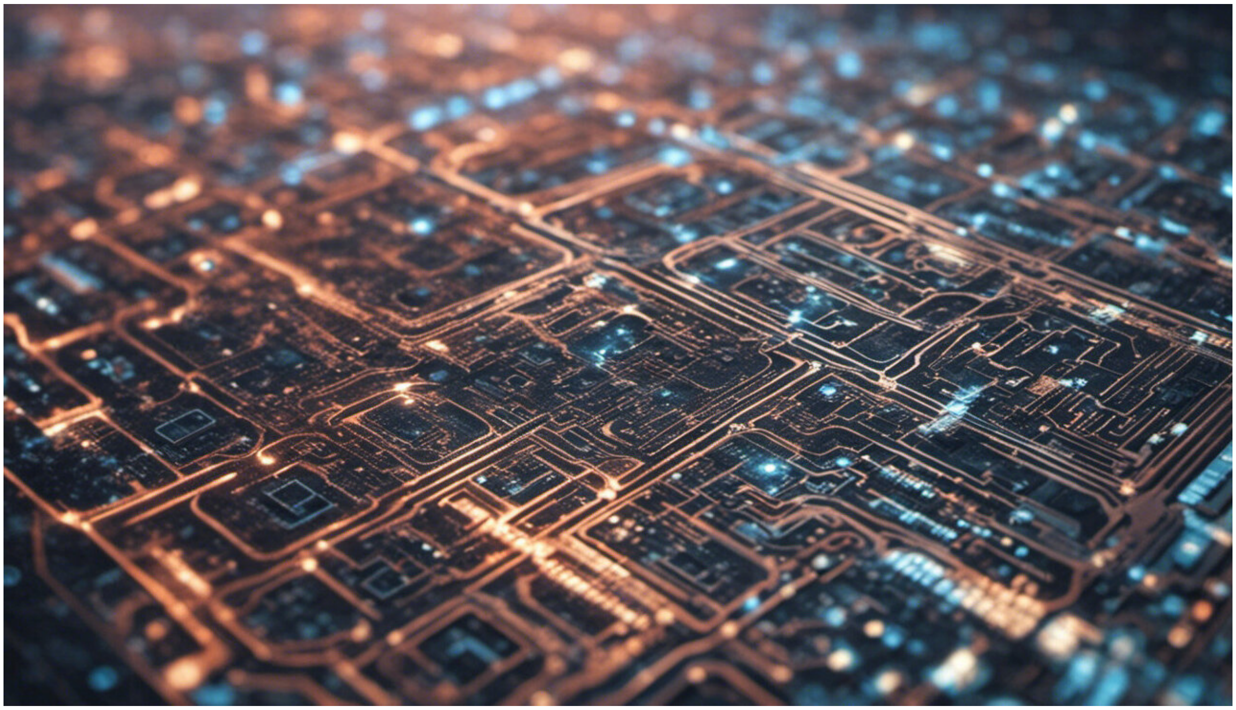
# Lessons on censorship from Syria's internet filter machines

November 18 2014, by Emiliano De Cristofaro



Credit: AI-generated image (disclaimer)

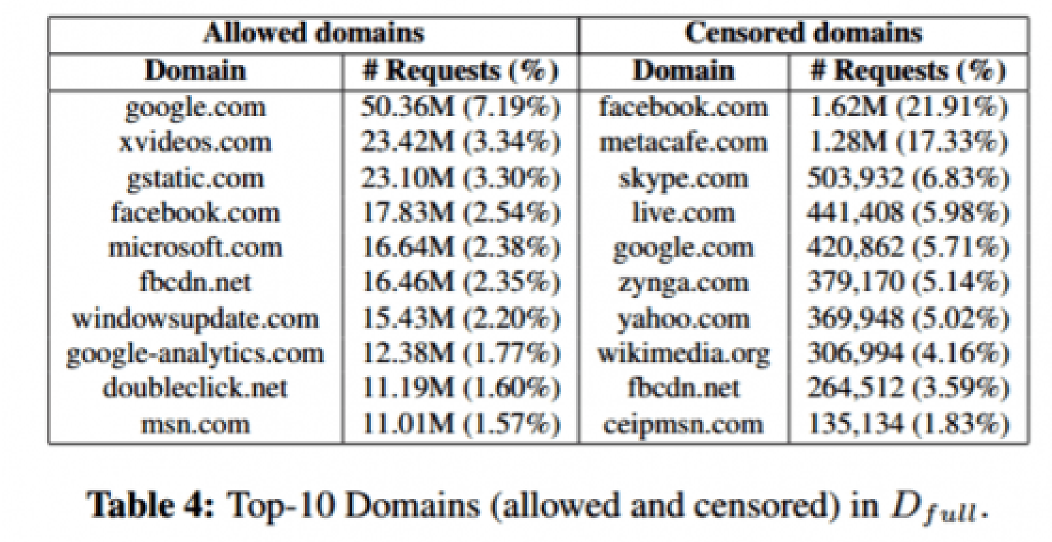
Norwegian writer Mette Newth once wrote that: "censorship has followed the free expressions of men and women like a shadow throughout history." As we develop new means to gather and create information, new means to control, erase and censor that information evolve alongside it. Today that means access to information through the internet, which motivates us to study internet censorship.

Organisations such as Reporters Without Borders, Freedom House, or the Open Net Initiative periodically report on the extent of censorship worldwide. But as countries that are fond of censorship are not particularly keen to share details, we must resort to probing filtered networks, that is, generating requests from within them to see what gets blocked and what gets through. We cannot hope to record all the possible censorship-triggering events, so our understanding of what is or isn't acceptable to the censor will only ever be partial. And of course it's risky, even outright illegal, to probe the censor's limits within countries with strict censorship and surveillance programs.

This is why the leak of 600GB of logs from hardware appliances used to filter internet traffic in and out of Syria is a unique opportunity to examine the workings of a real-world internet censorship apparatus.

Leaked by the hacktivist group Telecomix, the logs cover a period of nine days in 2011, drawn from seven SG-9000 internet proxies. The sale of equipment like this to countries like Syria is banned by the US and EU. California-based manufacturer Blue Coat Systems denied making the sales but confirmed the authenticity of the logs – and Dubai-based firm Computerlinks FZCO later settled on a US$2.8m fine for unlawful export. In 2013, researchers at the University of Toronto's Citizen Lab demonstrated how authoritarian regimes in Saudi Arabia, UAE, Qatar, Yemen, Egypt and Kuwait all rely on US-made equipment like those from Blue Coat or McAfee's SmartFilter software to perform filtering.

This technology is extremely powerful as it can perform deep-packet inspection, that is, examining in detail the contents of network traffic. They provide censors with a simple interface to fine-tune filtering policies, practically in real time.



| Allowed domains | | Censored domains | |
|---|---|---|---|
| Domain | # Requests (%) | Domain | # Requests (%) |
| google.com | 50.36M (7.19%) | facebook.com | 1.62M (21.91%) |
| xvideos.com | 23.42M (3.34%) | metacafe.com | 1.28M (17.33%) |
| gstatic.com | 23.10M (3.30%) | skype.com | 503,932 (6.83%) |
| facebook.com | 17.83M (2.54%) | live.com | 441,408 (5.98%) |
| microsoft.com | 16.64M (2.38%) | google.com | 420,862 (5.71%) |
| fbcdn.net | 16.46M (2.35%) | zynga.com | 379,170 (5.14%) |
| windowsupdate.com | 15.43M (2.20%) | yahoo.com | 369,948 (5.02%) |
| google-analytics.com | 12.38M (1.77%) | wikimedia.org | 306,994 (4.16%) |
| doubleclick.net | 11.19M (1.60%) | fbcdn.net | 264,512 (3.59%) |
| msn.com | 11.01M (1.57%) | ceipmsn.com | 135,134 (1.83%) |

**Table 4:** Top-10 Domains (allowed and censored) in $D_{full}$.

A sample of requests blocked. Abdelberi Chaabane et al., Author provided

## Inside a censor's mind

At the recent ACM Internet Measurement Conference we presented our paper detailing the relatively stealthy but targeted censorship system that we'd found from examining the logs.

Internet traffic in Syria was filtered in several ways. IP addresses (the unique addresses of web servers on the internet) and domain names (the URL typed into the address bar) were filtered to block single websites such as badoo.com or amazon.com, entire network regions (including a few Israeli subnets), or keywords to target specific content. Instant messaging, tools such as Skype, and content-sharing sites such as Metacafe or Reddit were heavily censored. Social media censoring was limited to specific content and pages, such as the "Syrian Revolution" facebook page.

The appliances were sometimes misconfigured, meaning the filter caused some collateral damage – for instance, all requests with the keyword "proxy" were blocked, probably in an effort to curb the use of censorship-evading proxies, but this also had the effect of blocking adverts and certain plug-ins that had no relation to banned content.

We found that Syrian users did try to get around the filters, using tools such as Tor, or virtual private networks (encrypted tunnels between two computers using the public internet), and that these were fairly effective. We also noticed that some tools not necessarily designed with circumventing censorship in mind could also be used to access blocked content – for example using peer-to-peer programs such as BitTorrent to download blocked software (such as Skype) and using Google Cache to access (over HTTPS) cached and mirrored versions of blocked web pages.

## Avoiding the censor's knife

What emerges is the importance of encrypting web traffic by using secure (HTTPS) rather than standard (HTTP) web browsing. Many requests caught by the filter were only possible because keywords in the content of unencrypted network traffic could be read by the appliances. If traffic is encrypted, the page requested from the target domain, or a specific keyword in the request are not accessible. Through their efforts to enforce HTTPS by default, providers like Google and Facebook are taking steps in the right direction. They also serve a double purpose: protecting users' privacy against mass-surveillance, while also making it harder to implement fine-grained censorship policies.

We did consider that our work might help organisations on both sides of the censorship line. But we decided to publish because we believe that evidence-based analysis of censorship practices can help understand the underlying technologies, policies, strengths and weaknesses – and can inform the design of tools designed to evade the censor's knife.

While Western countries rely on export regulations and sanctions to restrict the worldwide availability of surveillance and censorship technologies – while apparently deploying them for their own use, as the Snowden files have revealed – it is time we had an open debate about their effectiveness and what can be done to limit their proliferation.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Lessons on censorship from Syria's internet filter machines (2014, November 18) retrieved 26 April 2024 from https://phys.org/news/2014-11-lessons-censorship-syria-internet-filter.html