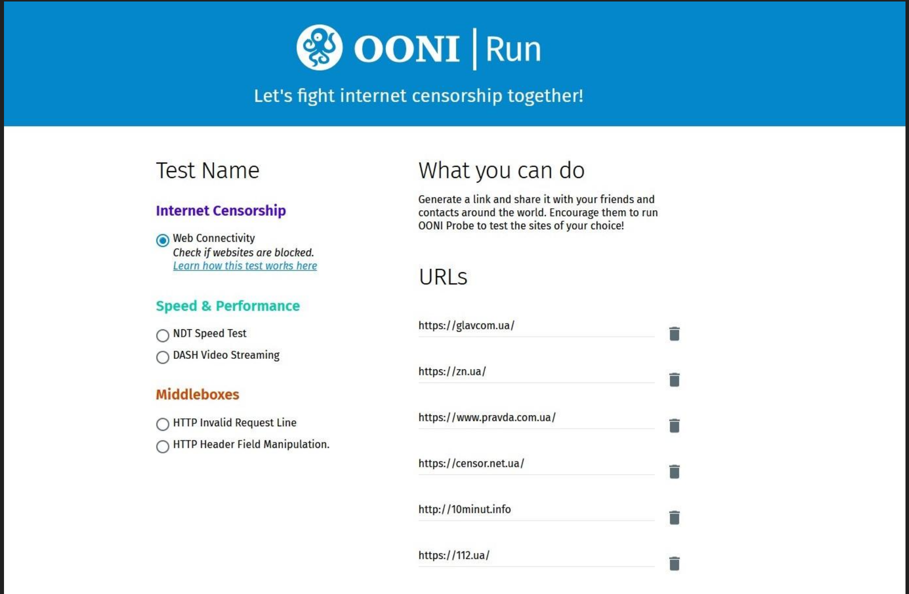
How we tried to establish a nationwide internet censorship measurement system in Ukraine

Digital
Security
Lab

Methodology

- Measurements are conducted by monitors using their personal mobile devices (except for Donbas and Crimea) on public WiFi access points with different ISPs.
- To prevent data distortion, each measurement should be done twice, if possible - 3 times.
- Monitors provide report_ids from tests, that are later used by our data analyst. Measurements are conducted on a weekly basis during the measurement months.
- Measurements are conducted on a weekly basis during the measurement months.

Lists



OONI | Run

Let's fight internet censorship together!

Test Name

Internet Censorship

● Web Connectivity
Check if websites are blocked.
Learn how this test works here

Speed & Performance

○ NDT Speed Test
○ DASH Video Streaming

Middleboxes

○ HTTP Invalid Request Line
○ HTTP Header Field Manipulation.

What you can do

Generate a link and share it with your friends and contacts around the world. Encourage them to run OONI Probe to test the sites of your choice!

URLs

https://glavcom.ua/
https://zn.ua/
https://www.pravda.com.ua/
https://censor.net.ua/
http://10minut.info
https://112.ua/

- 4 custom lists (main part of Ukraine, annexed Crimea, occupied parts of Donetsk and Luhansk regions) of sites created using OONI Run
- Links shared via email

Monitoring

- In each region of Ukraine (23 monitors), in annexed peninsula Crimea (4 monitors) and temporarily occupied and uncontrolled territories of Donetsk and Lugansk region (3 monitors).

Analysis

OONI API -> JSON -> CSV

The most important attributes:

- website name
- provider name and ASN
- connectivity status
- control
- predefined bocking reason
- DNS data
- HTTP code
- response text

Is it blocked?

If it says “the website’s blocked”, it’s definitely blocked.

Inaccessible for a long time - probably blocked
Consistent errors - probably blocked
Resolves to localhost or provider’s IP - almost definitely blocked

We tried to look at patterns, not just at isolated measurements

Problems

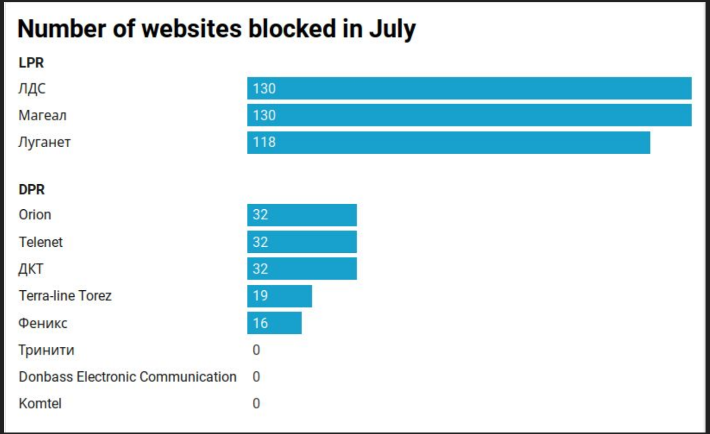
- Measurements conducted on different mobile devices, some of them running old and outdated OS, on Wi-Fi AP that are set up in a variety of ways and on different ISP with different bandwidth and other limitations) provides lots of messy and misleading data. For example, we faced a site being blocked one week, and accessible the other.
- Or we saw blocking patterns of Crimea ISPs being the same for all the ISPs one month, and changing the other. So, the dynamics mostly prove that our methodology does not provide clear and sustainable data to be analysed.
- The data quality was not very consistent. We lost some data due to timed out measurements, human errors (sometimes people measured wrong website lists or wrong providers), control failures and so on.

Notable findings for the occupied territories

Eastern occupied territory: DPR vs LPR
Lugansk providers generally block more websites while some Donetsk providers did not block anything at all.

The only website that was blocked by all providers (except for those not blocking anything) was a local Donetsk city news website, not some big Ukrainian media or an activist site.

Crimean data suggest that some local providers take initiative and block websites that are not in the official Russian blocking list.



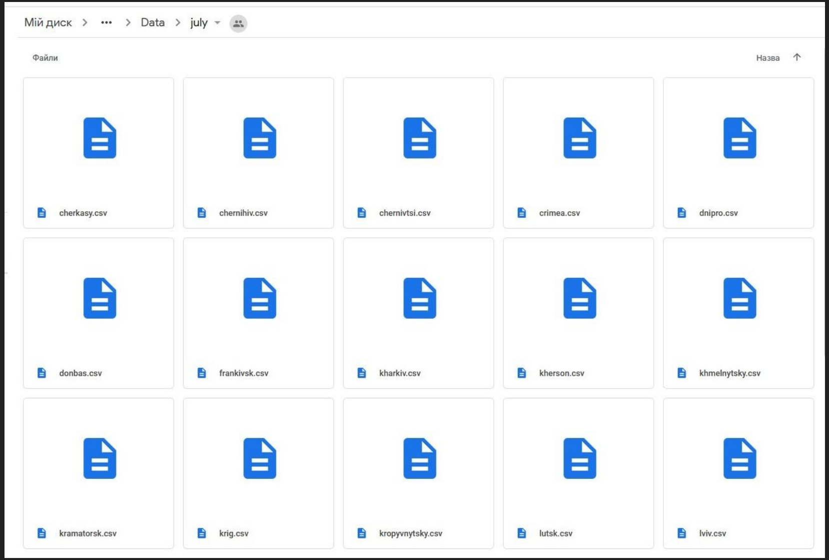
Notable findings about non-occupied territories

The most prolific blockers were the big providers working in all regions of Ukraine. Three such providers blocked almost all websites from our list. Local providers working only in one or several regions normally blocked much less. However, one of these major providers had a more relaxed blocking policy in one big Eastern city, leaving over 100 websites accessible.

Generally, providers exercised discretion regarding their blocking policies. Many of them did not even block half of the official list. However, we did not detect any website that would not be blocked by at least one provider.

The blockings were mostly consistent throughout the year, no major decrease or increase in blocking were detected.

Data



Мій диск > ••• > Data > july

Файли

Назва ↑

cherkasy.csv

chernihiv.csv

chernivtsi.csv

crimea.csv

dnipro.csv

donbas.csv

frankivsk.csv

kharkiv.csv

kherson.csv

khmelnytsky.csv

kramatorsk.csv

krig.csv

kropyvnytsky.csv

lutsk.csv

lviv.csv

- Stored in .csv files on our Google Disk and is available publicly for all the researchers: https://drive.google.com/drive/folders/1tdW8zISbvk-KPo-Wf8YCtfLSuQg7J6PV

Conclusions

We discovered that our methodology does not provide long-term and sustainable blockings measurement system.

First of all, there’s lots of differences in technical setups for conducting measurements (different mobile devices, some of them running old and un-updated OS, on Wi-Fi AP that are set up in a variety of ways and on different ISP with different bandwidth and other limitations).

Also, measurements should be conducted by monitors on a regular basis, but it’s hard to accomplish due to the human factor (people got sick, went on vacation, fail to do the job on schedule, etc) and technical problems (devices malfunction, measurements with errors, public WiFi AP closed, etc).

Contacts

Digital Security Lab Ukraine

facebook.com/cyberlabUkraine

koushnir@dslua.org