Internet Censorship Tracker

Data Intensive Internet Computing

Dr. Vasilis Ververis, Prof. Dr. Vaibhav Bajpai

https://hpi.de/bajpai/

***A* prototype for a free and open Internet censorship tracker.**
Internet censorship is an ongoing challenge, and the anti-censorship community lacks a unified approach to documentation and education. While there are efforts to measure and monitor network interference, censorship, and blocking. censorship, and blocking, there is no centralized database that is updated in real time with detailed technical evidence from multiple sources.

Objectives

In order to do so, the primary objective is to create a glossary that will collate and evaluate information on network interference incidents, which will then be publicly listed on an open database and relevant website for universal access. It will help to establish an open reporting methodology that can bring together the Internet freedom community and facilitate a collective response to incidents of Internet censorship.

Deployment

The proposed project aims to establish a system akin to CVE [1] that can monitor and document instances of Internet censorship, network disruptions, and physical infrastructure disruptions that affect Internet access and connectivity, encompassing a wide range of digital services and platforms that rely on the Internet for their functionality. This can include online applications, cloud-based services, social media platforms, and other services.

Who it will help?

This project is intended for journalists, researchers, activists, lawyers, policy regulators, technologists, and other entities that wish to gain insights into the prevalence of

censorship and network disruption in a specific country, region, or network. It may also serve to raise awareness about the issues surrounding Internet censorship, particularly in instances where a country experiences a complete network blackout.

What is CVE?

CVE (Common Vulnerabilities and Exposures) is free, publicly available methodology used by the digital security community to define and identify publicly known cybersecurity vulnerabilities and exposures. This standardized approach makes it easier to share data across various tools, databases, and services. Each CVE entry consists of:

- A unique identification number
- A detailed description of the vulnerability or exposure
- At least one public reference

By providing a common language and framework for describing security issues, CVE enables diverse security professional, research and the community to:

- Correlate vulnerabilities across different systems and data sources
- Compare the coverage and effectiveness of security tools and services
- Facilitate the sharing of security data and knowledge

For more information, please contact Vasilis Ververis (vasilis.ververis@hpi.de).

***Sources**:*

[1] CVE – Common Vulnerabilities and Exposures. Mitre Corporation. https://cve.mitre.org/