

# draft-hall-censorship-tech

Joseph Lorenzo Hall (CDT)

IETF 105, PEARG, 24 July 2019

# Background

- Presented first at IETF 91 (Nov 2014)... long time ago!
- Edited mucho, refactored to be structured according to layers
- Accreted authors and updated with things like SK ESNI-blocking, etc.
- JLH diverted his limited IETF time to the IASA 2.0 restructuring work until recently... that is done!

# Summary of the Draft

- Prescription (what to block)
- Identification (how to block)
- Interference (do the block)
- Network layer structure
- A number of small and medium [issues](#) in our [repo](#) to work through

## Table of Contents

|  |    |
|--|----|
| 1. Introduction . . . . .  | 3  |
| 2. Technical Prescription . . . . .  | 3  |
| 3. Technical Identification . . . . .  | 4  |
| 3.1. Points of Control . . . . .   | 4  |
| 3.2. Application Layer . . . . .   | 5  |
| 3.2.1. HTTP Request Header Identification . . . . .                            | 5  |
| 3.2.2. HTTP Response Header Identification . . . . .                           | 6  |
| 3.2.3. Instrumenting Content Providers . . . . .                               | 7  |
| 3.2.4. Deep Packet Inspection (DPI) Identification . . . . .                   | 8  |
| 3.3. Transport Layer . . . . .   | 10 |
| 3.3.1. Shallow Packet Inspection and TCP/IP Header<br>Identification . . . . . | 10 |
| 3.3.2. Protocol Identification . . . . .                                       | 11 |
| 4. Technical Interference . . . . .  | 12 |
| 4.1. Application Layer . . . . .   | 12 |
| 4.1.1. DNS Interference . . . . .  | 12 |
| 4.2. Transport Layer . . . . .   | 14 |
| 4.2.1. Performance Degradation . . . . .                                       | 14 |
| 4.2.2. Packet Dropping . . . . .   | 15 |
| 4.2.3. RST Packet Injection . . . . .  | 15 |
| 4.3. Multi-layer and Non-layer . . . . .                                       | 16 |
| 4.3.1. Distributed Denial of Service (DDoS) . . . . .                          | 16 |
| 4.3.2. Network Disconnection or Adversarial Route<br>Announcement . . . . .    | 17 |
| 5. Non-Technical Prescription . . . . .  | 18 |
| 6. Non-Technical Interference . . . . .  | 18 |
| 6.1. Self-Censorship . . . . .   | 18 |
| 6.2. Domain Name Reallocation . . . . .  | 19 |
| 6.3. Server Takedown . . . . .   | 19 |
| 6.4. Notice and Takedown . . . . .   | 19 |
| 7. Contributors . . . . .  | 19 |
| 8. Informative References . . . . .  | 20 |
| Authors' Addresses . . . . .   | 29 |

# Bigger Issues

- Mitigations: PEARG Co-chair (Shivan) stated that this draft should include a section on mitigations to be in scope for PEARG
  - That is, not just descriptive about *techniques* but about also about *measures to circumvent*
  - May stem from [RFC 6973](#) (cited in charter) which is organized as threats and mitigations
  - Thoughts: techniques change regularly, mitigations even moreso
- Framing: “Censorship” may be too negative of a framing (Bertola)
  - Do it need to say “worldwide blocking techniques”?
- Non-technical forms of prescription and interference should be removed
  - This was to highlight threats that might be of the “rubber hose” variety in censorship
- Does this need to be a regularly-updated-draft?
  - How do people feel? Is this getting to far out in front of the “living standard” discussion?