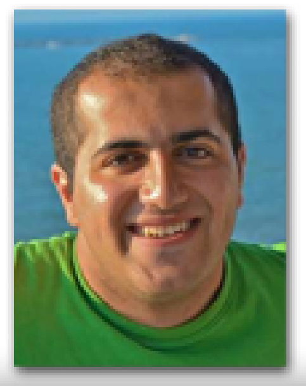
# Who Controls Anonymity?: Control Point Analysis of The Onion Routing Anonymity Network (Tor) 2012

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University



MIT Political Science Department
Supervisor: Dr. Nazli Choucri
Mina Rady

Workshop on
People, Power, and CyberPolitics
November 6 and 7, 2012
MIT Media Lab

PROBLEM DEFINITION: Anonymity networks have played major roles in censorship circumvention and various benign or malicious activities in the cyber domain. Hence, those networks became well defined targets of repressive regimes or law enforcement. In this research, we attempt to infer the various control capacities over the operation of such networks and we take the Tor network as an example. We decompose the operation and process of Tor network across the Cyberspace layers. Then we do survey of existing literature about possible control mechanisms over various locations in the network. Then we extrapolate from the control actions to infer possible political actors who would be able to exercise each control action. We use Tor network model as the subject of this investigation due to its distinctive pervasiveness. We conclude with a comprehensive model that depcits distribution of contol capacities across the actors at different political levels of analysis.

## Research Organization:

1- We identify and depict the process necessary to establish a Tor routing connection and high level diagram of communication activity.

2- Based on core literature on "vulnerabilities" of Tor Network, we extend our analysis by including two critical control capacities:

A) Network Survival Control (i.e. actions that can/did influence the existence of Tor network)

B) Anonymity Threatening Control (i.e. actions that can only undermine the purpose of the network [anonymity]).

3- Then we map actors that p can exploit each network layer, anchored to the control action and outcome.

## Conclusions:

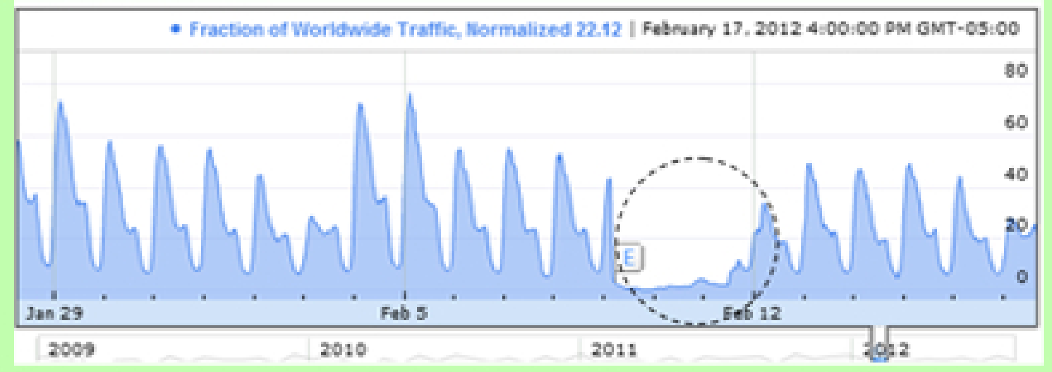
- State Control seems to be ubiquitous. However, most state control actions have been taken solely by China. For rest of nation states, it is very expensive to impose same actions without collateral damage to network integrity (as in Iran's attempt to block SSL packets)
- Control actions of individuals can be very influential if taken collectively by groups of proxy operators; the larger the group, the higher the influence.
- Collective reaction by individuals can overpower a single state's control action.

## Future Research:

1- Map the actors within the Integrated System Framework of Cyberspace -Levels of Analysis and Internet Layers. (Choucri; Clark)

2- Investigate jurisdictional boundaries of various anonymity networks.

| Cyberspace Layer(s) | Political Actor/Level | Control Capacity |
|---|---|---|
| Internet (ISP) | State: China, United Arab Emirates, Saudi Arabia, Iran (Blocked TorProject Site) | Block Tor Website/Mirrors |
| People,Information | Unknown (possible State) : Arab Republic of Syria (Malicious copies of Green Simurgh anonymity software that contained a keylogger malware) | Provide Malicious Copy |
| Logical: Services(DNS) | | Redirect to Malicious Site |

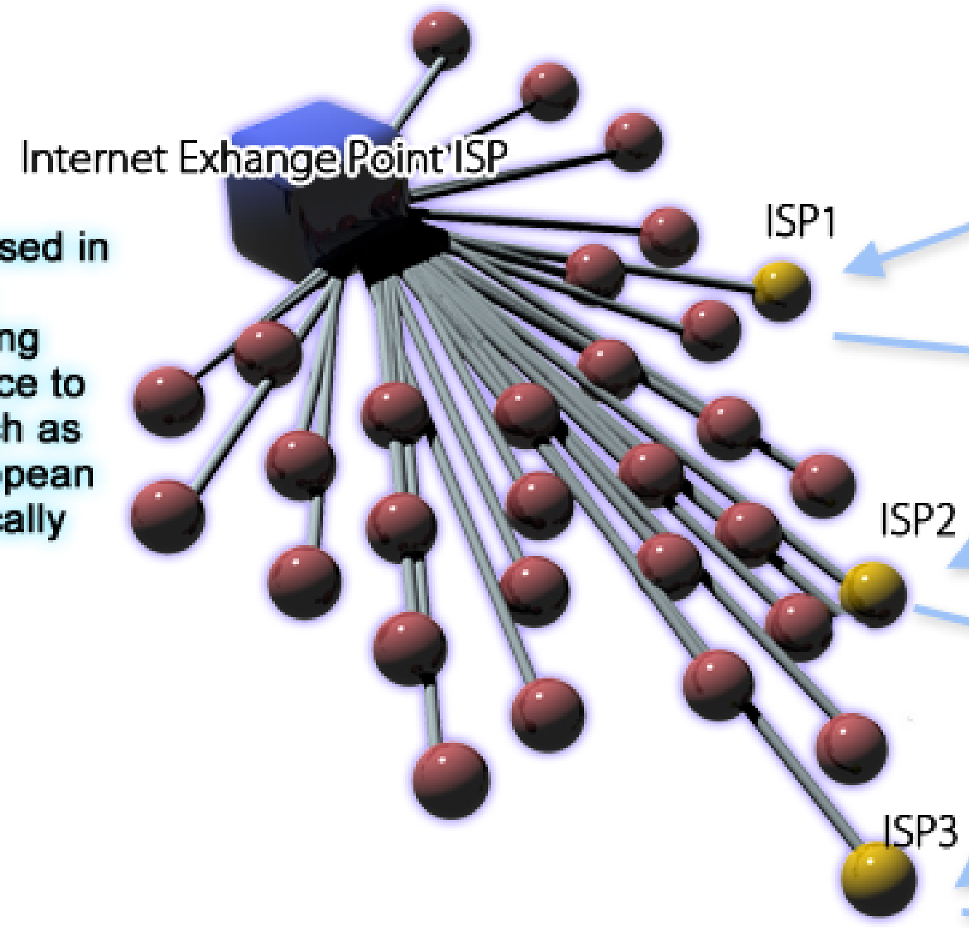
| | | |
|---|---|---|
| Services (Logical), Internet, Application | State: Iran Collateral Blockage of SSL Connections blocked Gmail  Drop down and rise of traffic from Iran to Google's Gmail encrypted service across February 2012 | Block access to Encrypted and/or Unencrypted Gmail |

| | | |
|---|---|---|
| Physical | State: Egypt exercised this action fully during January 2011 and partially during Sinai army operations aginst Jihadists, 2013 | Shut down Internet connectivity (partially or fully) |

| | | |
|---|---|---|
| Internet | State/ISP: Great Firewall of China | HTTP Header Filtering (By distinguishing desintation I Ps ∈ Public Relays IPs) |
| Internet | State/ISP: Great Firewall of China | Deep Packet Inspection (DPI) to distinguish Tor Protocol |
| Internet | State/ISP: Iran (January 2011) | DPI to distinguish and block SSL connections |

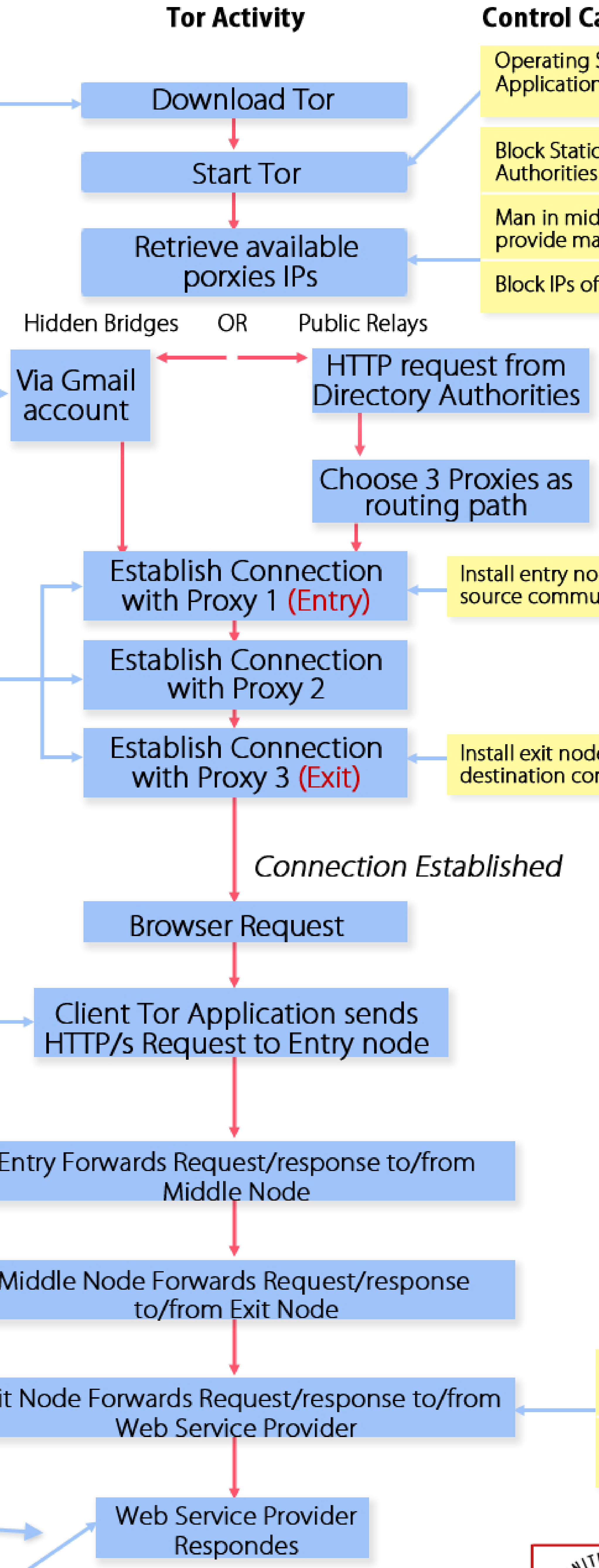
### Internet Exchange Level Traffic Analysis*

Physical Layer



*Traffic Analysis attacks were proposed in various papers exploiting data of IX points. They were experimented using historical data. This gives significance to high degree IX points in regions such as Europe (because of clusters of European language sites and users are physically intense in Europe)

| | | |
|---|---|---|
| People, Information, Application (Web Service Provider) | Sate/Individuals/Organiztions Wikimedia blocks edits from Tor Exit nodes | Block response or embed tracking code in response |



Tor Activity

Download Tor

Start Tor

Retrieve available porxies IPs

Hidden Bridges OR Public Relays

Via Gmail account

HTTP request from Directory Authorities

Choose 3 Proxies as routing path

Establish Connection with Proxy 1 (Entry)

Establish Connection with Proxy 2

Establish Connection with Proxy 3 (Exit)

*Connection Established*

Browser Request

Client Tor Application sends HTTP/s Request to Entry node

Entry Forwards Request/response to/from Middle Node

Middle Node Forwards Request/response to/from Exit Node

Exit Node Forwards Request/response to/from Web Service Provider

Web Service Provider Responds

| Control Cacapacity | Political Actor/Level | Cyberspace Layer(s) |
|---|---|---|
| Operating System Blocks Application | Individual,State (Machine owner) Global (OS manufacturer) | OS Manufacturers/ Providers/ Firewall, Machine Owner |
| Block Static IPs of Directory Authorities | State: Great Firewall of China | Services, Internet |
| Man in middle attack to provide malicious proxy IPs | State, Indvidual in local network/ISP | Application, Information, People |
| Block IPs of Public Relays | State: Great Firewall of China | Services, People, Internet |

| | | |
|---|---|---|
| Install entry node that monitors source communication | Individual, State, Non Profit:Any Proxy Operator. | People, Interenet |
| Install exit node that monitors destination communication | Individual, State, Non Profit:Any Proxy Operator. | People, Internet |

| | | |
|---|---|---|
| sslstrip attack on exit SSL redirects | Individual, State, Non Profit:Any Proxy Operator. | People, Application |
| Embed Malicious Code uncrypted terminal exit/entry traffic | State, Non Profit | People, Application |

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s)and do not necessarily reflect the views of the Office of Naval Research.
Also, I extend my deepest appreciation to the many members of the Internet community that have contributed their time, interest, and feedback to this research. This work would not be possible without their help and support.