1M5

UNCENSORED COMMUNICATIONS

1M5 supports freedom of speech through censorship resistant intelligent routing across a number of peer-to-peer anonymity networks.

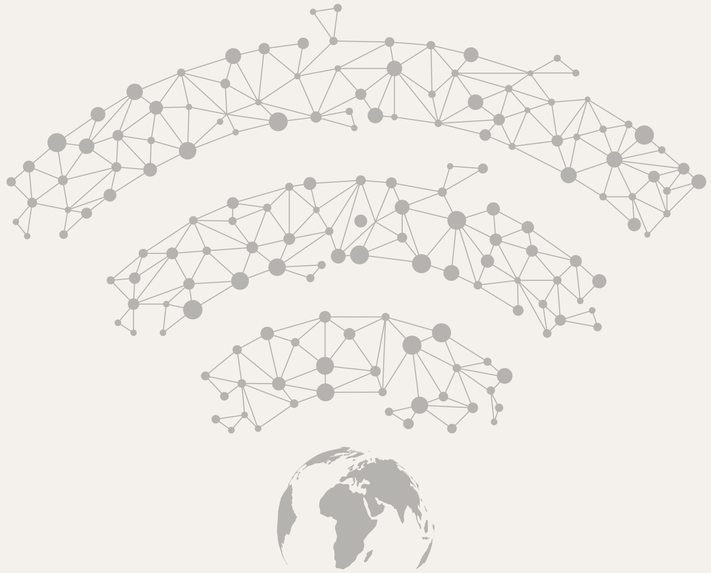
1M5.IO | INFO DECK (2.0) | INVERT EDITION

1M5

Invisible Matrix Service (1M5 using leet) is the first decentralized services platform with intelligent routing between anonymity networks to bypass censorship.

When a user's device gets blocked on one network, other networks are used to route around the block until another node can make the request.

Censorship resistance is currently accomplished using Tor and I2P. In the future, it will include 1DN (a direct wireless ad-hoc network using radio and LiFi) as well as other future anonymity networks.



1M5

THE CORE MISSION

1M5's mission is to protect freedom of speech, expression, association, and assembly over electronic communications for all beings by ethical, sustainable means.

”

1M5

GUIDING PRINCIPLES

Freedom of Speech

All people have a natural right to freedom of speech, expression, association, and assembly.

Voluntaryism

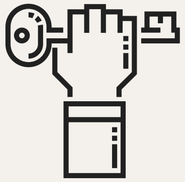
All relationships must be voluntary.

Privacy

Privacy is the bedrock of freedom. We should be able to communicate as we please, privately and anonymously

Transparency

Transparency in code and governance.



Data

Individuals own their data and should be the ones who profit from it.

Identity

Self-sovereign identity. Individuals must establish and maintain their own identities, removing 3rd parties from the process.

Money

Self-sovereign money: Empower people to be their own bank, indebted to no one, with the keys to their own money.

1M5

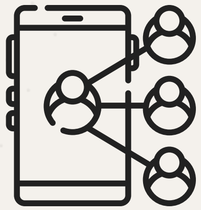
FREEDOM OF SPEECH

Whistleblowers, the abused, minorities, and a myriad of other people could be emboldened by anonymity to speak out in a manner that would otherwise be unavailable if they were forced to identify themselves.

”

1M5

OBJECTIVES

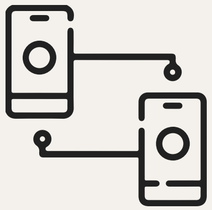


Freedom of Information

Support sharing of and access to information free from censorship.

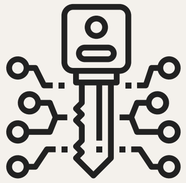
Shielded Distribution

Support sharing of and access to information without fear of prosecution.



Peer-to-Peer (P2P)

Support P2P communication without the need to depend on servers nor the Internet (The People's Direct Network). Cut the cord to ISPs for good.



Self-Sovereign Identity

Provide a self-sovereign identification system to establish reputation whereby the keys are owned and maintained by the individual.

Self-Funded Protocol

Ensure sustainability by providing a platform that is self-funded.

Privacy Control

Enable control over monetization of personal information. Users determine what is shared with and sold to 3rd parties.

ARTICLE 19, 2018

Global trends from our metric show that media freedom is at its lowest level in ten years.

1M5

GLOBAL PROBLEMS

JOURNALISM - BROWSING - MESSAGING - ACTIVISM - DOT

Solutions, implementations, etc.

JOURNALISM

702

professional journalists killed in the last 10 years

348

detained journalists in 2018

49

journalists murdered or deliberately targeted in 2018

60

journalists currently held hostage

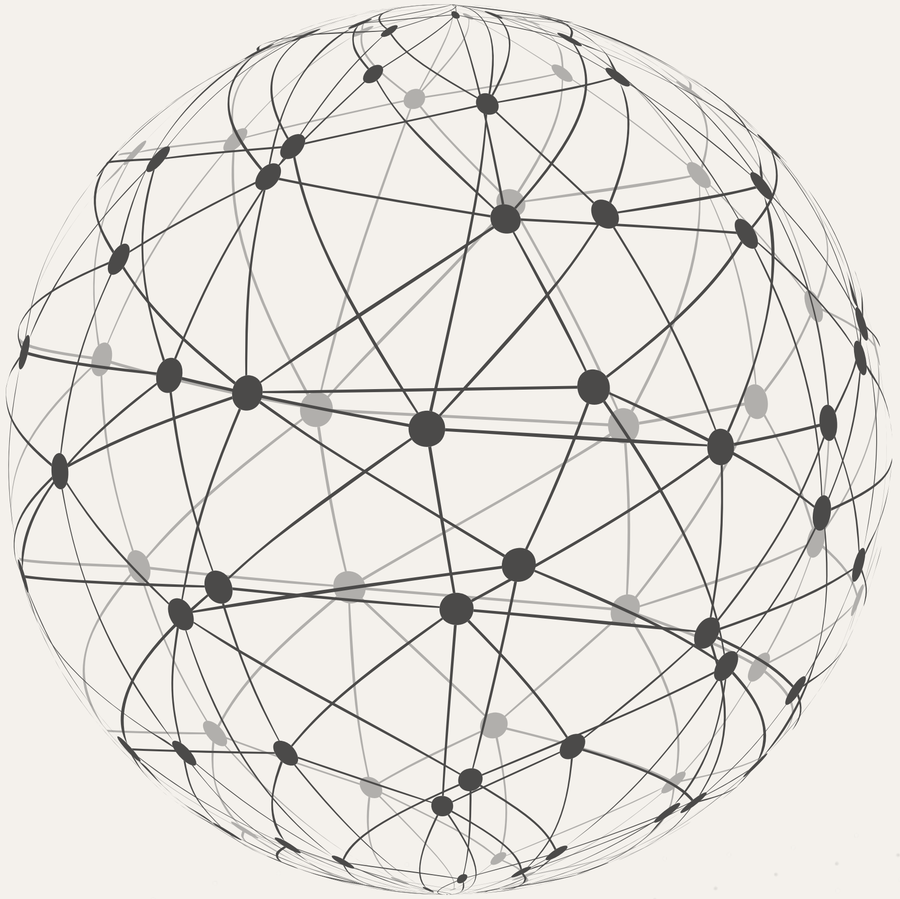
The 2018 round-up figures compiled by Reporters Without Borders (RSF) include professional journalists, non-professional journalists, and media workers.

Source: https://rsf.org/sites/default/files/worldwilde_round-up.pdf.

BROWSING

3.7B
people with access to the Internet, 2018

55%
live in countries where political, social, or religious content was blocked online



8
consecutive years of global internet freedom declines

17
number of governments that approved laws restricting online media in the name of fighting “fake news”

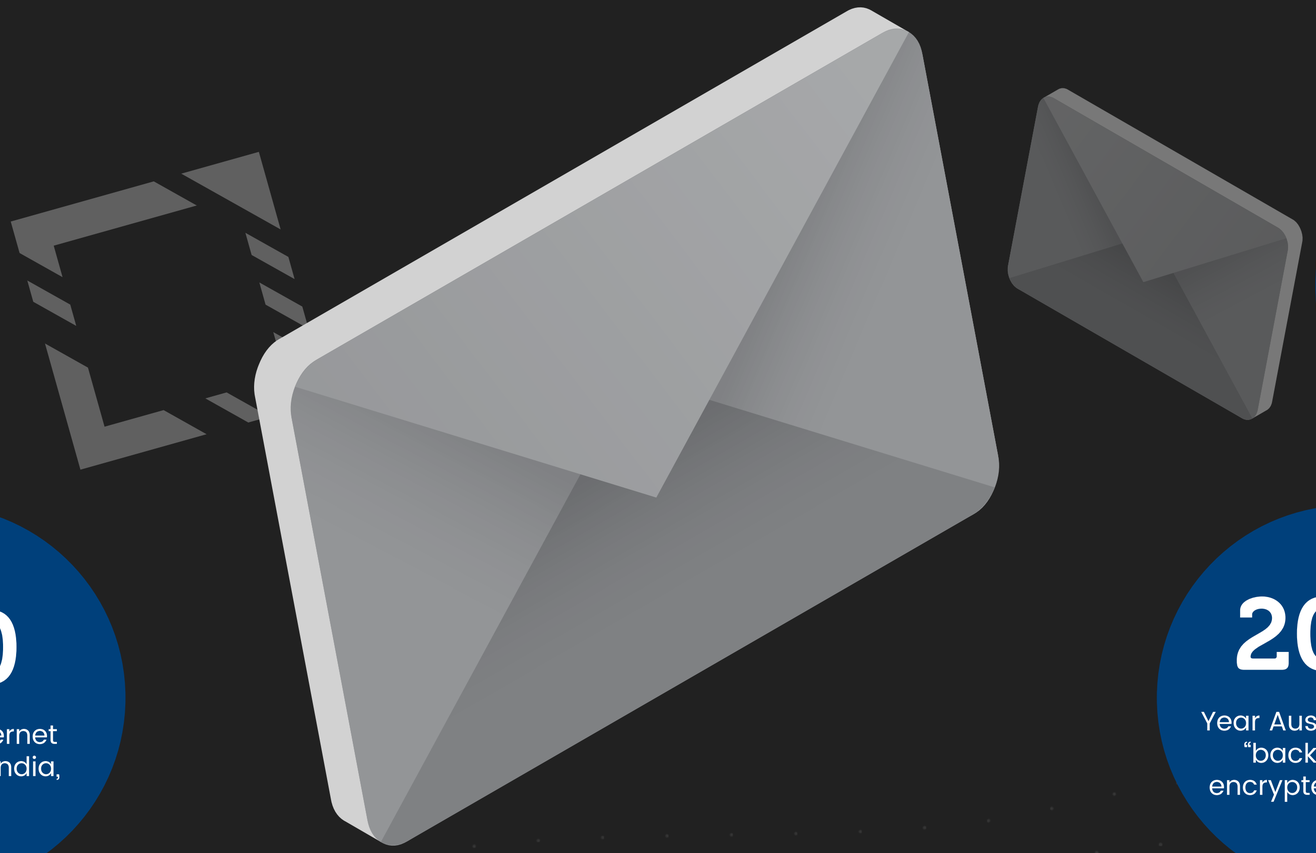
A summary of findings for the 2018 edition of Freedom on the Net. Narrative reports of the 65 countries assessed in this year’s study and a full list of contributors can be found on.

Source: https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf

MESSAGING

2017

Telegram groups with over 5K followers were asked to register with authorities in Iran



18M

number of IP addresses blocked in Russia, 2018

100

number of internet shutdowns in India, 2018

2018

Year Australia requests “back doors” into encrypted technology

A summary of findings for the 2018 edition of Freedom on the Net. Narrative reports of the 65 countries assessed in this year’s study and a full list of contributors can be found on:

Source: https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf

ACTIVISM

2M

number of people who took to the streets of Hong Kong, 2019

20K

number of people exposed after a Telegram group administrator was arrested during protests in Honk Kong, 2019

816

number of protesters, journalists, doctors, lawyers, and opposition party leaders arrested during the protests in Sudan (2018-19)

3

number of major social media platforms (FB, twitter, instagram) that were blocked during the protests in Sudan, 2019

We can no longer rely on centralized applications and services to help promote freedom of speech. It is a human right to be able to express your thoughts and opinions.

Source: https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf | https://www.hrw.org/news/2019/01/18/sudan-hundreds-protesters-arrested
https://qz.com/africa/1510229/sudan-shuts-down-facebook-twitter-instagram-amid-bread-protests

DoT (DECENTRALIZATION OF THINGS + EMBEDDING)

50B
estimated number of connected things by 2020

$6T
projected cost of cybercrime annually by 2021

6B
estimated internet users by 2022

55%
estimated percentage of smartphones representing total IP traffic by 2025

Problems of centralization: “Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history...”

Source: https://cybersecurityventures.com/cybersecurity-almanac-2019 | https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016
https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

1M5

BRIAN TAYLOR, 1M5

It’s time to take Bitcoin’s lead and decentralize the IoT. Let’s build the Decentralization of Things (DoT) by replacing these centers of control with decentralized peer-to-peer networks.

1M5

EMBEDDED COMMUNICATION TECHNOLOGIES

TOR - I2P - 1DN

Censorship Resistance Routing

1M5

EMBEDDED TECHNOLOGIES: TOR + I2P

Tor

Provides onion-routing, layered encryption, and bidirectional channels for IP anonymity. Best for accessing clearnet web sites/services.

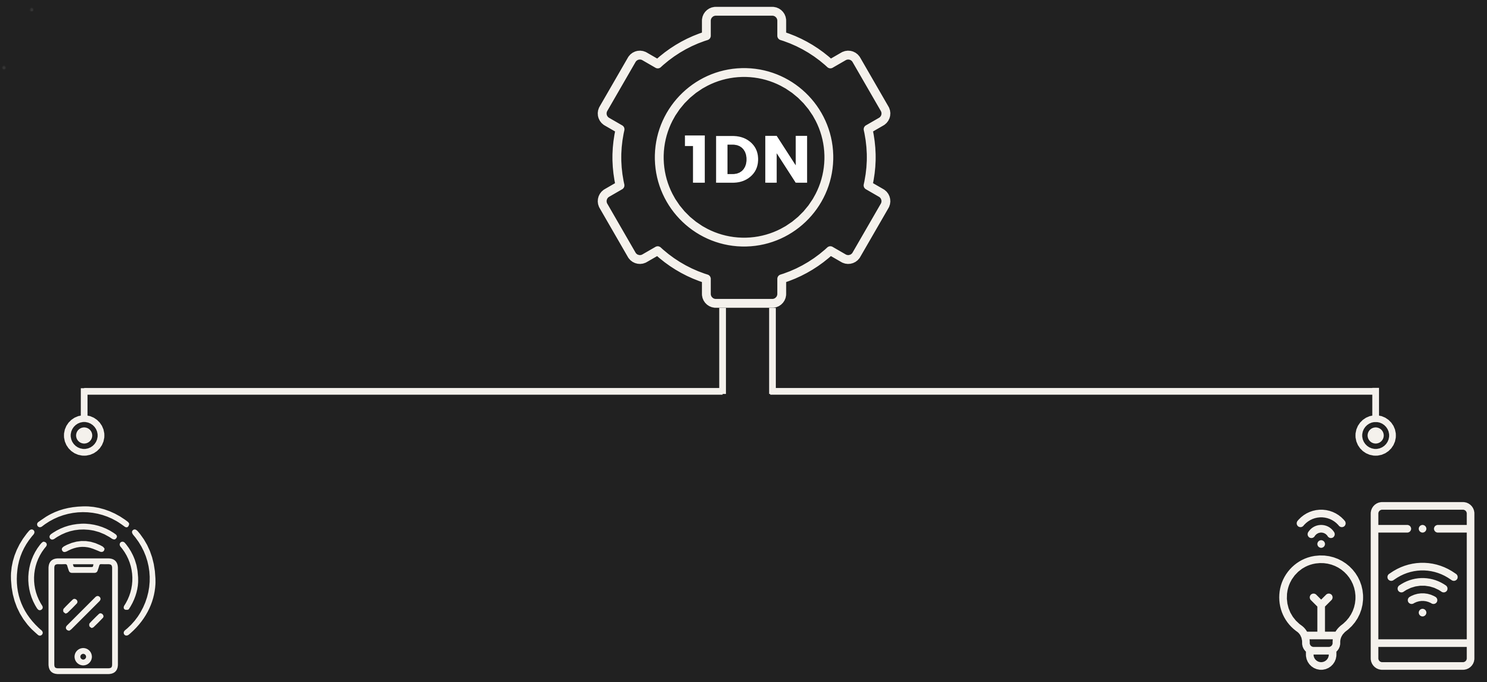
I2P (Invisible Internet Project)

Provides garlic routing, layered encryption, and unidirectional channels for IP anonymity. Best for communicating P2P with other I2P users.

The first layer in a secure highly network-based application must be a layer supporting anonymity. This is accomplished by 1M5's Sensor Service by using I2P as the basis for routing over the Internet.

1M5

1DN: WIRELESS AD-HOC NETWORK (FUTURE)



Full Spectrum Radio

Radio (cell/WiFi/full spectrum) is the technology of signaling or communicating using radio waves. The radio sensor uses the complete radio wave spectrum.

LiFi

LiFi is wireless communication technology that uses light to transmit data between devices.

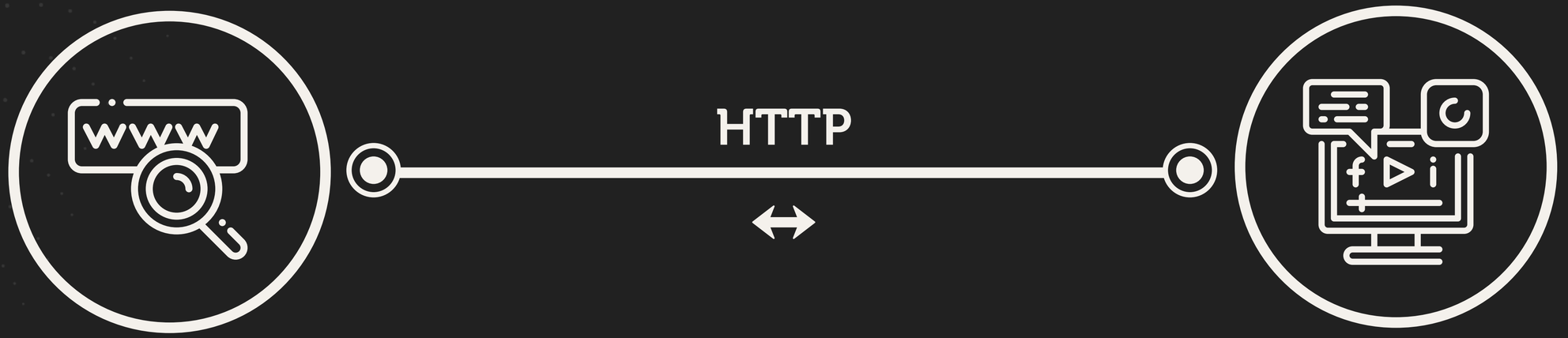
1DN is a wireless ad-hoc network within 1M5 as a sensor to provide private communications outside of the Internet using the full radio spectrum (Software Defined Radio – SDR), and LiFi (Light Fidelity). As of 2019, LiFi is an emerging technology.

1M5

HOW IT WORKS

SCENARIO 1: VIEWING A CLEARNET WEBSITE

SITUATION 1: STANDARD ACCESS



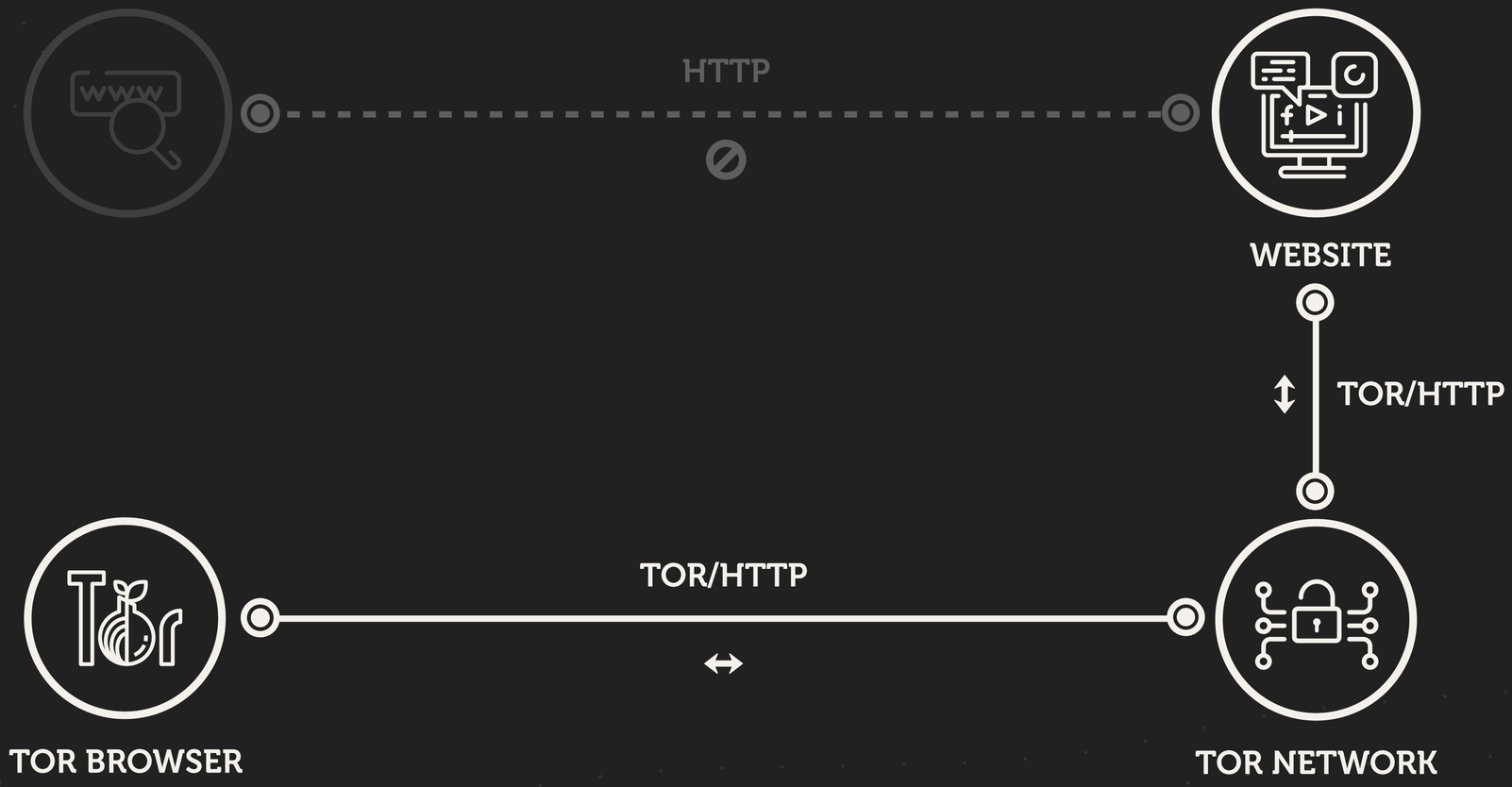
BROWSER

WEBSITE/SERVER

(YouTube, Facebook, etc.)

A browser is used to connect to a web site. If this path is blocked by the Internet Service Providers (ISP) or the government, users look for a way around the block.

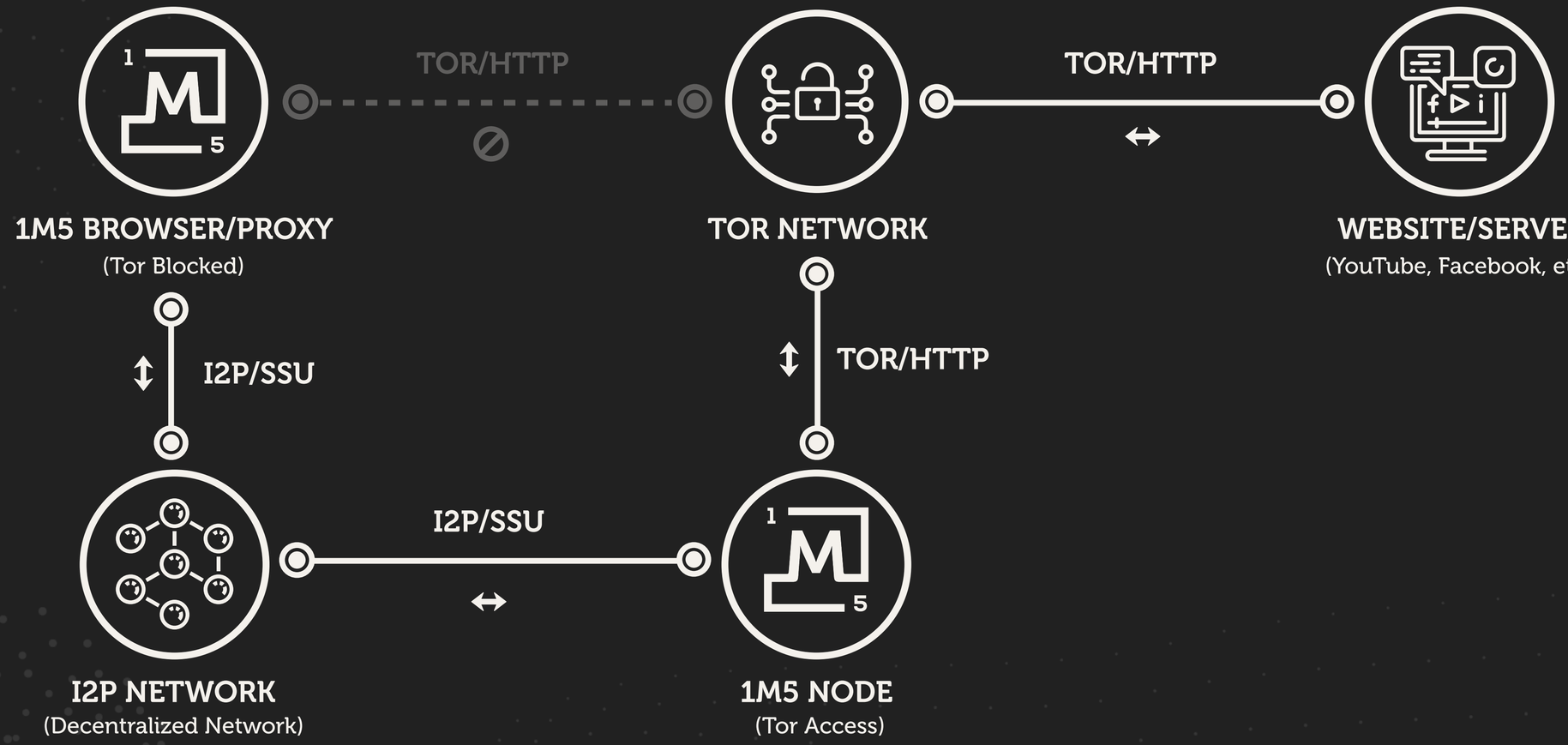
SITUATION 2: DOMAIN/IP BLOCKED (E.G. IRAN)



The Tor browser is successful in bypassing blocks as long as the exit nodes are not blocked. But more astute governments (e.g. China, Iran) find the entrance nodes running Tor and blacklist the IP addresses, preventing access to the Tor network.

1M5

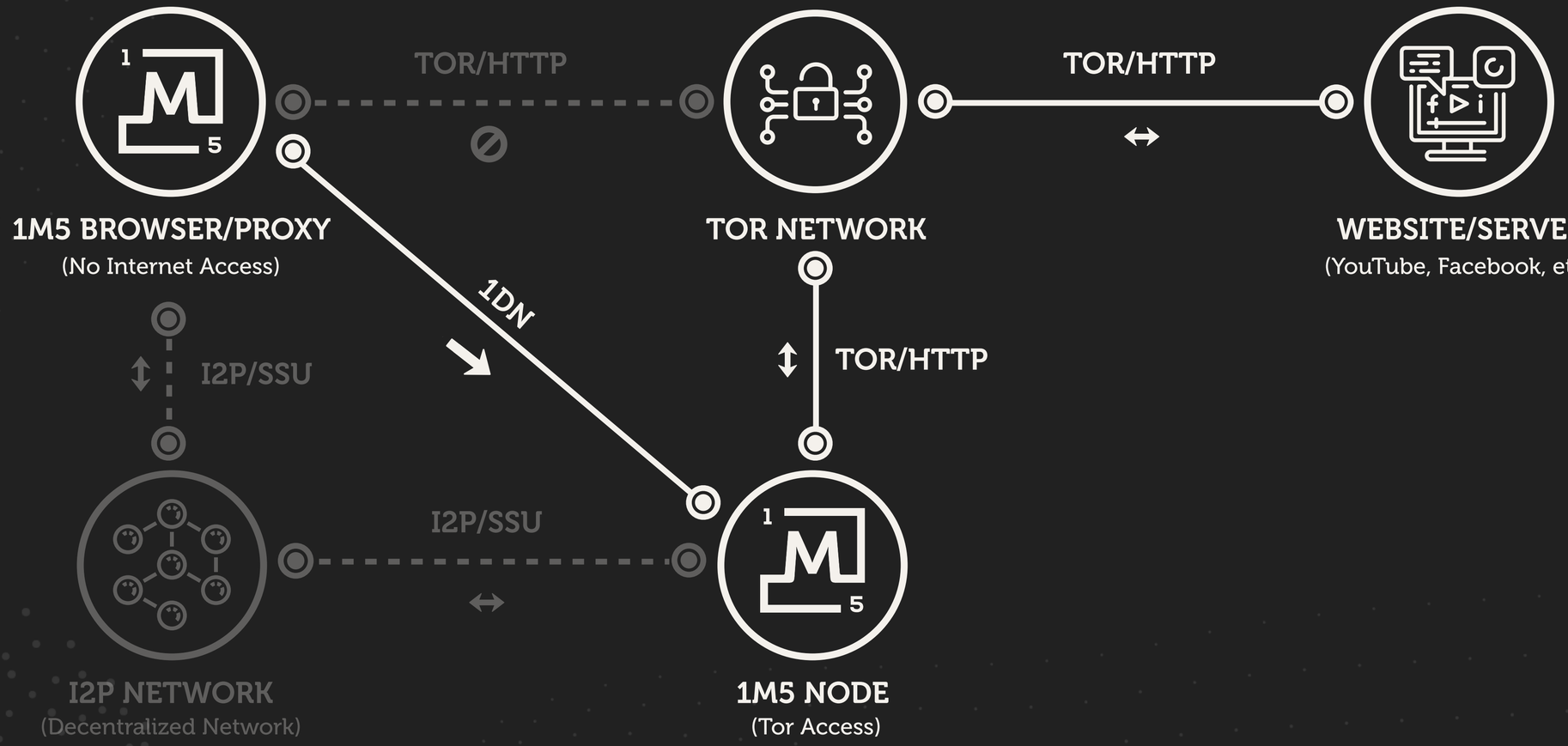
SITUATION 3: TOR BLOCKED (E.G. CHINA)



Unable to access the Tor network, the request is sent to another 1M5 node that has access to Tor (using I2P). The secondary DApp node's 1M5 instance connects to the site desired, collects the response, and forwards it to the original requester.

1M5

SITUATION 4: NO INTERNET ACCESS (E.G. DURING A PROTEST)



1M5 uses the 1DN ad-hoc network (e.g. WiFi radios in your phone) to route out until it successfully locates a 1M5 node with Tor access.

HOW IT WORKS

SCENARIO 2: PERSON-TO-PERSON / PEER-TO-PEER (P2P) APPLICATIONS

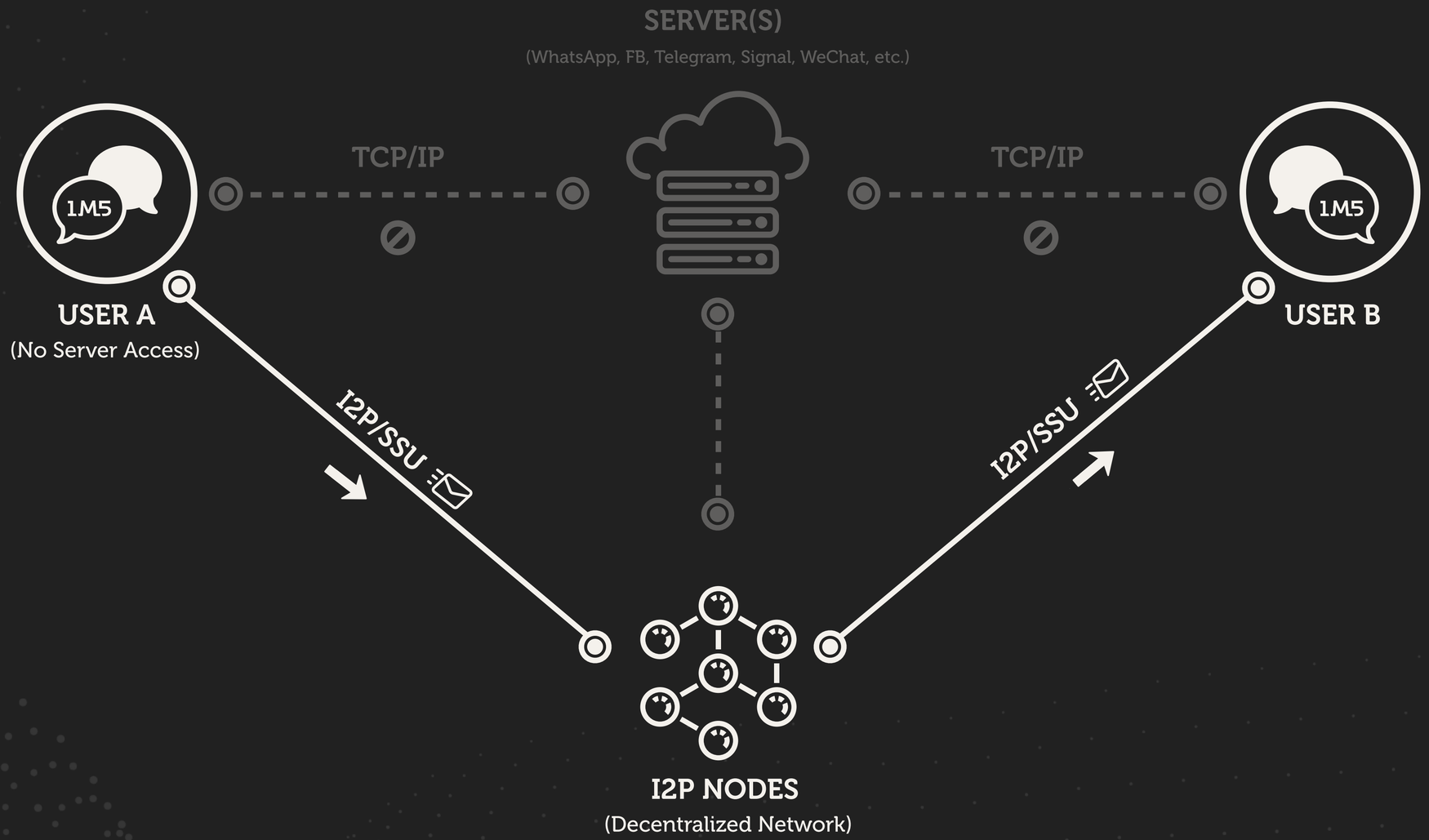
Messengers, email, voice, etc.

SITUATION 1: CENTRALIZED ACCESS (THE NORM)

(WhatsApp, FB, Telegram, Signal, WeChat, etc.)

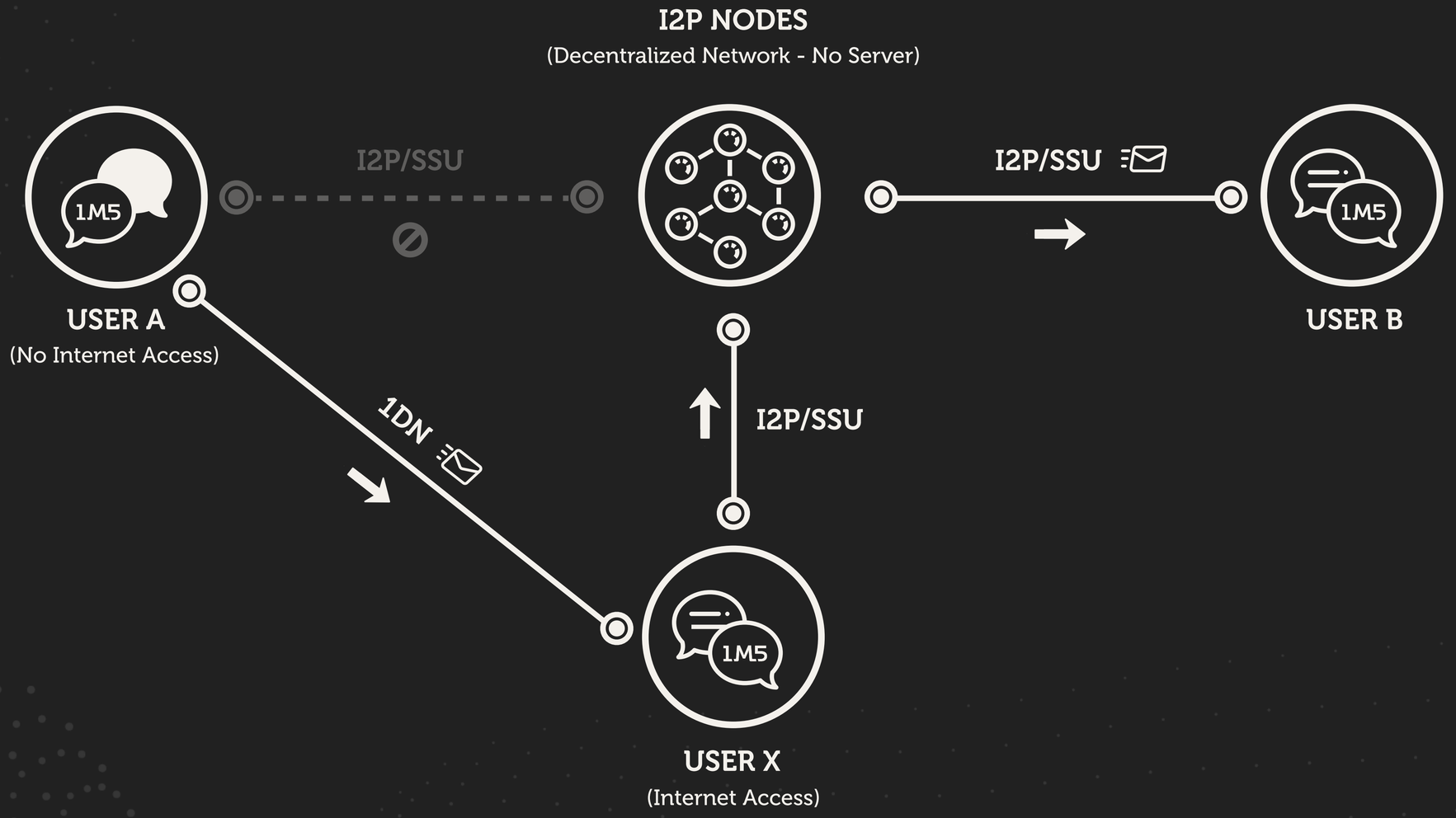
A typical messenger using TCP/IP (the Internet) to communicate with a centralized server.
The message is then forwarded to the end-user by the server.

SITUATION 2: SERVERS ARE BLOCKED (E.G. HK PROTEST 2019)



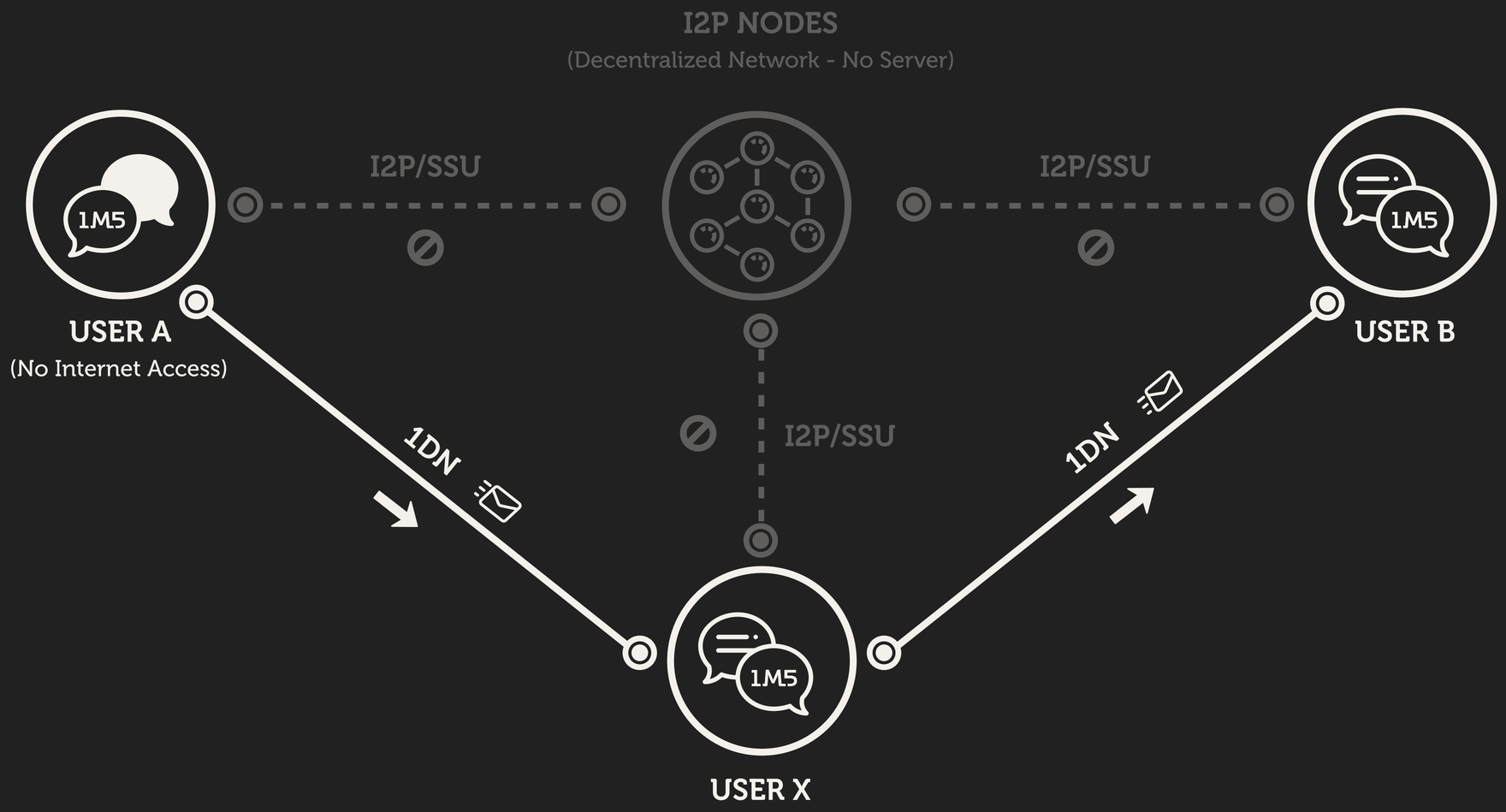
A messenger (1M5 embedded) is used for messaging over I2P (SSU) preventing censorship by shutting down or blocking a server (no servers are used).

SITUATION 3: NO NATIONAL INTERNET ACCESS (E.G. EGYPT 2011)



User A has no Internet access to reach User B. The protocol uses the 1DN sensors (radio and/or LiFi) depending on latency and/or security requirements to get the message to a 1M5 peer who has Internet access (User X). The message can then continue through I2P's decentralized network until it reaches User B.

SITUATION 4: GLOBAL INTERNET SHUTDOWN



User A has no internet access and protocol is unable to find any users with an active internet connection. The protocol uses the 1DN sensors (radio and/or LiFi) for all communications. The message will relay through the 1M5 network of peers until it can reach User B.

1M5

MEASURING THREATS TO FREEDOM OF SPEECH / EXPRESSION

MANCON

Maneuvering / Alert System

MANCON - FREEDOM OF EXPRESSION

MANCON is similar to the United States Armed Force's DEFCON. It is an alert state signaling the maneuvering required to achieve freedom of expression.

MANCON is highly responsive and adjusted to reflect changing conditions. The base MANCON for a claimed jurisdiction is largely based on the Press Freedom Index.

MANCON 5 - GOOD SITUATION

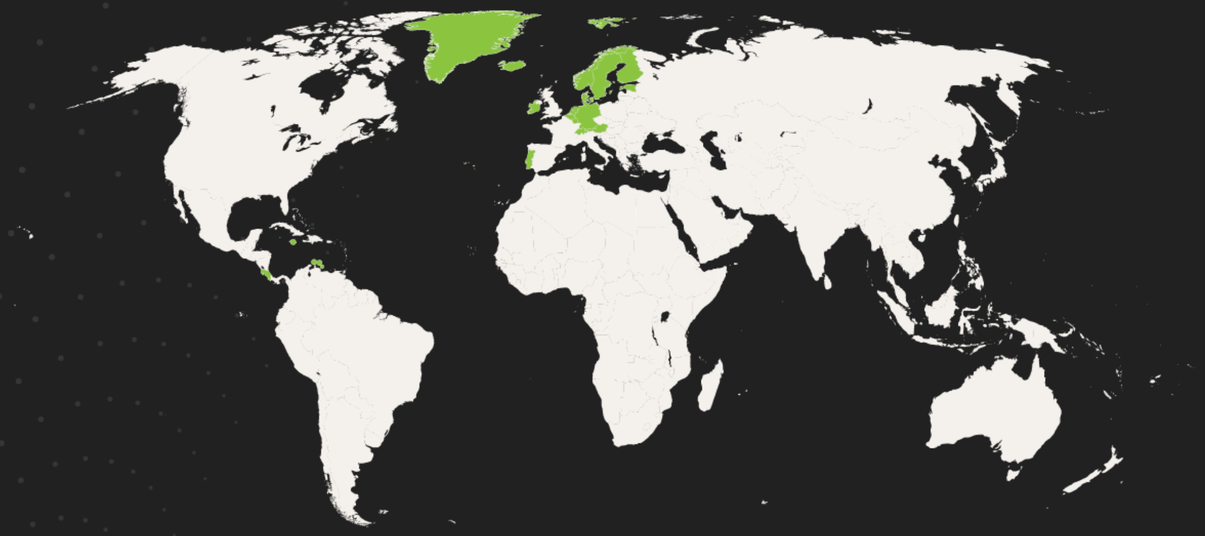
MANCON 4 - SATISFACTORY SITUATION

MANCON 3 - NOTICEABLE PROBLEMS

MANCON 2 - DIFFICULT SITUATION

MANCON 1 - VERY SERIOUS SITUATION

MANCON 5: LOW SECURITY (E.G. SWITZERLAND)



MANCON 5 - GOOD SITUATION

WEB (Latency: Normal)

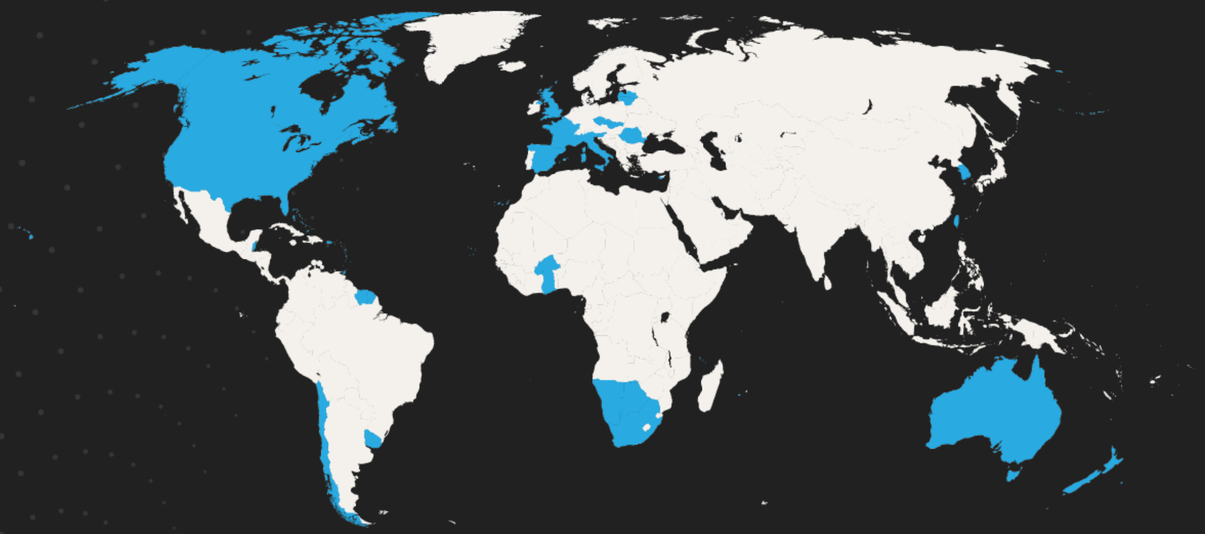
- Uses HTTPS normally.
- Tor for .onion addresses.
- I2P for .i2p addresses.
- Failures will not attempt HTTP but will use other peers to assist.
- If peers assistance fails, the site is assumed down.

P2P (Latency: 100ms to 10 seconds)

- I2P is used for P2P services such as messaging.

Open/normal SSL based communications with no expected censorship or privacy intrusion attempts.
Minimal censorship or privacy intrusion attempts. Freedom of speech is respected.

MANCON 4: MEDIUM SECURITY (E.G. AUSTRALIA)



MANCON 4 - SATISFACTORY SITUATION

WEB (Latency: 500ms to 2 seconds)

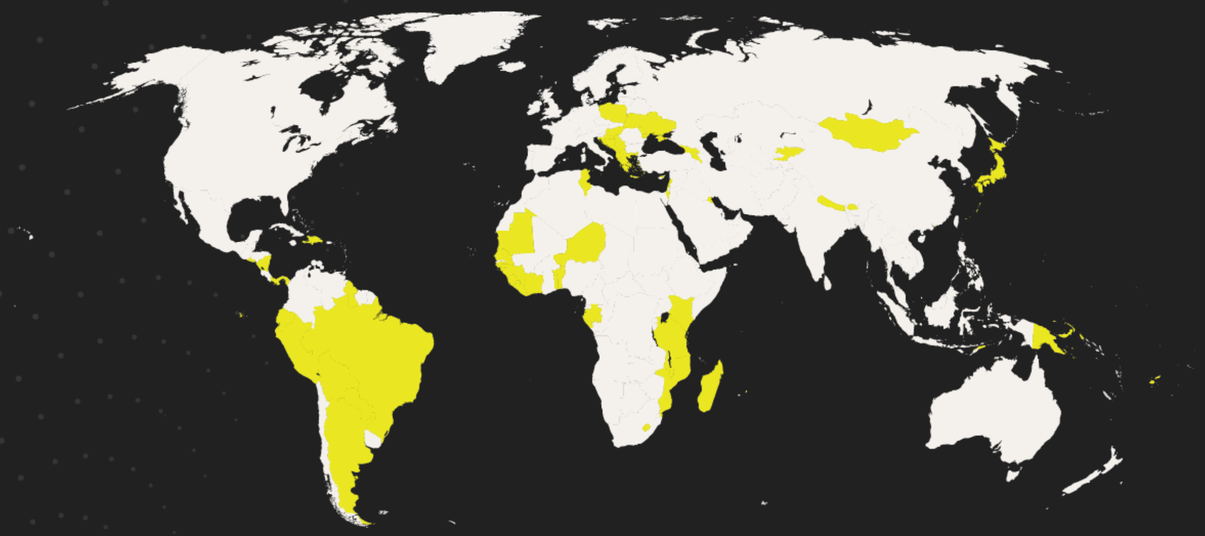
- When a Tor site gets blocked, other peers will be used to assist. If those are unable to assist (the site was taken down) and the site has an associated Tor hidden service, that Tor hidden service will be used.
- All other routing remains unchanged.

P2P (Latency: 500ms to 10 seconds)

- I2P is used for P2P services such as messaging.

Government attempted censorship of news-centric public web sites with routine shutdown of cloud CDN content or blocking of websites. Tor is used for normal web browsing. All other routing remains unchanged.
Respect for freedom of speech may be limited.

MANCON 3: HIGH SECURITY (E.G. BRAZIL)



MANCON 3 - NOTICEABLE PROBLEMS

WEB (Latency: 1 to 10 seconds)

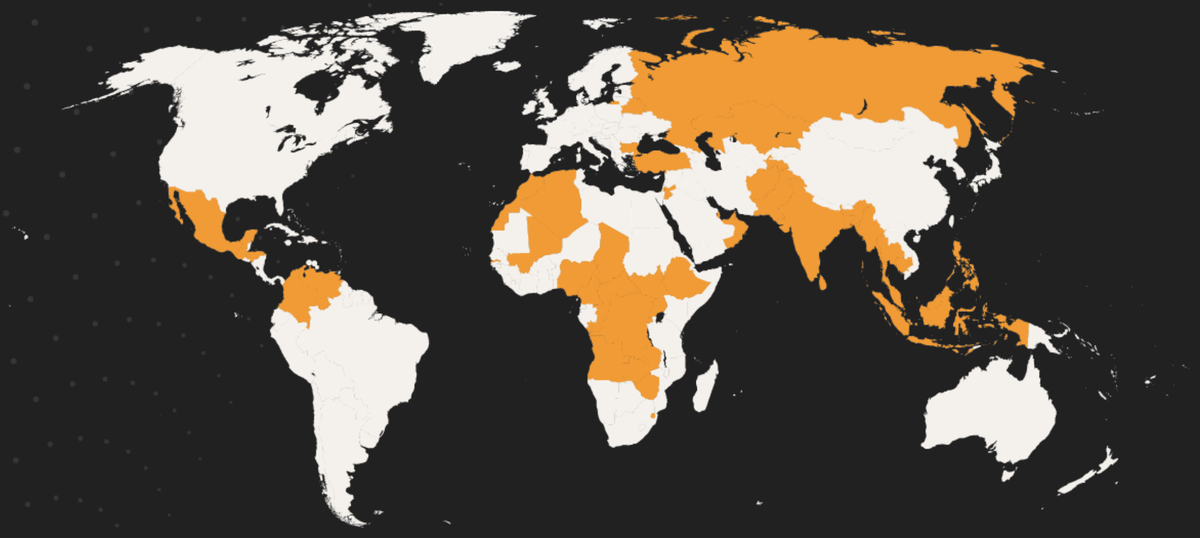
- Will use Tor as default access to clearnet sites. When Tor gets blocked, will use I2P/IDN to route around blocks.

P2P (Latency: 1 to 10 seconds)

- I2P is used for P2P services such as messaging.

Heightened censorship is present including Deep Packet Inspection (DPI). Tor entrance and exit nodes as well as hidden services may have been discovered and taken down. Likely little respect for Freedom of Expression.

MANCON 2: VERY HIGH SECURITY (E.G. RUSSIA)



MANCON 2 - DIFFICULT SITUATION

WEB (Latency: 4 seconds to 3 minutes)

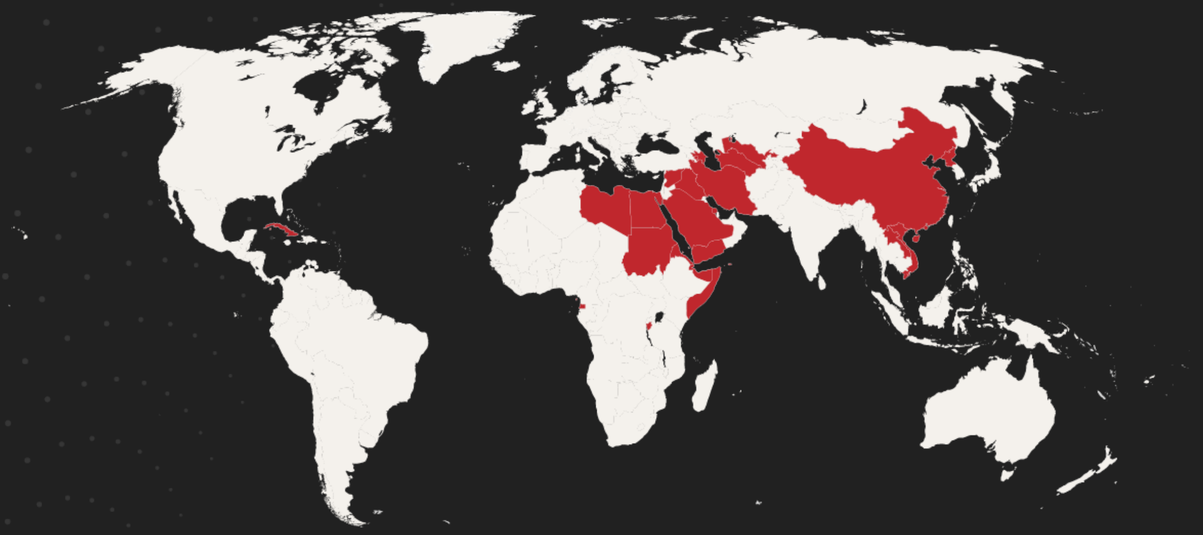
- I2P with random delays is used to route requests through a peer with Tor access.
- I2P eep sites will be used with random delays.

P2P (Latency: 4 seconds to 3 minutes)

- Direct comms with I2P but with random delays up to 90 seconds per I2P relay node.

Tor is likely completely blocked. I2P might be getting DDOS attacks slowing it down. I2P is used with random delays. Only able to access information directly via I2P using a decentralized content distribution network such as Inkrypt. Actual threats and prison time for speaking out.

MANCON 1: EXTREME SECURITY (E.G. CHINA)



MANCON 1 - VERY SERIOUS SITUATION

WEB (Latency: 4-30 minutes)

- 1DN peers will be used to access Tor/I2P.

P2P (Latency: 4-30 minutes)

- 1DN peers or I2P (if available) will be used for P2P services such as messaging.
- Intentional random delays 90 seconds to 5 minutes per 1M5 relay node (up to 90 seconds per I2P relay node) will be used to help protect end-users.

Internet access shutdown in areas. Strong censorship attempts with massive number of nodes blocked, deep packet inspections across internet on unencrypted payloads, and/or I2P timing/DDOS attacks. Use 1M5 with 1DN to route to peers with internet access. Expect wide-ranging latencies but with strong privacy. People getting murdered for speaking out. No respect for freedom of expression by governments.

COLLABORATORS

BRIAN TAYLOR

objectorange@1m5.io

PGP: DD08 8658 5380 C7DF 1B4E 04C2 1849 B798 CF36 E2AF

Over 20 years developing software as a Software Architect, from bootstrapped startups to global enterprises. Focusing on decentralized computing, privacy, scalability, security, and real-time analytics. Open sourcing all aspects of computing while promoting voluntary, transparent relationships and private personal lifestyles for all.

AMIN RAFIEE

evok3d@protonmail.com

PGP: E3AA 4FDC0 AFC68 1CBBC 0266 BED5 BCCF CAEF F94DB

Advocate of decentralization, privacy and bottom-up strategies. Entrepreneur, designer & public speaker. Specialized in product development & innovation pathways. Over 10 years of experience as a product designer and developer.

ERBIL KAPLAN

erbilkaplan@protonmail.com

PGP: 2EBC 2239 E9B8 2BCA 7176 77FE FD80 A0C2 95FD EBAC

Senior full stack developer with over 10 years of professional experience in design and development of web based application. Strong knowledge of Java/J2EE, database management systems and OOP concepts.

1M5 contributors working towards developing the mission and the software that implements it. Assistance on any and all components is most welcomed as well as integration with and service deployment to the platform.

1M5

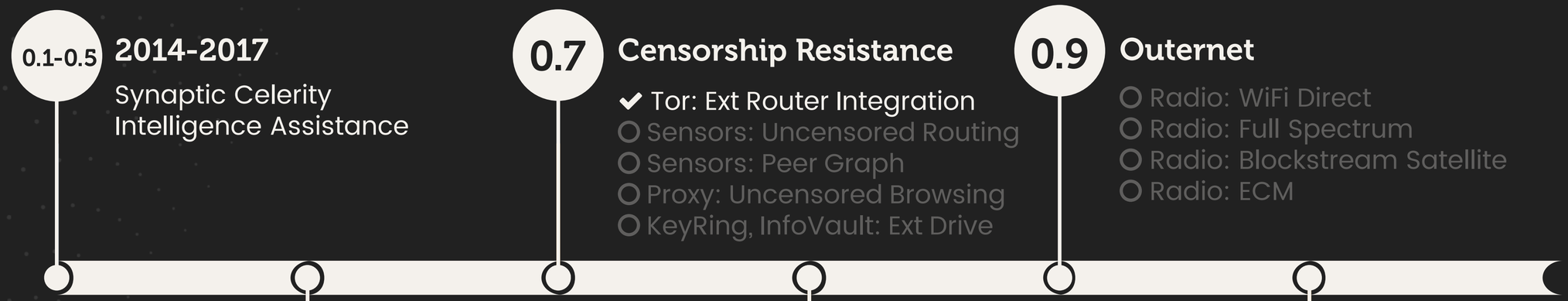
DEVELOPMENT ROADMAP

TECHNOLOGICAL OVERVIEW

Solutions, implementations, etc.

1M5

DEVELOPMENT ROADMAP



0.1-0.5 2014-2017

Synaptic Celerity
Intelligence Assistance

0.6 Infrastructure

- ✔ Core: Framework
- ✔ I2P: Embedded Router
- ✔ DID: OpenPGP
- ✔ KeyRing: Encrypt/Decrypt

0.7 Censorship Resistance

- ✔ Tor: Ext Router Integration
- ○ Sensors: Uncensored Routing
- ○ Sensors: Peer Graph
- ○ Proxy: Uncensored Browsing
- ○ KeyRing, InfoVault: Ext Drive

0.8 Sustainability

- ○ Komodo: Integration
- ○ Prana: Monetization
- ○ Aten: Monetization
- ○ DID: Reputation

0.9 Outernet

- ○ Radio: WiFi Direct
- ○ Radio: Full Spectrum
- ○ Radio: Blockstream Satellite
- ○ Radio: ECM

1.0 Advanced DMesh

- ○ LiFi: Static Host
- ○ LiFi: Mobile Host
- ○ LiFi: Drone Host

1M5's development is solely dependent on the support received via donations and contributions. These plans may change due the nature of technological development and advancements. The goal will remain to support the best technologies available.

1M5

INTEGRATION

CHAT - BROWSING - EMAIL - SOCIAL - OFFICE SUITE - OS

Exploring possibilities

INTEGRATION

Chat

1M5 would use I2P to route messages between messaging apps switching to 1DN (radio & LiFi) when internet access is blocked.

Browsing

1M5 would work to ensure end-users can browse any publicly available web site globally regardless of block attempts. All .onion and .i2p sites would automatically work without configuration. Tor entry node blocks (e.g. China) would get routed around using I2P/1DN.

Email

1M5 would initially use I2P's email system using public keys as destinations with optional aliases. Future 1M5 work would result in the 1M5 network having a decentralized email system to ensure email would work regardless of internet access, which is required by I2P.

Social

IM5 would enhance messaging functionality to include a reputation system.

Office Suite

1M5 would provide google-docs like office sharing workspace with censorship-resistant access and decentralized content distribution (e.g. Inkrypt).

OS

1M5 would be integrated directly in the operating system. All communications can take advantage of the decentralized censorship-resistant communications. Would likely require rewriting 1M5 in C++/Rust/etc away from Java.

1M5

info@1m5.io

Thank you

This presentation is being circulated for general information purposes and is based on the current 1M5 plans. These plans are subject to change. In addition, this presentation is subject to further revision.

This effort is a mission not confined to any jurisdiction as doing so would risk alienating individuals and providing a vector for attack. This doesn't mean that others will not attempt to exercise control over it: that is to be expected, as free speech is given more lip service world-wide than actual support. No one person speaks for the natural right to free speech, expression, association, and assembly and this mission seeks to uphold that natural right.

Decentralized autonomous missions like 1M5 are new efforts not associated with any one state and therefore have none of the protections or support of state-registered organizations. World-wide jurisdictions may establish laws in an attempt to govern efforts like 1M5 or others in the future. Therefore, members are responsible for taking precautions to protect themselves and their families.