Investigating Nation-state Internet Censorship Methods

Alexander Master, Christina Garman  
Computer Science - Purdue University

Summary

Nation-states impose various levels of censorship on their Internet communications. As access to Internet resources has grown among the global population, some governments have demonstrated an increased willingness to filter content, throttle connections, or deny access to Internet resources within their sphere of influence. Researchers, policymakers, and civil liberty advocates need an understanding of the technical means that Internet censors implement. This work presents a research framework that provides a worldwide view of nation-state Internet censorship, derived from Internet measurement data and systematic literature review.

Motivation

Framework & Data (Abridged)

Our Contributions

(1) Extensive cross-sectional study of 70 countries  
(2) Systematic Literature Review over 20-year period  
(3) Easily reproducible framework for global data analysis

Takeaways

Decline in use of blunt/naive techniques

• IP blocklists less effective, difficult to maintain  
• IPv6 implementations  
• Collateral damage – CDNs, political considerations  
• Port blocking is rare

Historical URL filtering (HTTP) is less effective

• Mozilla Telemetry report, Oct 2021 82% of the web is TLS traffic [6]

Troubling rise in use of Internet Shutdowns (29/70 nations)

Formerly resource-intensive methods gaining traction

• Use of SNI-based blocking via DPI (ECH is needed!)  
• Protocol targeting as E2EE encryption proliferates  
• More regimes willing to invest in deep packet inspection (DPI) technology to meet their goals, while avoiding overblocking which results in economic collateral damage

Surprising incidents in understudied countries, such as Canada and the United Kingdom

References: