eQualitie

 WEB SECURITY

 CAPACITY BUILDING

 CENSORSHIP RESISTANCE

Dmitri Vitaliev. Founder. CEO. dmitri@equalitie.org

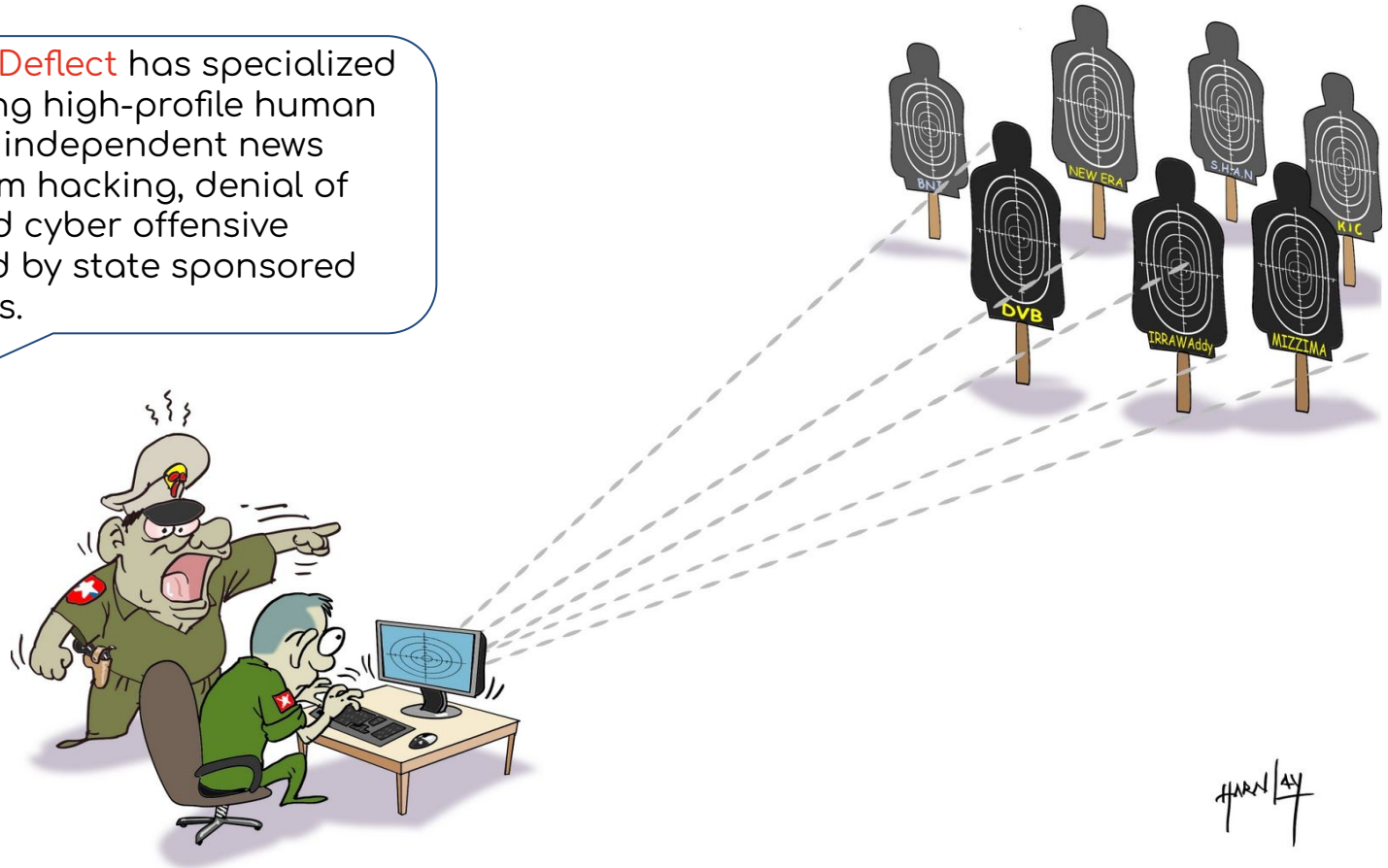
@equalitie @vitaliev:matrix.org

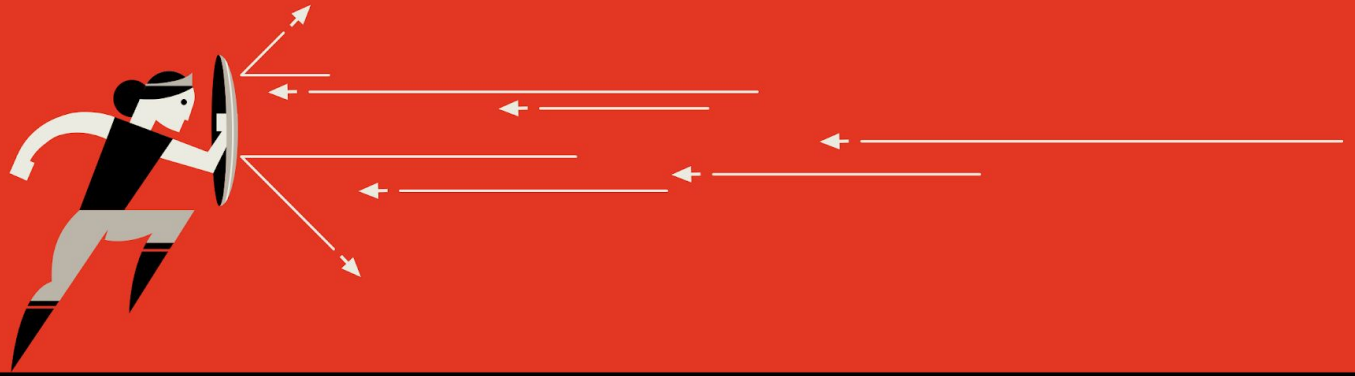
Github: equalitie; deflect-ca; censorship-no

Article 19. Article 20.

In defence of freedom of expression and association online

Since 2011, Deflect has specialized in defending high-profile human rights and independent news groups from hacking, denial of service and cyber offensive efforts lead by state sponsored adversaries.





DEFLECT NETWORK

Get Protected. Stay Connected.

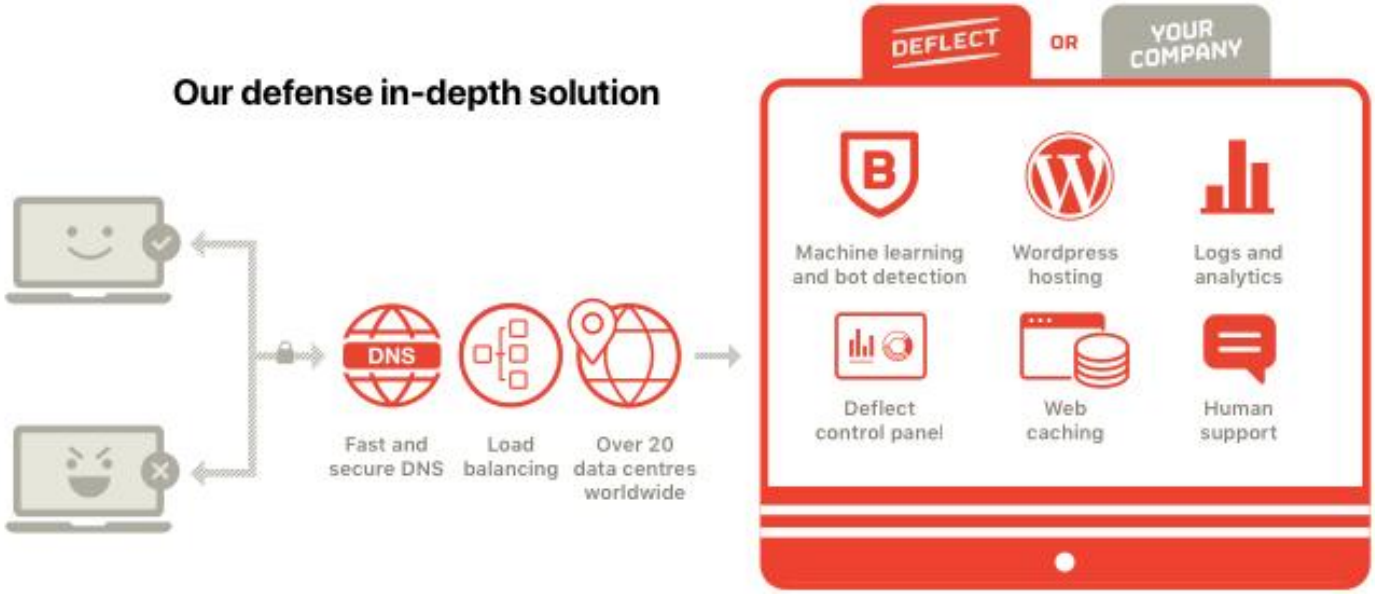
Protection

Performance

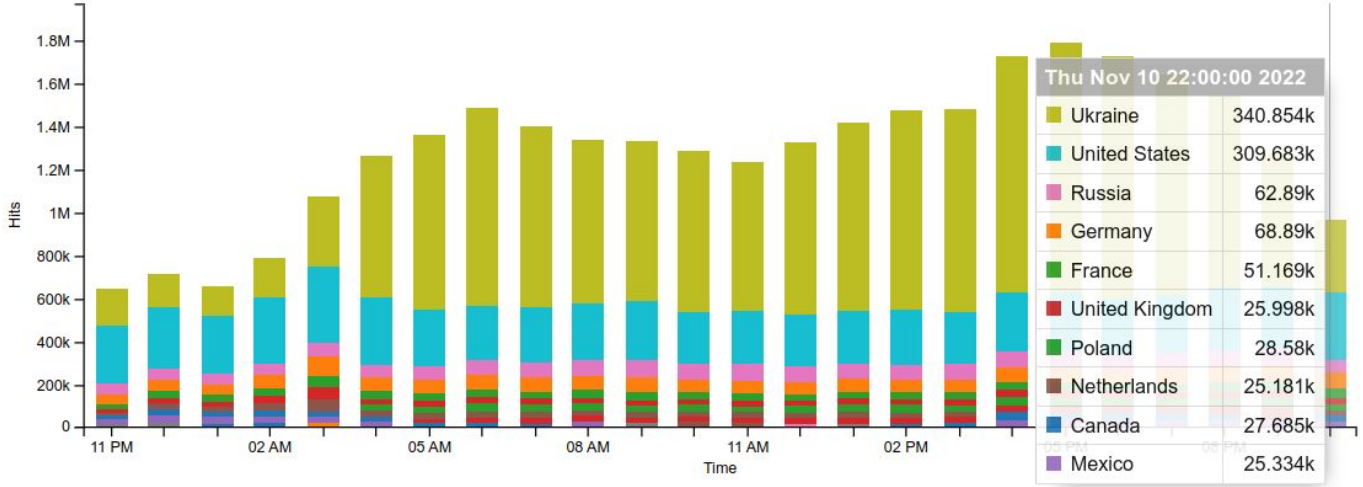
Principles

Philanthropy

Website defenses, hosting, analytics and more…



Serving a million people everyday



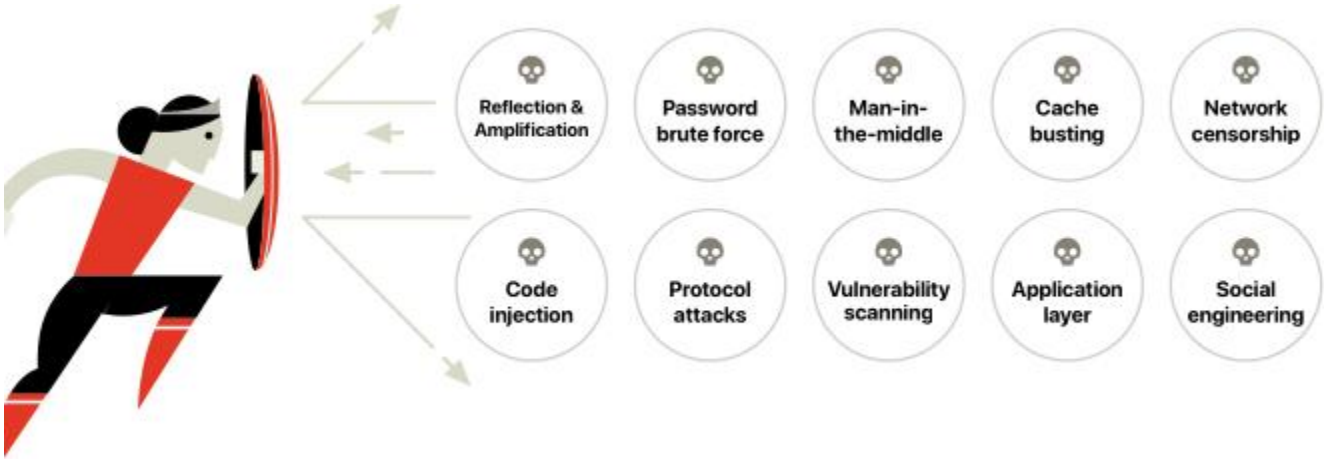
$0.002
Monthly cost to serve a unique client

75M
Annual readers on the Deflect network

99.995%
Network up-time on our SLA

11
Years in frontline DDoS mitigation

Deflect.ca protects your web assets from…



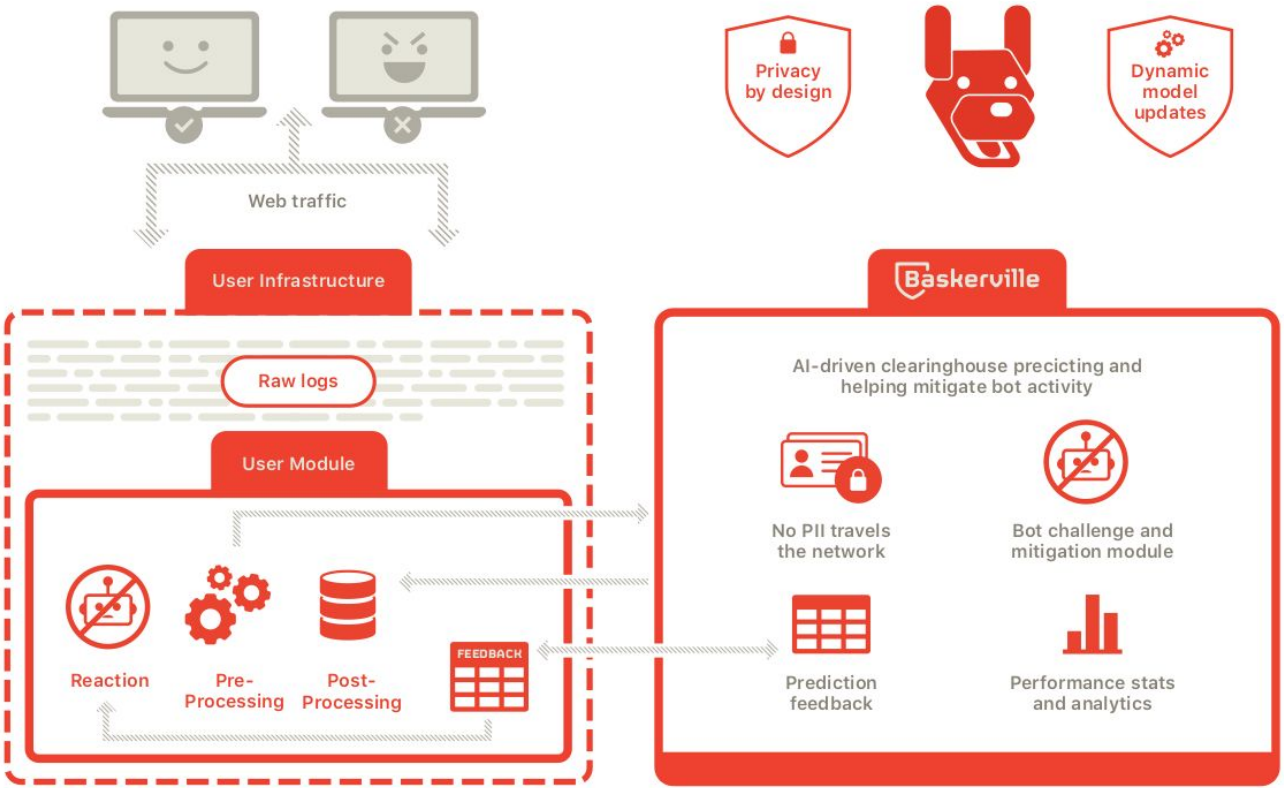
PROTECTED BY DEFLECT

ПОД ЗАЩИТОЙ DEFLECT

PROTEGIDO POR DEFLECT

PROTÉGÉ PAR DEFLECT

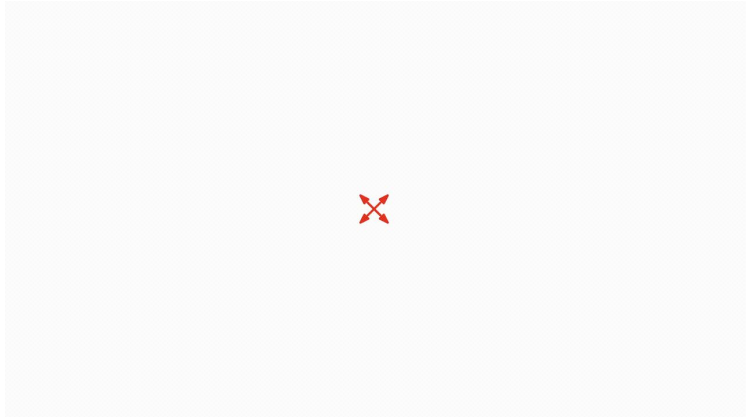
Log ingestion and predictions pipeline



Baskerville provides predictions on IP behaviour

Using machine learning (anomaly detection) to distinguish between normal and abnormal traffic.

- 2 minute sliding window (adjustable)
- Adapts to any web traffic
- Provides a prediction and a score for every IP
- Private by design - no user data travels on the network
- Flexible deployment options
- Mitigation module for verifying and blocking anomalous traffic



99.95%
Bot identification accuracy

40M+
Daily records processed and predictions returned

35+
Behavioural features modelled

100%
Canadian-built machine learning

Baskerville in action on the Deflect network

151,010

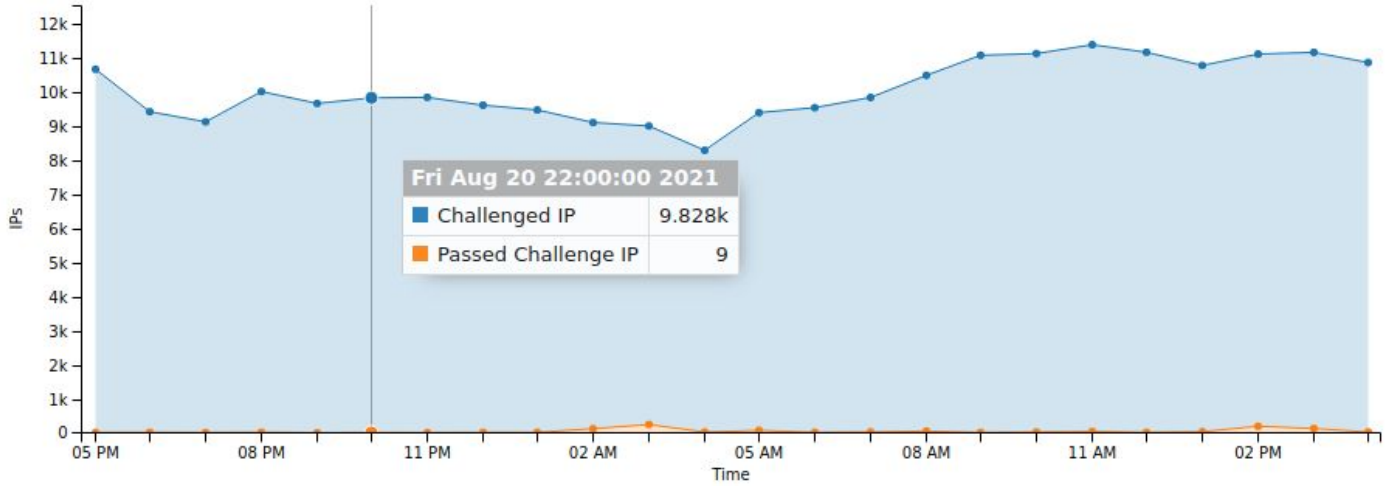
Challenged (past 24 hours)

99%

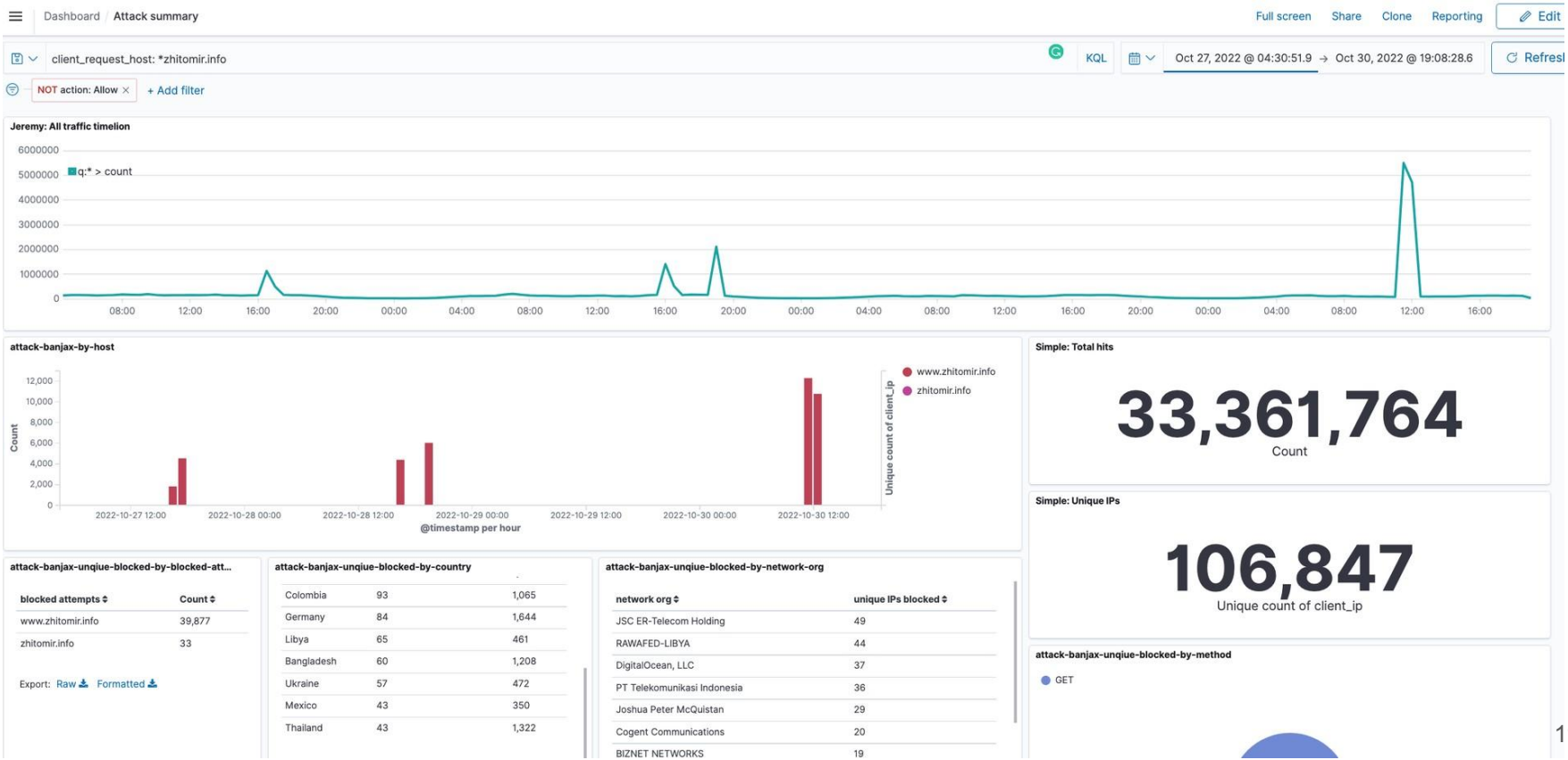
Precision (past 24 hours)

1,097

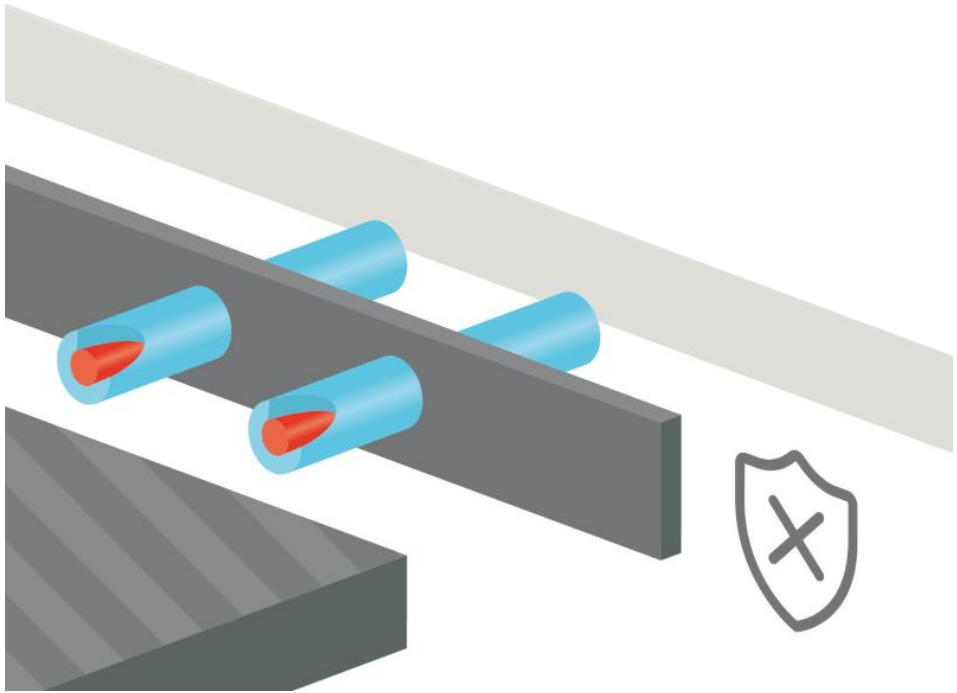
Passed Challenge (past 24 hours)

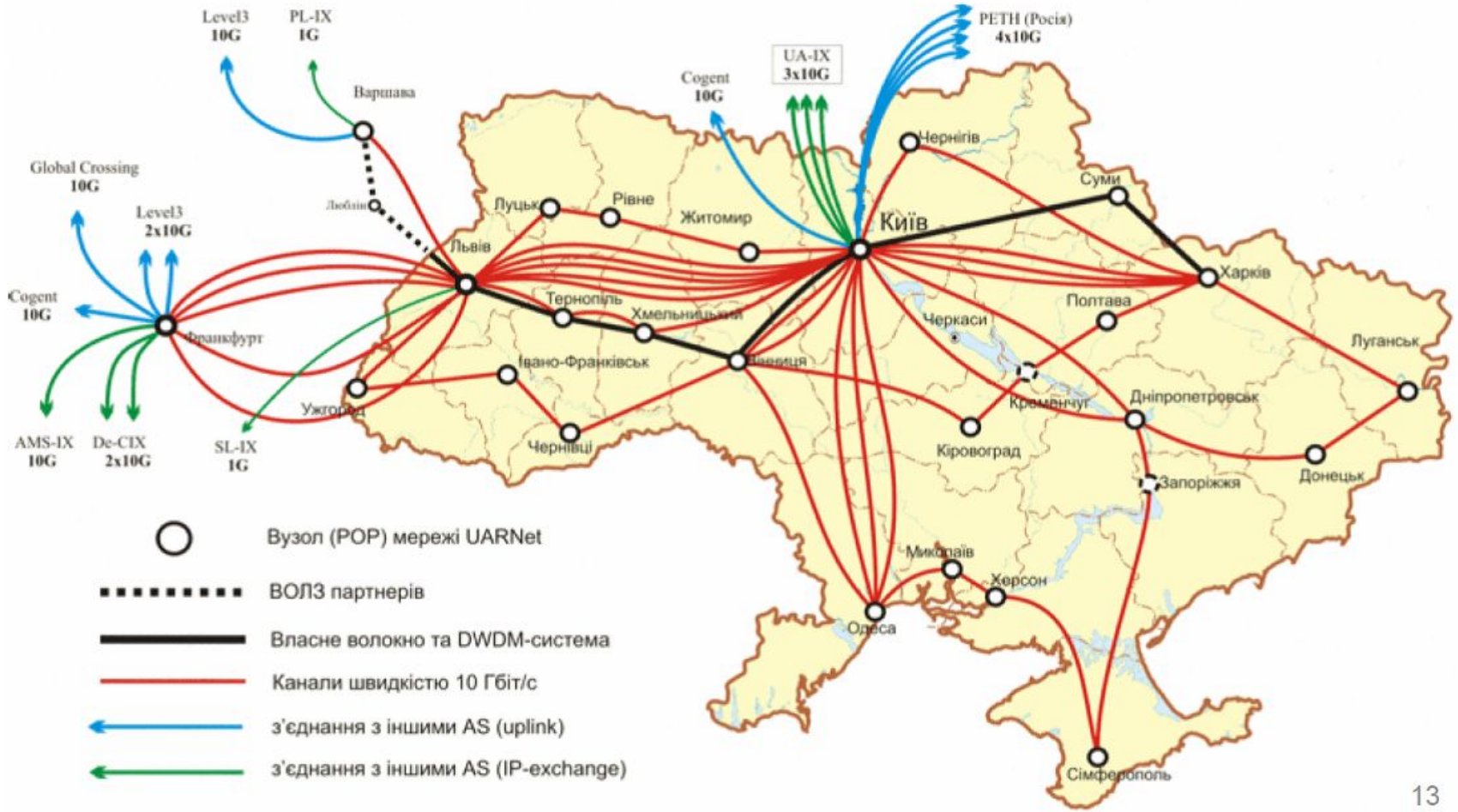


Deflect.ca - attacks on zhitomir.info



Filtering, censorship and shutdowns




Level3
10G
PL-IX
1G
Варшава
Люблін
Global Crossing
10G
Level3
2x10G
Cogent
10G
Франкфурт
AMS-IX
10G
De-CIX
2x10G
SL-IX
1G
Cogent
10G
UA-IX
3x10G
РЕТН (Росія)
4x10G
Луцьк
Рівне
Житомир
Львів
Київ
Чернігів
Суми
Харків
Тернопіль
Хмельницький
Полтава
Черкаси
Івано-Франківськ
Вінниця
Луганськ
Ужгород
Кременчуг
Дніпропетровськ
Чернівці
Кіровоград
Донецьк
Запоріжжя
Миколаїв
Херсон
Одеса
Сімферополь
Вузол (POP) мережі UARNet
ВОЛЗ партнерів
Власне волокно та DWDM-система
Канали швидкістю 10 Гбіт/с
з'єднання з іншими AS (uplink)
з'єднання з іншими AS (IP-exchange)

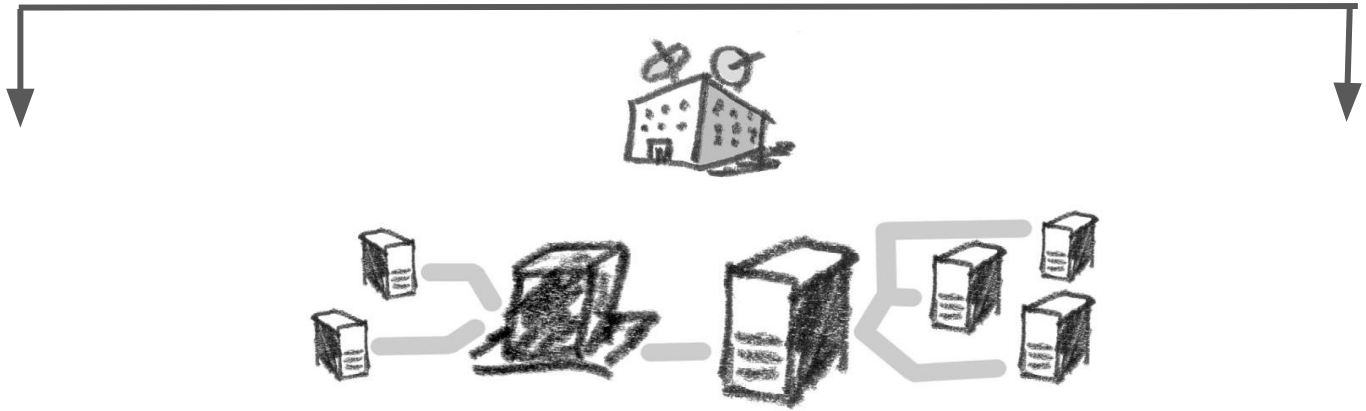
13

aws facebook Google Cloud Azure OVH.com

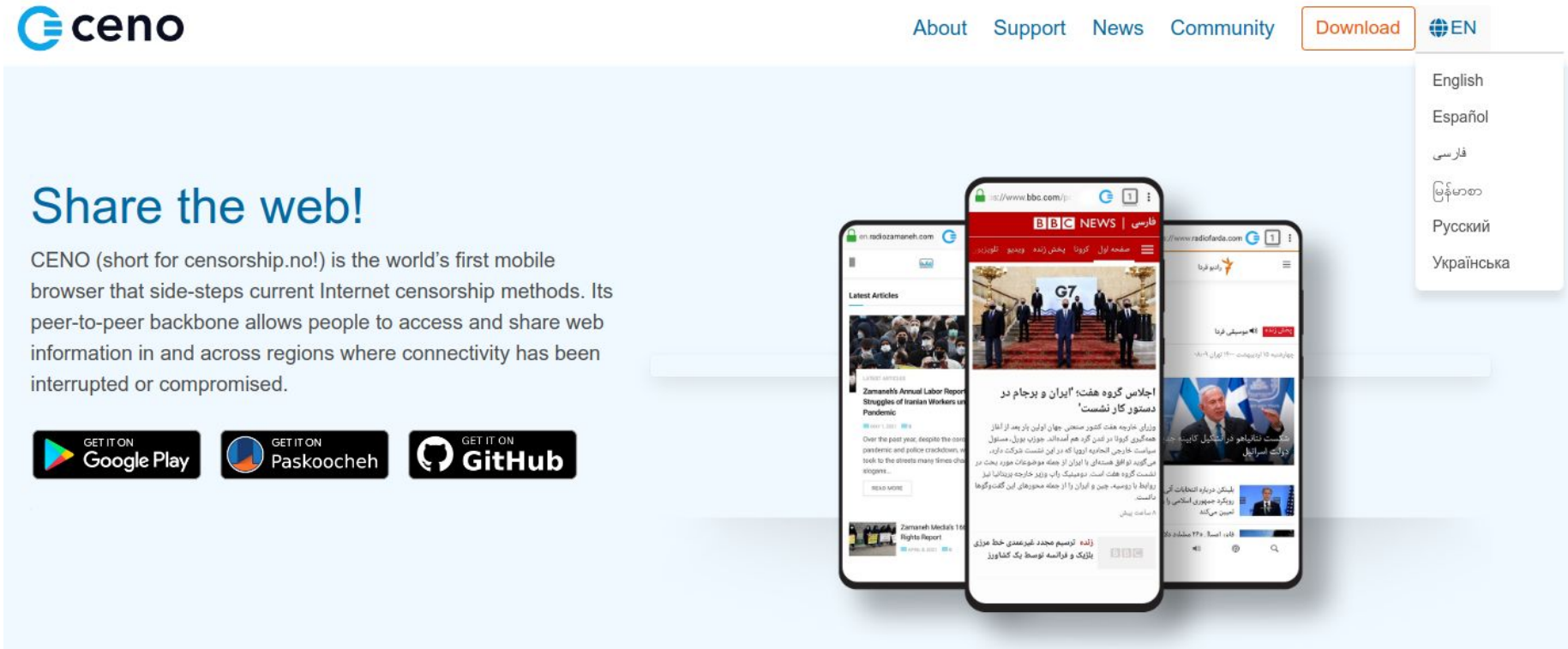
Akamai CLOUDFLARE linode iCloud

TOR

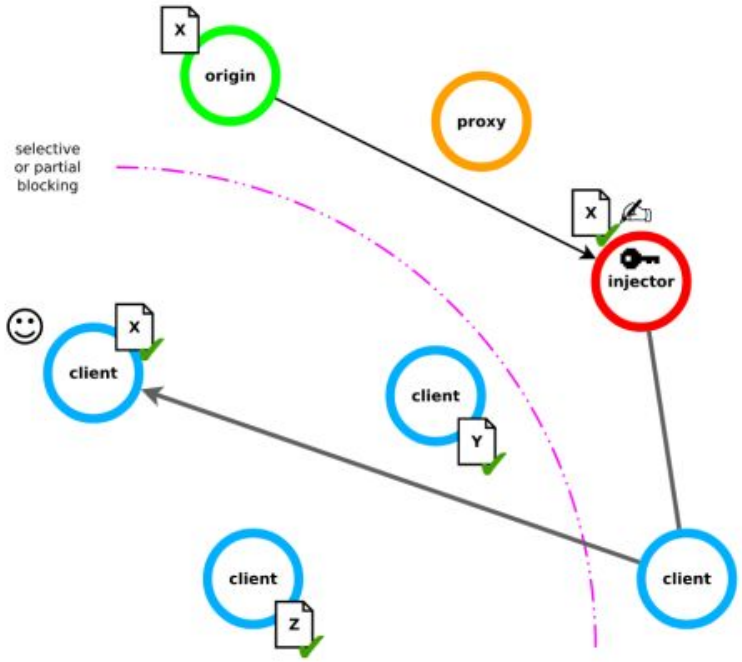
Internet shutdown - scenario #1
Disconnection of popular services

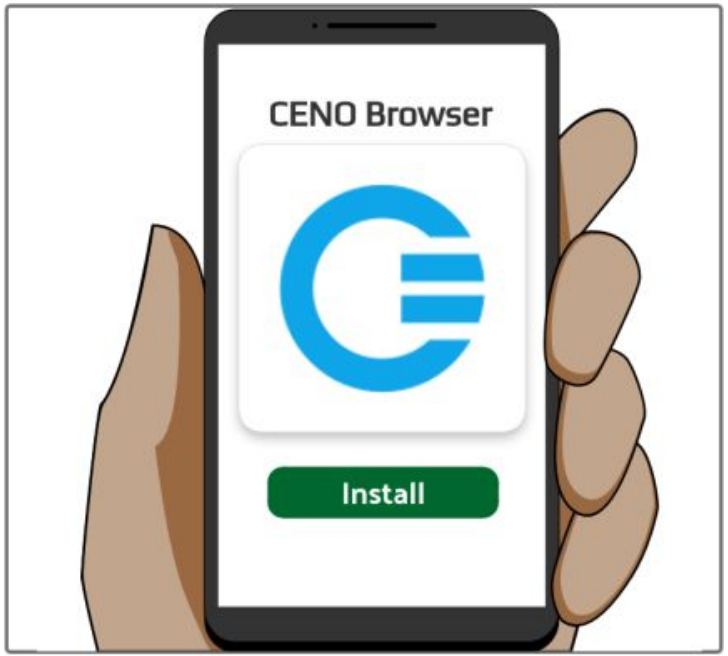


Scenario 1 solution - CENO Browser (Censorship.no)



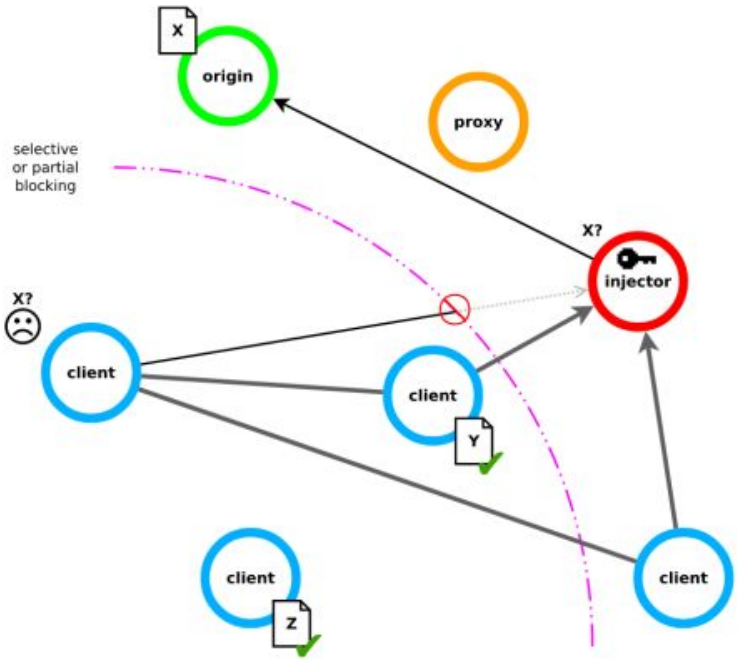
CENO - web browsing via Bitorrent

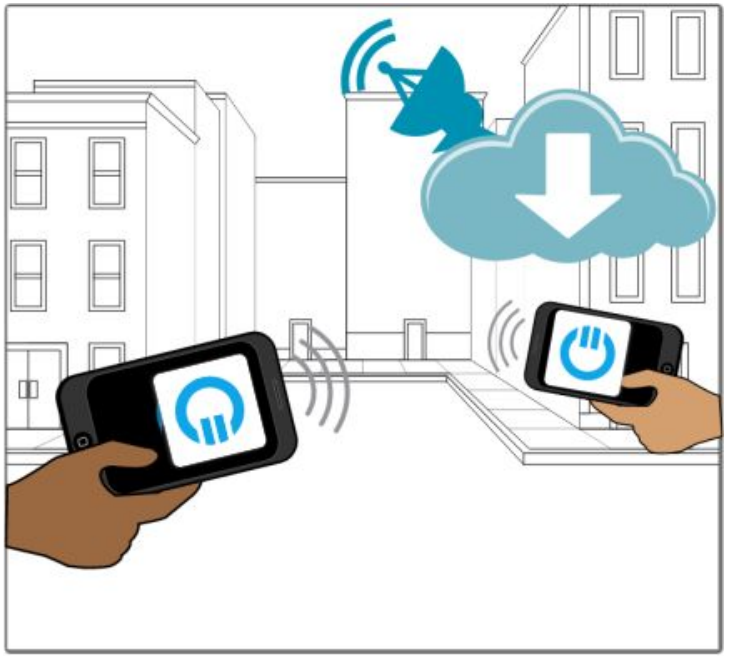




CENO is a mobile web browser for storing and sharing web content anywhere.

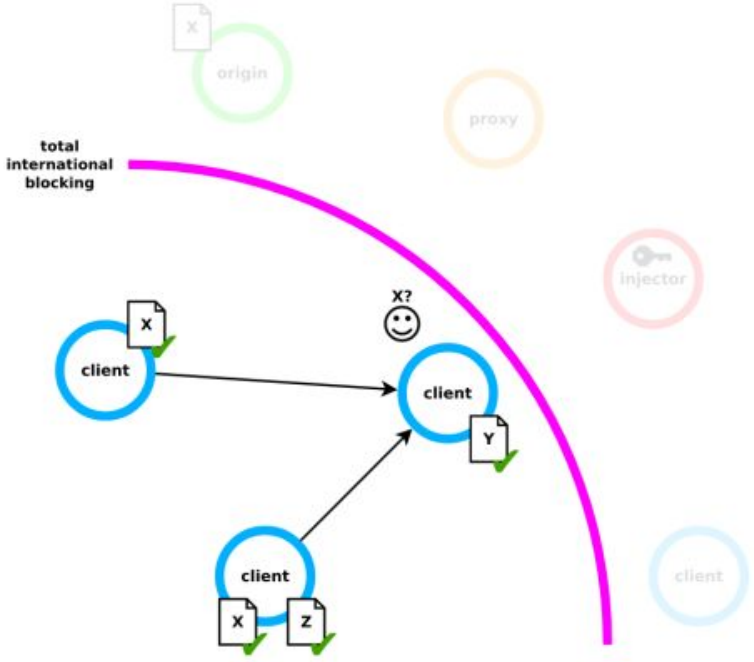
CENO - cooperative browsing

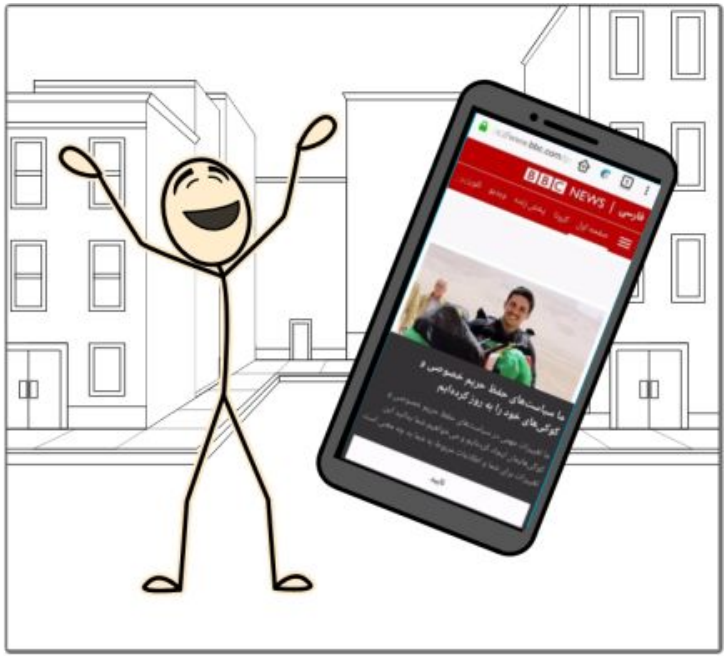




CENO users create small-world networks to connect to each other, and thereafter to a bridge outside the censored zone.

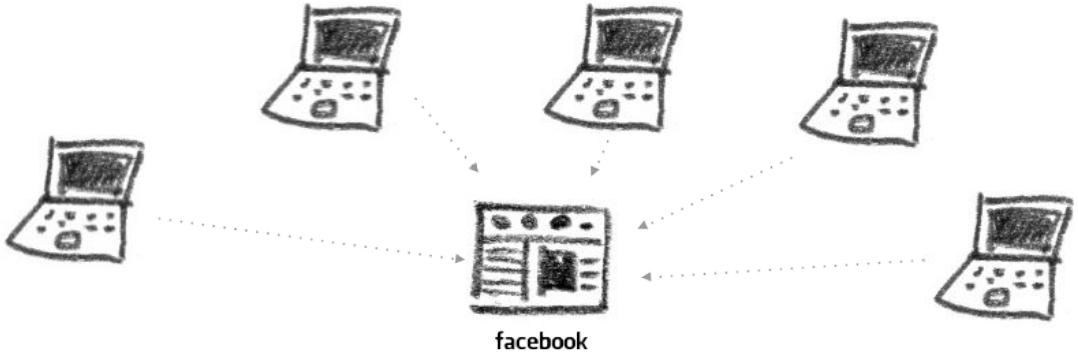
CENO - decentralized caching





Once a website is accessed by a single CENO user, it is stored and shared inside the country peer-to-peer.

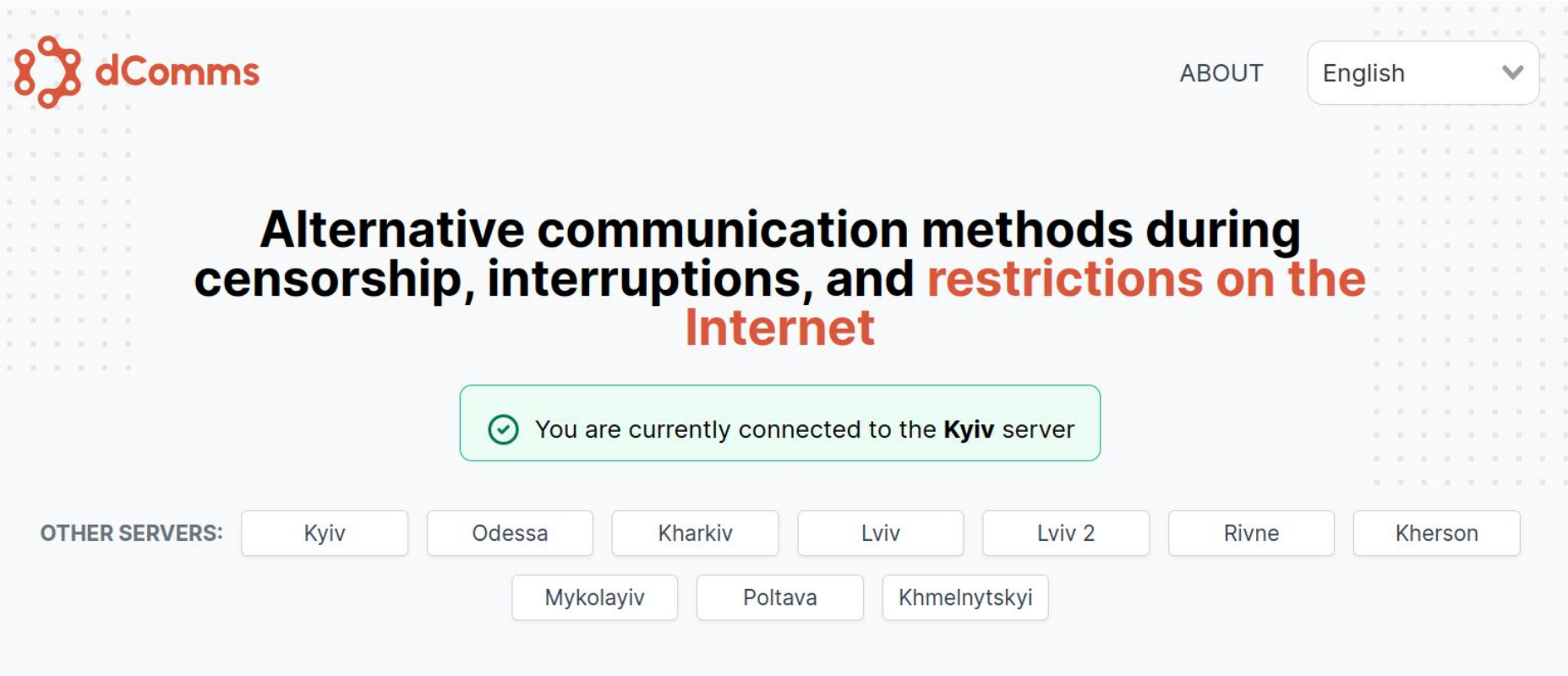
Internet shutdown - scenario #2
Disconnection of external connectivity



Internet 1 + 2 = 3

dComms OUINET ceno

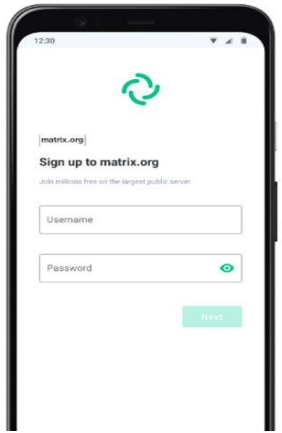
Scenario 2 solution - decentralized communications

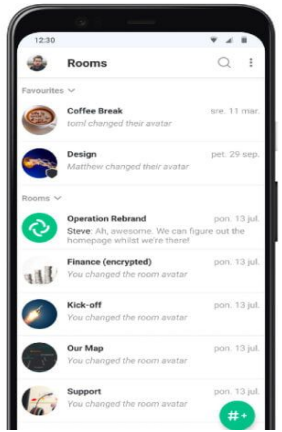


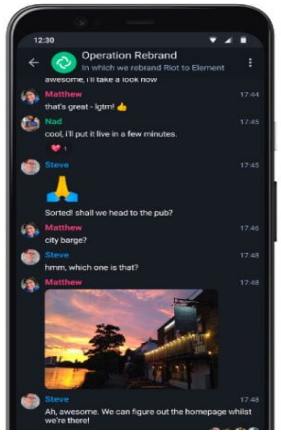
Scenario 2 solution - decentralized communications

BRIAR

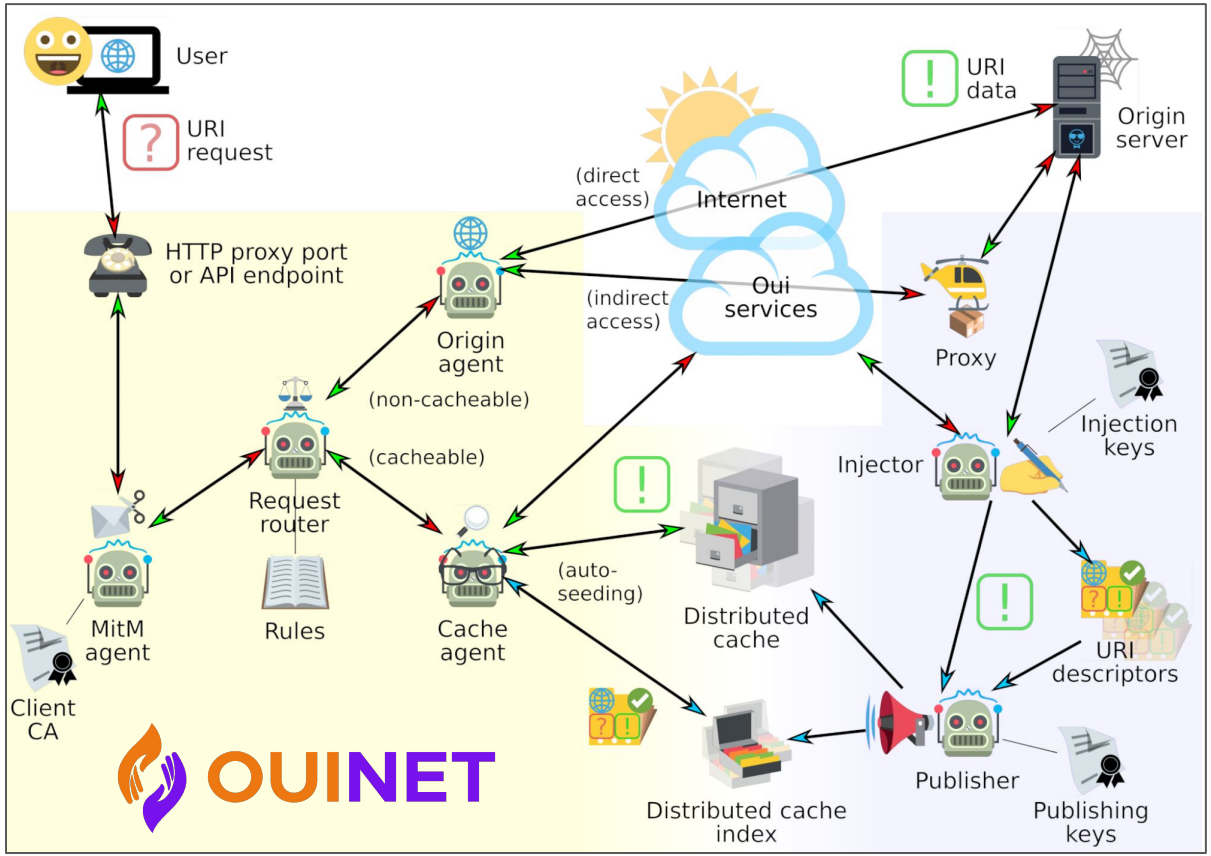
ceno







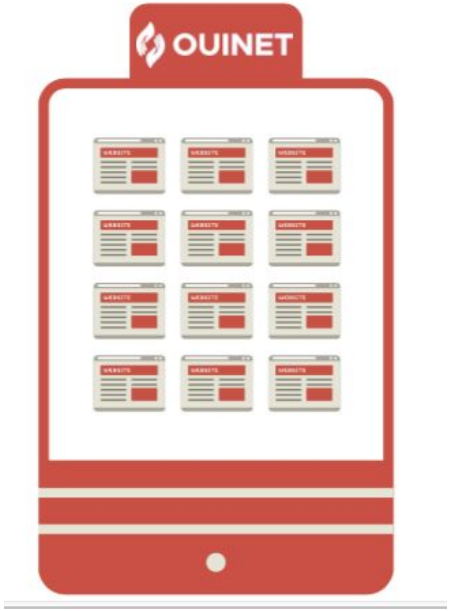
Scenario 2 solution - decentralized content distribution

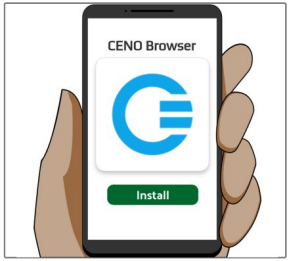


OuiCrawl - It’s all about the cache

+

OuiCrawl

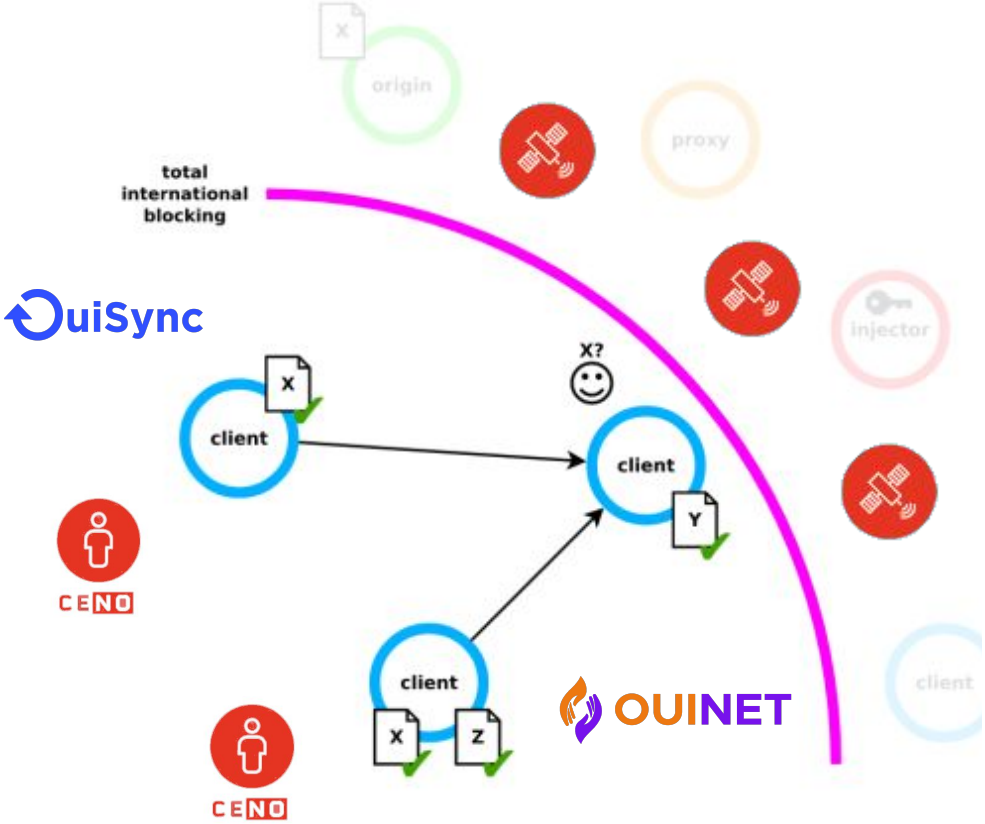




IP over MPEG-TS

```
SERVICES ANALYSIS REPORT
Global PID's
TS packets: 115,844, PID's: 3 (clear: 3, scrambled: 0)
   PID  Usage                                  Access        Bitrate
 Total  Global PID's ..... C       21,929 b/s
 Subt.  Global PSI/SI PID's (0x00-0x1F) ..... C       18,143 b/s
0x0000  PAT ..... C       15,136 b/s
0x0011  SDT/BAT ..... C        3,006 b/s
0x1FFF  Stuffing ..... C        3,785 b/s
Service: 0x0001 (1), TS: 0x0001 (1), Original Netw: 0xFF01 (65281)
Service name: TooshehTV, provider: Toosheh
Service type: 0x01 (Digital television service)
TS packets: 36,862,639, PID's: 4 (clear: 4, scrambled: 0)
PMT PID: 0x1000 (4096), PCR PID: 0x03E9 (1001)
   PID  Usage                                  Access        Bitrate
 Total  Digital television service ..... C     6,978,069 b/s
0x03E9  MPEG-2 Video (720x576p, @25 Hz, 16:9, 4:2:0) . C       256,160 b/s
0x03EA  MPEG-1 Audio (Audio layer II, 384 kb/s, @44,1  C       403,016 b/s
0x03EB  AC-3 Audio ..... C     6,303,755 b/s
0x1000  PMT ..... C       15,136 b/s
        (C=Clear, S=Scrambled, +=Shared)
```

Resistance to shutdowns - cache and deliver



\+ OuiCrawl

OUINET

Deliver and propagate

Satellite Internet

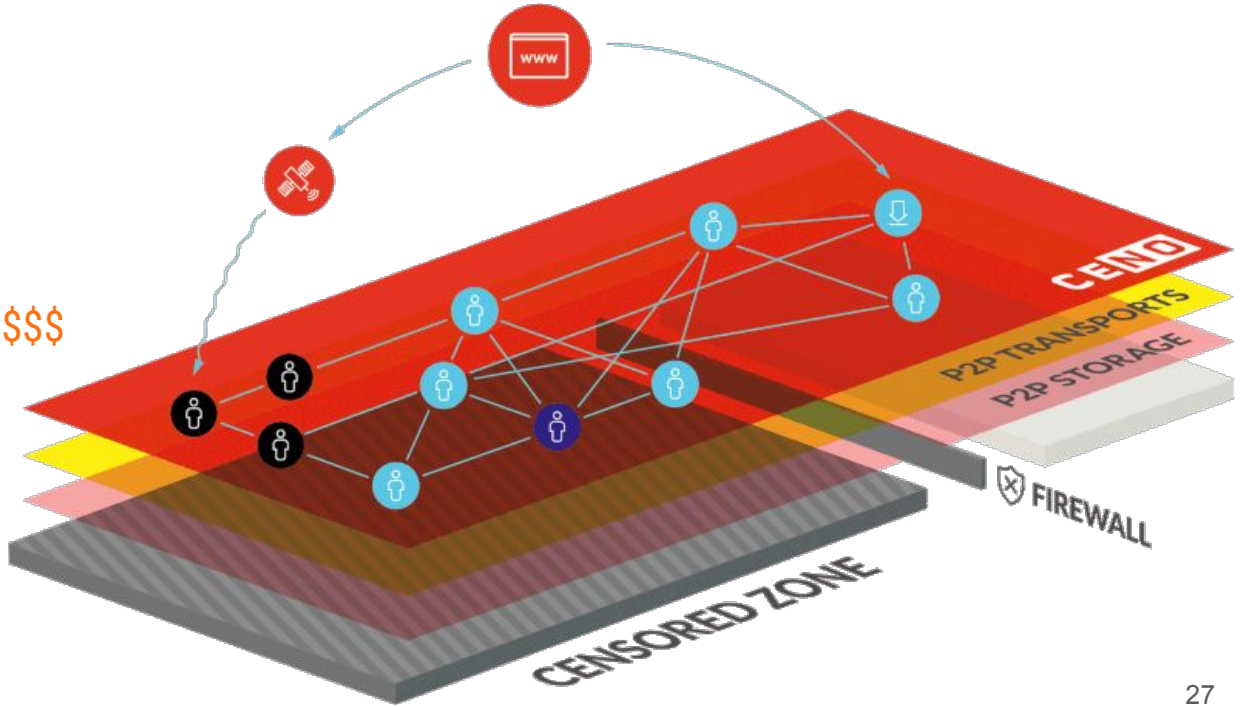
- Just a few injection nodes
- Near border coverage

Satellite TV

- Pay for upstream / broadcast $$$
- Donated time from TV show
- Donated null packets

Propagation

- Ouinet
- Web caching standard



GLOBAL NOG ALLIANCE

deflect.ca
censorship.no
dcomm.net.ua
nadiyno.org

@equalitie

dmitri@equalitie.org