DIGITAL MEDUSA

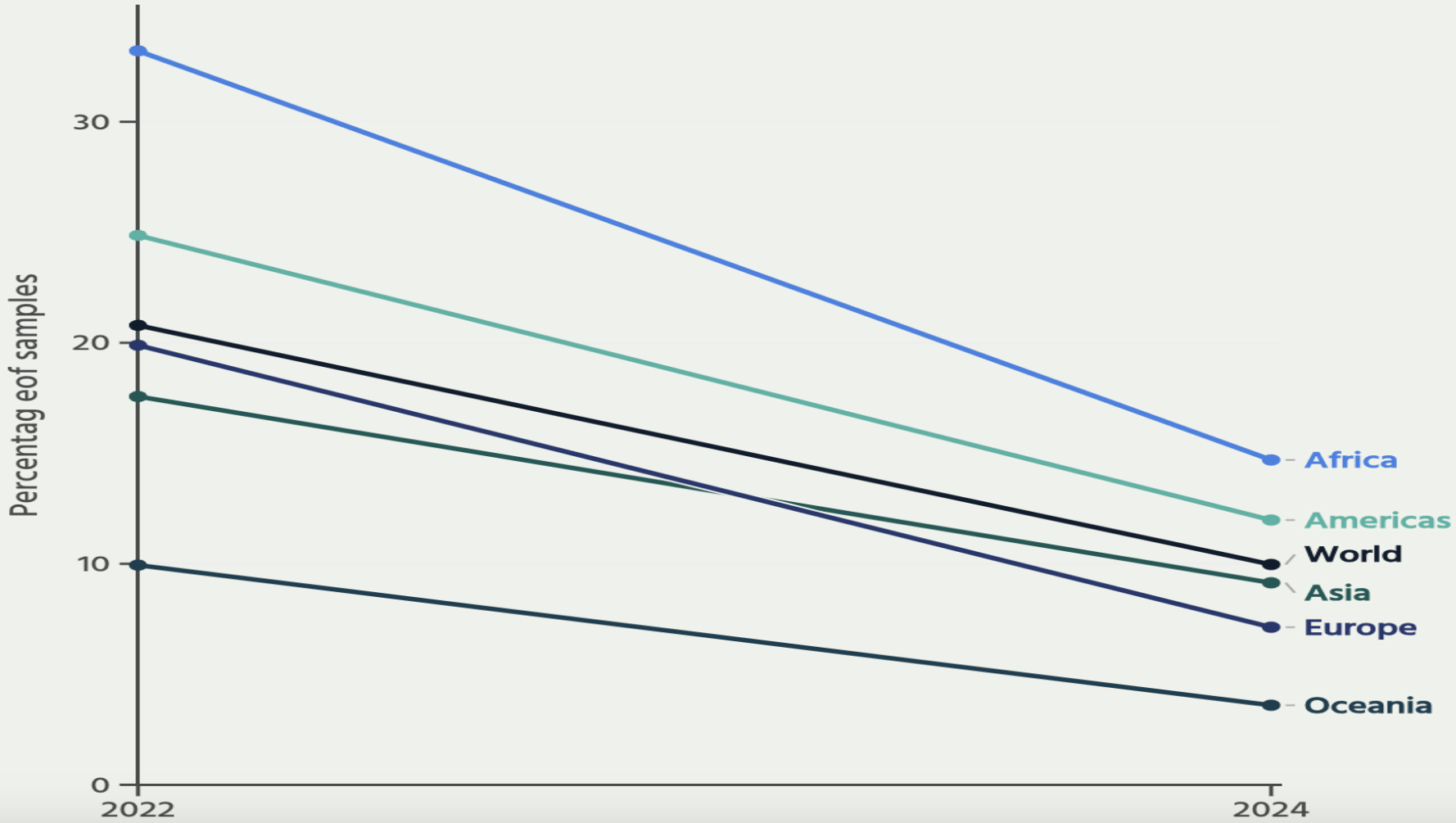
IS BIG DNS TAKING OVER?

Digitalmedusa.org
Funded by Digital Infrastructure Insights (Ford Foundation, Sloan, Omidyar, and Schmidt Futures)

Preliminary report

- Based on APNIC LAB data, Since 2022, the use of public DNS services has halved in many regions.
- Read the draft report here: https://digitalmedusa.org/wp-content/uploads/2023/12/Upload-DNS-Resolvers-First-Draft-October.pdf
- Final draft will be published Beginning of April 2025

Change in usage globally and regionally between 2022 and 2024



DIGITAL MEDUSA

Stopping the tragedy of open source DNS resolvers: how can the Internet community help with providing and maintaining open source DNS resolvers?

Digitalmedusa.org

Funded by Digital Infrastructure Insights (Ford Foundation, Sloan, Omidyar, and Schmidt Futures)

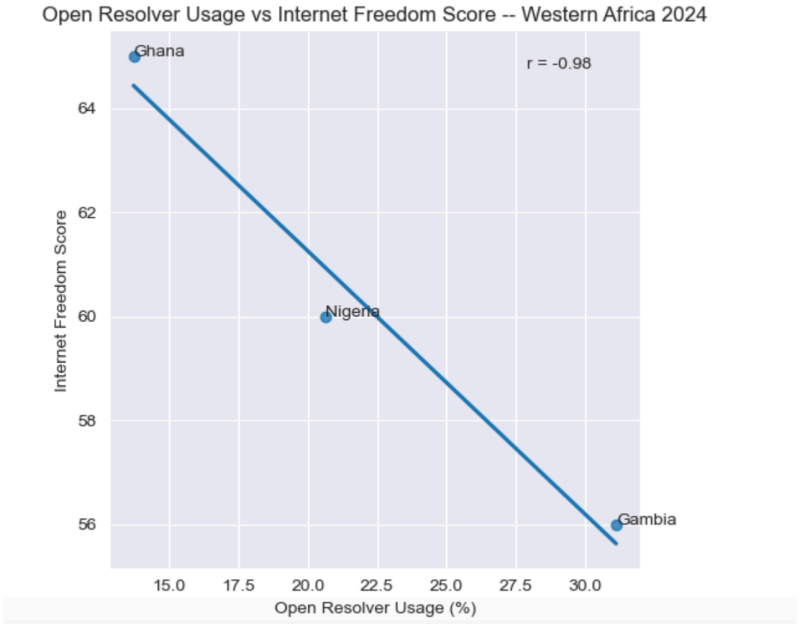
Public DNS resolvers are needed for freedom and decentralization

- We identified a high percentage of Internet users in regions with low Internet and Press freedoms, including Central Asia and Middle and West Africa, still using public DNS resolvers. Which might show a possible correlation.

- Open source software in DNS resolvers can provide a more affordable solution which might be easier to maintain and less costly, hence lead to proliferation of popular independent DNS resolvers and encourages the ISPs to provide their own

Correlation: Western Africa

There was a negative correlation between Internet freedom index and usage of open resolvers in Western Africa. Where there was lower Internet freedom, there was a higher usage of public resolvers.



How can we promote the use of open source and free public DNS resolvers?

- There are only a few public DNS resolvers that are popular and use open source software, Cloudflare and Google DNS are not among them but are the most popular DNS public resolvers
- One hypothesis was that perhaps ISPs don't use open source DNS resolvers or are open source averse. But our interviewees did not express such hesitations
- So why do we not see a proliferation of public DNS resolvers and why do some ISPs and network operators prefer to use closed source resolvers?
    - Legal liability: Regulatory frameworks and government requests to block the domain names they don't like (costly, causes liability)
    - Scaling of not for profit and open source DNS resolvers is hard
    - Network Operators legacy decision to use closed source from early on that cannot be changed
    - Some network operators had hesitation that open source software in DNS resolvers might be less secure but that was not a deal breaker for them
- global regulatory tracker of government requests to block domain name resolution. It also aims to explore whether there are any kinds of correlation between specific political incidents and changes in the use of public DNS resolvers

Debunking the myth that open source DNS software is insecure

PowerDNS competitor Nominum lauds its closed source credits!

Sep 23, 2009 6:00:00 AM

This morning, I was unpleasantly surprised by an advertorial on ZDNET, where PowerDNS competitor Nominum stated that since they are closed source, their technology is inherently more secure. They also cleverly compared Open Source to malware. Nice.

In addition, Nominum stated they have not had any security problems, "unlike the freeware legacy DNS", but this simply is not true as can be seen on their own webpage (which will probably be 'cleaned up' shortly).

There are some true gems in the interview, cleverly titled "Why open-source DNS is 'internet's dirty little secret'".

About the Author

Bert Hubert
Principal, PowerDNS

Categories

PowerDNS

Creating best practices on how to run DNS resolvers with open source software

- Look at RIPE Task Force DNS Resolver Best Practices: https://www.ripe.net/publications/docs/ripe-823/
- “Software Considerations”
    - Open Source
    - Choose any well-maintained DNS software you are comfortable using.
    - Regardless of which software you choose, ensure you have somewhere to go for support. In the case of open source software, consider providing financial support to ensure continued development. Some open source maintainers take donations, while others offer support contracts.
    - There are both open source and proprietary implementations of DNS resolver software. Mixing these is also possible, for example, by using proprietary extensions with open source software or deploying open source software modified in-house.
    - General observations:
    - Software licensing is orthogonal to software security. Neither is proprietary software less secure on principle nor are contributions by "unknown" developers more of a risk in open source.
    - Benefits of open source:
    - Open source allows for inspection, independent auditing, and troubleshooting.
    - Open source can avoid vendor lock-in.
    - Open source can aid internet standards development.
    - Widely-deployed open source implementations allow proponents of standards drafts to contribute proof of concept implementations without permission or cooperation of vendors.

Help with legal compliance

- Creating a legal and policy track to help Public DNS providers to comply with the law
- Keep the DNS as much as possible global!

Contact DigitalMedusa

- farzaneh@digitalmedusa.org