, botnets, malware, and malvertising. Specific domains and their associated threats are listed, showing the volume of blocks across different months.

Increasing legal cases are targeting DNS resolvers in various countries, demanding the blocking of certain content, often under the guise of copyright protection. Quad9 has faced lawsuits in multiple European countries, including France and Germany, with more expected in the future. As the legal landscape shifts, the pressure on DNS resolvers increases, leading to more censorship, surveillance, and manipulation of internet traffic.

Encryption can be a potential solution to protect user privacy and prevent DNS manipulation, but implementing it effectively remains challenging. The language surrounding "blocking" vs. "censorship" is evolving, and there is a need for clearer standards and commitment to an open and secure internet. It is crucial to maintain open DNS infrastructure while navigating the legal and technical challenges posed by government censorship and the growing need for encryption to protect users.

As for the DNS-based censorship, several protocols may be able to bypass it:

1. **Splitting the TLS record.** In this way, SSI doesn't go in one flow — like 'face' and 'book.com'. It also requires a modification to the client instead of the previous method.
2. **TCP packet segmentation.** Imagine that on the server side there's a window size configuration that forces the client to send smaller packets. In this case, Server Name Indication just doesn't appear as a single unit for the ISP. It only requires a change to the server and not the client, which is an advantage of this method. However, recent research indicates supervisors may be able to reassemble TCP packets.

3. **Domain fronting.** It involves a mismatch between the HTTP Host header and the SNI extension. For example, if your domain is blocked.com and another domain on the same server is notblocked.com, you can use notblocked.com in the SNI but blocked.com in the encrypted HTTP request's HOST header. The service will then forward the request to blocked.com. However, majorcloud providers (Google, Amazon, Cloudflare, Azure) have stopped supporting domain fronting. Fastly is one provider still offering this service. For instance, here is the mirror of the official SplinterCon website: https://iucjibmeljdwfivy.w12mhmsaporr.live/
4. **DNS over HTTPS (DoH**) offers an advantage over DoT because it doesn't run on a specific port, making it harder to block without shutting down all HTTPS traffic. However, there is evidence that Iran has started to block DoH based on the destination servers. Using this protocol with a less popular server configured expressly for this purpose still grants access to services using DoH.
5. **DNS over TLS (DoT)** encrypts DNS requests. With support from Android and iOS, implementing DoT is relatively straightforward. However, DoT runs on a specific port (853), and there is evidence that Iran has blocked this protocol entirely at times. Cloudflare and Google’s DoT endpoints have also faced blocks.

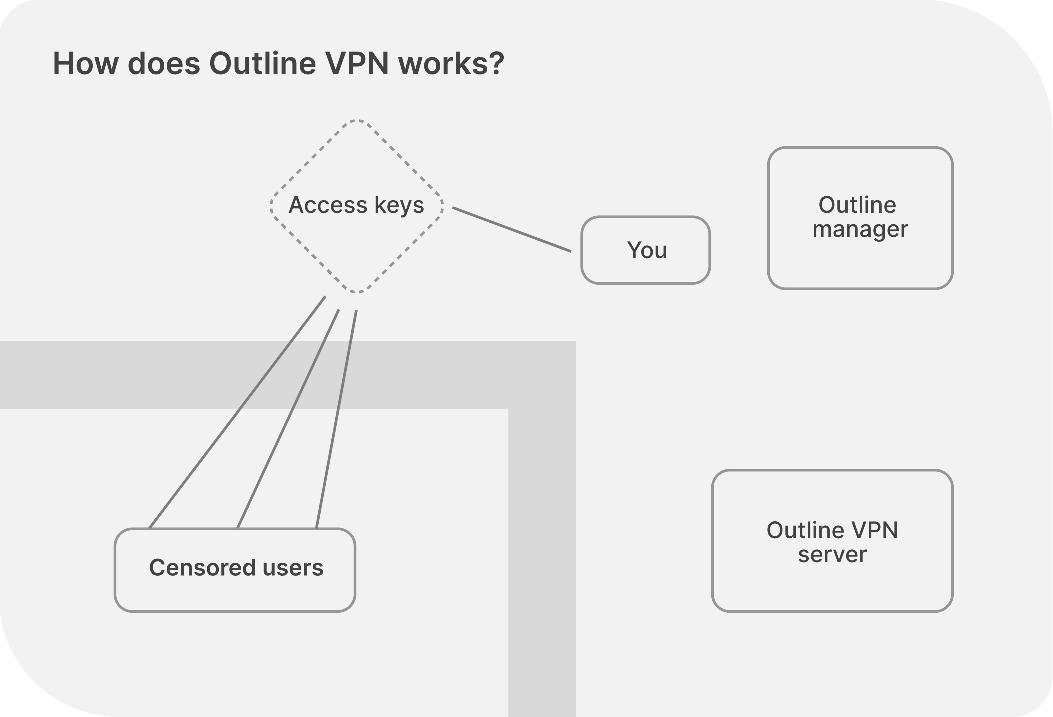
Some of the aforementioned methods work in the medium term, and others in the long term. Unfortunately, for example, for domain fronting, the most robust solution, the CDN should be able to support it. For TLS segmentation, server-side support is required. On the policy level, major service and cloud providers should be convinced to offer these configuration options. Therefore, it is important to deploy protocol-level solutions and SDKs that may offer additional traffic obfuscation, security and connectivity.

Outline SDK

Outline SDK offers reusable, composable and cross-platform components to empower apps against censorship. With several kinds of libraries, Outline SDK may help VPN providers to add network resilience to their apps, and to adapt them better to “pre-splinternet” situations. It offers libraries for transports (shadowsocks, tls, websocket), proxy protocols (shadow-socks, socks5, http) or proxyless strategies (encrypted DNS, packet manipulation etc); support for ”tun2socks” and mobileproxy to integrate into mobile apps.

A use-case of Outline SDK integration was presented at SplinterCon focusing on Meduza mobile app. Meduza is a Russian opposition media blocked by the Russian Internet watchdog Roskomnadzor, that successfully implemented an Outline mobile proxy inside their mobile app to keep Meduza accessible for their readers in Russia.

How does Outline VPN works?



Another successful use-case of Outline SDK integration was an implementation of proxyless solution for Iranians. It was very well received, even for multimedia platforms such as Youtube.

Outline SDK has proven its advantages forthose building circumvention tools and those using them. It facilitates proliferation of community VPN providers and therefore contributes to increasing overall connectivity. It lets providers control both the server and the client and make changes at the application layer (e.g. domain fronting, padding). It also has lower barriers to entry, making it easier for developers and researchers to implement new strategies.

However, the war on VPNs as it is unfolding nowadays in Russia or Iran urges technologists and content providers to “think out of the tunnels”, develop and deploy new solutions that are (yet) beyond the reach of the censor. SplinterCon has become a meeting point for those projects, a testing ground where these new approaches can be showcased, tested and discussed. The next part of this report focuses on tools that offer connectivity inside isolated environments.

Section 4

Self-Determination Within Isolated 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? The projects presented at different editions of SplinterCon can be grouped around several approaches: federated self-hosted alternatives, mesh-based or p2p solutions, resilient messaging apps. These technologies often creatively reuse older protocols and infrastructures, propose a sustainable approach,

Hermes: Affordable Digital Telecoms

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.

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.

dComms deploying resilient infrastructures

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.

Today **dComms** has moved forward to serve 5 more countries and is establishing active partnerships with CSOs and media that operate in areas with intermittent connectivity.

Ouisync secure p2p filesharing

Securely backing up, sharing and transporting data has been a challenge for as long as recorded media has existed. **Ouisync,** eQualitie's newest software 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.

Several use-cases make this new tool relevant for a splintered network:

1. A “digital emergency suitcase” with a set of pre-downloaded apps that can work inside a shutdown area or help bypass censorship (for instance Ceno, Outline, Delta Chat, Briar or other tools presented at SplinterCon).
2. Scenario for media organizations operating inside censored areas to distribute their content using Ouisync and circumvent blocking of their websites.
3. Finally, since Ouisync can work on a local network, it can also help organizations to maintain collaborative work on common projects even during shutdowns.

Awala: an Offline-First Network Suite

Awala is a network protocol suite that enables compatible apps to communicate with and without the Internet. It currently runs on Android and Desktop and undergoes a security audit.

One of the first apps based on Awala network is Letro (currently only exists for Android), a messaging app based on email. Like email, Letro is decentralized and based on open standards, but all messages are end-to-end encrypted. It also guarantees protection from spam and phishing, and users can send and receive messages even if they don't have access to the Internet.

Awala's proof of concept is a Twitter client that can run without the Internet, and potentially any of the popular apps (from Instagram to Western Union or Binance) could use the Awala network for resilience.

Awala relies on a network of so-called couriers. Awala is decentralized with a federated architecture where servers (called "gateways") act as brokers. Awala is ready to face various possible censorship scenarios. For instance, in case of a blocklist approach, where specific services, such as Awala gateways, are blocked, they could turn any HTTPS website into a proxy, and censors couldn't do active probing. Of course, censors could potentially analyze the traffic, but Awala could also make it follow an "organic" web browsing pattern.

In the case like Iranian (National intranet), where only domestic services are accessible, Awala would use couriers as if it were an Internet blackout, and leverage intranet services to relay high-priority data using steganography.

In the case of whitelist-based scenario, where only select services are allowed, Awala would also use couriers as if it were an Internet blackout. However, it is less likely that they'd be able to leverage sanctioned services to relay data.

Butterbox: a Communication Kit For Shutdowns

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.

Solving The “Messaging Problem”: Resilience In Diversity

SplinterCon became the meeting point for many pioneering messaging projects addressing issues of decentralization, privacy, censorship-resilience, collaborative work and standardization. Our conference series has shown that the “messaging apps problem” can not be solved in one and only way, but a multitude of approaches is required, to fit various threat models, use-case scenarios and network conditions. SplinterCon experts emphasize the importance of standardization work, open standards being key in advancing robust, trustworthy protocols and tools that can build on each other and resist digital fragmentation. Another key takeaway is the usability and work with communities on the ground, in order to guarantee reliability in real-life situations, such as splinternets or strict censorship.

In this sub-section we list some of the key messaging projects presented at SplinterCon. Other projects that were presented but are not described here include: Nahoft, Briar, Quiet.

Delta Chat: Resilient Federated Messaging for Organizations

Delta Chat is an instant messenger that uses email transport protocol (SMTP/IMAP) for message delivery. Messages in Delta Chat are end-to-end encrypted using rPGP and Delta Chat doesn't need a phone number. Its federated architecture and the configuration of specialized servers called “chatmail” makes Delta Chat resilient and censorship-proof. Tested with various user groups since 2018 during Internet shutdowns (Ukraine, Russia, Belarus, Cuba, Europe, Georgia), it has proven its ability to function in the context of precarious connectivity.

Email being costly to censor, Delta Chat’s architecture makes it hard to block. When Iran blocked Signal + WhatsApp, Delta Chat still worked with many email servers, because the state economy depended on email. Recently Delta Chat has implemented proxy support in Android and iOS apps for shadowsocks proxies. Other circumvention measures have been embedded, e.g. long term IP caching and hardcoded IPs for several providers to prevent DNS blocking.

Delta Chat works with almost every email provider (as long as it supports SMTP + IMAP) but there are also special servers called chatmail. On registration, no personal data is requested and the account is generated automatically. Chatmail enforces end-to-end encryption, no unencrypted message can be sent. Chatmail servers are cheap and easy to self-host, based on standard postfix and dovecot with minimal configurations and a script to generate necessary DNS records. Chatmail should be approached as an “email router” rather than an email server. Messages are only stored for a very short time (options to be deleted on delivery).

Recently, Delta Chat has implemented webxdc apps that are offline-first mini apps that can be shared in a one-on-one or group chat. They offer a variety of collaborative tools for team work (from a text editor and a calendar, to a time tracker and a poll). Webxdc apps can only send and receive data within the chat, not with the internet. No servers are pinged, and no authorization is needed.

These webxdc apps are based on html, css, javascript and are packed into a zip file, renamed to .xdc, and sent as an attachment. Webxdc is an open standard, implemented in other messengers as well (for example, XMPP messengers Cheogram and monocles). It is a form of distributed computing, where servers are only a dumb transport layer. Recently webxdcs became real-time thanks to implementing the new powerful peer-to-peer protocol called iroh.

Phoenix

Members of Phoenix R&D presented their efforts on Messaging Layer Security (MLS) protocol, a modern cryptographic framework designed to enhance secure and private messaging. The session covered current issues with messenger UX, how MLS improves security, and what is still missing for full adoption.

Current messaging apps often face trade-offs between security, usability, and efficiency. User expectations for seamless communication often conflict with the need for strong encryption. While traditional messaging security relies on point-to-point encryption, which can be inefficient for large groups, MLS is designed to provide scalable encryption, supporting both 1-to-1 and group messaging.

Core Features of MLS:

1. Forward Secrecy (FS): Ensures past messages remain secure even if encryption keys are compromised.
2. Post-Compromise Security (PCS): If an attacker gains access, future messages remain protected via key updates.
3. Efficient Key Updates: MLS significantly improves rekeying efficiency, especially in group chats.

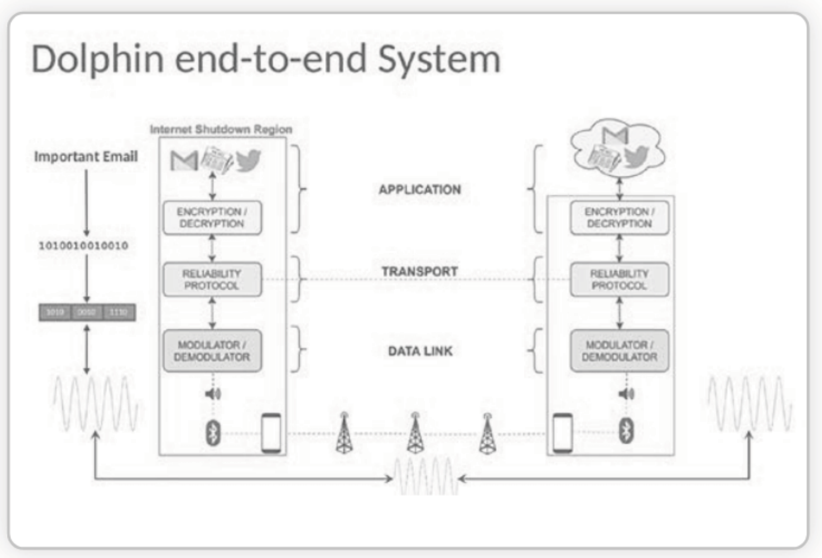
However, the protocol itself is generic but requires implementation-specific adaptations for real-world use. Some security features still need to be optimized for low-latency communication and resistance to metadata leaks.

Phoenix R&D is precisely focused on enhancing privacy protections by integrating MLS with stronger anonymity guarantees and ensuring practical adoption in mainstream messaging applications. MLS represents a major leap forward, enabling more efficient and scalable encryption. Adoption in major messengers could increase privacy across the board while maintaining good UX. However, more work is needed to bridge the gap between MLS specifications and real-world deployment.

The session concluded with a call for further research, implementation, and industry collaboration to improve secure messaging solutions while keeping privacy at the forefront.

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.



Qaul: a Zero-Config P2P Messenger

Qaul 2.0 is a zero-Config, OS agnostic mobile p2p messenger. It can interconnect via LAN/Wifi, Bluetooth Low Energy (BLE) and Internet Overlay. Users are identified via a hash of their cryptographic key; they are automatically discovered and all connections are meshed. Qaul offers one on one chatsand group chats, all chats are end-to-end encrypted, and interconnections between devices have transport encryption (TCP stack & QUIC stack). Interface is translatable and available in many languages

Conclusion: The Net will be decentralized...

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

1. 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).
2. Rely on active users / relays "on the ground" who can propagate information inside an isolated network.Are hybrid and rely on several protocols and communication channels (see eQSat, that uses satellite tv infrastructures on 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).
3. Rely on active users / relays "on the ground" who can propagate information inside an isolated network.

The interest in mesh, p2p and near-field communication solutions is growing, 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.

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 hope that the SplinterCon adventure will continue in 2025 and onward to foster these communities, creating an accessible base for developers and researchers working on breaking informational isolation.

Since 2018, **eQualitie** has been developing a new generation of censorship circumvention and evasion technologies, built on decentralized protocols, distributed routing and storage mechanisms, wireless communication and broadcast services. Since early 2022, we have deployed several country-wide fediverse networks, decentralized and encrypted content sharing tools, and launched a datacasting effort that rebuilds important web content in isolated networks - a 21st century sneakernet. Our programming focuses on digital resilience and capacity building for communities living under heavy censorship, frequent shutdowns and at risk of permanent disconnection from the global Internet.

We believe that only through collaborative efforts can we begin to comprehend and address issues posed by the looming splinternet. Through the SplinterCon series, we are building a network of human expertise and a resource pool of skill and knowledge to support the existence and proliferation of digital communications and connectivity to the global internet for the years to come.

Join us!

splintercon.net/community

SplinterCon

MONTREAL, BRUSSELS, ESTORIL, BERLIN, TAIPEI
2023, 2024, 2025

- FRAGMENTATION & FREEDOM: THE NEW DIGITAL DIVIDE
- THE NATIONAL INFORMATION NETWORK – CHALLENGES AND OPPORTUNITIES
- ECOSYSTEMS OF DIGITAL RESILIENCE

splintercon.net

eQualitie