

# Métodos governamentais de censura e vigilância na Internet

Rodolfo Cesar de Avelar Ferraz

Centro de Informática – Universidade Federal de Pernambuco

2 de outubro de 2013

# Agenda

- **Motivação**
- **Fundamentos**
- **Censura na Internet**
- **Vigilância na Internet**
- **Métodos para contornar censura e vigilância na Internet**
- **Considerações Finais**

# Motivação

# Motivação

- Great Firewall of China

# Motivação

- Great Firewall of China
- Tor

# Motivação

- Great Firewall of China
- Tor
- Cypherpunk

# Motivação

- Great Firewall of China
- Tor
- Cypherpunk
- John Perry Barlow

# Fundamentos



# Fundamentos

- O Protocolo IP
  - Conteúdo exposto

# Fundamentos

- O Protocolo IP
  - Conteúdo exposto
- Criptografia

# Fundamentos

- O Protocolo IP
  - Conteúdo exposto
- Criptografia
- Servidores DNS

# Fundamentos

- O Protocolo IP
  - Conteúdo exposto
- Criptografia
- Servidores DNS
- ISPs e suas relações
  - Peering

# Fundamentos

- O Protocolo IP
  - Conteúdo exposto
- Criptografia
- Servidores DNS
- ISPs e suas relações
  - Peering
  - Trânsito (\$)

# Fundamentos

- O Protocolo IP
  - Conteúdo exposto
- Criptografia
- Servidores DNS
- ISPs e suas relações
  - Peering
  - Trânsito (\$)
  - Ponto de Troca de Tráfego (PTT) ou *Internet Exchanging Point* (IXP)

## Censura na Internet

- Remoção de conteúdo
- Bloqueio de acesso a conteúdo

## Remoção de conteúdo

- Terceirização da censura
- Legitimidade da censura
- Países diferentes, leis diferentes



## Bloqueio de acesso a conteúdo

- DNS Poisoning (exemplo: Eleições no Irã)

# Bloqueio de acesso a conteúdo

- DNS Poisoning (exemplo: Eleições no Irã)
- Filtragem de pacotes
  - Bloqueio a IPs

# Bloqueio de acesso a conteúdo

- DNS Poisoning (exemplo: Eleições no Irã)
- Filtragem de pacotes
  - Bloqueio a IPs
  - Inspeção automática de conteúdo (exemplo: palavras proibidas na Internet da China)



www.CoxAndForkum.com

## Vigilância na Internet

- Transmissão involuntária dos dados
- Interceptação dos dados em trânsito
- Aquisição dos dados já enviados

## Transmissão involuntária dos dados

- Método: Infecção do computador
- Possibilidades:
  - Leitura de arquivos pessoais
  - Leitura de registro das teclas pressionadas
  - Leitura da lista de processos abertos
  - Leitura total dos dados enviados à Internet
  - Visualização da tela
  - Visualização da imagem capturada pela *webcam*
  - Escuta do áudio capturado pelo microfone
  - Controle total sobre a máquina
- Exemplo: *GhostNet*

## Interceptação dos dados em trânsito

- Método: “Grampear” infraestrutura
- Possibilidades:
  - Leitura total dos dados enviados à Internet
  - Leitura parcial dos dados enviados à Internet
    - Identificação dos destinatários
- Exemplo: Sala da *NSA* no PTT da AT&T em 2003

# Aquisição dos dados já enviados

- Métodos:
  - “Grampear” infraestrutura
  - Requisitar registros de elementos da infraestrutura
  - Requisitar dados de serviços
- Possibilidades iguais às de interceptação em trânsito

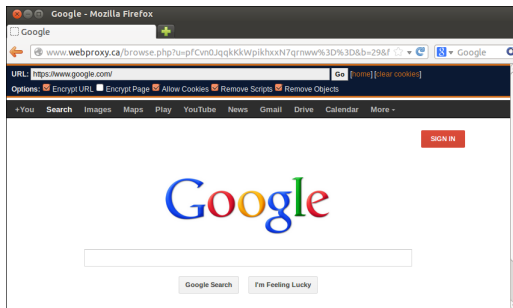
## Métodos para contornar censura e vigilância na Internet

- Criptografia
- Proxy
- Acesso via satélite
- Esteganografia



# Proxy

- Web proxy
- HTTP proxy
- SOCKS proxy
- Redes de anonimidade (exemplo: Tor)

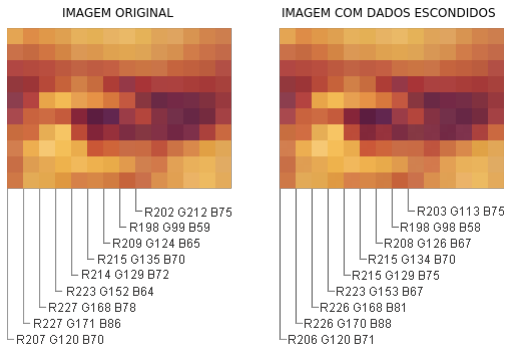


## Acesso via satélite

## Possível solução para censura em alguns países

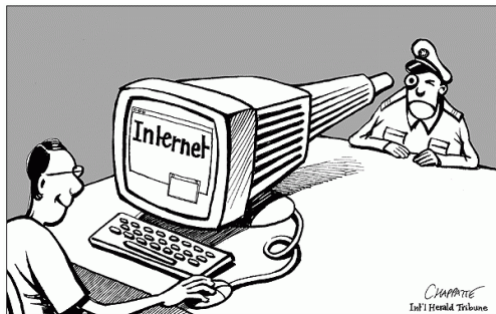
# Esteganografia

Possível solução contra vigilância em situações críticas



## Considerações finais

# Relação entre vigilância e censura – Autocensura



# Empresas que lucram com a censura e a vigilância

buggedplanet.info/index.php?title=Main\_Page

Log in

page discussion view source history

## Main Page

**Contents** [hide]

- 1 Policy for BUGGEDPLANET.INFO: Please read before editing
- 2 Vendors of SIGINT/COMINT/LI and supporting Technologies and Systems
- 3 Country Knowledgebase on SIGINT/COMINT/LI Installations
  - 3.1 Africa
  - 3.2 Americas
  - 3.3 Asia
  - 3.4 Europe
  - 3.5 Oceania / Other
- 4 Transnational Issues and Installations
  - 4.1 Standards
  - 4.2 SIGINT/COMINT related Systems and Material
  - 4.3 Transnational Telecommunication Infrastructure
  - 4.4 Telecommunication Systems
- 5 Other Resources
  - 5.1 Studies
  - 5.2 Books
  - 5.3 Movies
  - 5.4 Websites
  - 5.5 Torrents

**Policy for BUGGEDPLANET.INFO:** Please read before editing

**Vendors of SIGINT/COMINT/LI and supporting Technologies and Systems**

www.bluecoat.com/products/packetshaper

PRODUCTS WHO'S SECURE PARTNERS COMPANY SUPPORT GET SECURED

## PACKETSHAPER

### ASSERT CONTROL

## IT'S YOUR NETWORK. OWN IT.

Does your network know the difference between important web traffic like online meetings, and lower-priority traffic like games or streaming media? Your security solution might block entire categories of content, such as gambling or pornography, but how do you control everything else?

PacketShaper gives you content-aware control of today's web-integrated WAN. Prioritize important applications like Oracle, SAP, Salesforce.com and Office365. Assure quality for VoIP and videoconferencing. Contain recreational traffic to any level you specify. PacketShaper's unique integration of application and web content intelligence gives you the x-ray vision needed to monitor today's network traffic, and enforces your rules with priority, partition and rate control technologies.

PacketShaper analyzes and positively identifies traffic generated by hundreds of business and recreational applications. And thanks to its integration with WebPulse – Blue Coat's real-time web intelligence service – PacketShaper can even control application traffic by web content category. For example, you can permit low-impact social networking like Facebook status updates, but squeeze time-wasting games like Farmville. PacketShaper makes it easy to collectively control related applications and content, while giving you precise tools to get

# Trabalhos futuros

- Direito:
  - Regularizar processo de censura: transparência e participação popular
  - Sugerir que seja criado órgão internacional de fiscalização da infraestrutura de rede
  - Impedir exportação de tecnologia que possibilita censura e vigilância a países que não respeitam direitos fundamentais e a utilizam para perseguir dissidentes políticos
- Computação:
  - Desenvolvimento de novas ferramentas de contorno à censura e vigilância ou melhora das atuais
  - Sugerir novos protocolos de rede tendo privacidade como requisito

Obrigado