



Universidade Federal de Pernambuco  
Centro de Informática

Graduação em Engenharia da Computação

## **Métodos governamentais de censura e vigilância na Internet**

Rodolfo Cesar de Avelar Ferraz

Trabalho de Graduação

Recife  
2 de outubro de 2013



Universidade Federal de Pernambuco  
Centro de Informática

Rodolfo Cesar de Avelar Ferraz

## **Métodos governamentais de censura e vigilância na Internet**

*Trabalho apresentado ao Programa de Graduação em Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Engenharia da Computação.*

Orientador: *Prof. Ruy José Guerra Barretto de Queiroz*

Recife  
2 de outubro de 2013



*À minha família, aos meus amigos e aos meus professores,  
por terem me ajudado na minha formação, cada um à sua  
maneira. Ao universo, por ter me dado a chance de  
conhecê-los.*



*This concern with the basic condition of freedom – the absence of physical constraint – is unquestionably necessary, but is not all that is necessary. It is perfectly possible for a man to be out of prison, and yet not free – to be under no physical constraint and yet to be a psychological captive, compelled to think, feel and act as the representatives of the national State, or of some private interest within the nation, want him to think, feel and act. There will never be such a thing as a writ of habeas mentem; for no sheriff or jailer can bring an illegally imprisoned mind into court, and no person whose mind had been made captive by the methods outlined in earlier articles would be in a position to complain of his captivity. The nature of psychological compulsion is such that those who act under constraint remain under the impression that they are acting on their own initiative. The victim of mind-manipulation does not know that he is a victim. To him, the walls of his prison are invisible, and he believes himself to be free. That he is not free is apparent only to other people.*

—ALDOUS HUXLEY (Brave New World Revisited, 1958)





# Resumo

Assim como aconteceu após o aperfeiçoamento da mídia impressa no século XV no início do Renascimento, a Internet popularizou ainda mais o fácil e rápido acesso à informação. Com a popularização de redes sociais e sites de compartilhamento multimídia, qualquer indivíduo conectado à rede é capaz de gerar conteúdo e tornar seus semelhantes mais informados, retirando das mãos das grandes companhias de comunicação o oligopólio sobre a informação. Essa mudança está trazendo um forte impacto na cultura, pois o acesso à arte e literatura de várias partes do mundo foi facilitado, e também na política, pois os cidadãos que possuem ideias e ideais em comum podem se comunicar em tempo real, mesmo sem se conhecerem, vigiando melhor as ações do governo e possivelmente indo às ruas para se expressar.

É da natureza da legislação caminhar mais lentamente do que a tecnologia. Somente após enxergar o problema, discutem-se as melhores soluções e após chegar em uma conclusão, implementa-se em forma de lei, se necessário. Neste momento, já é possível enxergar alguns pontos em que a Internet pode ser melhorada através de leis regulamentadoras. É da natureza do mercado ir em busca do lucro de todas as formas possíveis, e como Jérémie Zimmermann já disse “cada vez mais nossos dados digitais tornam-se um *commodity*, servindo não somente para tornar as nossas vidas mais fáceis, mas também para nos controlar e obter lucro sobre nós”. É necessário enxergar os abusos do mercado e tentar encontrar soluções, possivelmente em forma de leis.

Além disso, a massiva adoção dos novos meios de comunicação pela sociedade trouxe grandes poderes novamente a um grupo restrito. Os responsáveis pela infraestrutura da rede e pelos grandes provedores de conteúdo e serviços têm poder sobre que informação temos acesso, possivelmente censurando os cidadãos, e também têm condições de obter conhecimento de tudo o que fazemos na rede, que inclui nossas conversas privadas e até nossos pensamentos, que expressamos através de buscas em sites como o *Google*.

Com a intenção de fazer a sociedade enxergar esses problemas, acelerando o processo de regulamentação da nossa rede de forma consciente, este trabalho discrimina as formas mais comuns de censurar e vigiar cidadãos, especificamente executado por governos. Enquanto nada é feito, e também para aqueles que encontram-se sob um governo não democrático, podem ser utilizadas algumas técnicas para contornar a censura e a vigilância empregada atualmente. Essas também serão apresentadas brevemente neste trabalho.

**Palavras-chave:** censura, vigilância, segurança, privacidade, anonimidade, internet, tecnologia e sociedade, direitos humanos



# Abstract

As it happened after the print media improvement occurred in the fifteenth century at the beginning of the Renaissance, the Internet turned information access easier and faster for the masses. As social networks and media sharing became mainstream, any individual connected to this network is able to generate content and make theirs fellows more informed, taking from the hands of the big companies of communication the oligopoly on information. That change is bringing a deep impact in culture, as the access to arts and literature of all the world can be

**Keywords:** censorship, surveillance, network security, privacy, anonymity, internet, technology and society, human rights



# Sumário

<b>1</b>	<b>Introdução</b>	<b>1</b>
1.1	Motivação e Contextualização	1
1.1.1	A influência da Internet na sociedade	1
1.1.2	O perigo da ignorância sobre o funcionamento da Internet	3
1.2	Objetivos	3
1.3	Estrutura do trabalho	3
<b>2</b>	<b>Fundamentos do funcionamento e infraestrutura da Internet</b>	<b>5</b>
2.1	Analogia com serviço postal	5
2.2	O uso da criptografia na Internet	6
2.3	Pacotes IP	7
2.3.1	Como funcionam a Web e os servidores de nomes	7
2.4	Algumas definições	8
<b>3</b>	<b>Censura na Internet</b>	<b>11</b>
3.1	Remoção de conteúdo	11
3.1.1	Terceirização da censura	12
3.1.2	Legitimidade da censura	12
3.2	Bloqueio de acesso a conteúdo	12
3.2.1	DNS Poisoning	12
3.2.2	Filtragem de pacotes: Bloqueio a IPs	14
3.2.3	Filtragem de pacotes: Inspeção de pacotes	14
<b>4</b>	<b>Vigilância na Internet</b>	<b>15</b>
4.1	Transmissão involuntária dos dados	15
4.1.1	Infecção do computador	15
4.2	Interceptação dos dados em trânsito	16
4.2.1	Interceptação total dos dados	16
4.2.2	Descoberta dos seus destinatários	16
4.2.3	Grampos na Web ( <i>Web Bugs</i> )	17
4.3	Aquisição dos dados já enviados	18
<b>5</b>	<b>Métodos para contornar vigilância e censura na Internet</b>	<b>19</b>
5.1	Proxy	19
5.2	Acesso via satélite	20
5.3	Esteganografia	20

5.3.1	Esteganografia utilizada como apoio à vigilância governamental	21
<b>6</b>	<b>Conclusão</b>	<b>25</b>
6.1	A relação entre vigilância e censura – Autocensura	25
6.2	Empresas que lucram com a censura e a vigilância	25
6.3	Considerações finais	26

# Lista de Figuras

1.1	Página com transmissão do Mídia NINJA ao vivo	2
1.2	Gráfico do Arab Social Media Report	4
3.1	Página recebida ao tentar acessar sites proibidos nos Emirados Árabes Unidos	13
5.1	Captura de tela de um navegador acessando um Proxy Web	22
5.2	Captura de tela de uma página com uma lista de <i>proxies</i> SOCKS	23
6.1	Imagem capturada da página da Blue Coat	27





## CAPÍTULO 1

# Introdução

## 1.1 Motivação e Contextualização

### 1.1.1 A influência da Internet na sociedade

Pablo Capilé<sup>1</sup> expressa bem a mudança da dinâmica informacional no Brasil e no mundo: “Antes existia apenas mídia de massa, agora também temos massa de mídia”. Antes da Internet, os fatos eram filtrados e apresentados por grupos restritos, para uma grande massa de ouvintes e leitores. Agora, aqueles que agiam passivamente, apenas lendo e ouvindo podem ser geradores de conteúdo, indo para a rua fazer registros com seu *smartphone*, publicando em um blog ou rede social e mostrando sua visão dos fatos. A maior pluralidade de pontos de vista nas notícias permite que o cidadão faça sua interpretação dos fatos com mais precisão. Dependendo da origem da notícia, haverá atenuação de alguns fatos e destaque em outros, para induzir alguma conclusão específica no leitor. Com diferentes graus de atenuação e destaque, é possível tirar uma “mídia” entre as notícias e se aproximar mais da realidade.

A Figura 1.1 mostra um exemplo de *streaming* de vídeo, feito pela Mídia NINJA de Pernambuco. Nela podemos perceber uma aproximação maior do repórter com o público, através do campo de comentários, que inclusive é utilizado pelo repórter como fonte de informações. O que o público informa ao repórter da Mídia NINJA, pode acabar influenciando na transmissão, às vezes comandando o que deve ser mostrado, ou avisando de algum risco que o repórter pode correr.

Em regimes autoritários, a influência sobre as fontes de notícia são muito importantes para o governo garantir a quietude da população e a manutenção do poder. Sem notícias sobre manifestos e revoluções, a população não se inspira e não se “contamina” com ideias subversivas. A Internet é um meio mais difícil de controlar do que as transmissoras de rádio e TV. Nela, os cidadãos podem ouvir e expressar opiniões de descontentamento, tornando o povo mais unido a ponto de derrubar governos há décadas estabelecidos.

Um exemplo do impacto da Internet e das redes sociais na sociedade são as revoluções recentes ocorridas no norte da África e Oriente Médio, coletivamente conhecidas como A Primavera Árabe. As novas mídias são vistas e usadas como agentes de mudança na região árabe, segundo pesquisa publicada em [15]. Esse estudo também fez pesquisas de opinião do povo

---

<sup>1</sup>Pablo Capilé é um dos idealizadores do grupo Mídia NINJA (Narrativas Independentes, Jornalismo e Ação), declarada como uma alternativa à imprensa tradicional. Sua característica marcante é transmitir acontecimentos ao vivo, utilizando streaming via *smartphones*, muitas vezes apresentando opinião e apoio explícito a algumas causas, diferentemente da mídia tradicional que tenta transmitir uma imparcialidade, embora muitas vezes tente apresentar a informação de forma que suporte seus interesses. A transmissão pode ser feita por mais de uma pessoa simultaneamente, podendo apresentar diferentes pontos de vista sobre um mesmo tema.



**Figura 1.1** Através de um aplicativo para celular e conexão 3G, centenas de pessoas puderam assistir à ocupação da Câmara de Vereadores do Recife por manifestantes reivindicando passe livre de ônibus. O celular do "ninja"(como alguns chamam os jornalistas que transmitem nesses moldes) perdia o sinal ao se aproximar muito da Câmara. Por isso, muitas vezes a transmissão era interrompida. No momento, a Mídia NINJA era a fonte de informação mais atualizada sobre a ocupação da câmara.

árabe sobre as mudanças trazidas pelas redes sociais como se pode ver na Figura 1.2.

### **1.1.2 O perigo da ignorância sobre o funcionamento da Internet**

A Internet traz benefícios a todos, no entanto, praticamente apenas aqueles ligados a área de Tecnologia da Informação têm conhecimento sobre seu funcionamento. Quando se dirige um automóvel, não é necessário que o motorista domine o funcionamento interno do motor do veículo. O mesmo acontece com a Internet, pois não precisamos conhecer como funciona para utilizá-la, no entanto através dela podemos nos expressar livremente e ter acesso a informações que não seriam alcançáveis através de outro meio. Ou seja, a Internet é uma ferramenta que nos permite praticar diversos direitos fundamentais e qualquer mudança na forma como ela funciona pode impactar na prática desses direitos.

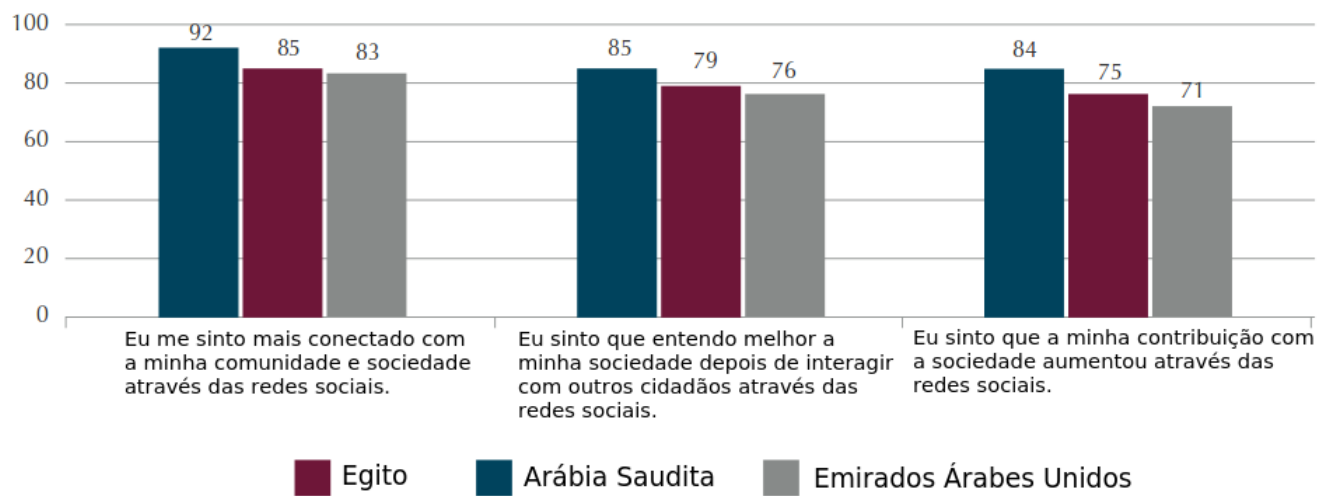
Por este motivo, é importante que a sociedade tenha um mínimo de conhecimento sobre o funcionamento desta ferramenta, e assim poder cobrar que ela esteja funcionando em favor dos seus direitos. Diferentemente do que se acredita, e este trabalho tentará mostrar o contrário, a Internet não é um espaço público, inviolável e incensurável. Para que a rede esteja a serviço dos cidadãos, é importante que esses cobrem por isso.

## **1.2 Objetivos**

Este trabalho tem por objetivo explicar o funcionamento interno da Internet, num nível técnico acessível para leigos em computação e na profundidade necessária para entender como ela pode ser desvirtuada para ferir os seus direitos em vez de favorecê-los. Com este conhecimento em mãos, serão apresentados ao leitor as maneiras que diferentes governos utilizaram para controlar as informações acessíveis aos cidadãos, assim como os meios utilizados para monitorar o que todos acessam e publicam. Também serão apresentados alguns métodos para contornar bloqueios e monitoramentos. Ao fim do trabalho, o leitor deve estar ciente de que os benefícios trazidos pela Internet estão em constante ameaça, e que somente com a vigilância do povo sobre o governo e companhias de telecomunicação, poderemos ter a rede ao nosso favor.

## **1.3 Estrutura do trabalho**

No Capítulo 2 serão apresentados alguns fundamentos sobre a Internet e seu funcionamento, para tornar o leitor suficientemente familiarizado com a terminologia e conceitos que serão abordados no restante do trabalho. Começando pelo Capítulo 3, serão mostradas diferentes formas que a infraestrutura da Internet pode ser manipulada para evitar que os cidadãos tenham acesso a informações que seu governo considere indesejáveis. Em seguida, no capítulo 4, as técnicas de monitoramento e vigilância do comportamento dos cidadãos na rede serão classificadas e explicadas, ilustrando com exemplos reais. Finalmente, no capítulo 5, serão listadas as principais técnicas utilizadas para burlar a censura configurada pelos governos, assim como dificultar o monitoramento empregado por esses.



**Figura 1.2** Em pesquisa feita pela Dubai School of Government [15], o povo árabe foi consultado a respeito do impacto das redes sociais em sua relação com a sociedade. As porcentagens acima correspondem à quantidade de indivíduos que concordaram com a afirmação escrita abaixo das barras.

## CAPÍTULO 2

# Fundamentos do funcionamento e infraestrutura da Internet

*Any sufficiently advanced technology is indistinguishable from magic.*  
—ARTHUR C. CLARKE (Profiles Of The Future: An Inquiry into the  
Limits of the Possible, 1958)

Neste capítulo, será explicado de forma simplificada o funcionamento da rede que nos conecta a bilhões de outras pessoas todos os dias. Primeiro, será apresentada uma analogia com um serviço postal, para explicar como os dados são transmitidos pela rede, e as pequenas diferenças para um correio normal, que a tornam um meio de comunicação facilmente susceptível a vigilância e censura. Em seguida, serão apresentadas algumas definições necessárias para o entendimento do trabalho.

### 2.1 Analogia com serviço postal

A Internet funciona como o serviço de um correio. Cada encomenda possui um certo conteúdo e deve apresentar uma etiqueta contendo o endereço do remetente e o endereço destino. Antes de chegar ao destino final, os pacotes da Internet precisam passar por diversas agências e centros de distribuição. Neste correio, no entanto, o conteúdo das encomendas não é protegido. Qualquer elemento que participe da entrega pode ver o conteúdo, armazenar cópias, e o mesmo pode ser feito com a etiqueta contendo os endereços. Na verdade, muitos governos exigem que os responsáveis pelo trânsito destas “encomendas” copiem e armazenem esses dados por um tempo mínimo, para possíveis investigações policiais futuras.

Qualquer ponto que participe do reencaminhamento de pacotes, portanto, pode ser utilizado como elemento atuador de uma política de censura e vigilância. Para censurar, basta descartar pacotes que possuam conteúdo considerado inapropriado. Ou então, apenas a partir das informações da etiqueta, pode-se descartar mensagens remetidas por endereços específicos, ou endereçadas a tais destinos. Já a vigilância pode ser praticada com a simples gravação dos da-

dos, instalando uma espécie de gravador em um ponto de convergência de mensagens (centros de recebimento e reenvio).

## 2.2 O uso da criptografia na Internet

Infelizmente não são apenas as entidades envolvidas no tráfego dos dados que têm a chance de visualizar todo o conteúdo transmitido na rede. Os “piratas de computador”, com toda sua expertise em computação e segurança, sem muita dificuldade encontram brechas de segurança e conseguem interceptar esses pacotes sem serem notados. Esses piratas podem ser criminosos, tentando auferir lucro a partir de informações como dados do cartão de crédito, ou podem ser agentes do governo ou espões contratados para obter informações sigilosas de indivíduos, empresas ou países. Para contornar esse problema, foram desenvolvidas soluções que têm como objetivo tornar a mensagem ilegível para leitores não autorizados. Apenas o destinatário é capaz de tornar a mensagem legível. Essas soluções se baseiam nos conceitos da criptografia, que existem há milênios, desde que o ser humano sentiu a necessidade de ocultar mensagens a indivíduos indesejados.

O processo de criptografia de mensagens trata-se apenas de uma série de operações matemáticas executadas sobre a mensagem com o objetivo de descaracterizá-la e tornar o processo inverso uma tarefa virtualmente impossível<sup>1</sup>. No entanto, é possível inverter o processo se for utilizada uma chave. Com a chave correta, a mensagem original pode ser obtida facilmente.

Existem dois tipos de chaves para criptografia. Chaves assimétricas e chaves simétricas. No caso das chaves assimétricas, a chave utilizada para esconder a mensagem (criptografar) é diferente daquela utilizada para decodificá-la (descriptografar). No caso das chaves simétricas, a chave para criptografia e descriptografia são idênticas.

Uma aplicação das chaves assimétricas é o conceito de chave pública e chave privada. Um servidor que deseja proteger as mensagens que recebe deve gerar as duas chaves. A chave pública é a chave utilizada para criptografar as mensagens, já a chave privada é aquela utilizada para a descriptografia. Como o próprio nome diz, a chave pública não precisa ser escondida, ela deve estar disponível para quem quiser se comunicar com aquele servidor. O usuário criptografa a mensagem usando a chave pública e envia para o servidor. Já a chave privada deve ser conhecida apenas pelo servidor que a gerou e deve ser protegida a qualquer custo. Somente ela é capaz de descriptografar as mensagens criptografadas com a chave pública. Muitas vezes se utilizam chaves assimétricas apenas para iniciar uma comunicação e combinar uma chave simétrica que apenas os dois conheçam.

Um risco da utilização de chaves públicas e privadas é o conhecido ataque *man in the middle* (homem no meio, em inglês). Como o nome diz, trata-se de uma forma de ouvir a conversa, posicionando-se entre as duas entidades que desejam se comunicar. Para o servidor o atacante finge ser o usuário, e para o usuário ele finge ser o servidor, funcionando como uma

---

<sup>1</sup>Um exemplo de operação que é fácil de ser calculada seria o produto entre dois números primos muito grandes. Realizar este cálculo é simples e qualquer computador é capaz. No entanto, conhecendo apenas o resultado, encontrar quais foram os números utilizados na multiplicação é uma tarefa difícil até mesmo para supercomputadores. É possível, mas pode levar anos, talvez séculos, sendo na prática, impossível de reverter o processo para fins práticos.

ponte entre eles sem que percebam. Primeiro, o elemento mal intencionado induz o usuário utilizar uma chave pública diferente daquela realmente oferecida pelo servidor. Esta chave pública é na verdade uma gerada pelo agente do ataque, cuja chave privada correspondente ele conhece. O que ele faz então é se passar pelo servidor, recebendo os pacotes que o usuário envia, descriptografando-os, lendo-os e criptografando-os novamente, utilizando a chave pública verdadeira do servidor, e os envia, fingindo ser o usuário.

## 2.3 Pacotes IP

Outra diferença para um correio normal é que os carteiros, ou veículos que levam as encomendas, só são capazes de levar pacotes bem pequenos. Então, quase sempre o conteúdo a ser enviado é dividido em pacotes menores e enviados separadamente. Ao chegar no destinatário, o conteúdo das frações da encomenda são reunidos, formando-se o dado enviado originalmente.

Para tornar possível a comunicação e o entendimento entre diversos tipos de dispositivos em uma mesma rede, foi necessário estabelecer certos padrões. Estes padrões compõem o chamado protocolo de comunicação IP (Internet Protocol) e determinam o formato das mensagens transmitidas. Essas mensagens são digitais, ou seja, são formadas apenas por números. Não há etiquetas físicas, nem caixas, como num correio real. Na Internet, o endereço remetente é um número, o endereço destino é outro, e o conteúdo a ser enviado são mais números. Estes números são enviados em sequência e não há espaços, nem divisórias entre eles. Portanto, é preciso que o emissor e receptor combinem que informação vem primeiro e qual o comprimento de cada uma. O protocolo IP define isso. A sigla IP também é utilizada para se referir ao endereço que identifica cada participante da rede IP (outro nome para a Internet). Como dito anteriormente, os endereços são formados apenas por números. O comprimento do endereço IP é 32 bits, ou 4 bytes e pode ser representado como 4 bytes separados por pontos. Como um byte pode guardar valores de 0 a 255, então os endereços IP variam de 0.0.0.0 a 255.255.255.255.

Tudo que é acessível via Internet precisa ter um endereço IP. O Facebook possui um, o Youtube possui outro, e você, para acessá-los, também precisa de um.

Os pacotes trocados via Internet podem transportar vários tipos de dados: o texto de um e-mail, um vídeo do *Youtube*, a senha da sua conta do *Facebook* depois de você clicar em "Entrar", ou seja, tudo que trafega na rede são transformados em zeros e uns e enviados através destes pacotes. Ao chegar no destino, estes zeros e uns são reconvertidos para o tipo de conteúdo original, seja o texto de e-mail ou vídeo do Youtube.

Logo, quando enviamos um pacote a partir do nosso computador, este pacote acompanha nosso endereço IP, o endereço IP do destinatário e o dado que será recebido por ele. Todas estas informações são lidas por diversos dispositivos que são responsáveis por encaminhar nosso pacote até o destino. Estes dispositivos muitas vezes armazenam todos estes dados por longos períodos.

### 2.3.1 Como funcionam a Web e os servidores de nomes

Quando acessamos um website como `www.loremipsum.com/posts/3`, primeiro é enviado um pacote ao computador (também chamado de servidor) que contém a página procurada.

O conteúdo deste pacote é um pedido, requisitando um certo recurso. Neste caso . O Website então responde com outros pacotes, contendo a página, que ao chegar no computador do internauta, é exibida no navegador. Quando o usuário clica em algum link do site, uma nova requisição é enviada, que por sua vez é respondida novamente com outra página. A navegação na Web funciona basicamente desta forma: requisições dos usuários e respostas dos servidores Web, em forma de páginas.

No entanto, para o correio entregar os pedidos de página do usuário, ele precisa do endereço IP destino. Este endereço é formado apenas por alguns números. Não há nomes, nem ruas, nem cidades neste endereço.

Como ficaria difícil para os internautas decorar os números dos endereços IP de todos os seus Websites favoritos, foi criada uma espécie de agenda de endereços, compartilhada em todo o mundo, que contém nomes associados a endereços IP. Assim, em vez de decorarmos que o endereço do Google é 74.125.234.240, basta que decoremos seu nome: *www.google.com*.

Essa agenda é armazenada em servidores conhecidos como Servidor DNS (*Domain Name System*) ou Servidor de Nomes. Como é de se esperar, os Servidores DNS também possuem um endereço IP, e se o usuário desejar, pode configurar qual servidor DNS será utilizado. Todavia, não há necessidade de ficar trocando o Servidor DNS, visto que todos devem responder da mesma forma. A agenda de nomes e endereços deve ser idêntica para todos conectados na Web.

Quando digitamos apenas um nome como *www.youtube.com* na página de endereços, por padrão nos é apresentada a sua página inicial. No entanto, podemos querer acessar uma página (ou recurso) específica. Se acessarmos *www.youtube.com/watch?v=b-gG5qmXFUA* estamos pedindo ao Youtube o recurso *"/watch?v=b-gG5qmXFUA"*. Então nosso navegador fica encarregado de consultar um servidor DNS, transformar o nome *www.youtube.com* em um endereço IP, e mandar um pacote para este IP pedindo o recurso *"/watch?v=b-gG5qmXFUA"*. Por ser possível acessar recursos de servidores, estes endereços WWW muitas vezes são chamados de URL (*Universal Resource Location*).

## 2.4 Algumas definições

*Provedor de Acesso Serviços e Informações da Rede Internet (Internet Service Provider - ISP).* Garante que um indivíduo tenha acesso a toda a Internet e, para o caso de provedores de conteúdo, garantir que outros usuários possam visualizar seus serviços disponibilizados na rede. Exemplos: GVT, Oi.

*Peering.* Para um cliente de um ISP poder acessar o conteúdo de um cliente de outro ISP, é necessário que exista uma conexão entre estes ISPs. Uma conexão direta entre os ISPs é chamada de peering.

*Trânsito.* Uma forma de um ISP fornecer acesso a vários outros ISPs para seus clientes, seria fazer Peering com todos os outros ISPs. No entanto há mais de 10000 ISPs independentes no mundo, então torna-se inviável que um ISP se conecte diretamente a todos os outros.

Caso a rede do ISP1 queira se conectar com a rede do ISP2, não é necessário que crie um



peering (conexão direta) entre elas. A rede do ISP1 pode negociar com uma terceira rede ISP3, que já possui Peering com a ISP2, e pedir para usar a rede ISP3 para ganhar acesso a ISP2. O uso de uma ou várias redes ISPs para alcançar uma rede destino é chamada de trânsito.

*Tier One peer.* Alguns ISPs no mundo tem acesso a toda a Internet, mas não pagam por "trânsito" a nenhum outro ISP. Eles são chamados de "Tier One" e fazem "peering" entre si, para vender trânsito para os outros ISPs (ISPs menores).

Portanto, para ter acesso a toda a Internet, ou o seu ISP ou um de seus "up-stream provider" terá conexão com pelo menos um "tier one".

*Peering privado e Ponto de Troca de Tráfego.* Se você não for um Tier One, obrigatoriamente terá que pagar por trânsito a algum outro ISP para ter acesso a toda a Internet. No entanto, se você possuir Peering com algum ISP, você economiza, pois esta conexão não passa por nenhum atravessador e você não precisa pagar por ela, apenas o custo de manutenção do link. Portanto, peering é de interesse de qualquer ISP, pequeno ou grande.

Peering pode ser feito um a um, via interconexão direta (peering privado) ou através de um ponto de troca de tráfego (PTT), um local com uma infraestrutura compartilhada, onde os ISPs se juntam para interconectar suas redes. No caso, cada ISP pagará pelo uso dessa infraestrutura, mas não estarão pagando por trânsito, uma vez que estão conectados diretamente aos ISPs que participam deste PTT.

Idealmente, existe no máximo um PTT em uma metrópole.

*Ponto de Troca de Tráfego (PTT) ou Internet Exchange Point (IXP).* Infraestrutura necessária para a interconexão direta entre as redes de diferentes ISPs.



## CAPÍTULO 3

# Censura na Internet

*he who controls the past controls the future, and he who controls the  
present controls the past*

—GEORGE ORWELL (Nineteen Eighty-Four, 1949)

A prensa de tipos móveis inventada por Johannes Gutenberg, no século XV, revolucionou a disseminação de informação no ocidente, quando a impressão de livros era muito trabalhosa e pouco eficiente. O fato de mais pessoas terem acesso a livros foi considerado essencial para o início do Renascimento, período em que a sociedade se transformou em cultura, economia, política, religião, marcando o fim da Idade Média e início da Idade Moderna.

É notável que mudanças no acesso e fluxo de informação causam impactos na sociedade. Impactos também acontecem quando surgem novos meios de comunicação. Os governos e entidades censoras precisam se adaptar às novas formas de comunicação. Na época em que a comunicação escrita e impressa era a única forma de guardar conhecimento, a censura era feita através do recolhimento de livros e posterior incineração. Ao surgirem a radiodifusão e televisão, o conteúdo a ser veiculado poderia ser censurado pela própria emissora, temendo sofrer penalidades. Em alguns casos, o conteúdo a ser veiculado precisava ser revisado antes por entidades do governo, como já aconteceu durante a ditadura militar brasileira.

Na Internet, não é mais tão claro quem difunde informação e quem consome. Logo, a censura torna-se mais complexa. Muitas vezes, graças à falta de conhecimento técnico e ao desespero, peca-se pelo excesso, censurando informações cuja veiculação não é proibida.

Além disso, devido à dinamicidade e complexidade da rede, as formas de censurar são menos triviais do que costumava acontecer no passado. Este capítulo irá descrever que formas um governo pode utilizar para realizar censura na Internet.

### 3.1 Remoção de conteúdo

O método mais simples de censura não utiliza meios tecnológicos, mas sim meios jurídicos, ou algum tipo de influência sobre o provedor de conteúdo a ser censurado. Através desta

influência, o autor do conteúdo, ou o servidor que contém a página é obrigado a remover o material indesejado pelo governo, sendo possivelmente penalizado caso não o faça.

A depender do país em questão, esse tipo de censura pode ser mais ou menos comum. Em alguns países, a quantidade de tipos de conteúdo proibidos é grande, sendo difícil para o governo monitorar todos os sites. Neste caso, pode-se terceirizar a censura.

### **3.1.1 Terceirização da censura**

Na China, os provedores de conteúdo precisam ter uma licença concedida pelo governo para funcionarem. Caso seja encontrado em suas páginas algum conteúdo proibido, o provedor é responsabilizado, podendo perder sua licença. Desta forma, devido ao risco que corre caso não o faça, o próprio provedor exerce a função de censor, que seria do governo.

### **3.1.2 Legitimidade da censura**

Nem todo tipo de censura é ruim. Certos tipos de ideias, por exemplo, se propagadas, podem levar ao ódio e violência. No Brasil, por exemplo, é proibido a apologia ao Nazismo. Já em alguns países árabes, é proibida a veiculação de pornografia. Quando o conteúdo fere de alguma forma as leis de um país, em que a nação como um todo é prejudicada devido à disponibilidade de um certo conteúdo, a remoção é legal.

No entanto, a lei dos países diferem e muitas vezes o conteúdo pode estar hospedado em outro país com legislação diferente. Neste caso, tudo que o governo pode fazer é recorrer a meios tecnológicos, bloqueando o acesso ao conteúdo externo.

## **3.2 Bloqueio de acesso a conteúdo**

### **3.2.1 DNS Poisoning**

Como explicado na seção 2.3.1 da página 7, os servidores DNS são responsáveis por transformar endereços como *www.facebook.com* no endereço IP correspondente. Dessa forma, o usuário não precisa decorar o IP dos seus sites favoritos, basta lembrar a URL e digitá-la no navegador.

Uma forma de dificultar o acesso de usuários a certos sites é alterar as tabelas dos servidores DNS utilizados em um dado país, colocando endereços IP inválidos para os sites a serem censurados. Assim, quando o usuário digitar o endereço *www.facebook.com* no seu navegador, a sua requisição irá para um IP diferente daquele que o Facebook utiliza, provavelmente um IP inválido, ou de alguma página do governo avisando que aquele site está bloqueado.

No entanto, este método não é muito eficaz. Para contorná-lo, bastaria trocar de servidor DNS, ou decorar o IP do Facebook e digitá-lo na barra de endereços do navegador. Por isso, os governos também bloqueiam pacotes originados ou destinados a certos endereços IP.

A Figura 3.1 mostra um exemplo do que acontece nos Emirados Árabes Unidos quando se acessa um site proibido pelo governo.



# خطر!

## تصفح بأمان!

عذرا، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتراكه محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كانت لديك وجهة نظر مختلفة، الرجاء [انقر هنا](#).

## Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates

If you believe the website you are trying to access does not contain any such content, please [click here](#).

© 2009 Lamtlara FZ LLC.

**Figura 3.1** Com textos em árabe e em inglês, avisa-se que a Internet é um poderoso meio de comunicação, compartilhamento e de aprendizado diário. No entanto, o conteúdo que o usuário está tentando acessar contém conteúdo proibido pela “Política Reguladora de Gerenciamento de Acesso à Internet”, da Autoridade Reguladora de Telecomunicações dos Emirados Árabes Unidos.

### 3.2.2 Filtragem de pacotes: Bloqueio a IPs

Os roteadores que recebem e reencaminham pacotes, podem ser configurados para descartar pacotes com certos endereços como remetente ou destinatário. Desta forma, torna-se impossível enviar pacotes diretamente a alguns servidores. Esta é uma forma mais eficaz de censura, visto que torna-se impossível estabelecer conexão com algumas páginas, se a requisição partir de dentro do país a ser censurado. Um exemplo de uso desta técnica foi percebido por pesquisadores em [1], em que nas vésperas das eleições presidenciais do Irã em Junho de 2013, não se podia acessar um site local de notícias <http://presstv.ir>, nem o *The Guardian*, nem o *Le Monde*. Há no entanto, formas de se utilizar um intermediário fora do país para burlar o bloqueio governamental. Mais informações sobre estas técnicas estão presentes no Capítulo 5.

### 3.2.3 Filtragem de pacotes: Inspeção de pacotes

Também é possível filtrar pacotes não apenas pelos endereços envolvidos, mas também pelo conteúdo da mensagem. Esta técnica é conhecida como *Deep Packet Inspection* e é utilizada por alguns provedores de Internet, inclusive no Brasil, para limitar o uso de serviços como *Torrent* e *streaming* de vídeos. O Governo Chinês vai além e não só detecta que tipo de serviço os cidadãos utilizam, mas também que conteúdo eles acessam e transmitem na rede. De acordo com os experimentos feitos em [7], na China não é possível buscar no Google por certas palavras como “democracia” e “Tiananmen Square” (praça onde aconteceu o famoso “Massacre da Praça de Paz Celestial” em 1989, em que aconteceram milhares de mortes de civis feitas por força militar, para dissolver um protesto. O Governo Chinês aparentemente tenta apagar esses acontecimentos da história). Ao clicar no botão de busca, é exibida uma mensagem de erro, como se a conexão tivesse sido resetada. Além disso, o usuário não consegue voltar a acessar o Google por cerca de quinze minutos. A Wikipédia inclusive mantém uma lista de quais palavras são censuradas na Internet da China em [2].

## CAPÍTULO 4

# Vigilância na Internet

*How many of you have broken no laws this month? That's the kind of society I want to build. I want a guarantee – with physics and mathematics, not with laws – that we can give ourselves real privacy of personal communications.*

—JOHN GILMORE (Privacy, Technology and the Open Society – Discurso durante a “First Conference on Computers, Freedom and Privacy”, 1991)

A intrínseca falta de transparência das agências de inteligência governamentais, somada aos seus poderes de interceptar comunicações privadas, acabam implicando em ações possivelmente ilegais ou criminosas. Exemplos dessas ações podem ser escutas telefônicas sem autorização judicial ou a detenção e interrogatório de estrangeiros, sem respaldo legal<sup>1</sup>. Essa “falha de caráter” desse tipo de entidade se estende também ao contexto dos bits e bytes, onde estão espalhadas informações de todos nós. Neste capítulo serão abordados os diferentes métodos que tais entidades podem utilizar para invadir a privacidade dos cidadãos – legitimamente ou não.

## 4.1 Transmissão involuntária dos dados

### 4.1.1 Infecção do computador

Esta estratégia é mais comumente utilizada por criminosos que desejam roubar senhas de banco, por exemplo. Mas há registros de governos utilizando desta técnica ([18]). Também conhecidos como Cavalos de Troia, são softwares que à primeira vista são inofensivos, como uma barra de ferramentas extra no navegador, enfeites para a área de trabalho, algum anexo recebido por e-mail, ou geradores de chaves seriais, para piratear programas pagos. Estes soft-

---

<sup>1</sup>Foi publicado nos principais jornais a história de David Miranda, companheiro do jornalista Glenn Greenwald, que foi detido por autoridades britânicas durante quase nove horas, em um aeroporto de Londres em 18 de agosto de 2013. A lei permite esse tipo de detenção em caso de suspeita de terrorismo, no entanto, estava claro que não havia essa suspeita contra David Miranda. Glenn Greenwald escreveu no The Guardian uma série de notícias revelando os projetos de vigilância eletrônica empregados pelo NSA – Agência Nacional de Segurança dos Estados Unidos. Estes projetos foram publicados por um agente interno, Edward Snowden, que hoje procura asilo político, pois é perseguido pelo governo americano.

wares quando executados, instalam um programa secundário, que executa sem o usuário saber, e pode gravar tudo o que ele digita, o que ele vê na tela, e até o que a *webcam* e seu microfone estão captando. Tudo isso pode ser enviado via Internet para alguém interessado em monitorar as ações do usuário e é possível ainda controlar o que a máquina faz (controlar mouse e teclado remotamente).

Esta técnica é perigosa para o espião, pois é possível instalar uma máquina apenas para analisar o tráfego da máquina infectada e descobrir comunicações suspeitas, possivelmente resultando na identificação do invasor. Foi o que aconteceu com a *GhostNet*, rede de espionagem supostamente montada por agentes chineses ([12]) em que computadores de cerca de 100 países foram infectados e monitorados, incluindo computadores de escritórios de funcionários de alto escalão de governos estrangeiros. O esquema foi descoberto após pesquisadores analisarem o tráfego de máquinas do escritório do Dalai Lama, que estavam infectadas. Devido ao risco de serem descobertos, para alguns, pode ser mais interessante o monitoramento instalando escutas nos provedores de acesso à Internet (ISPs) ou Pontos de Troca de Tráfego (PTT ou IXP, em inglês) (explicação desses termos estão presentes no Capítulo 2). Essa foi a estratégia da Agência Nacional de Segurança dos Estados Unidos (NSA) ao instalar uma sala de operações de espionagem dentro de um Ponto de Troca de Tráfego da empresa *AT&T* em 2003 ([16] e [9]).

## 4.2 Intercepção dos dados em trânsito

### 4.2.1 Intercepção total dos dados

Assim como mencionado na seção anterior, mesmo com a máquina livre de vírus e *malwares*, os dados que o usuário transmite e recebe podem ser escutados à distância. Neste caso, o usuário não tem como descobrir que está sendo vigiado. A interceptação pode ser feita em vários pontos: interceptação de sinal *Wi-Fi*, instalação de escutas no *ISP* a quem ele se conecta, ou em um *PTT* que o seu *ISP* utiliza, ou monitorando o destinatário com quem o usuário está se comunicando no momento.

### 4.2.2 Descoberta dos seus destinatários

Caso você esteja usando uma comunicação criptografada, o conteúdo da mensagem pode estar protegido (ou não, como explicado sobre ataque *man in the middle* na seção 2.2). No entanto, escutando o seu tráfego, ainda é possível descobrir com quem você se comunica, pois os endereços IP (remetente e destinatário) dos pacotes não podem ser encriptados. É através deles que os roteadores sabem a quem sua mensagem deve ser entregue, por isso devem estar legíveis a todos. Logo, essa informação está disponível para todas as entidades que participam da transmissão dos seus pacotes, a começar pelo seu *ISP*. Pode parecer uma informação pouco comprometedora, mas em países com intensa perseguição a dissidentes políticos, a descoberta de quem conversa com quem é uma informação estratégica muito valiosa.

Ou seja, é possível descobrir os principais servidores com os quais você se comunica, mesmo que você tenha o cuidado de encriptar os dados enviados. Isto pode ser feito não apenas



lendo os endereços do seus pacotes IP, mas também através da leitura das suas requisições a servidores DNS.

### 4.2.3 Grampos na Web (*Web Bugs*)

Ao acessar um site, algumas das informações recebidas não são exibidas na página, mas armazenadas no computador para uso posterior. Alguns desses dados são conhecidos como *cookies* e são trocados entre seu navegador e os sites sem o usuário ter conhecimento. Seu uso mais comum é evitar que o usuário tenha que digitar usuário e senha toda vez que acessa sua página de *webmail* ou rede social, por exemplo. Ao autenticar-se pela primeira vez, o site em questão envia um *cookie* ao navegador do usuário contendo um identificador, assim quando o usuário acessar o site pela segunda vez, o navegador enviará junto com a requisição da página esse mesmo *cookie* para mostrar ao servidor que trata-se do mesmo navegador que havia se logado há pouco tempo atrás, tornando desnecessária uma nova autenticação pelo usuário.

*Cookies* também são utilizados por diversos outros sites, como sites de compras, para lembrar das suas preferências, ou guardar os produtos no seu carrinho de compras, mesmo sem você ser cadastrado no site em questão.

Já os *Pixel tags* são outro tipo de dispositivo para capturar informações de usuários na Web. O Facebook explica o que eles são em sua página <https://www.facebook.com/help/cookies>:

“Pixel tags (também conhecidos como GIFs limpos, Web beacons ou pixels) são pequenos blocos de código em uma página da web que permitem que os sites realizem ações, como ler e armazenar cookies. A conexão resultante pode incluir informações como os endereços de IP de uma pessoa, o horário em que a pessoa visualizou o pixel e o tipo de navegador usado.

Nós usamos pixels dentro e fora do Facebook, como quando você visita o nosso site ou o site de um de nossos parceiros. Os pixels nos permitem ler quaisquer cookies existentes do Facebook ou também depositar um novo cookie em seu navegador ou dispositivo. Nós usamos pixel tags para personalizar sua experiência e saber sobre como as pessoas usam produtos e serviços. Por exemplo, podemos usar pixel tags para saber se alguém, usando certo navegador, visualizou um anúncio no Facebook e também se comprou um produto de um anunciante. Isso nos ajuda a mostrar aos anunciantes que os anúncios que veiculam são eficazes. Também podemos usar pixels para ajudar a exibir anúncios dentro e fora do Facebook. Por exemplo, um parceiro pode usar um pixel para nos avisar quando você visitou seu site, para que futuramente possamos lhe exibir um anúncio no Facebook. Além disso, usamos pixels para saber quando você viu ou interagiu com o conteúdo do Facebook, como quando você lê uma notificação de e-mail que enviamos, de modo que seja possível evitar a exibição da mesma notificação quando você acessar o site ou aplicativo do Facebook, ou então para avaliar, entender e aprimorar nossos serviços.”

Ou seja, através de *cookies* e *pixel tags* empresas como Facebook e várias outras registram suas ações em vários outros sites, registrando as suas compras, visualizações de notícias,

pesquisas entre outras. Uma motivação para agregar tanta informação sobre os usuários da Internet é classificar cada usuário como um perfil de consumidor, e assim apresentar-lhe anúncios relevantes, com mais chances de serem clicados. Esse tipo de informação pode inclusive ser vendida para qualquer serviço interessado, ou requisitada por agentes governamentais.

Já existem aplicações que tentam evitar esse tipo de monitoramento desconhecido pela maioria dos usuários, como o *Disconnect.me* que funciona como uma extensão do navegador, evitando comunicação com uma “lista negra” de URLs voltadas apenas para monitoramento de usuários na Web (<http://disconnect.me>). Outra forma de evitar esse tipo de invasão é bloquear totalmente os anúncios na Web, também através de uma extensão no navegador como o *AdBlock Plus*. A *Electronic Frontier Foundation* recomenda a instalação dessas aplicações em [8].

### 4.3 Aquisição dos dados já enviados

Pode-se investigar um indivíduo sem necessariamente ele estar conectado na Internet naquele momento. O espião pode simplesmente conseguir acesso a registros que ficam armazenados em dispositivos da infraestrutura da rede, internos ao ISP, por exemplo. Ou então, acessar dados mais ricos, registros de utilização de um serviço como uma rede social, mensageiro instantâneo ou e-mail. Adquiridos através das grandes bases de dados de serviços que utilizam *cookies* e *pixel tags* para armazenar as ações dos usuários (mencionados na seção anterior).

## CAPÍTULO 5

# Métodos para contornar vigilância e censura na Internet

*Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds.*

—JOHN PERRY BARLOW (Decrypting the Puzzle Palace.  
Communications of the ACM. Vol.35, No. 7, 1992)

Para vencer a censura, basicamente o que se deve fazer é utilizar ferramentas que possibilitem a conexão com servidores bloqueados pelo governo. Se o bloqueio do governo for completo, ou seja, não envolver apenas alteração de servidores DNS, mas também o bloqueio do IP dos servidores, a resposta para isso é simples: *Proxy*.

### 5.1 Proxy

Um *proxy* funciona como um entregador terceirizado. Você estabelece comunicação com uma máquina escolhida por você e todas as suas requisições partirão daquela máquina. Como se você estivesse sentado em frente a ela, acessando a Web. Se você estiver na China e acessar a Web através de um *proxy* num país vizinho, você não será afetado pela censura empregada na China, pois sua navegação funcionará como se você estivesse naquele país vizinho.

No entanto, governos podem criar obstáculos para utilização de *proxies*. Em primeiro lugar, países que queiram implantar censura, em geral têm na sua lista de IPs bloqueados não só os provedores de conteúdo proibido, mas também servidores que funcionam como *proxy*. E se o IP do *proxy* está bloqueado, não haverá como utilizá-lo, naturalmente. Em segundo lugar, o governo pode deixar intencionalmente alguns *proxies* abertos pelo próprio governo, apenas com a intenção de atrair usuários e monitorar suas ações.

Há mais de uma forma de utilizar Proxies. Web Proxies são páginas acessíveis através de navegadores comuns, que possuem um campo para o usuário digitar o endereço que quer acessar. A página é então requisitada por este servidor, e exibida ao usuário *dentro* da mesma página que possui o campo do endereço. Um exemplo de Web Proxy encontra-se na Figura

## 5.1.

Há também o HTTP Proxy e o SOCKS Proxy. Para utilizar esses, é necessário conhecer o IP e Porta deles e configurar o seu navegador, ou aplicação como *Skype*, por exemplo, para utilizá-los. HTTP Proxies servem apenas para navegação. Já os SOCKS Proxies servem para outras aplicações. A Figura 5.2 mostra uma página com uma lista de *proxies* SOCKS.

Estas soluções, no entanto, não são ideais para o caso de se estar sendo vigiado. Para descobrir com quem o usuário se comunica, bastaria instalar uma escuta com o objetivo de monitorar o *proxy* que o usuário utiliza. Para isso existem as redes de anonimidade, que são métodos mais sofisticados de burlar censura e vigilância. O *Tor*, por exemplo, é uma rede de voluntários que ao executarem o programa, podem optar por servir como intermediários para outros usuários. No momento em que se inicia o *Tor*, são escolhidos três voluntários para servirem como intermediários na comunicação, como se fossem uma sequência de *proxies*. Esses intermediários se comunicam utilizando criptografia e os protocolos foram projetados para nenhum deles poder identificar ao mesmo tempo ambos os envolvidos na comunicação: remetente e destinatário. O primeiro intermediário conhece apenas o remetente, mas não conhece o destinatário, sabe apenas que deve encaminhar para o segundo intermediário. Já o segundo não conhece nem o remetente, nem o destinatário, apenas sabe que deve reencaminhar para o terceiro, que por sua vez conhece o destinatário, mas nunca saberá quem é o remetente.

Existem outras soluções com propósitos parecidos, como o *I2P*.

## 5.2 Acesso via satélite

Uma possível forma de combater censura em qualquer país é oferecer acesso à Internet via satélite. Nesse caso, o usuário não dependerá da infraestrutura de seu país. Em [14] *Hackers* demonstram esforços para alcançar isso.

## 5.3 Esteganografia

Em situações em que o usuário esteja sendo constantemente vigiado e ou perseguido, ainda é possível transmitir informações sigilosas sem levantar tanta suspeita quanto quando se utiliza criptografia pura – em alguns casos, o fato de estar usando criptografia já pode ser suficiente para chamar a atenção das autoridades. Além disso, em alguns países o uso de criptografia é proibido por lei, então mesmo sem conhecer o conteúdo da mensagem, o governo pode prender o cidadão, por apenas utilizar a criptografia.

Esteganografia é o nome dado a técnicas de ocultação de mensagens, onde duas mensagens são enviadas através de um mesmo meio, uma com conteúdo qualquer, banal e outra com conteúdo crítico, a ser escondido. A mensagem que se deseja esconder é apresentada de forma não intuitiva ou invisível sem as devidas ferramentas. Ao leitor desavisado, a mensagem lida será apenas uma e será a desimportante ou banal.

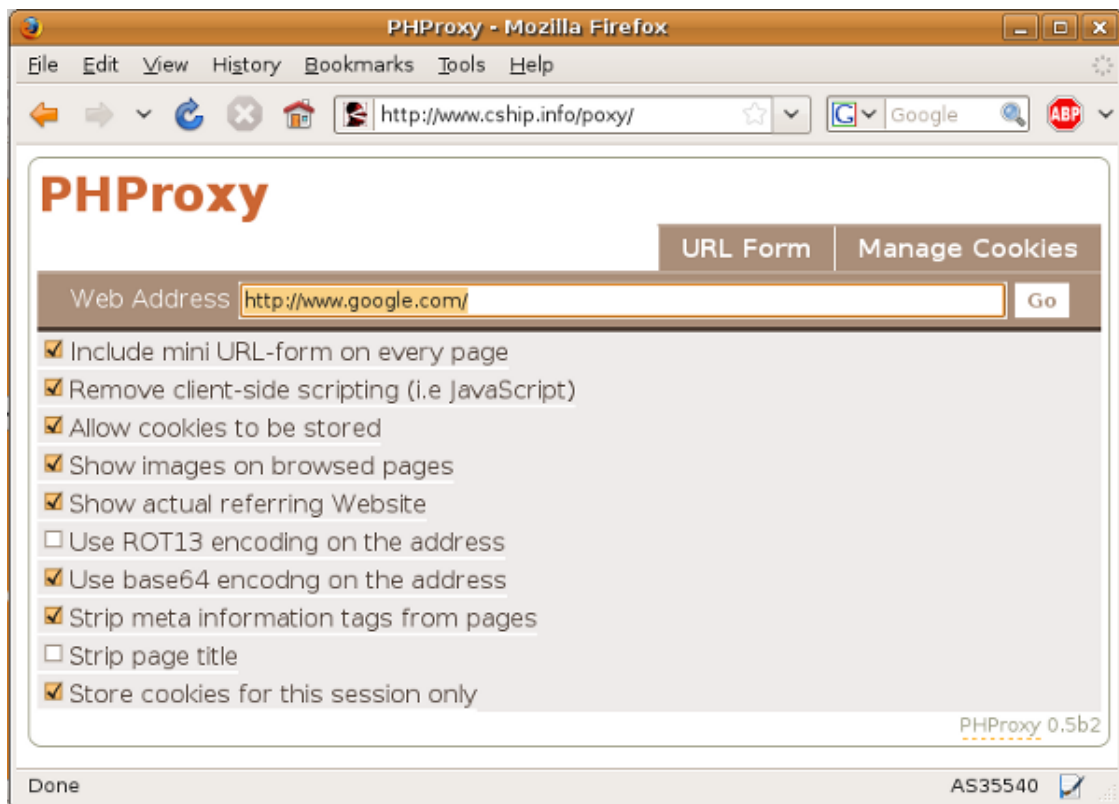
O primeiro uso do termo data de 1499, mas o primeiro registro de utilização deste tipo de técnica data de 400 a.C., tratando-se portanto de técnicas seculares, que foram apenas adaptadas para o mundo dos computadores. Entre as diversas técnicas não-digitais, há a utilização de

tinta invisível, que só é revelada sob circunstâncias específicas como alto calor, ou luz especial. Portanto, o remetente pode escrever uma lista de compras, por exemplo, usando tinta normal, e nos espaços em branco que sobraem, escrever com tinta invisível a mensagem a ser escondida. Obviamente o receptor, e apenas ele, deve conhecer a forma de revelar a mensagem.

No âmbito digital, pode-se por exemplo alterar minimamente o tom de cor de cada pixel de uma imagem. Tais modificações são imperceptíveis para um ser humano, mas são suficientes para guardar um texto inteiro, ou até mesmo uma outra imagem. Para decodificar a mensagem escondida, deve-se utilizar a ferramenta correta de extração da mensagem.

### **5.3.1 Esteganografia utilizada como apoio à vigilância governamental**

Algumas impressoras, especialmente as coloridas à *laser*, imprimem pontos amarelos praticamente imperceptíveis em todas as páginas, sem consentimento do usuário. Para o usuário desavisado, estes pontos podem ser entendidos como um defeito na impressora, ou característica estranha do papel. No entanto, estes pontos amarelos são posicionados de forma que guardem uma informação valiosa: a marca e o número de série da impressora utilizada. Desta forma, é possível utilizar a informação para rastrear o dono da impressora e possivelmente quem imprimiu um certo documento. Esta tecnologia foi implementada por grandes companhias como a *Xerox*, *Canon* e várias outras, motivados pela preocupação de alguns governos, de que estas impressoras fossem utilizadas para falsificar dinheiro. A *Electronic Frontier Foundation* mantém uma lista de impressoras que foram testadas se possuem esse tipo de tecnologia ou não em [10].



**Figura 5.1** Nesta página é possível observar um campo para endereços, no caso preenchido com a URL da página inicial do *Google*. Logo abaixo há algumas opções a serem configuradas pelo usuário. Assim que o usuário clica em “Go”, a página será atualizada, substituindo a área com as opções de configuração pela página do *Google* requisitada pelo usuário.

www.idcloak.com/proxylist/socks5-proxy-list.html

## IDCLOAK SOCKS5 PROXY LIST

### SOCKS5 PROXY LIST

Our freshly updated SOCKS5 proxy list is compatible with all the latest programs that use SOCKS5. You can configure the list to show a specific country, port and anonymity level. The list will be sorted by update time, and you can see the fastest proxy showing up in green colours.

**Proxy selection**

**Proxy Country**  
All -> 2121  
Countries:  
ID -> 255  
CN -> 232  
US -> 209

**Proxy ports**  
All ports  
Ports:  
8080 -> 895  
3128 -> 464  
80 -> 240

**Protocol**  
http ☐  
https ☐  
socks4 ☐  
socks5 ☒

**Characteristic**

	Low	Medium	High
Anonymity:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Connection speed:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Speed:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Show selected proxies

New to proxies? Here's how to use them.

Update time	Country	Connection Speed	Speed	Anonymity	Protocol	Port	IP Address
25m 45s	KR			High	socks5	5577	59.21.114.99
1h 1m 19s	US			High	socks5	10080	24.103.219.72
1h 49m 44s	CN			High	socks5	9123	61.147.67.2
1h 49m 54s	CN			High	socks5	8888	180.169.125.49
4h 39m 30s	US			High	socks5	443	50.16.153.115
7h 39m 24s	CN			High	socks5	1080	202.198.17.141
7h 39m 55s	KR			High	socks5	8888	114.207.246.17
9h 58m 7s	RU			High	socks5	2214	80.93.49.145
11h 19m 46s	CN			High	socks5	1080	210.27.145.144
12h 1m 45s	UA			High	socks5	8181	80.91.190.188
13h 17m 27s	US			High	socks5	1553	75.73.144.197
13h 40m 41s	BD			High	socks5	1080	180.211.191.25
14h 26m 53s	DK			High	socks5	1080	80.63.56.146
18h 54m 51s	CN			High	socks5	9124	61.147.67.2

**IMPORTANT:** The public proxy servers displayed on the idcloak.com website are not operated or owned by idcloak Technologies Inc. We provide the list to you as an information resource only. It is impossible for us to vet the listed proxies, so idcloak Technologies Inc. cannot in any way guarantee their functionality, security or privacy. Use them at your own risk.

**Figura 5.2** Este site tem a intenção de divulgar SOCKS Proxies, para pessoas que estão dentro de redes com alguns serviços censurados como a navegação Web, ou utilização de *messengers*, ou comunicação por voz (e.g. *Skype*). Ao configurar seu navegador, ou *messenger* para utilizar algum desses *proxies*, o usuário fica livre da censura.





## CAPÍTULO 6

# Conclusão

### 6.1 A relação entre vigilância e censura – Autocensura

A vigilância e a censura podem trazer consequências adversas em uma sociedade. Um efeito por exemplo é o *chilling effect*, em que os indivíduos de uma sociedade, por medo de estarem sendo vigiados o tempo todo, acabam evitando expressar ideias contrárias ao seu governo, tornando-os mais “calmos” e inertes às ações do governo que consideram incorretas. Essa mesma estratégia já foi utilizada por governos da antiguidade, mesmo sem tecnologia, ao misturar governo e religião. Por medo de alguma punição divina, tornavam-se mais obedientes ao governo e facilmente manipuláveis.

Ronald Deibert em [6] compara o sistema de censura chinês ao livro 1984 de George Orwell e ao conceito de penitenciária idealizado por Jeremy Bentham, o Pan-óptico. No livro de George Orwell, o “Big Brother” se mostra presente em vários momentos do dia-a-dia dos cidadãos. Logo que acordam, por exemplo, ouvem alguma mensagem do “Big Brother”. Portanto, sentem-se vigiados pois está explícita a presença do vigia. Já no Pan-óptico, todas as celas são construídas lado a lado, formando uma circunferência, de modo a serem igualmente e completamente visíveis a uma torre de vigilância central. Nessa torre os guardas ficam escondidos atrás de venezianas, não sendo possível para os presos saber se estão sendo olhados naquele momento ou não. Ou seja, a intenção é dar a impressão que todos estão sendo vigiados o tempo todo, mesmo havendo poucos guardas. Ronald Deibert diz que o sistema de censura chinês se assemelha mais ao Pan-óptico do que ao “Big Brother” de George Orwell. A vigilância é implícita, o que gera uma auto-censura nas pessoas, por medo de serem pegadas, sem saber se estão sendo vigiadas naquele momento ou não.

### 6.2 Empresas que lucram com a censura e a vigilância

Andy Müller-Maguhn, co-autor do livro *Cypherpunks* ([3]) de Julian Assange, é fundador do site *Bugged Planet* - <http://buggedplanet.info> (Planeta grampeado, em inglês). Lá há uma página no formato *wiki*, colaborativa, onde se compartilham informações sobre vigilância na Internet, incluindo listas de empresas e pessoas que ganham dinheiro com este nicho mercadológico.

Uma delas é a *Blue Coat*, alvo de pesquisas como [17], [13] e [5]. É um exemplo de empresa que produz tecnologia classificada como de “uso dual”. Ou seja, pode ter usos pacíficos e benéficos, assim como usos militares e violentos. Um exemplo de tecnologia de uso dual são os foguetes, que podem ser utilizados para levar homens ao espaço, ou para lançar satélites,

como também serem utilizados como armas, como mísseis de longo alcance.

Os dispositivos da *Blue Coat*, podem ser utilizados para gerenciar a rede interna de uma empresa, evitando que funcionários acessem conteúdo inadequado para a realização de suas atividades, ou para garantir o desempenho e segurança da rede. Da mesma forma, pode ser instalado nas fronteiras da Internet de um país e monitorar o tráfego de todos os cidadãos, assim como filtrar o que eles podem acessar. Na Figura 6.1 é mostrada a página da empresa, apresentando seus produtos.

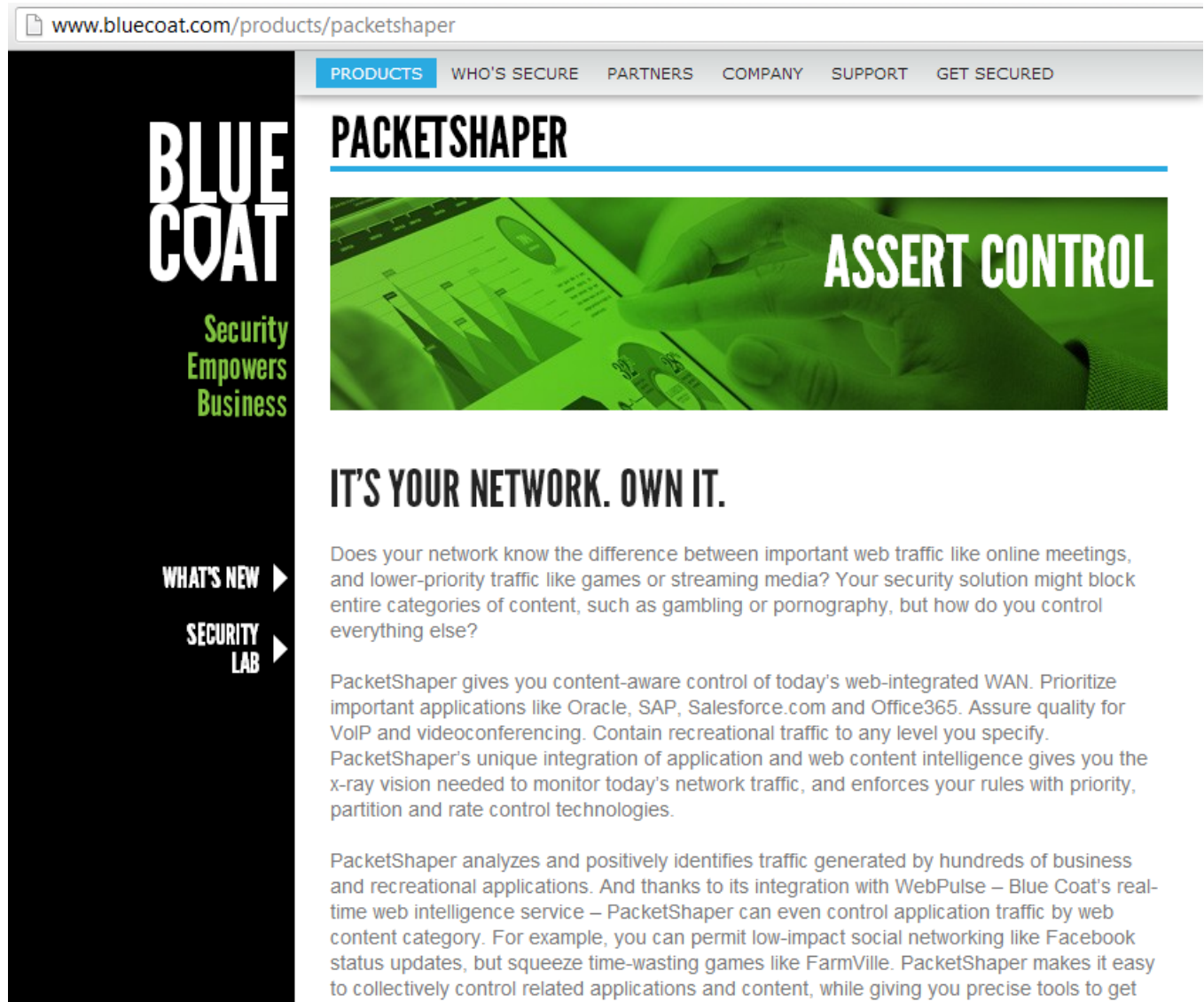
Foi descoberto que dispositivos da *Blue Coat* eram utilizados pelo governo Sírio, conhecido por perseguir civis contrários ao governo de Bashar Al-Assad. Os mesmos dispositivos foram descobertos sendo utilizados por vários outros países do oriente médio, Ásia e África, segundo relatório do *Citizen Lab* da Universidade de Toronto ([13]).

### 6.3 Considerações finais

De acordo com [4] um grande problema da censura na Internet é que ela é empregada de forma pouco transparente. Deve-se observar a robustez do processo pelo qual os cidadãos decidem tornar uma informação indisponível. A censura é legítima quando o estado a faz de forma aberta, descreve transparentemente o conteúdo bloqueado, bloqueia estritamente o material proibido e oferece poder de decisão aos cidadãos que estão sendo afetados. Enquanto não se alcança o mundo ideal, algumas pessoas tentam ao menos catalogar a censura nos países, com serviços como o *Herdict* ([www.herdict.org](http://www.herdict.org)), onde as pessoas espontaneamente apontam o que está sendo censurado e onde.

Já o grampeamento das nossas comunicações, inclusive de um país para outro, como foi publicado recentemente a espionagem ao governo brasileiro, partindo dos Estados Unidos ([11]), poderia ser melhor controlada, caso a infraestrutura física da rede e suas instalações fossem fiscalizadas por um órgão internacional. Dessa forma, se evitaria que um governo utilizasse suas instalações como grampos e ouvir todo o tráfego que passa pelo seu país.

Julian Assange define bem a nossa situação na introdução do seu *Cypherpunks* ([3]): “À medida que os estados se fundem com a internet e o futuro da nossa civilização se transforma no futuro da internet, nós precisamos redefinir as relações de força. Se não o fizermos, a universalidade da internet irá se fundir com a humanidade em uma gigante rede de controle e vigilância massivos. É preciso acionar o alarme. Este livro é o grito de advertência de uma sentinela na calada da noite.”.



www.bluecoat.com/products/packetshaper

PRODUCTS WHO'S SECURE PARTNERS COMPANY SUPPORT GET SECURED

# BLUE COAT

Security Empowers Business

## 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

**Figura 6.1** A tecnologia *Packetshaper* oferecida pela *Blue Coat*, como mostrado na figura, possibilita o administrador restringir o tipo de tráfego que entra e sai dos seus domínios. Pode inclusive restringir os sites acessíveis de acordo com a classificação do seu conteúdo.



## Referências Bibliográficas

- [1] La cybercensure iranienne vue de l'intérieur à la veille des élections présidentielles... Powered by Cisco Systems. <http://reflets.info/la-cybercensure-iranienne-vue-de-linterieure-a-la-veille-des-elections-presidentielles-powered-by-cisco-systems/>, June 2013. [Online; acessado em 23 de Setembro de 2013].
- [2] List of blacklisted keywords in the People's Republic of China. [http://en.wikipedia.org/wiki/List\\_of\\_blacklisted\\_keywords\\_in\\_the\\_People%27s\\_Republic\\_of\\_China](http://en.wikipedia.org/wiki/List_of_blacklisted_keywords_in_the_People%27s_Republic_of_China), 2013. [Online; acessado em 23 de Setembro de 2013].
- [3] J. Assange, J. Appelbaum, A. Müller-Maguhn, and J. Zimmermann. *Cypherpunks: Freedom and the Future of the Internet*. OR Books, LLC, 2012.
- [4] Derek E. Bambauer. Censorship v3.1. *IEEE Internet Computing*, 17(3):26–33, 2013.
- [5] bluetouff. #OpSyria: Web censorship technologies in Syria revealed [EN]. <http://reflets.info/opsyria-web-censorship-technologies-in-syria-revealed-en/>, October 2011. [Online; acessado em 23 de Setembro de 2013].
- [6] R.J. Deibert. *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart, 2013.
- [7] Feng Ding, Zhiqing Yang, Xuelong Chen, and Jianfeng Guo. Effective methods to avoid the internet censorship. In *Parallel Architectures, Algorithms and Programming (PAAP), 2011 Fourth International Symposium on*, pages 67–71, 2011.
- [8] Electronic Frontier Foundation. 4 Simple Changes to Stop Online Tracking. <https://www.eff.org/deeplinks/2012/04/4-simple-changes-protect-your-privacy-online>. [Online; acessado em 23 de Setembro de 2013].
- [9] Electronic Frontier Foundation. Hepting v. AT&T. <https://www.eff.org/cases/hepting>. [Online; acessado em 23 de Setembro de 2013].
- [10] Electronic Frontier Foundation. List of Printers Which Do or Do Not Display Tracking Dots. <https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots>. [Online; acessado em 23 de Setembro de 2013].

- [11] Glenn Greenwald. The NSA's mass and indiscriminate spying on Brazilians. <http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying>, July 2013. [Online; acessado em 23 de Setembro de 2013].
- [12] John Markoff. Vast Spy System Loots Computers in 103 Countries. <http://www.nytimes.com/2009/03/29/technology/29spy.html>, March 2009. [Online; acessado em 23 de Setembro de 2013].
- [13] Morgan Marquis-Boire, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman. Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. <https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/>, January 2013. [Online; acessado em 23 de Setembro de 2013].
- [14] David Meyer. Hackers plan space satellites to combat censorship. <http://www.bbc.co.uk/news/technology-16367042>, January 2012. [Online; acessado em 23 de Setembro de 2013].
- [15] Dubai School of Government. Social media in the arab world: Influencing societal and cultural change? <http://www.arabsocialmediareport.com/UserManagement/PDF/ASMR%204%20updated%2029%2008%2012.pdf>, 2012. [Online; acessado em 23 de Setembro de 2013].
- [16] Ryan Singel. Whistle-Blower Outs NSA Spy Room. <http://www.wired.com/science/discoveries/news/2006/04/70619>, July 2006. [Online; acessado em 23 de Setembro de 2013].
- [17] University of Toronto The Citizen Lab. Behind Blue Coat: Investigations of commercial filtering in Syria and Burma. <http://citizenlab.org/2011/11/behind-blue-coat/>, November 2011. [Online; acessado em 23 de Setembro de 2013].
- [18] BBC UK. Google says Vietnam mine opponents under cyber attack. <http://news.bbc.co.uk/2/hi/asia-pacific/8596846.stm>, March 2010. [Online; acessado em 23 de Setembro de 2013].

