

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



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



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

**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 depicts distribution of control capacities across the actors at different political levels of analysis.

### Research Organization:

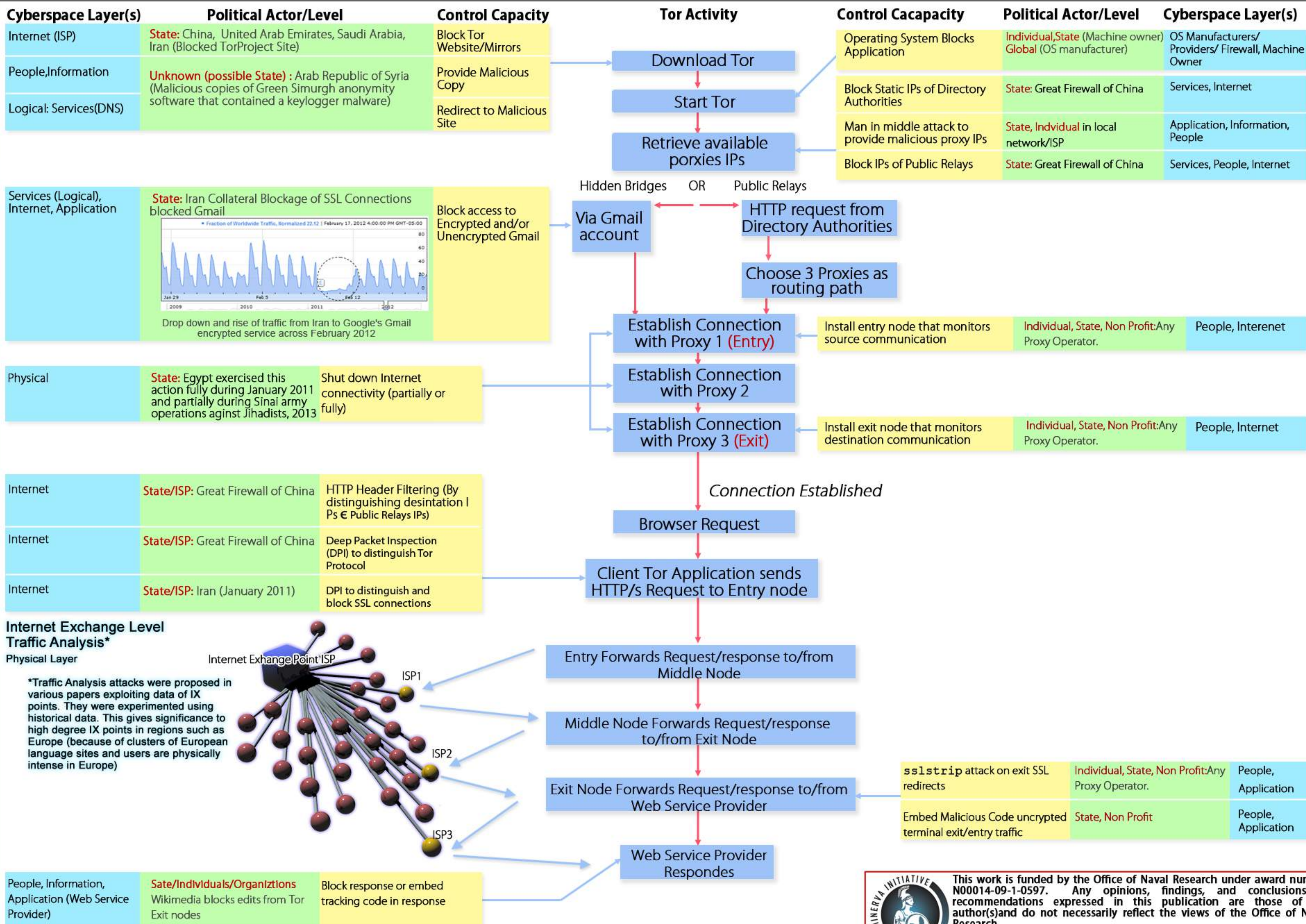
- 1- We identify and depict the process necessary to establish a Tor routing connection and high level diagram of communication activity.
- 2- Based on core literature on "vulnerabilities" of Tor Network, we extend our analysis by including two critical control capacities:
  - A) Network Survival Control (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.



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.