SplinterCon

Brussels. June 12-13

content

<SECTION 1: Introduction>

<SECTION 2: Splinternet architecture>

<SECTION 3: Tools for Splintered Networks>

<SECTION 4: Blockathon>

SECTION 1

Introduction

The second international and interdisciplinary conference SplinterCon took place in Brussels in June 2024. It united around eighty participants — network engineers, researchers, journalists, civil society activists, and software developers around the challenging topic of the splinternet.

While splinternet is becoming a global trend, it remains understudied and largely without reply from the internet freedom community — few solutions exist to measure it's characteristics, impact and technical means to breakout. As a multilayered and complex process, splinternetization can be driven by several forces: governmental control, vendor lock-in (silos or closed "ecosystems" maintained by proprietary digital platforms), digital divide and finally, bots. This second edition of Splintercon focused on the first type of splinternet, and precisely on Iranian National Information Network (NIN) — a decade-old initiative to create a national intranet replete with local services under government control.

Presentations delved into technical and political realities of the NIN, but also compared it with experiences from other countries living under – or working their way towards network isolation. Besides, a new format of technical competition called "blockathon" took place on the second day of the conference. Blockathon offered participants a chance to experience an isolated network with strict censorship – and to find innovative ways to break through it.

In a Splinternet context, access to the global network and/or interoperability of services is obstructed or significantly restricted. This distinguishes splinternet from Internet shutdowns (defined as temporary suspensions of Internet services in specific regions) and from censorship (which involves the blocking of particular websites or services).

To restore global connectivity for users in a splintered network, traditional methods of bypassing censorship won't work. Standard methods of VPNs and relay proxies might not work in this instance. Splinternet remedies require new protocols, as well as innovative rediscovery of older standards and solutions, sometimes combining various approaches. SplinterCon's mission is therefore twofold — reaching out to isolated networks, and second, deploying technologies that offer secure and resilient communications for users stuck inside a splinternet.

This report guides you through real-life scenarios of government-driven splinternets, from Iran to Cuba and Russia. It then dives deeper into tools and methodologies for "pre-splinternet" and splinternet contexts.

This report presents key abstracts of the talks enhanced with links to presentations and additional material that can be found on the conference website. Some of the project titles are withheld to respect speakers' requests for anonymity. The conference was organized by eQualitie with help from ASL19. The event followed Chatham House rules.

SECTION 2

Splinternet architecture

National Information Network in Iran

While in the first report we have largely covered the creation of the Iranian NIN, in this second report we focus on technical nuances and layers that constitute the architecture of this sovereign Network. We pay particular attention to mobile Internet control and to specific methods of censorship deployed in Iran.

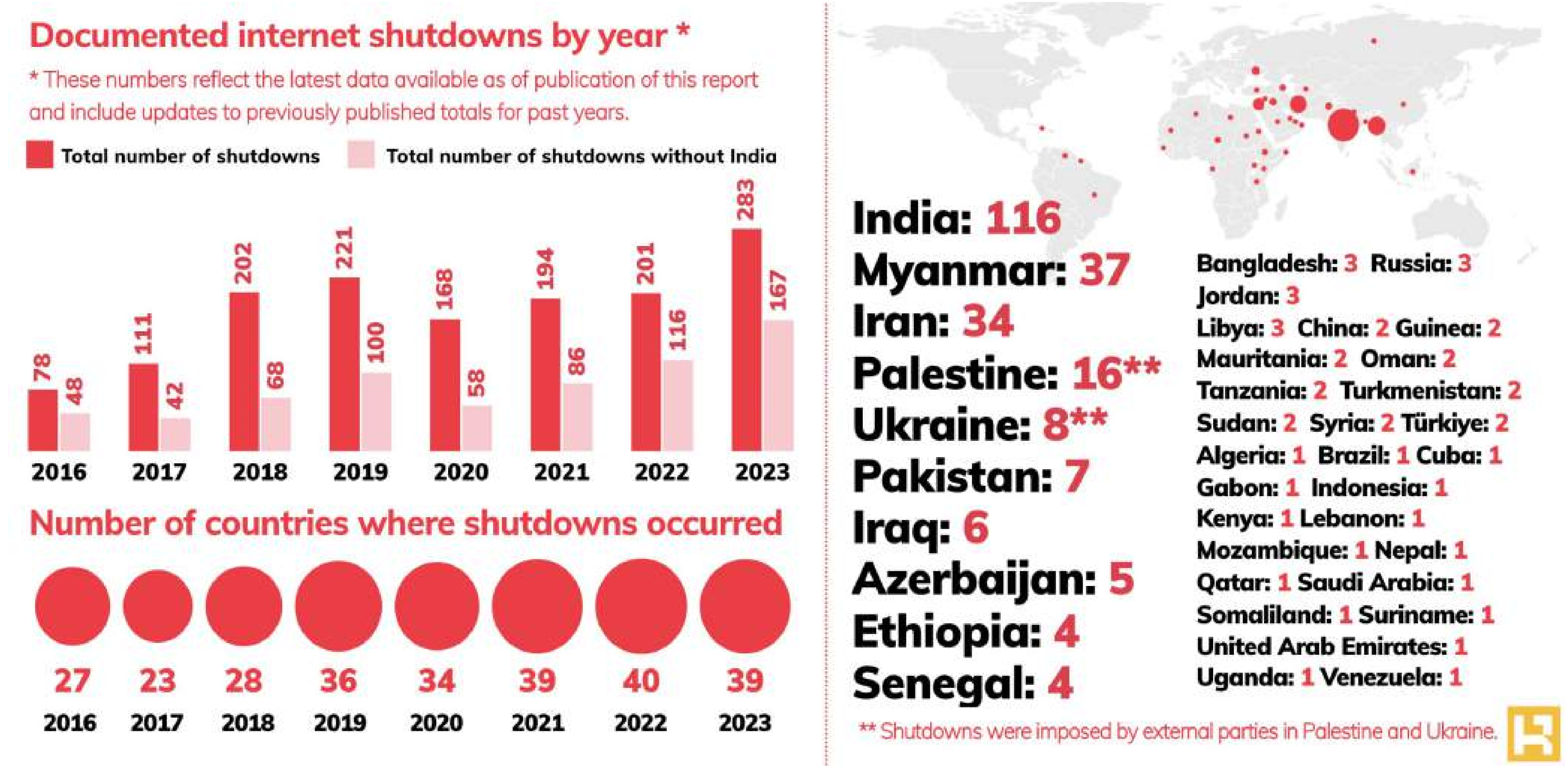
A brief summary of the history of NIN

In 2009, during the "Green Revolution" mass protests erupted in response to the announcement of the presidential election results. In response, the authorities shut down the Internet nationwide, causing a collapse in the banking and healthcare systems, halting information exchange between agencies, and even preventing the delivery of text messages.

Following these events, officials and IT specialists sought to reorganize the Internet infrastructure and policy to ensure basic usability during Internet shutdowns by maintaining access to state-approved and locally hosted web sites and services. The Criminal Code and Press Law were amended, the Supreme Council of Cyberspace was established, and the authority of the Supreme Council for National Security increased.

Over the next decade, Iran systematically worked towards a national, isolated intranet. Cross-border communication channels were slowed, while international traffic costs for consumers increased several times over. Foreign online platforms were required to open offices and move data centers within Iran, responding promptly to judicial requests and removing "illegal content" within twelve hours.

Shutdowns were systematically used in Iran in response to protests, elections, and school exams. For example, in 2019, widespread protests erupted over a sharp rise in gasoline prices. The police response was brutal, resulting in the deaths of many protesters; various estimates range from 304 to 1,500 people. During this time, the Internet was shut down.



India:	116
Myanmar:	37
Iran:	34
Palestine:	16**
Ukraine:	8**
Pakistan:	7
Iraq:	6
Azerbaijan:	5
Ethiopia:	4
Senegal:	4
Bangladesh:	3
Russia:	3
Jordan:	3
Libya:	3
China:	2
Guinea:	2
Mauritania:	2
Oman:	2
Tanzania:	2
Turkmenistan:	2
Sudan:	2
Syria:	2
Türkiye:	2
Algeria:	1
Brazil:	1
Cuba:	1
Gabon:	1
Indonesia:	1
Kenya:	1
Lebanon:	1
Mozambique:	1
Nepal:	1
Qatar:	1
Saudi Arabia:	1
Somaliland:	1
Suriname:	1
United Arab Emirates:	1
Uganda:	1
Venezuela:	1

** Shutdowns were imposed by external parties in Palestine and Ukraine.

The second example is the protests following the death of Mahsa Amini, who was detained in 2022 for "wearing the hijab improperly." Internet was cut off fifteen times in different parts of the country, and eight of the shutdowns affected ethnic minorities: Kurds, residents of Sistan and Baluchistan province, and others. Overall, in 2023, Access Now and the #KeepItOn coalition recorded a surge in Internet shutdowns in Iran, reaching 34 compared to 19 in 2022.

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 Iran already had a mobile monitoring and surveillance system built by Nokia Siemens. 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.

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.

In 2017, the Hamta platform was introduced, mandating the registration of every smartphone and data modem. Disguised as a measure against illegal imports, this new law enabled the government to track which smartphones or modems were owned by each citizen by linking IMEI numbers, phone numbers, and identities. The next step was the association of social media messenger accounts with phone numbers, further tightening the grip on digital communications.

Government services, such as passport delivery or renewal, required an app with extensive access permissions (e.g. sevice's camera, location, microphone, call history, SMS, and storage. This comprehensive database of citizens' "digital assets” enabled the Iranian state to monitor and control activists online, for instance, by selectively cutting mobile connectivity on their devices, or sending targeted SMS messages pressuring them to cooperate with the government. Moreover, the import of new smartphones was banned. The iPhone 14 and 15 will not register in the system, making it impossible to use them. Next step in tightening information controls is the development of a national operating system, granting the state access to lists of installed apps, network data directly on the device etc.

Splinternet in action: methods of Iranian censorship

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

1

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.

2

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.

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:

1

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 lot of effort, blocking the protocol entirely — or accepting that they can't censor specific services.

2

Encrypted Client Hello. It 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.

As for the DNS-based censorship, several protocols were presented as able to bypass it:

DNS over TLS (DoT), which 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's and Google's DoT endpoints have also faced blocks.

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.

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.

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, major cloud 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/

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.

Some of the aforementioned methods work in the medium term, and others in the long term. Unfortunately, many of them depend on big cloud service providers. 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. However, running your own infrastructure or using Outline SDK can make some of these methods simpler to implement. In the second section of this report we focus on self-hosted and community-managed circumvention tools and Outline SDK, as possible ways to communicate in a “pre-Splinternet” environment.

Stone soup: Russian national technologies of splinternetization

The “Iranian” transition from a centralized censorship model based on blocklists to a decentralized blocking architecture based on deep packet inspection (DPI) — hardware installed in each local provider’s network — is quite similar to another budding splinternet model: the Russian sovereign Internet.

While in our first report we have extensively covered the history of Runet’s splinternetization, in this report we will dive into details of two specific technologies used in the Russian Splinternet: the domestic certification authority (CA) and the National Domain Name system.

A brief summary of the history of Sovereign Runet

The Russian case significantly differs from Iranian or Cuban examples, and is described in literature as a “decentralized control” model. 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.

However, there are also similarities between splinternets. As in the case of Iran and Cuba, 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 150 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. In addition, as of March 1, 2024, regulatory authorities prohibit media from publishing instructions on circumventing blockages.

Russian National Certificate Authority

In 2022, after Russia's full-scale invasion of Ukraine started, many sanctions were imposed on Russia in a short period, including economic sanctions prohibiting Western IT companies from providing services to some Russian companies. This also meant that Western certificate authorities cannot offer or issue certificates for Russian domain owners. Several major CAs, such as DigiCert, GoDaddy, and IdenTrust, have issued statements that they are ceasing to provide such services. One of the centers even started revoking certificates already issued. Russian domains were considered sites in the domain zones .ru, .rf, etc. Russia responded by accelerating the transition towards a domestic certification center. Similar attempts have been previously made in Kazakhstan and Iran.

A Certification Authority requires browsers to trust the certificates it issues to be valid. Today, neither Google Chrome, Firefox, nor Safari trusts Russian certificates. Opening a Russian state-owned or state-affiliated website through these browsers, results in a warning to the user about a potential security risk. These websites can open only in Yandex.Browser or the Atom browser — Russian products that already contain the state certificate.

Control over a CA opens the way for an attack called HTTPS interception. HTTPS interception already happens on most corporate closed networks to control employees' online behavior. But on a national scale HTTPS interception grants the censor advanced control over the networks, as it opens up unprecedented possibilities to intercept private communications, forging contacts and availability, aids in orchestrating large censorship events and shutdowns. HTTPS interception is also hard to detect and to circumvent.

As of today, the Russian TLS certificate is exceptionally modest in popularity — only six hundred domains have implemented it. However, the government consistently promotes this certificate among users, mainly through banks. Therefore, we can expect a much more severe growth in adopting this certificate in the future.

Russian National Domain Name System

The Sovereign Internet Law adopted in 2019 stated that Russia should be able to manage Runet's DNS root zone autonomously. The legitimation for this project was that if Russia is disconnected from the DNS system at the will of the Western countries, Runet should continue to exist as a separate network. And on March 28, 2022, such a system was established. Today it works in a backup posture: providers will turn to the national system if access to the global DNS system is lost. Connecting to NDNS is mandatory for ISPs, social networks, and other services.

What is NDNS theoretically capable of?

1. DNS poisoning and substitution,
2. server compromise and record replacement,
3. fake servers,
4. BGP hijacking,
5. advertising statistics collection
6. surveillance by DNS fingerprint.

On January 31st, 2024, the .ru zone in DNS was signed incorrectly for two hours, making all .ru internet resources unavailable. The global domain operators quickly resolved this issue, but during the problem period, NDNS turned off DNSSEC validation on the Russian resolvers.

Authorities reported that NDNS users were not affected. This incident prompted the authorities to issue a paper stating that all ISPs must use the NDNS system as their primary system in the future, although not immediately. This experience led to the resolution of the previous problem with the signature of the root zone. As a result, in Russia, only government-approved DNS resolvers are now allowed, and all users and services must use their lists directly, with no caching or validation.

What comes next? Russia is implementing internet restrictions in a different way than Iran and Cuba. However, a specific set of technologies facilitates this fragmentation. Two such technologies are the domestic certification authority (CA) and the National Domain Name System, which are Russia's contributions to this collection.

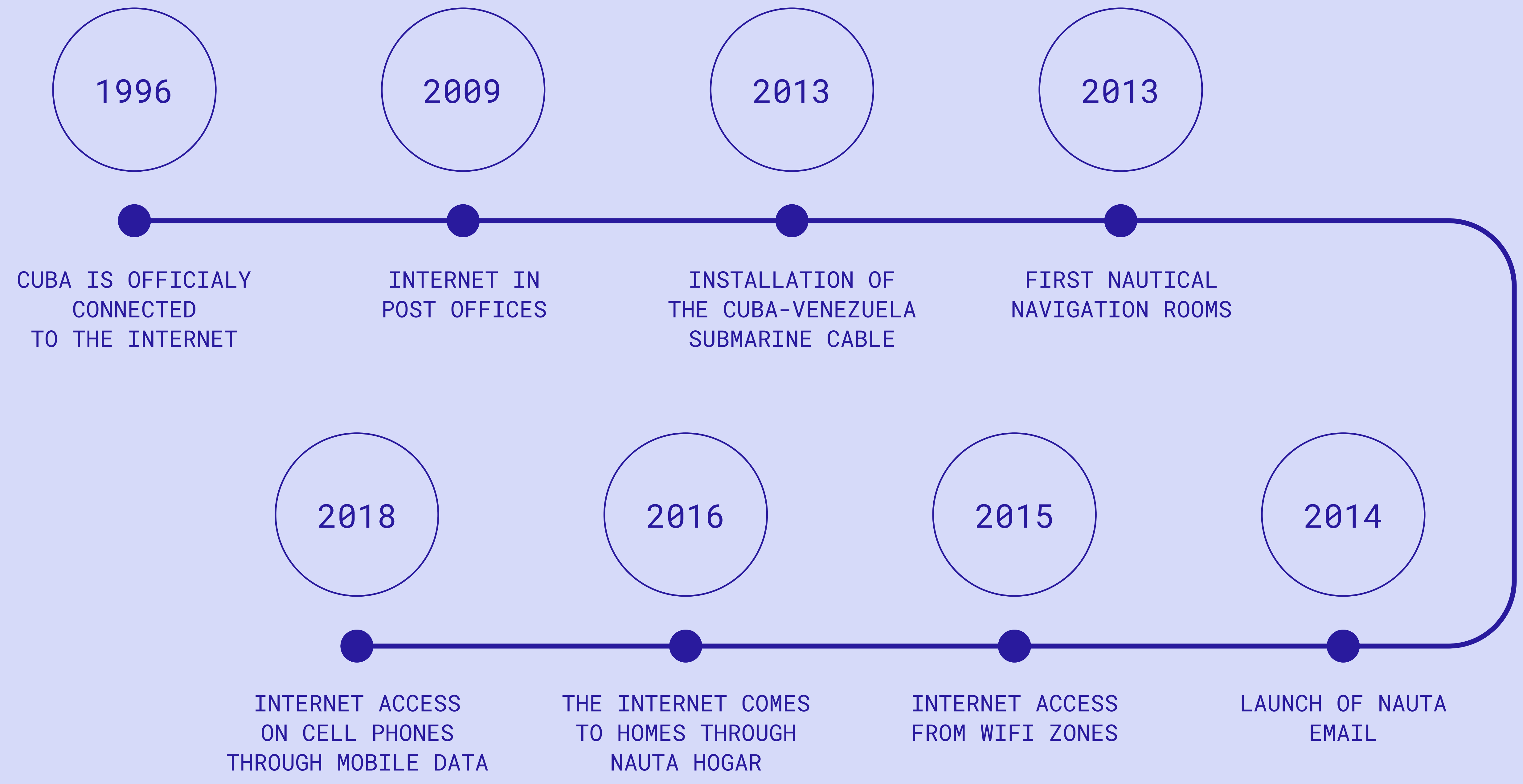
The authorities envisage creating a splinternet by gradually replacing all core elements of the global Internet infrastructure with national ones, akin to the folk tale of stone soup.

Cuba’s digital evolution: from an Intranet to the Internet and back

Founded in 2022, The Cuban Internet freedom project Diktyon presented an analysis of the Cuban digital landscape and its transition from an intranet to the Internet. Dyktion monitors daily access to websites that are potential targets of censorship, as well as access to circumvention tools (Tor, Psiphon) and communication platforms such as WhatsApp, Facebook Messenger, Telegram, and Signal.

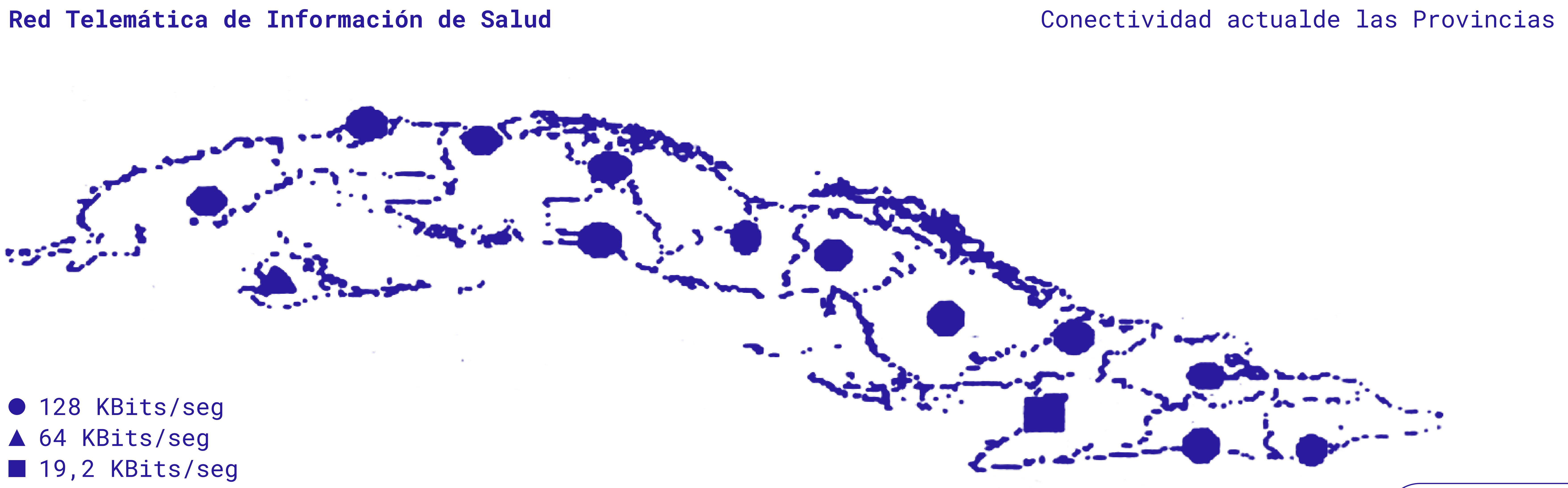
Cuba has a long history of stringent Internet control. Its unique approach to network governance is influenced by foreign sanctions but is primarily characterized by multi-layered local government control. This control combines economic, legal, and technical measures to maintain its grip on the country's digital landscape.

Chronology of Internet in Cuba


1996
CUBA IS OFFICIALY CONNECTED TO THE INTERNET
2009
INTERNET IN POST OFFICES
2013
INSTALLATION OF THE CUBA-VENEZUELA SUBMARINE CABLE
2013
FIRST NAUTICAL NAVIGATION ROOMS
2014
LAUNCH OF NAUTA EMAIL
2015
INTERNET ACCESS FROM WIFI ZONES
2016
THE INTERNET COMES TO HOMES THROUGH NAUTA HOGAR
2018
INTERNET ACCESS ON CELL PHONES THROUGH MOBILE DATA

Cuba was officially connected to the Internet in 1996 using a satellite connection from a single point in Cuba near Havana, which is still in use. However, widespread access to the Internet was not available until 2009.

As a result, a black market for Internet access quickly emerged. For instance, university professors would have a home modem and allocate the connectivity hours they had available to sell them on the black market. In the meantime, all the departments had internal networks, intranets. Access to a university's network also granted access to materials from other universities. The same was true for the Ministry of Culture, the Ministry of Health, and so on. Moreover, some of these intranets, such as the Informatica network, still exist today.


Red Telemática de Información de Salud
Conectividad actualde las Provincias
● 128 KBits/seg
▲ 64 KBits/seg
■ 19,2 KBits/seg

Informed (2003)

In 2009, Fidel Castro's brother became president, and things changed. This year, the country's residents were able to access the Internet at post offices — they installed computers and started selling tickets with Internet hours. An hour of Internet access cost half the minimum wage, nine dollars.

In 2011, an underwater cable connected Cuba with Venezuela and Jamaica, but the authorities decided to conceal this fact for two years, waiting for the outcome of the Arab Spring. So, in 2013, 118 navigation rooms had Internet access, but it was still highly costly. In parallel, the development of intranets, which cost 13 times cheaper than Internet access, continued.

So, the Internet in Cuba emerged as a state-controlled network. This led to the creation of national "equivalents" of popular international services: a Wikipedia analog Ecured contains the official version of the country's history and other information; Nauta Mail, a local e-mail system run by the national ISP, which is run by the government; and APKlis, a regional app store, only contains approved applications; a local equivalent of Google's App Store.

Against this backdrop, the civilian network El Paquete emerged in Cuba in 2008. It was a physical package from Miami through Mexico, a one-terabyte hard disk with the latest information — games, movies, news, etc. The package was updated every week. There were different versions of this package. Some were ultra-censored (and could include pornography or politically radical information), while others were not so censored.

In 2014, the government launched Nauta Mail, which became a great alternative to expensive international phone calls. People have also started using this mail engine for creative ways to access the web, from shortcodes to automation services like IFTTT. Several apps like Apretaste! allowed access to Internet navigation through email. Later on, Delta Lab, a fork of Delta Chat messenger (which uses email for instant messaging) was developed and became popular as it offered bots and mini-games.

In 2014 website blocking began. One of the first websites to block was the Generación Y blog of famous dissident and journalist Yoani Sánchez.

In 2015, the so-called "Parknet" was born with the launch of public Wi-Fi zones to purchase Internet: the price was halved to $2 per hour. The official name of this project was 'Nauta Wi-Fi Service'. It was still costly because the minimum salary wasn't raised.

Another big issue with those parks was privacy. Authorities have installed cameras everywhere. There were cases when they were used to peek at the password that an activist entered on his laptop. As we know from independent investigations, cameras were imported from Russia or China with a decent resolution. Nevertheless, parks have also become territories of user creativity. People living nearby began to retransmit Wi-Fi from the park — to resell it. Such street networks stretched for kilometers. And although the speed inevitably dropped, the price was also low — 50 or even 25 cents.

In 2016, connecting the Internet to your home via ADSL became possible. However, that possibility was available in a few areas — and obviously only in places with phone lines. The cheapest tariff cost $15 for 30 hours of connection, and the most expensive was $70. With this evolution, censorship has also started to expand. By 2017, 41 websites were censored via DPI.

In 2018, mobile data was allowed on mobile phones but remains very expensive ($7 for 600 megabytes), and real IDs are required for registration, as in Iran or Russia.

Today, Cuba has blocked 61 websites via DNS, TCP, HTTP, Server Name Indication filtering, and DPI. For example, the regulator interferes with the TLS handshake structure and returns an HTTP 500 error. In addition, during the March 2024 protests, the authorities staged a "partial shutdown" — slowing down mobile internet speeds from 3G to 2G and thus limiting the sending of multimedia files, as well as disrupting several popular VPN services. Ookla's Speedtest Global Index Cuba last in both mobile and fixed Internet connection speeds.

SECTION 3

Tools for Splinternet 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.

Before Splinternet: Community-managed circumvention tools and network measurements

In hybrid environments (or “pre-splinternets”) where connectivity with the global network is throttled but still present, more traditional circumvention tools such as VPNs or overlay networks may be helpful. However, SplinterCon’s area experts argue that states are constantly improving their capacity to detect and successfully filter or slow down popular VPN protocols and apps.

This is why, based on our analysis of VPN solutions presented at SplinterCon, we conclude that virtual private networks for highly censored areas should ideally meet several requirements:

smaller scale with less users sharing the same IP-address (makes it harder for censors to detect and block)

community-managed and decentralized token distribution based on a web of trust

using new generation of obfuscation protocols

constantly iterating from end-user feedback (not only based on automated or manual network measurements, but also based on qualitative feedback from users on the ground that might report about previously unknown issues and novel, hardly categorizable forms of blocking)

cooperating with other projects and sharing network measurement data (to advance understanding of the censors’ capacities and to facilitate deployment of new circumvention solutions)

The three VPN or overlay projects presented in Brussels fall under these criteria and offer potentially viable solutions for highly censored areas “before Splinternet”.

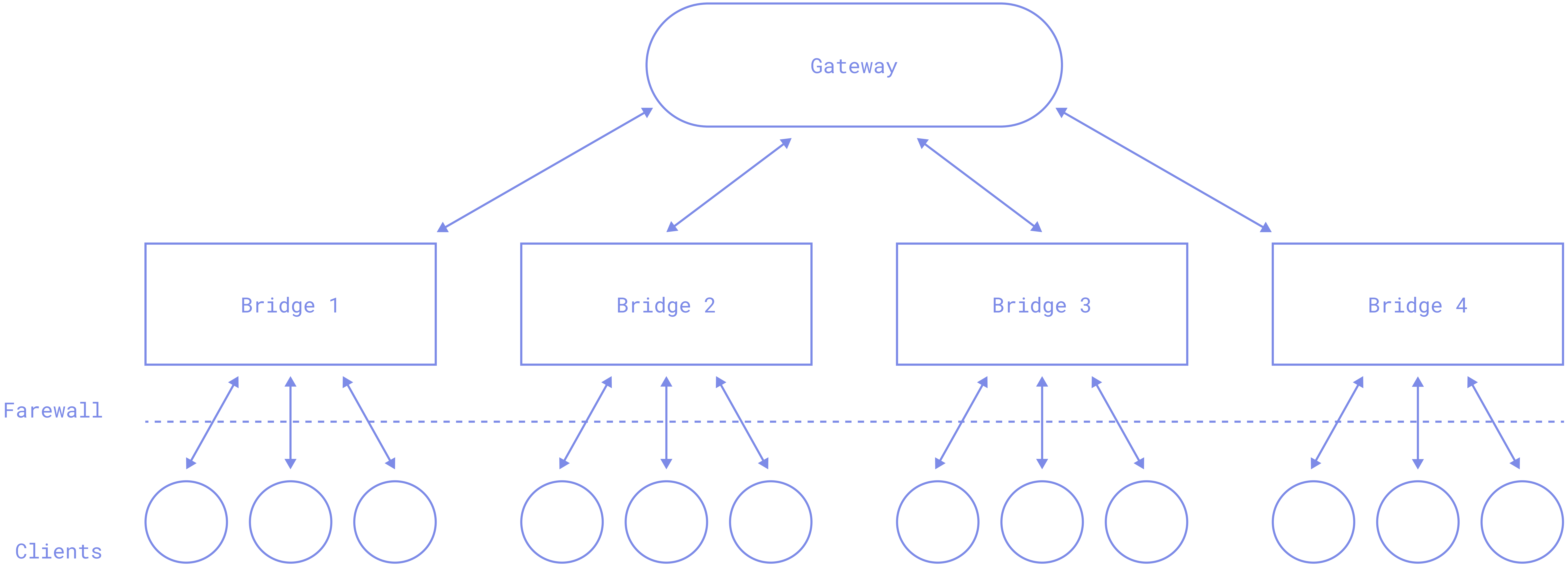
Solitech is an activist community-oriented VPN project from the founders of LEAP Encryption Access and Privacy, focused on users in Russia as their testing ground but also potentially promising for Iran and other pre-splinternet areas.

Besides a VPN service, Solitech is running a series of regular network measurements to detect protocol throttling, analyze speed and quality of connection and collect qualitative feedback. In collaboration with OONI they introduced a new kind of test called tunnel-telemetry (see Proof of concept source code). It is a research-action project that offers a way to improve our understanding and prognosis of censors' next steps (such as, for instance, "blanket blockings" when IPs are blocked in large ranges).

Solitech's innovative approach to measuring VPN accessibility consists in combining manual and automated testing and also collecting verbal feedback from users located inside Russia in different regions across the country. Initially limited to 5 testers, their testing network has grown considerably and now counts more than 30 people testing twice a week from various vantage points not only in central Russia, but also in areas with strong indigenous movements that are frequently affected by shutdowns and other local connectivity issues.

In collaboration with the project DPI Detector run by Roskomsvoboda, a Russian internet freedom and advocacy NGO, they are working on new DPI resistant obfuscation protocols. They propose invite-only token distribution for small regional user-groups, inspired by projects such as Amnezia VPN or VPN Generator.

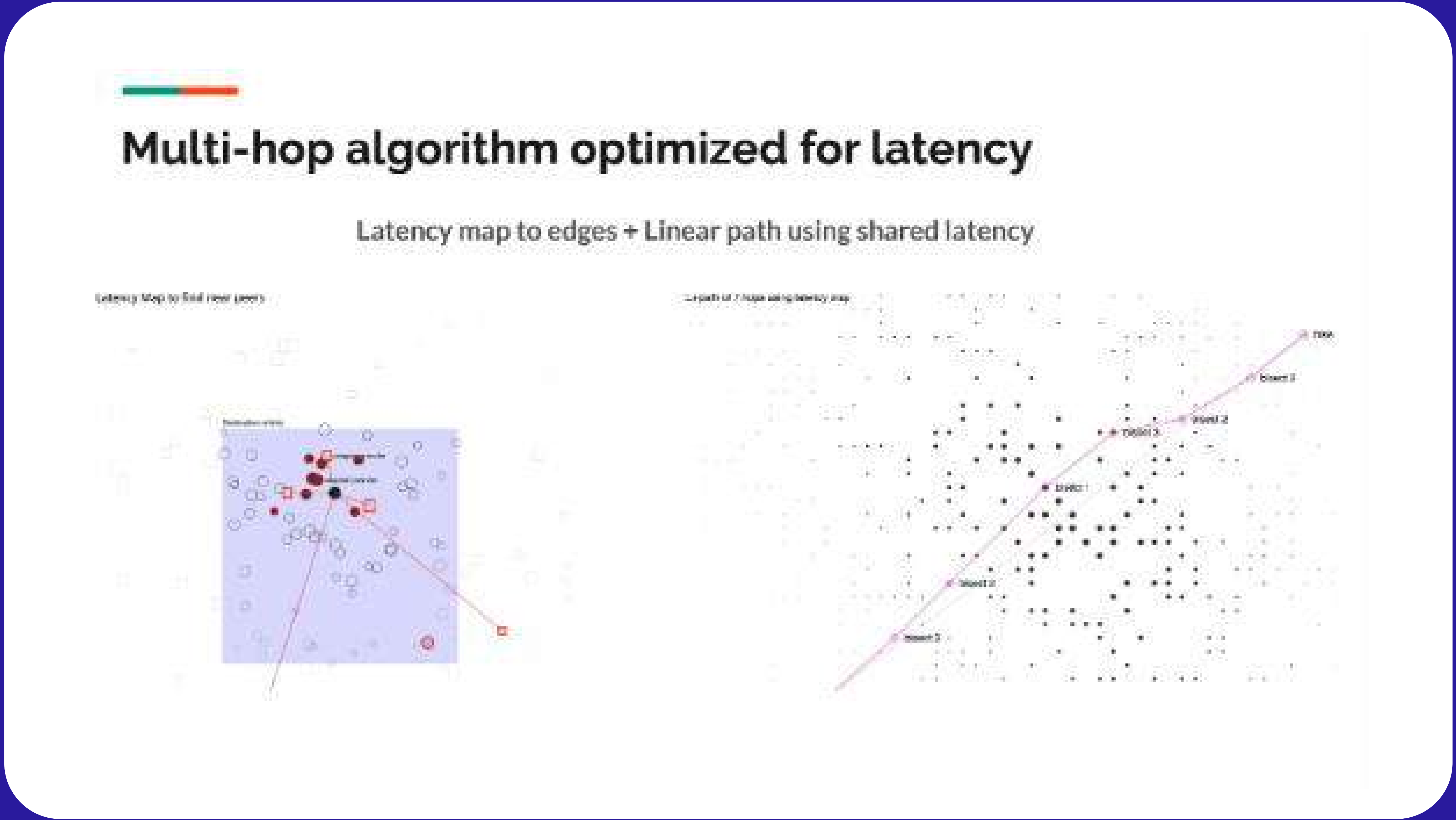
Regional and small-scale user pools



BringYour

BringYour is a community-run decentralized overlay network with focus on access, privacy, and safety. BringYour supports Multi-hop algorithm optimized for latency and multi-path routing to find the best routes for each destination.

It allows users to actively participate in the network and become a “hop” of encrypted traffic, enhancing anonymity of internet access for themselves and other BringYour users. Encryption makes it impossible to read or access the content of the traffic that goes through community-run hops.



Multi-hop algorithm optimized for latency

Latency map to edges + Linear path using shared latency

BringYour relies on web standards (HTTPS1,2, WebRTC) and also supports various extenders to make it harder to block. It supports built-in payments for community service providers who want their users to share costs of infrastructure. It also gives a lot of modularity for administrators and users to control how their community is using the service. It can disable unencrypted protocols, disable specific protocols that may hurt the community (e.g. BitTorrent), disable unused protocols for mainstream — most restricted ports, set up a rate limit for new connections per contract.

Outline SDK

Outline SDK offers reusable, composable and cross-platform components to empower your app 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 splinternet-lilke or “pre-splinternet” situations. It offers libraries for transports (shadowsocks, tls, websocket), proxy protocols (shadowsocks, 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.

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 first category of tools offering opportunities for Iran and other splintered areas is satellite datacasting.

Satellites for Iran: challenges and opportunities

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. This panel illustrated the many possible use cases for innovative wireless tech, but it also demonstrated some limits and opened pathways for further collaborations

GEO&LEO Satellite Internet: 2-way

Border LTE coverage: 2-way

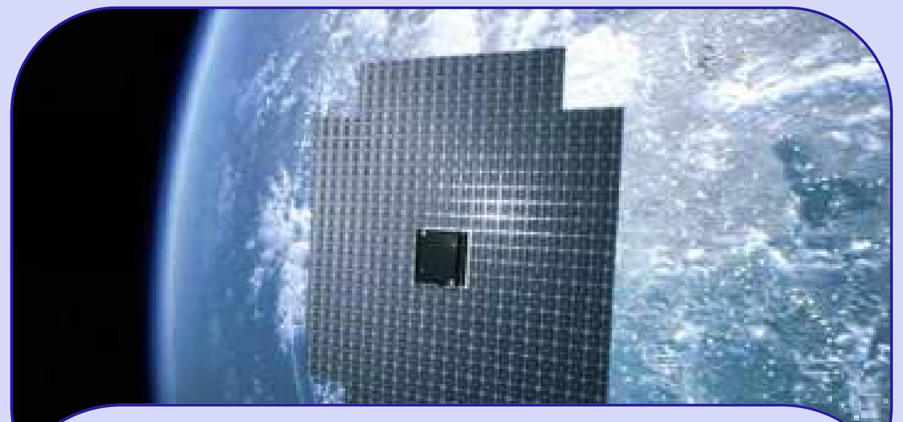
Data over DVB-T(2): 1-way within 100km from borders

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



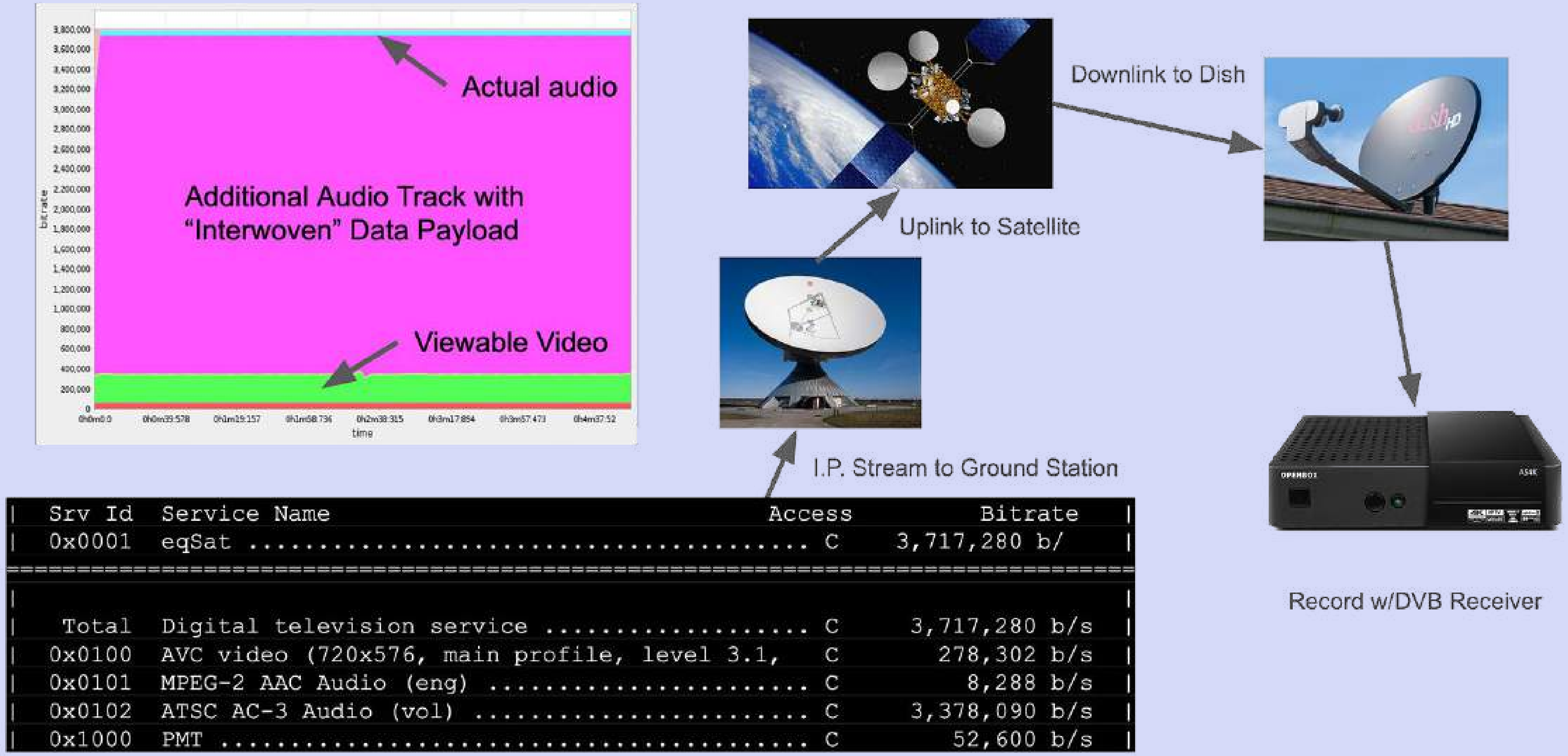
5G (3GPP) Broadband: Phones to LEO, 2-way

eQSat

eQsat is a one-way datacasting project deployed by eQualitie. It is dedicated to enabling unfettered digital content delivery, using advanced technologies to overcome internet shutdowns and digital isolation in multiple regions worldwide.

eQsat uses low-cost, easily accessible satellite communication technologies to deliver digital content in areas with restricted connectivity. This technology is particularly effective in circumventing censorship, bypassing local infrastructure controlled by restrictive regimes. Users can receive websites, videos, and software updates without needing a traditional connection to the global internet. eQSat can deliver up to 2 gigabytes of new content every day, with potential to rapidly scale up.

eQsat relies on a decentralized ecosystem called Ouinet. Selected partner media websites are scraped regularly, then packaged and sent over television sattellite channels. Local receivers record the data, unpack it on a PC and inject it in the Ouinet network. Thereafter users of the Ceno browser (covered in the last section of this report) can browse these websites as before, directly from the national network cache.



```
|   Srv Id  Service Name                                  Access       Bitrate  |
|   0x0001  eqSat ...................................... C    3,717,280 b/     |
================================================================================
|                                                                               |
|    Total  Digital television service ................. C      3,717,280 b/s  |
|   0x0100  AVC video (720x576, main profile, level 3.1,  C        278,302 b/s  |
|   0x0101  MPEG-2 AAC Audio (eng) ..................... C          8,288 b/s  |
|   0x0102  ATSC AC-3 Audio (vol) ...................... C      3,378,090 b/s  |
|   0x1000  PMT ........................................ C         52,600 b/s  |
```

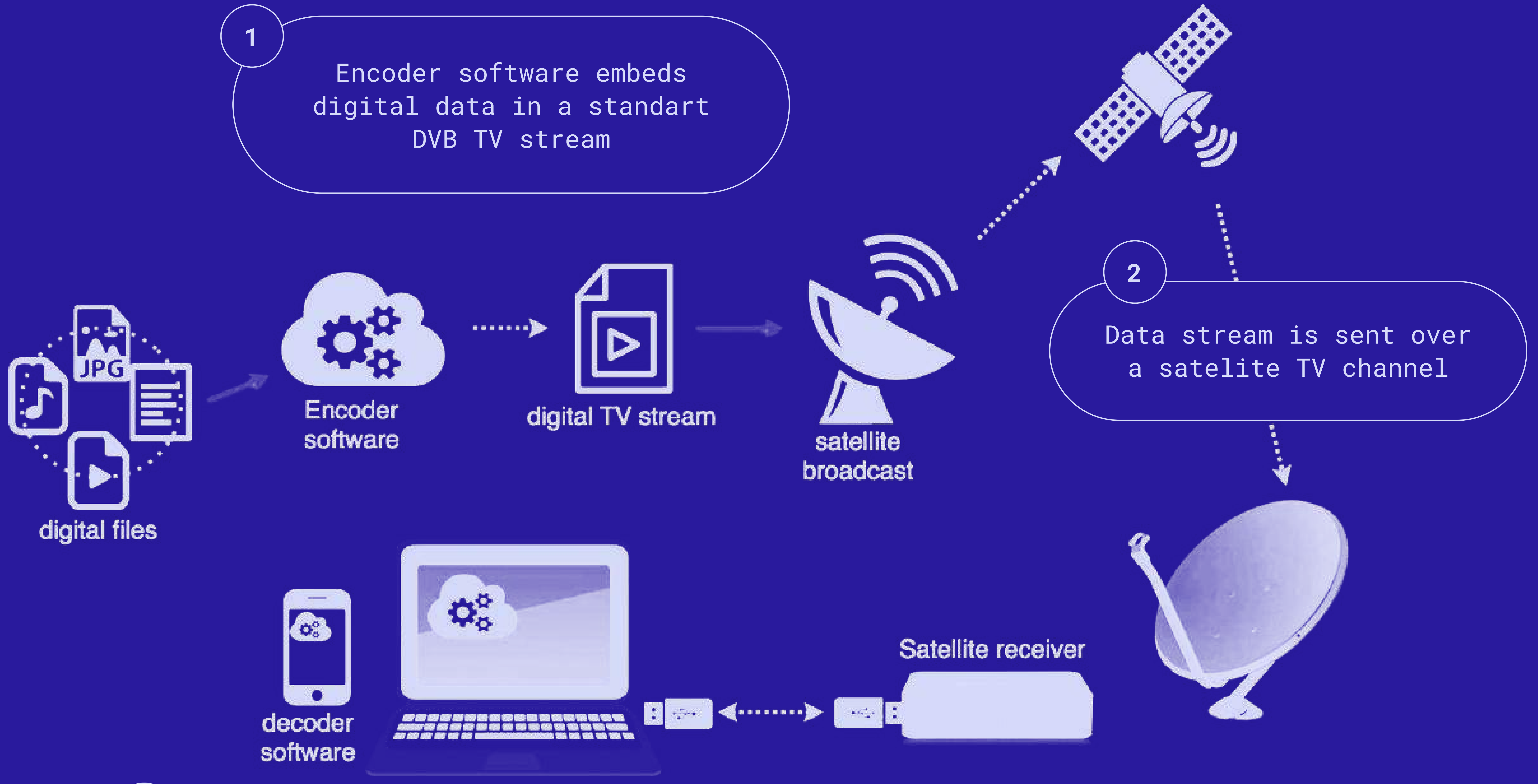
Toosheh

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 websites.

Use Cases:

- 5M Users
- 7GB daily bundles
- Interner Shutdown Solution



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

Starlink for Iran

The third solution presented at the panel suggested using Starlink terminals to deliver international content to Iran and also let Iranians communicate beyond the NIN borders.

Nowadays there are 5000 Starlink terminals inside Iran, but there are a few major challenges, namely high cost of terminals and subscriptions. Payment may also be tricky and is done mostly via cryptocurrency.

Starlink is being used more and more. Detection is quite difficult by local authorities due to the higher frequency used, and the phased array antenna which focuses the EMF energy into a sharper angle. Based on a report from Iran's Parliament Research Center, they have imagined a mesh network with Starlink.

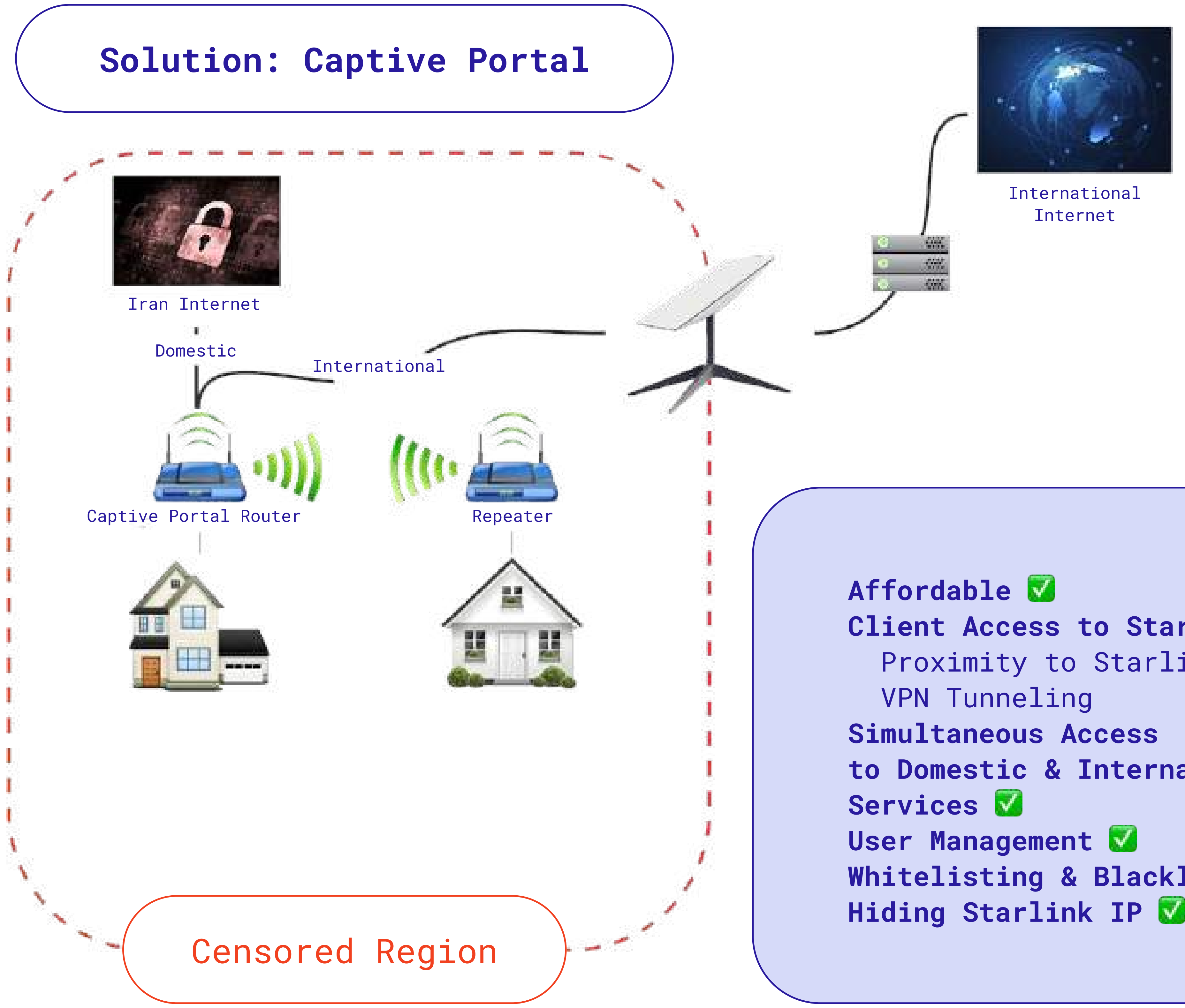
Core features for an acceptable solution to internet shutdowns in Iran include:

- Affordability
- Client access to starlink
- Simultaneous access to domestic and international services (as many essential services are only on the domestic network)
- User management
- Whitelisting and blacklisting / split-tunneling
- Ability to hide starlink IP (because starlink has limited IP ranges and could be easy to identify)

A prerequisite for using such a solution is a Flashing Wireless Router with OpenWRT firmware

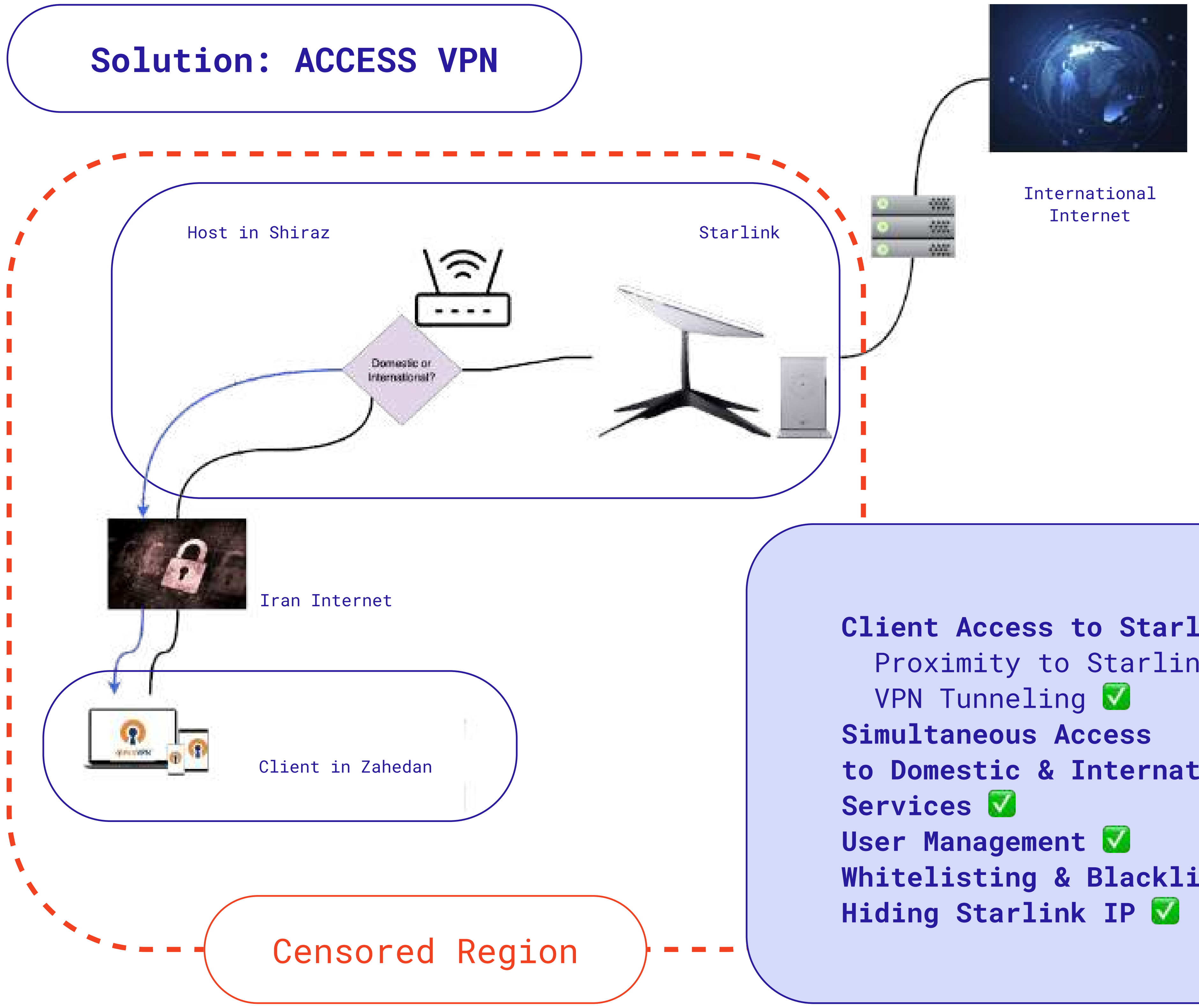
Two main types of solutions were discussed: a captive portal and a private access VPN.

Solution: Captive Portal



- **Affordable ✅**
- **Client Access to Starlink**
  - Proximity to Starlink ✅
  - VPN Tunneling
- **Simultaneous Access to Domestic & International Services ✅**
- **User Management ✅**
- **Whitelisting & Blacklisting**
- **Hiding Starlink IP ✅**

Solution: ACCESS VPN



- **Client Access to Starlink**
  - Proximity to Starlink
  - VPN Tunneling ✅
- **Simultaneous Access to Domestic & International Services ✅**
- **User Management ✅**
- **Whitelisting & Blacklisting**
- **Hiding Starlink IP ✅**

Section 3: Network technologies

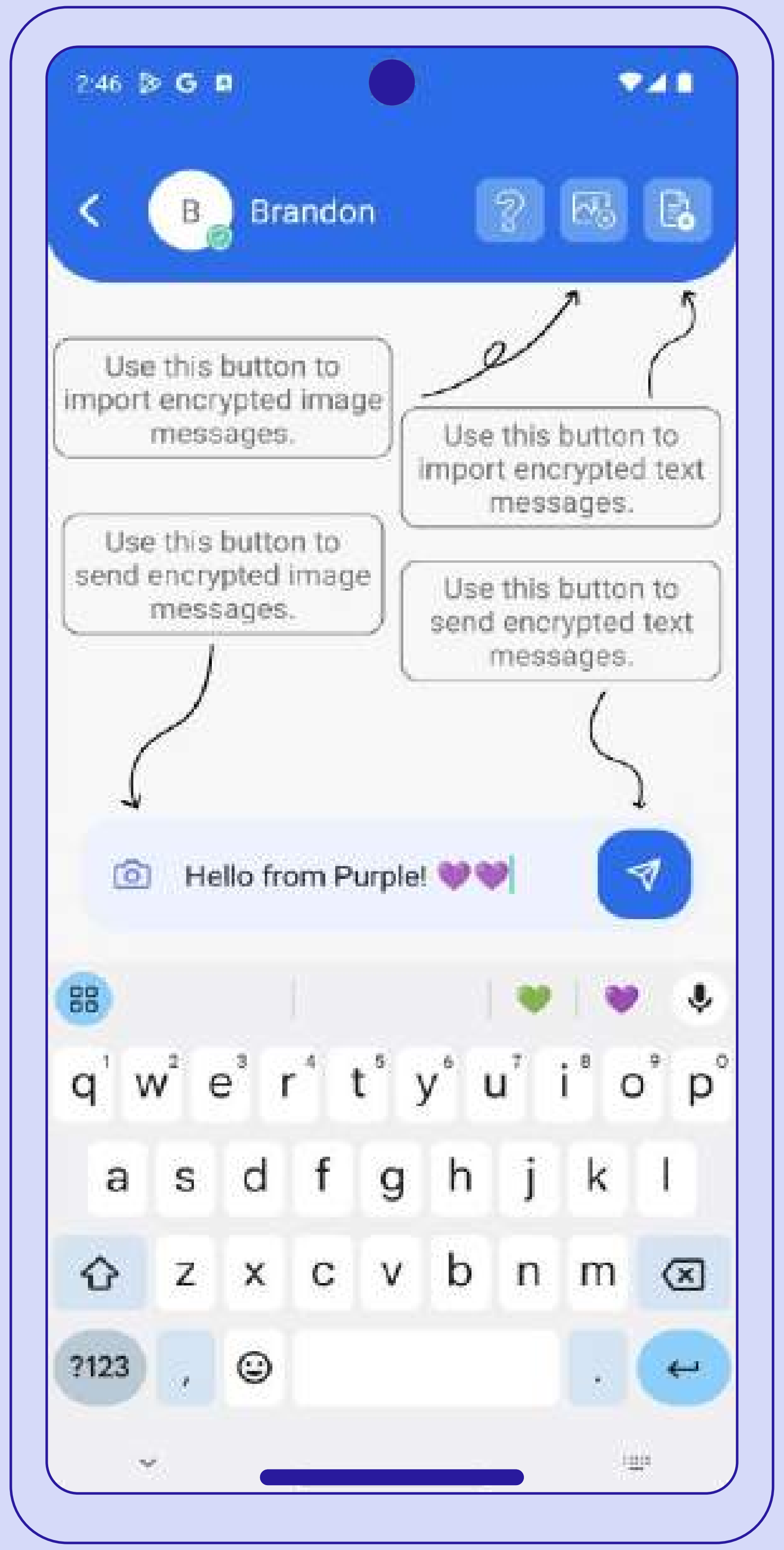
While satellite technologies open many possibilities for an informational breakthrough, they might imply a rather high entry barrier for end-users and require additional equipment, such as satellite dishes, routers and dedicated software. Other technologies presented at SplinterCon included new protocols and end-user oriented apps with relatively low-entry access, designed specifically for Iran or similar splinternet models. Some of these projects focused on circumvention (Outline), others on communications (such as Qaul or Nahoft) while others proposed an ecosystemic approach (such as Awala, dComms or the eQsuite – Ceno+Ouicrawl).

Qaul.net

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.

Nahoft



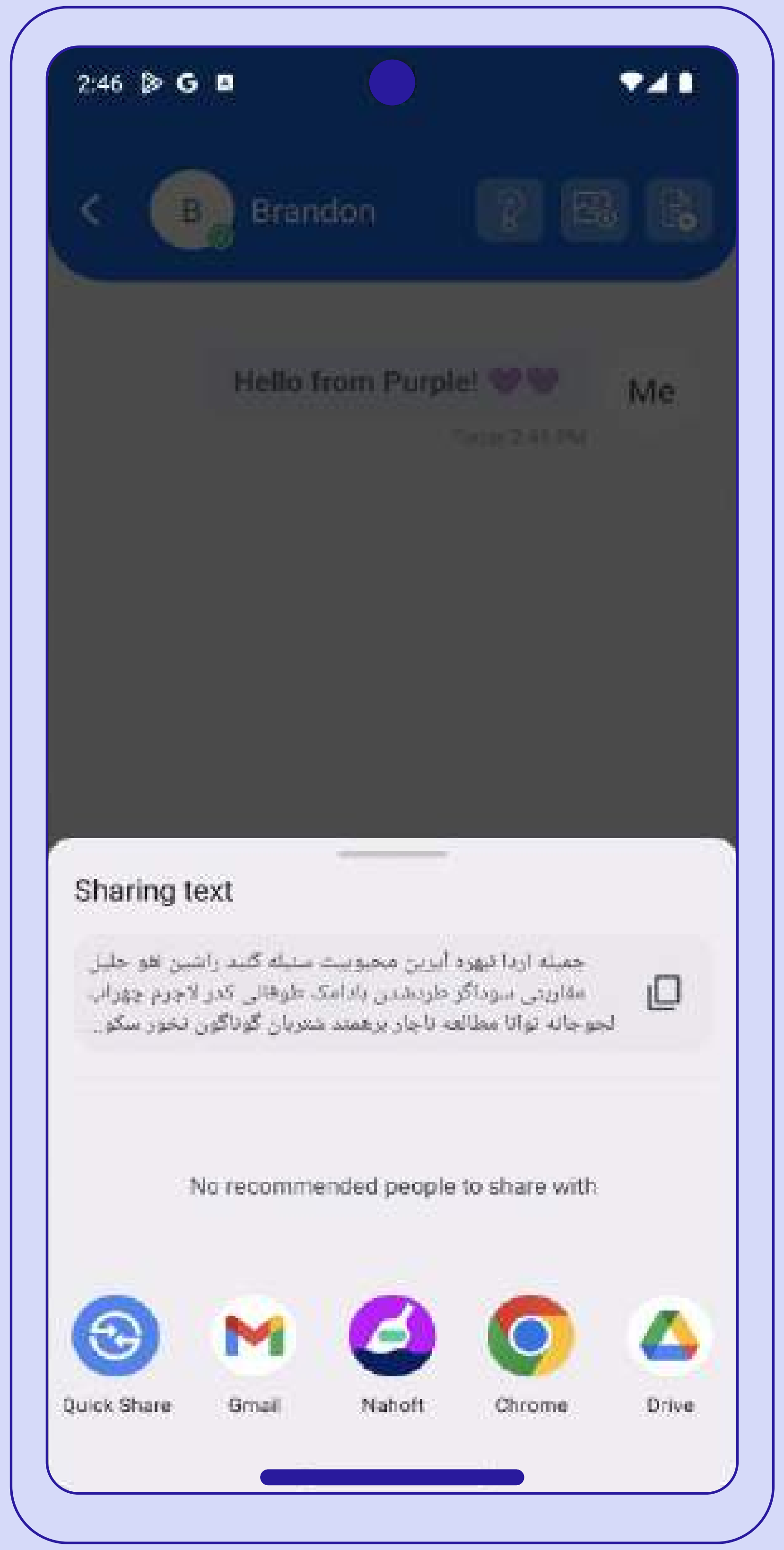
Use this button to import encrypted image messages.

Use this button to import encrypted text messages.

Use this button to send encrypted image messages.

Use this button to send encrypted text messages.

Hello from Purple! 💜💜

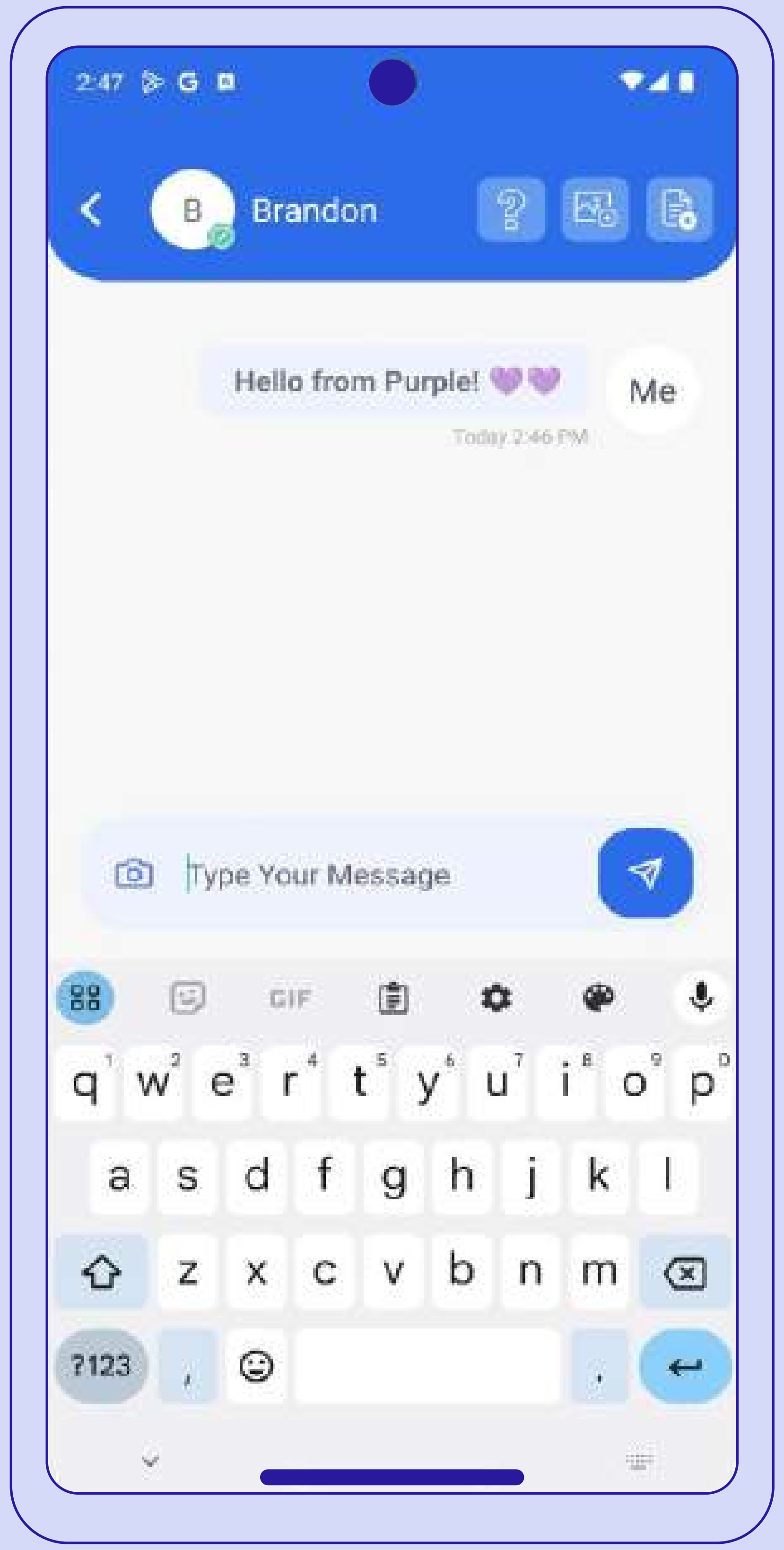


Hello from Purple! 💜💜 Me

Sharing text

جمله اردا قهوه آیین محبوبیت سیله گند راشین هو حلز
مقاورتی سوداگر طردشدن بادامک طوفانی کدر لاجرم چهراب
لحوجانه توانا مطالعه ناچار برهمند شتربان گوناگون نخور سکو.

No recommended people to share with



Hello from Purple! 💜💜 Me

Today 2:46 PM

Type Your Message

Nahoft is an encryption app made for Android and iOS. It lets users easily encrypt private messages into a string of Persian words or in a photo before sending it safely via another messaging app. Therefore, Nahoft is not a messenger, but a tool for encrypting messages. It is also fully offline. It is not using any server to send or receive or encrypt your messages. The special destruction code lets you purge all your data if entered during login.

Awala

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 decentralised 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.

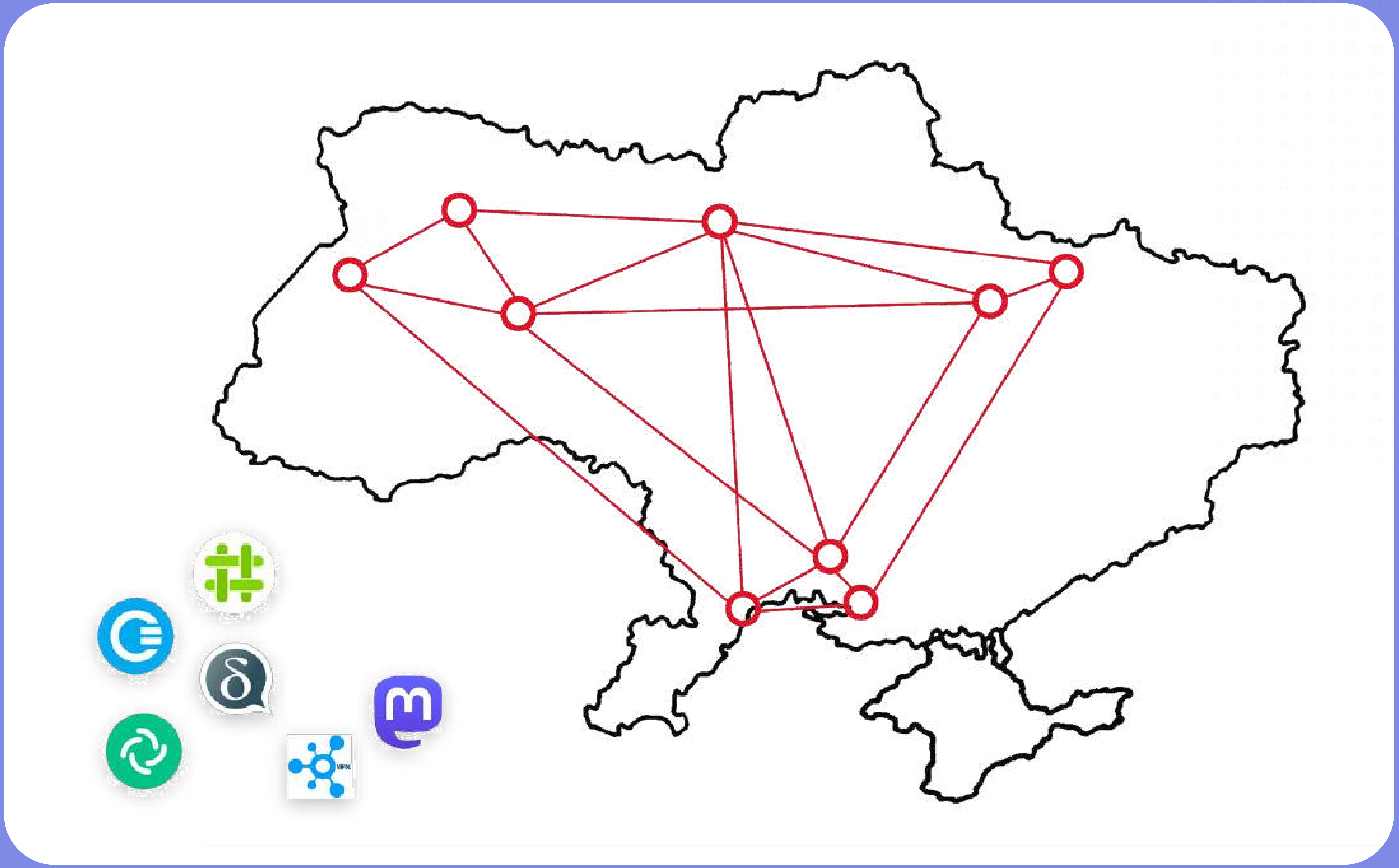
Awala relies on a network of so-called couriers. Awala is decentralized with a federated architecture where servers (called “gateways”) act as brokers.

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.

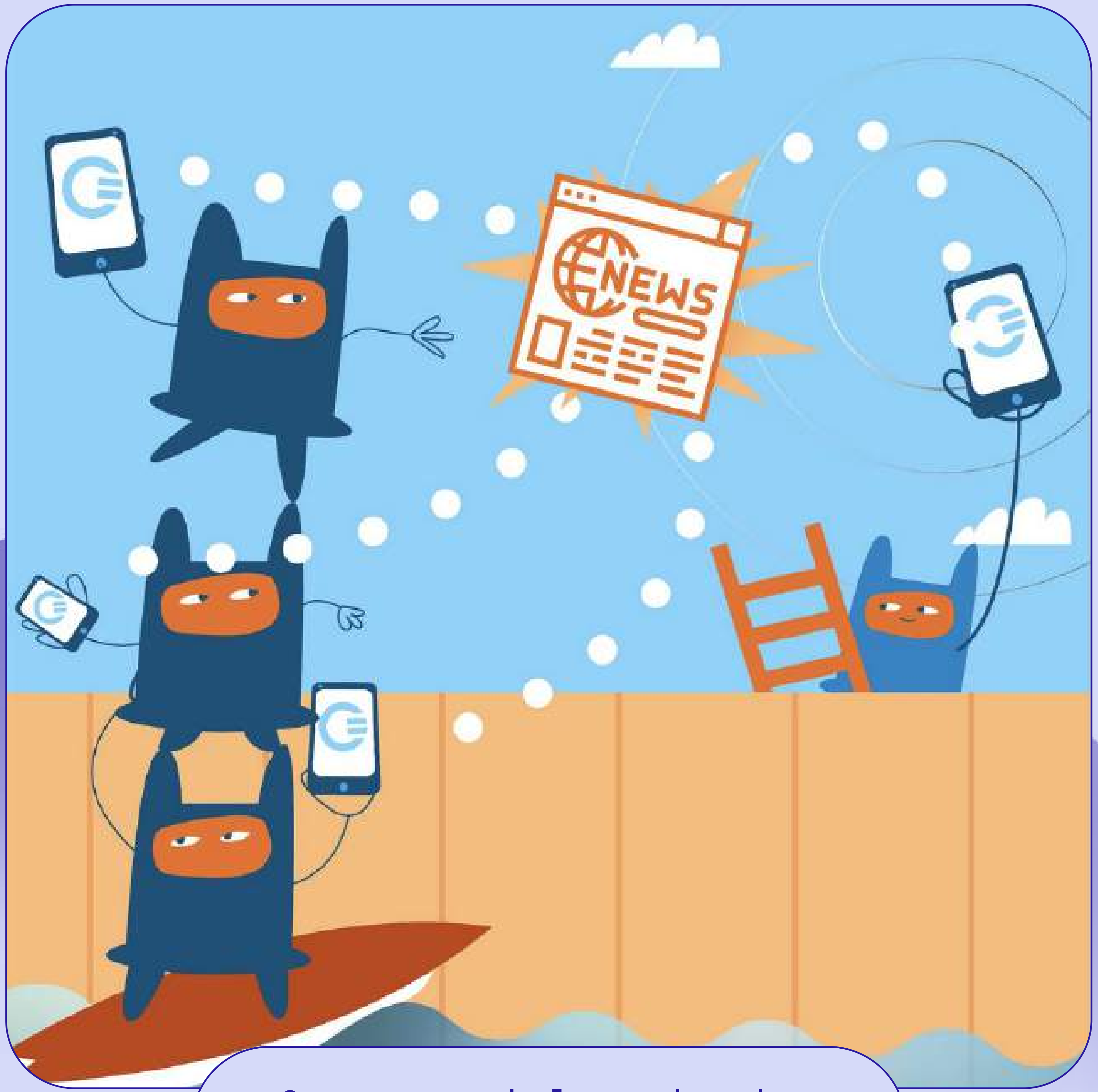
dComms



dComms stands for decentralized communications.
It is a containerized bundle of decentralized and federated communications tools capable of working in a Splinternet or shutdown situation — without any connection to the global network. eQualitie operates ten servers in Ukraine and one in Iran to support this system. The package includes Element (with a web version that doesn't require separate installation), Ceno Browser, Mastodon (also with a web version), Delta Chat, and NewNode VPN. These servers are federated, allowing users in different cities to communicate with each other. Even if one server goes down, the dComms network remains connected.

One of the benefits of this system is that all the services are not owned by major tech companies and do not gather excessive user data. Additionally, censorship targeting Matrix or Mastodon central servers will not impact dComms users.

Ceno



Ceno users help each other reach censored content

Once retrieved, content is shared inside the network peer-to-peer

Ceno Browser is part of an ecosystem created by eQualitie to provide network access in a Splinternet or shutdown situation. It is a mobile browser based on Firefox Mobile and includes the Ouinet network library. This library enables the browser to use multiple methods to access a website. If the website is accessible, the browser can open it like any other browser. However, if the website is blocked, Ceno will attempt to access it through a network of bridges. Ceno users in other countries will redirect traffic through their devices to help bypass the blockage.

Additionally, the traffic will pass through an injector — an intermediate server that will ensure the requested page is genuine and sign it with its key. The signed web page will then be stored in the Ceno Browser's cache and made available to other users via the BitTorrent protocol. Adapting to challenging blocking conditions allows the browser to remain functional in complex environments.

To support the distributed cache, eQualitie creates and maintains a centralized cache using the Ouicrawl mechanism. It regularly caches the sites of 43 independent media — a list can be found here — so updated copies of these sites are always available on the BitTorrent network. To ensure this content's availability, which is highly sought after during political events, eQualitie uses the eQSat satellite channel, as described in this report.

The Ceno + Ouinet + Ouicrawl + eQSat ecosystem enables users to maintain access to websites that the government seeks to censor and continue receiving impartial information even when completely disconnected from the global network.

SECTION 4

Blockathon

Living in a splinternet 🎶 — a demo

SplinterCon in Brussels introduced the Blockathon - a simulated shutdown scenario to serve as a live demonstration and as a future test bed for testing new methods and protocols to break out of a splintered network. The setup is relatively 'simple' — we create a wireless network that is running open source censorship software (or deep packet filtering, if you prefer). Participants connect to the wifi network and try to use their existing circumvention tools and knowhow to break out.

The first scenario simulated a regular censorship event - deploying all available filtering rules against the website example.org Quite a number of participants were able to reach it using VPNs and Ceno browser. The second scenario was much tougher, we blocked the entire IP range of the Internet apart from the one address that is hosting example.org The task was to reach any other website.

Since all other IPs addresses were blocked, no one could connect to their VPN server. The Ceno browser also could not reach an injector or a bridge user. Everything was blocked! This was an example of a 'white list' shutdown, one of the gloomiest and probably most realistic examples of future long-term shutdown scenarios — nothing is allowed apart from a pre-determined number of addresses.

Luckily, one of the participants had figured out that since example.org was resolving in the browser — it meant that DNS was also running (port 53, protocol UDP). They then tunneled an OpenVPN connection (we don't have fingerprinting rules for the OpenVPN protocol as yet) over port 53 and were able to connect to a server and get out! Another participant used a similar strategy with the Iodine library.

The Blockathon had proven itself as an interesting and challenging demonstration of the splinternet experience. Many questions as to the privacy and ethical considerations of this effort remain and were discussed during the meeting. How should eQualitie and its partners manage the (currently) open source stack of censorship software it is developing for the purpose of the blockathon and finding new vulnerabilities/opportunities to break out; how should we document and publicize new findings; who owns and how do we share them and how widely? The growing Splintercon community of practitioners will be involved in helping to consider and propose answers to these questions in the coming months.

Further Blockathon development will involve simulating the complexity and chaos of the Internet itself, looking to adapt and build on the Seed Emulator package of virtualizing key components of the Internet, such as IXPs, BGP routers, DNS infrastructure and so on. The next iteration of the Blockathon will be run at this year's Global Gathering. See you there!