O Vale da Vigilância

A história secreta e militar da Internet

Yasha Levine

Sumário

Prólogo: Oakland, Califórnia.....5

Parte I: História Perdida

Capítulo 1: Um novo tipo de guerra.....17

Capítulo 2: Comando, Controle e contrainsurgência.....39

Capítulo 3: Espionando os gringos.....77

Parte II: Falsas Promessas

Capítulo 4: Utopia e privatização.....105

Capítulo 5: Vigilância S.A.....143

Capítulo 6: A Corrida armamentista de Edward Snowden.....193

Capítulo 7: Privacidade na Internet… financiada por espiões.....227

Epílogo: Mauthausen, Áustria.....281

Agradecimentos

Sobre o Autor

Notas

Índice

Prólogo

Oakland, Califórnia.

Era 18 de fevereiro de 2014 e já estava escuro quando cruzei a Bay Bridge de São Francisco e estacionei meu carro no centro de Oakland. As ruas estavam desertas, a não ser por alguns moradores de rua amontoados na frente de uma loja fechada. Dois carros da polícia furaram o sinal vermelho com as sirenes ligadas.

Aproximei-me da prefeitura de Oakland a pé. Mesmo à distância, pude ver que algo incomum estava acontecendo. Uma fileira de carros de polícia estacionados descia pelo quarteirão, e âncoras de notícias e equipes de câmeras de TV correram em disparada, disputando posições. Um grande grupo de pessoas se amontoou perto da entrada, algumas montando o que parecia ser um rato gigante de papel machê, presumivelmente destinado a ser um símbolo para intromissão. Mas a ação de verdade estava acontecendo dentro. Várias centenas de pessoas lotaram a câmara ornamentada do conselho da cidade de Oakland. Muitas delas carregavam cartazes. Era uma multidão furiosa, e policiais flanqueavam os lados da sala, prontos para empurrar todo mundo para fora caso as coisas saíssem do controle.

A comoção estava ligada ao principal item da agenda da noite: o conselho da cidade estava programado para votar um ambicioso projeto de 11 milhões de dólares para a criação de um centro de vigilância policial em toda a cidade. Seu nome oficial era “Centro de Consciência do Domínio” – mas todos o chamavam de “DAC” (*Domain Awareness Center*). As especificações de design exigiam a conexão de imagens de vídeo em tempo real de milhares de câmeras em toda a cidade e sua canalização para um centro de controle unificado. A polícia poderia selecionar em um local e assisti-lo em tempo real ou voltar no tempo. Eles poderiam ativar sistemas de reconhecimento facial e rastreamento

de veículos, conectar *feeds* de mídia social e melhorar sua visão com dados provenientes de outras agências para a execução da lei (*law enforcement agencies*) – locais e federais.1

Os planos para esse centro de vigilância vinham agitando a política da cidade há meses, e a indignação agora estava fazendo sentir sua presença. Moradores, líderes religiosos, ativistas trabalhistas, políticos aposentados, anarquistas mascarados do "bloco negro" e representantes da União Americana das Liberdades Civis – todos estavam presentes, ombro a ombro com um grupo de ativistas locais dedicados que se uniram para barrar o DAC. Um funcionário prefeitura, nervoso e de óculos, vestindo um terno bege, subiu ao pódio para tranquilizar a agitada multidão. Ele disse que o Centro de Consciência de Domínio foi projetado para protegê-los – e não espioná-los. "Este não é um centro que irá fundir diversas agências. Não temos acordos com a NSA, a CIA ou o FBI para acessar nossos bancos de dados", disse ele.

O salão explodiu em pandemônio. A multidão não se deixava enrolar. As pessoas vaiavam e assobiavam. "Isso tudo é pra monitorar manifestantes", alguém gritou da galeria. Um jovem, com o rosto coberto por uma máscara, foi até a frente da sala e, ameaçadoramente, enfiou o *smartphone* no rosto do oficial da cidade e tirou fotos. – Como você se sentiu? Como é ser vigiado o tempo todo?! ele gritou. Um homem de meia-idade – calvo, usando óculos e calças cáqui amarrotadas – subiu ao pódio e abriu espaço à força entre os líderes políticos da cidade. "Vocês, membros do conselho, acreditam que o Departamento de Polícia de Oakland, que tem uma história incomparável de violação dos direitos civis de seus cidadãos e que não consegue seguir suas próprias políticas, seja uma política de controle de multidões ou uma política de uso de câmeras corporais pelos policiais, pode de alguma forma ser confiável para usar o DAC?" E ele saiu gritando: "O único DAC bom é um DAC morto!" Aplausos selvagens irromperam.

Oakland é uma das cidades mais diversas do país. É também o lar de um departamento de polícia violento, que muitas vezes não responde pelos seus atos, e que opera sob supervisão federal há mais de uma década. O abuso policial vem ocorrendo em um cenário de crescente gentrificação, impulsionada pelo boom da Internet na região e pelo aumento nos preços dos imóveis que a acompanha. Em São Francisco,

bairros como o Distrito da Missão, historicamente o lar de uma vibrante comunidade latina, transformaram-se em condomínios e *lofts* e em sofisticados *pubs* gastronômicos. Professores, artistas, adultos mais velhos e qualquer outra pessoa que não tenha um salário de seis dígitos estão tendo dificuldade em se sustentar. Oakland, que por um tempo foi poupada desse destino, agora estava sentindo a queda também. Mas os moradores locais não estavam caindo sem brigar. E muito da raiva deles estava focada no Vale do Silício.

As pessoas reunidas na prefeitura naquela noite viram o DAC de Oakland como uma extensão da gentrificação impulsionada pela tecnologia que estava empurrando os residentes de longa data mais pobres para fora da cidade. “Não somos estúpidos. Sabemos que o objetivo é monitorar os muçulmanos, as comunidades negras e pardas e quem se manifesta”, disse uma jovem usando um lenço de cabeça. “Este centro surge em um momento em que se está tentando desenvolver Oakland como uma comunidade de *playgrounds* e dormitórios para profissionais de São Francisco. Esses esforços exigem que se torne Oakland mais silenciosa, mais branca, menos assustadora e mais rica – e isso significa se livrar de muçulmanos, negros e pardos e manifestantes. Você sabe disso e as construtoras também. Estivemos nas suas reuniões. Estão assustados. Eles verbalmente admitem isso.

O argumento dela era importante. Poucos meses antes, dois jornalistas investigativos de Oakland haviam obtido um pacote de documentos internos de planejamento urbano relacionados ao DAC e descobriram que as autoridades da cidade pareciam estar mais interessadas em usar o centro de vigilância proposto para monitorar protestos políticos e atividades sindicais nas docas de Oakland do que para combater o crime.2

Houve outra agitação. Oakland havia inicialmente contratado o desenvolvimento do DAC da *Science Applications International Corporation* (SIAC), uma grande terceirizada militar sediada na Califórnia que faz tantos trabalhos para a Agência de Segurança Nacional (NSA) que é conhecida no ramo de inteligência como “NSA do Oeste”. A empresa também é uma grande contratada da CIA, envolvida em todo tipo de ações, desde monitoramento de funcionários da agência (como parte dos seus programas de “ameaça interna”) até a administração de sua frota de

drones para assassinato. Vários moradores de Oakland vieram para impedir a decisão da cidade de fazer parceria com uma terceirizada que era parte integral do aparato militar e de inteligência dos EUA. “A SAIC fornece as telecomunicações para o programa de drones no Afeganistão, que matou mais de mil civis inocentes, incluindo crianças”, disse um homem de suéter preto. “E esta é a empresa que vocês escolheram?”

Olhei ao redor da sala com espanto. Este era o coração de uma área supostamente progressista da Baía de São Francisco, e a cidade planejava fazer parceria com uma poderosa empresa terceirizada de inteligência para construir um centro de vigilância policial que, se as reportagens estivessem corretas, as autoridades queriam para espionar e monitorar os moradores locais. Algo fez a cena ainda mais estranha para mim naquela noite. Graças a uma dica de um ativista local, fiquei sabendo que Oakland estava conversando com a Google sobre uma demonstração de produtos. Ao que tudo indica, aquilo era uma tentativa da empresa de conseguir uma parte do contrato do DAC.

A Google, possivelmente, ajudando Oakland a espionar seus moradores? Se fosse verdade, seria particularmente condenável. Muitos moradores de Oakland viram as empresas do Vale do Silício, como a Google, como os principais impulsionadores do aumento vertiginoso dos preços das moradias, da gentrificação e do policiamento agressivo que tornavam a vida miserável para os moradores pobres e de baixa renda. De fato, apenas algumas semanas antes, os manifestantes haviam formado um piquete na frente da casa de um rico gerente da Google que estava pessoalmente envolvido em um empreendimento imobiliário de luxo nas proximidades.

O nome da Google nunca apareceu durante a tumultuada reunião da prefeitura naquela noite, mas consegui ter acesso a uma breve troca de e-mails entre um “gerente estratégico de parcerias” da Google e um funcionário de Oakland que encabeçava o projeto DAC, o que sugeria que algo estava em andamento.3

Nas semanas após a reunião do conselho da cidade, tentei esclarecer essa relação. Que tipos de serviços a Google ofereceu ao centro de vigilância policial de Oakland? Até que ponto as negociações progrediram? Elas foram frutíferas? Meus pedidos para a cidade de Oakland foram ignorados e a Google também não disse nada – tentar obter res-

postas da empresa era como falar com uma pedra gigante. Minha investigação estagnou ainda mais quando os residentes de Oakland conseguiram temporariamente que a cidade suspendesse seus planos para o DAC.

Embora o centro de vigilância da polícia de Oakland tenha sido suspenso, a questão permaneceu: como a Google, uma empresa obcecada com sua imagem progressista "não seja malvado", estava oferecendo um centro de vigilância policial controverso?

Na época, eu era repórter da Pando, uma pequena mas destemida revista de São Francisco que cobria a política e os negócios do Vale do Silício. Eu sabia que a Google fazia a maior parte de seu dinheiro por meio de um sofisticado sistema de publicidade segmentada que rastreava seus usuários e criava modelos preditivos de comportamento e interesses. A empresa teve um vislumbre das vidas de quase dois bilhões de pessoas que usaram suas plataformas – de e-mail, vídeo e celulares – e realizou um tipo estranho de alquimia, transformando dados de pessoas em ouro: quase US $ 100 bilhões em receita anual e uma capitalização de mercado de US $ 600 bilhões; seus fundadores Larry Page e Sergey Brin tinham um patrimônio pessoal combinado estimado em US $ 90 bilhões.

A Google é uma das corporações mais ricas e poderosas atualmente, mas se apresenta como um dos mocinhos: uma empresa com a missão de tornar o mundo um lugar melhor e ser um baluarte contra governos corruptos e intrusivos ao redor do globo. E, no entanto, enquanto eu traçava a história e procurava os detalhes do contrato da Google com o governo, descobri que ela já era uma empresa militar em todos os sentidos, vendendo versões de sua tecnologia de mineração e análise de dados de consumo para departamentos de polícia, prefeituras e quase todas as principais agências de inteligência e militares dos EUA. Ao longo dos anos, havia fornecido tecnologia de mapeamento usada pelo Exército dos EUA no Iraque, hospedado dados para a Agência Central de Inteligência, indexado os vastos bancos de dados de inteligência da Agência de Segurança Nacional, construído robôs militares, lançado um satélite espião em colaboração com o Pentágono e arrendado sua plataforma de computação em nuvem para ajudar os departamentos de polícia a prever crimes. E a Google não está sozinha. Da Amazon ao

eBay e Facebook – a maioria das empresas de Internet que usamos todos os dias também se transformou em corporações poderosas que rastreiam e fazem o perfil de seus usuários enquanto buscam parcerias e relações de negócios com as principais agências militares e de inteligência dos EUA. Algumas partes dessas empresas estão tão completamente interligadas com os serviços de segurança estadunidense que é difícil dizer onde elas terminam e o governo dos EUA começa.

Desde o início da revolução do computador pessoal e da Internet nos anos 1990, nos disseram várias vezes que estamos no controle de uma tecnologia libertadora, uma ferramenta que descentraliza o poder, derruba burocracias entrincheiradas e traz mais democracia e igualdade ao mundo. Os computadores pessoais e as redes de informação deveriam ser a nova fronteira da liberdade – uma tecno-utopia em que estruturas autoritárias e repressivas perdiam seu poder e onde a criação de um mundo melhor ainda era possível. E tudo o que nós, internautas globais, precisávamos fazer para esse novo e melhor mundo florescer era sair do caminho e deixar as empresas de Internet inovarem e o mercado fazer sua mágica. Essa narrativa foi plantada profundamente no subconsciente coletivo de nossa cultura e detém uma poderosa influência sobre a maneira como vemos a Internet hoje.

Mas tire um tempo para olhar para os detalhes da Internet e a história se torna mais sombria, menos otimista. Se a Internet é realmente essa ruptura revolucionária com o passado, por que empresas como a Google dormem com policiais e espiões?

Tentei responder a essa pergunta aparentemente simples depois de visitar Oakland naquela noite em fevereiro. Mal sabia que isso me levaria a um mergulho profundo na história da Internet e, finalmente, a escrever este livro. Agora, depois de três anos de trabalho investigativo, entrevistas, viagens em dois continentes e incontáveis horas de correlação e pesquisa de registros históricos e desclassificados, sei a resposta.

Pegue qualquer história popular da Internet e você geralmente encontrará uma combinação de duas narrativas descrevendo de onde veio essa tecnologia de rede de computadores. A primeira narrativa é que surgiu da necessidade das forças armadas de ter uma rede de comunicação que pudesse sobreviver a uma explosão nuclear. Isso levou ao desenvolvimento da primeira Internet, a ARPANET, construída pela

Agência de Projetos de Pesquisa Avançada do Pentágono (hoje conhecida como Agência de Projetos de Pesquisa Avançada em Defesa, ou DARPA). A rede entrou em operação no final dos anos 1960 e apresentava um design descentralizado que podia encaminhar mensagens mesmo se partes da rede fossem destruídas por uma explosão nuclear. A segunda narrativa, que é a mais dominante, sustenta que, no início, não houve nenhuma aplicação militar da Internet. Nesta versão, a ARPANET foi construída por jovens engenheiros de computação radicais e hackers brincalhões profundamente influenciados pela contracultura cheia de ácido da área da baía da São Francisco. Eles não se importavam nem um pouco com a guerra ou a vigilância ou qualquer coisa do tipo, mas sonhavam com utopias mediadas por computador que tornariam as forças armadas obsoletas. Eles construíram uma rede civil para trazer esse futuro à realidade, e é essa versão da ARPANET que cresceu na Internet que usamos hoje. Durante anos, houve um conflito entre essas interpretações históricas. Hoje em dia, a maioria das histórias oferece uma mistura das duas – reconhecendo a primeira, mas inclinando-se muito mais para a segunda.

Minha pesquisa revela uma terceira corrente histórica na criação da primeira Internet – uma vertente que praticamente desapareceu dos livros de história. Aqui, o ímpeto estava enraizado não tanto na necessidade de sobreviver a um ataque nuclear, mas nas obscuras artes militares da contrainsurgência e na luta dos Estados Unidos contra a aparente disseminação global do comunismo. Nos anos 1960, os Estados Unidos eram uma potência global que supervisionava um mundo cada vez mais volátil: conflitos e insurgências regionais contra governos aliados dos EUA, da América do Sul ao Sudeste Asiático e o Oriente Médio. Essas não eram guerras tradicionais que envolviam grandes exércitos, mas campanhas de guerrilha e rebeliões locais, frequentemente travadas em regiões onde os estadunidenses tinham pouca experiência anterior. Quem eram essas pessoas? Por que elas estavam se rebelando? O que poderia ser feito para detê-las? Nos círculos militares, acreditava-se que essas questões eram de vital importância para os esforços de pacificação dos Estados Unidos, e alguns argumentavam que a única maneira eficaz de respondê-las era desenvolver e impulsionar a tecnologia da informação auxiliada por computador.

A Internet surgiu desse esforço: uma tentativa de construir sistemas computacionais que pudessem coletar e compartilhar inteligência, observar o mundo em tempo real e estudar e analisar pessoas e movimentos políticos com o objetivo final de prever e prevenir a agitação social. Alguns até sonhavam em criar uma espécie de radar de alerta antecipado para as sociedades humanas: um sistema de computador em rede que observava as ameaças sociais e políticas e as interceptava da mesma maneira que o radar tradicional fazia com aeronaves hostis. Em outras palavras, a Internet foi programada para ser uma ferramenta de vigilância desde o início. Não importa para o que usamos a rede hoje – namoro, mapas, bate-papo criptografado, e-mail ou apenas ler as notícias –, ela sempre teve uma natureza de uso duplo enraizada na coleta de informações e na guerra.

Enquanto eu traçava essa história esquecida, descobri que não estava descobrindo algo novo, mas desvelando algo que era óbvio para muitas pessoas não faz muito tempo. A partir do início dos anos 1960, nos Estados Unidos, surgiu um grande receio quanto à proliferação de bases de dados computacionais e tecnologias de rede. As pessoas temiam que esses sistemas fossem usados por corporações e governos para vigilância e controle. Na verdade, a visão cultural dominante na época era que os computadores e a tecnologia de computação – incluindo a ARPANET, a rede de pesquisa militar que se tornaria a Internet que usamos hoje – eram ferramentas de repressão, não de libertação.

No decorrer de minha investigação, fiquei realmente chocado ao descobrir que, em 1969, o primeiro ano em que a ARPANET entrou em operação, um grupo de estudantes do MIT e de Harvard tentou fechar as pesquisas em suas universidades que estavam sob o guarda-chuva da ARPANET. Eles viam essa rede de computadores como o início de um sistema híbrido público-privado de vigilância e controle – o que eles chamavam de “manipulação computadorizada de pessoas” – e avisavam que ela seria usada para espionar os estadunidenses e travar guerras contra movimentos políticos progressistas. Eles entendiam essa tecnologia melhor do que nós hoje. Mais importante que isso, eles estavam certos. Em 1972, quase tão logo a ARPANET foi lançada em nível nacional, a rede foi usada para ajudar a CIA, a NSA e o Exército dos EUA a espionar dezenas de milhares de ativistas antiguerra e de direitos civis dentro do seu território. Foi um grande escândalo na época, e o papel da ARPA-

NET foi amplamente discutido na televisão americana, incluindo na *NBC Evening News*.

Este episódio, ocorrido há quarenta e cinco anos, é uma parte vital do registro histórico, importante para quem quer entender a rede que hoje intermedeia grande parte de nossas vidas. No entanto, você não vai encontrá-lo mencionado em qualquer livro ou documentário recente sobre as origens da Internet – pelo menos, não qualquer um que eu pude encontrar, e li e assisti a quase todos eles.

O livro *Vale da Vigilância* é uma tentativa de recuperar parte dessa história perdida. Mas ele é mais do que isso. O livro começa no passado, remontando ao desenvolvimento do que hoje chamamos de Internet durante a Guerra do Vietnã. Mas rapidamente passa para o presente, olhando para o negócio de vigilância privada que alimenta boa parte do Vale do Silício. Esta investigação foca na sobreposição existente entre a Internet e o complexo industrial-militar que a disseminou meio século atrás e revela os laços estreitos que existem entre as agências de inteligência dos EUA e o movimento pela privacidade e antigoverno que surgiu na esteira dos vazamentos de Edward Snowden. O Vale da Vigilância mostra que pouco mudou ao longo dos anos: a Internet foi desenvolvida como uma arma e continua sendo uma arma hoje. Os interesses militares estadunidenses continuam a dominar todas as partes da rede, mesmo aquelas que supostamente estão em sua oposição.

Yasha Levine

Nova Iorque, dezembro de 2017

Parte I

A História Perdida

Capítulo 1

Um novo tipo de guerra

Nosso ódio pelos estadunidenses
é tão alto quanto o céu.
- canção vietnamita do norte

Em 8 de junho de 1961, um oficial de inteligência militar chamado William Godel chegou a Saigon vindo de Washington, DC. Era um dia quente de verão quando ele desembarcou na capital do Vietnã do Sul, e Godel, sofrendo com o *jetlag* e gotejando de suor, visitou vários edifícios baixos, ao estilo de barracas militares, não muito longe do rio Saigon. Caminhou com dificuldade, com a perna manca de seus dias de guerra contra as forças japonesas no sul do Pacífico. Superficialmente, não havia nada de especial nessa excursão. Havia pouco para indicar que essas estruturas indefinidas, com suas paredes brancas e telhados inclinados, eram o centro do Projeto Agile, um programa ultrassecreto de contrainsurgência que desempenharia um papel importante na história da Guerra do Vietnã e na ascensão da tecnologia informática moderna.

De sua base no Pentágono, Godel pressionava por uma iniciativa como o Agile por mais de uma década. Agora, este projeto havia conseguido o apoio pessoal do presidente John F. Kennedy.1

Os primeiros resultados foram vistos em 10 de agosto de 1961, quando um helicóptero Sikorsky H-34, em forma de um enorme peixe de cauda larga, levantou-se preguiçosamente acima de Saigon e seguiu em direção às selvas impenetráveis de Kon Tum, na fronteira com o Laos e o Camboja.2 Uma vez que o piloto encontrou seu alvo, ele sinalizou, e a tripulação ligou um borrifador de colheita especial acoplado na parte de baixo da nave. Em um movimento de varredura lenta, eles pulverizaram a selva abaixo com uma mistura experimental de produtos químicos de desfolhação altamente tóxicos. Entre eles estava o infame

Agente Laranja. Aqueles que cheiraram disseram que se assemelhava a perfume.

Os Estados Unidos ainda não estavam oficialmente em guerra no Vietnã. No entanto, durante vários anos, haviam canalizado dinheiro e armas para a região para ajudar os franceses a empreender uma guerra contra o Vietnã do Norte, o Estado revolucionário comunista liderado por Ho Chi Minh que estava lutando para reunificar o país e expulsar seus governantes coloniais.3 Naquele momento, quando a tripulação de Godel pulverizou as selvas, os Estados Unidos estavam aumentando seu apoio em dinheiro e armas. Milhares de "conselheiros" militares foram enviados ao Vietnã do Sul para apoiar o governo fantoche de Ngo Dinh Diem, na esperança de conter o que os estadunidenses viam como uma crescente onda global de comunismo.4

Não foi uma luta fácil nas sufocantes selvas da Indochina. A densa cobertura vegetal era um problema persistente. Mas isso era uma das maiores vantagens táticas dos rebeldes, permitindo que eles levassem pessoas e suprimentos através dos países vizinhos Laos e Camboja sem serem detectados, e lançassem ataques mortais em território sul-vietnamita. Com o Projeto Agile, Godel estava determinado a acabar com essa vantagem.

O Império Britânico foi pioneiro no uso de desfolhantes como uma forma de guerra química, usando-os contra movimentos locais que se opunham ao seu domínio colonial. Na luta contra os rebeldes comunistas na Malásia, a Grã-Bretanha empregou-os implacavelmente para destruir suprimentos de comida e a cobertura das florestas.5 Os planejadores militares britânicos descreveram os desfolhantes como "uma forma de sanção contra uma nação recalcitrante que seria mais rápida que o bloqueio e menos repugnante que a bomba atômica".

Godel seguiu o exemplo. Sob o Projeto Agile, químicos de um laboratório secreto do exército dos EUA em Fort Detrick, Maryland, testaram e isolaram potenciais produtos químicos desfolhantes que poderiam consumir a densa cobertura de uma floresta. Estes foram levados para Saigon e testados em campo. Eles funcionaram com eficiência brutal. As folhas caíram várias semanas depois de serem pulverizadas, desnudando a cobertura vegetal. Uma segunda aplicação aumentou a eficácia e matou permanentemente muitas árvores. Bombardear a área ou

incendiá-la com napalm também tornou a desfolhação mais ou menos permanente.6 Com o sucesso dos testes, Godel elaborou planos ambiciosos para cobrir metade do Vietnã do Sul com desfolhantes químicos.7 A ideia não era apenas destruir a cobertura de árvores, mas também destruir plantações de alimentos para assim submeter os vietnamitas do norte.8

O presidente do Vietnã do Sul, Diem, apoiou o plano. Em 30 de novembro de 1961, o presidente Kennedy autorizou-o. Graças a Godel e ao Projeto Agile, a Operação Ranch Hand foi lançada.

Ranch Hand começou em 1962 e durou até a guerra terminar mais de uma década depois. Naquela época, os aviões estadunidenses de transporte C-123 borrifaram uma área igual em tamanho à metade do Vietnã do Sul, com vinte milhões de galões de desfolhantes de produtos químicos tóxicos. O Agente Laranja foi fortificado com outras cores do arco-íris: Agente Branco, Agente Rosa, Agente Roxo, Agente Azul. Os produtos químicos, produzidos por empresas gringas como a Dow e a Monsanto, transformaram áreas inteiras de florestas exuberantes em paisagens áridas, causando a morte e o sofrimento horrível de centenas de milhares de pessoas.9

A Operação Ranch Hand foi impiedosa e claramente violou as Convenções de Genebra. Este continua sendo um dos episódios mais vergonhosos da Guerra do Vietnã. No entanto, o projeto de desfolhação é notável por mais do que apenas sua crueldade inimaginável. O órgão governamental liderado por ele era um órgão do Departamento de Defesa chamado Agência de Projetos de Pesquisa Avançada (*Advanced Research Projects Agency*, ARPA) – mais conhecido hoje pelo nome ligeiramente reformulado de Agência de Projetos de Pesquisa Avançada em Defesa (*Defense Research Projects Agency*, DARPA). Nascido em 1958 como um programa para proteger os Estados Unidos de uma ameaça nuclear soviética vinda do espaço, ela lançou várias iniciativas inovadoras encarregadas de desenvolver armas avançadas e tecnologias militares. Entre elas, o Projeto Agile e a Pesquisa de Comando e Controle, duas iniciativas sobrepostas da ARPA que criaram a Internet.

Os EUA têm um chilique

No final de 1957, os estadunidenses assistiram à União Soviética lançar o primeiro satélite artificial, o Sputnik 1. O satélite era minúsculo, mais ou menos do tamanho de uma bola de vôlei, mas foi colocado em órbita pegando carona em cima do primeiro míssil balístico intercontinental do mundo. Isso foi ao mesmo tempo uma demonstração e uma ameaça. Se a União Soviética podia colocar um satélite no espaço, poderia também mandar uma ogiva nuclear em qualquer ponto dos Estados Unidos.

O Sputnik caiu na política paranoica dos EUA como um meteoro gigante. Os políticos viram o evento como um sinal de fraqueza militar e tecnológica dos EUA, e as reportagens se concentraram na vitória soviética por ter chegado primeiro no espaço. Como poderiam os EUA ficar atrás dos comunistas em algo tão vital? Foi uma afronta ao senso de excepcionalismo dos gringos.10

O presidente Dwight Eisenhower foi atacado por dormir no volante. Generais e políticos criaram histórias horripilantes sobre a iminente conquista soviética da Terra e do espaço e pressionaram por mais gastos com defesa.11 Até mesmo o vice-presidente Richard Nixon criticou Eisenhower em público, dizendo a líderes empresariais que a lacuna de tecnologia entre os EUA e a União Soviética era grande demais para que eles esperassem um corte de impostos. O país precisava do dinheiro das empresas para recuperar o atraso.12

Enquanto o público se recuperava dessa grande derrota na chamada Corrida Espacial, o presidente Eisenhower sabia que tinha que fazer algo grandioso e muito público para salvar sua imagem e aliviar os medos das pessoas. Neil McElroy, seu recém-nomeado secretário de defesa, tinha um plano.

Imaculadamente arrumado e com o cabelo perfeitamente penteado e repartido ao meio, McElroy tinha a aparência e os modos de um alto executivo de publicidade. O que é, na verdade, o que ele era antes que Eisenhower o chamasse para dirigir o Departamento de Defesa. Em seu emprego anterior como presidente da Procter and Gamble, a assinatura inovadora de McElroy era financiar “novelas” – dramas teatrais

diurnos feitos sob medida para as donas de casa – como veículos de puro marketing para vender a seleção de sabonetes e detergentes domésticos de sua empresa. Como a revista Time, que colocou McElroy na capa de sua edição de outubro de 1953, disse: “As novelas mandam mais mensagens publicitárias para o consumidor – e vendem mais sabão – simplesmente porque a dona de casa pode absorver as mensagens por horas a fio enquanto ela cuida de suas tarefas domésticas.”13

Nas semanas seguintes ao lançamento soviético do Sputnik, McElroy criou o projeto perfeito de relações públicas para salvar o dia. Ele requisitou a criação da Agência de Projetos de Pesquisa Avançada – ARPA – um novo corpo militar independente cujo objetivo era preencher a brecha espacial e garantir que uma derrota tecnológica embaraçosa como a do Sputnik nunca mais ocorresse.14 McElroy era um empresário que acreditava no poder dos negócios para resolver as coisas.15 Em novembro de 1957, ele apresentou a ARPA ao Congresso como uma organização que cortaria a burocracia governamental e criaria um veículo público-privado de pura ciência militar para impulsionar as fronteiras da tecnologia militar e desenvolver “vastos sistemas de armas do futuro”.16

A ideia por trás da ARPA era simples. Seria uma firma liderada por civis alojada dentro do Pentágono. Seria enxuta, com uma pequena equipe e um grande orçamento. Embora não construísse nem manejasse seus próprios laboratórios e instalações de pesquisa, funcionaria como um centro de gerenciamento executivo que descobriria o que precisava ser feito e então levaria o trabalho para universidades, institutos de pesquisa privados e terceirizadas militares.17

O plano atraiu a atenção do presidente Eisenhower, que desconfiava da disputa cínica pelo financiamento e poder de vários braços do exército – que ele acreditava ter inchado o orçamento e queimado dinheiro em projetos inúteis. A ideia de terceirizar pesquisa e desenvolvimento para o setor privado também atraía a comunidade empresarial.18 Os militares, por outro lado, não ficaram tão satisfeitos. A Força Aérea, a Marinha, o Exército e o Estado-Maior das Forças Armadas recuaram diante da ideia de que os civis estivessem sentados em cima deles e dizendo-lhes o que fazer. Eles temiam perder o controle sobre a aquisição de tecnologia, que era uma área de lucro e poder.

Os militares resistiram contra o plano de McElroy. O conflito entre eles foi tão grande que fez uma breve aparição no discurso anual de 1958 de Eisenhower: “Não estou tentando hoje fazer julgamentos sobre rivalidades daninhas entre serviços. Mas uma coisa é certa. Não importa quais sejam, os Estados Unidos quer que parem.”19 E ele conseguiu o que queria. Em 11 de fevereiro de 1958, um mês depois do discurso anual e apenas cinco meses após o lançamento do Sputnik, o Congresso escreveu a ARPA em um projeto de lei da Força Aérea dos Estados Unidos, concedendo US $ 520 milhões em financiamento inicial e um plano para um gigantesco orçamento de US $ 2 bilhões.20

McElroy escolheu Roy Johnson, executivo da General Electric, para dirigir a nova agência. Um relatório interno do Pentágono descreveu-o como um “indivíduo extremamente confiante, calmo e surpreendentemente bonito, que parecia em cada centímetro como um magnata da capa da revista Fortune”. Também observou que sua única preocupação em assumir o cargo era potencialmente perder uma lucrativa lacuna fiscal: “Johnson também era uma pessoa muito rica, deixando um emprego de US $ 158 mil para aceitar um cargo de US $ 18 mil na ARPA. Por razões fiscais, ele assumiu o cargo na ARPA com a condição de que pudesse estar fisicamente presente em Connecticut por um número mínimo de dias. Isso significava que ele geralmente saía de Washington na sexta-feira e retornava segunda ou terça. Frequentemente usava um avião particular. Proteger os EUA contra a União Soviética era importante. Mas uma pessoa teve que se importar com seu imposto de renda.21

Nos primeiros anos de existência, a ARPA assumiu diversos projetos importantes. Tinha uma divisão espacial desenvolvendo mísseis balísticos. Trabalhou em satélites de espionagem e meteorologia, bem como em sistemas de localização por satélite, e preparou-se desde cedo para colocar um ser humano no espaço. Também ajudou a executar testes nucleares como a Operação Argus, que envolveu a detonação de várias pequenas bombas nucleares nas camadas superiores da atmosfera acima do Atlântico Sul em uma tentativa radical de criar um escudo invisível de partículas eletricamente carregadas que fritaria os componentes eletrônicos de qualquer ogiva nuclear que voasse através dele.22

Com todos esses projetos, parecia que a ARPA estava tendo um começo glorioso, mas a excitação não durou. As disputas internas no Pentágono e a criação de uma NASA desmilitarizada – a Administração Nacional de Aeronáutica e Espaço – sugaram dinheiro e prestígio da agência. Menos de um ano depois de ter sido criada, o orçamento da ARPA foi reduzido a apenas US $ 150 milhões – uma bagatela comparado ao orçamento de US $ 2 bilhões prometido.23 Nos anos seguintes, mudou três vezes de diretor e lutou para permanecer viva. Todos estavam convencidos de que a ARPA estava a caminho do túmulo.

No entanto, uma pessoa tinha um plano para salvá-la: William Godel.

Guerras do Futuro

Com um metro e sessenta e cinco de altura, olhos amendoados, cabelo muito curto e uma maneira intelectual e suave, William Godel tinha os modos de um acadêmico bem-vestido ou talvez de um diplomata recém-contratado. Ele nasceu em Boulder, Colorado e em 1921, formou-se em Georgetown e conseguiu um emprego na área de inteligência militar no Departamento de Guerra dos EUA. Após o ataque do Japão a Pearl Harbor, foi convocado para o Corpo de Fuzileiros Navais como um oficial e participou de combates no Pacífico Sul, onde levou uma bala na perna, lesão que o deixou permanentemente aleijado. Depois da guerra, ele subiu nas fileiras da inteligência militar, elevando-se ao nível de GS-18 – a maior faixa salarial para funcionários do governo – antes de seu trigésimo aniversário.24

Com o passar dos anos, a carreira de Godel teve uma série de viradas bruscas e muitas vezes bizarras. Esteve no Gabinete do Secretário de Defesa, onde trabalhou em contato com a CIA, a NSA e o exército e ficou conhecido como especialista em guerra psicológica.25 Ele negociou com a Coreia do Norte para resgatar soldados americanos feitos prisioneiros durante a Guerra da Coréia26, ajudou a treinar e coordenar os antigos espiões nazistas da CIA na Alemanha Ocidental27 e participou de uma missão secreta para mapear a Antártida. (Por esse tra-

balho, nomearam dois glaciares com o seu nome: a Baía de Godel e o Iceport de Godel.) Durante parte de sua célebre carreira na inteligência militar foi assistente do general Graves Erskine, um velho general aposentado do Corpo de Fuzileiros Navais com uma longa história de operações de contrainsurgência. Erskine liderou o Escritório de Operações Especiais do Pentágono, que lidava com guerra psicológica, coleta de informações e operações de acesso clandestino (*black bag ops*).28

Em 1950, Godel se juntou ao general Erskine em uma missão secreta no Vietnã. O objetivo era avaliar a eficácia das táticas militares que os franceses estavam usando para pacificar uma crescente insurgência anticolonial e determinar que tipo de apoio os Estados Unidos deveriam fornecer. A viagem começou mal quando sua equipe escapou por pouco de uma tentativa de assassinato: três bombas explodiram no saguão de seu hotel em Saigon. Foi uma bela cerimônia de boas-vindas – e ninguém sabia se as bombas haviam sido colocadas pelos norte-vietnamitas ou por seus anfitriões franceses para servir como uma espécie de advertência de que deveriam cuidar de seus próprios negócios. O que quer que fosse, a festa seguia em frente. Eles se incorporaram às tropas coloniais francesas e percorreram suas bases. Em uma excursão, a equipe de Erskine acompanhou uma unidade vietnamita treinada na França em uma emboscada noturna. Seu objetivo era capturar alguns rebeldes para interrogatório e coleta de informações, mas a missão de inteligência rapidamente se transformou em uma invasão furiosa e assassina. Os soldados vietnamitas apoiados pelos franceses decapitaram seus prisioneiros antes que os rebeldes pudessem ser interrogados.29

Lá, nas selvas sufocantes, Godel e sua equipe entenderam que os franceses estavam fazendo tudo errado. A maior parte dos esforços militares franceses parecia se concentrar em proteger suas linhas de comboio de suprimentos, que eram constantemente atacadas por forças de guerrilha enormes que pareciam se materializar da própria selva. Para tanto, eles posicionaram em torno de seis mil homens ao longo de um trecho de três quilômetros de estrada. Os franceses estavam essencialmente encalhados em suas fortificações. Eles haviam “perdido a maior parte do seu espírito ofensivo” e estavam “presos em suas áreas ocupadas”, descreveu um colega de Godel.

“Do jeito que Godel viu, os colonialistas franceses estavam tentando combater os guerrilheiros do Viet Minh segundo as regras coloniais de guerra. Mas os vietnamitas do sul, que estavam recebendo armas e treinamento das forças francesas, estavam na verdade lutando um tipo diferente de guerra, baseado em regras diferentes”, escreve Annie Jacobsen, que escava a história esquecida de William Godel em The Pentagon's Brain, sua história da ARPA.30

Esse “tipo diferente de guerra” tinha um nome: contrainsurgência.

Godel compreendeu que os Estados Unidos estavam em rota de colisão deliberada com insurgências em todo o mundo: Sudeste Asiático, Oriente Médio e América Latina. E ele apoiou essa colisão. Godel também começou a entender que as táticas e estratégias exigidas nessas novas guerras não eram as mesmas da Segunda Guerra Mundial. Os Estados Unidos, ele percebeu, teriam que aprender com os erros da França. Teriam que lutar um tipo diferente de guerra, uma guerra menor, uma guerra secreta, uma guerra psicológica e uma guerra de alta tecnologia – uma "guerra que não tem armas nucleares, não tem a planície do norte da Alemanha e não necessariamente tem estadunidenses”, explicou Godel mais tarde.31

De volta aos Estados Unidos, ele esboçou como seria essa nova guerra.

A teoria da contrainsurgência não era particularmente nova. No início do século XX, os Estados Unidos haviam conduzido operações brutais de contrainsurgência nas Filipinas e na América do Sul. E a CIA estava no meio de uma violenta campanha de contrainsurgência secreta no Vietnã do Norte e no Laos – encabeçada pelo futuro chefe de Godel, o coronel da Força Aérea Edward Lansdale – que incluía incursões, esquadrões da morte, propaganda e tortura.32 O que tornou a visão de contrainsurgência de Godel diferente foi seu foco no uso da tecnologia para aumentar a eficácia. Claro, a contrainsurgência envolveu terror e intimidação. Tinha coerção e propaganda. Mas o que era igualmente importante era treinar e equipar combatentes – não importando se fossem equipes de operações especiais dos EUA ou forças locais – com a mais avançada tecnologia militar disponível: melhores armas, melhores uniformes, melhor

transporte, melhor inteligência e melhor entendimento de onde vinha a incrível força da resistência local. “Do jeito que Godel viu, o Pentágono precisava desenvolver armamento avançado, baseado em tecnologia que não fosse apenas tecnologia nuclear, mas que pudesse lidar com essa ameaça que estava por vir”, escreve Jacobsen.33

Godel fez proselitismo com essa nova visão nos Estados Unidos, dando palestras e falando sobre suas teorias de contrainsurgência em instituições militares de todo o país. Enquanto isso, a recém-criada ARPA o convocou para dirigir seu vagamente denominado Escritório de Desenvolvimentos Estrangeiros, a partir do qual ele administraria as operações secretas da agência. O trabalho era obscuro, altamente sigiloso e extremamente fluido. Godel supervisionaria os projetos ultrassecretos de mísseis e satélites da agência em um momento, e bolaria planos de ataques nucleares numa dada região em nome da Agência Nacional de Segurança no outro. Um desses planos envolveu a detonação de uma bomba nuclear em uma pequena ilha no Oceano Índico a mando da ARPA. A ideia era criar uma cratera perfeitamente parabólica onde pudesse caber uma antena gigante que a NSA queria construir para captar sinais de rádio soviéticos que se espalhavam pelo espaço e ricocheteavam de volta pela lua. “A ARPA garantiu uma radioatividade residual mínima e a forma adequada da cratera na qual a antena seria posteriormente colocada”, disse um funcionário da NSA. “Nunca acreditamos nessa possibilidade. A moratória nuclear entre os EUA e a URSS foi assinada um pouco mais tarde e esse plano desapareceu”.34

Quando Godel não estava planejando explodir pequenas ilhas tropicais, ele estava perseguindo sua principal paixão: contrainsurgência de alta tecnologia. Como Jacobsen relata no seu livro *Pentagon's Brain*: “Godel estava agora em posição de criar e implementar os próprios programas que ele vinha dizendo ao público das faculdades de guerra em todo o país que precisavam ser criados. Através da inserção de uma presença militar dos EUA em terras estrangeiras ameaçadas pelo comunismo – através de ciência e tecnologia avançadas -, a democracia triunfaria e o comunismo fracassaria. Essa busca rapidamente se tornaria a obsessão de Godel.”35

Enquanto isso, em seu trabalho para a ARPA, ele viajou para o Sudeste Asiático para avaliar a crescente insurgência do Viet Minh e

reservou uma viagem à Austrália para falar sobre contrainsurgência e explorar um potencial local de lançamento de satélites polares.36 Durante todo esse tempo, ele insistiu em sua linha principal: os Estados Unidos precisavam estabelecer uma agência de contrainsurgência para enfrentar a ameaça comunista. Em uma série de memorandos ao subsecretário de defesa, Godel argumentou: “Organizações militares convencionalmente treinadas, convencionalmente organizadas e convencionalmente equipadas são incapazes de funcionar em operações anti-guerrilha”. Apesar da esmagadora superioridade de tamanho do exército sul-vietnamita, ele não conseguira conter uma insurreição armada muito menor, ressaltou. Ele pressionou pela permissão de que a ARPA montasse um centro de pesquisa de contrainsurgência no campo – primeiro para estudar e compreender cientificamente as necessidades das forças anti-insurgência locais e depois usar as descobertas para treinar paramilitares locais. “Essas forças devem ser formadas não com pessoal com armas e equipamentos convencionais que exigem manutenção de terceiro e quarto nível, mas com pessoas capazes de serem agricultores ou taxistas durante o dia e forças anti-guerrilha à noite”, escreveu ele.37

A visão de Godel esbarrou de frente com o pensamento dominante do Exército dos EUA na época, e suas propostas não geraram muito entusiasmo com o pessoal do presidente Eisenhower. Mas, de qualquer maneira, eles estavam saindo do governo e ele acabou encontrando uma plateia ansiosa na administração que chegava.

Grampeando o Campo de Batalha

John F. Kennedy foi empossado como o trigésimo presidente dos Estados Unidos em 20 de janeiro de 1961. Jovem e arrojado, o ex-senador de Massachusetts era progressista em política interna e era um falcão da Guerra Fria comprometido com a política externa. Sua eleição deu início a uma safra de jovens tecnocratas de elite que realmente acreditavam no poder da ciência e da tecnologia para resolver os problemas do mundo. E havia muitos problemas a serem resolvidos. Não era apenas a União Soviética. Kennedy enfrentou insurgências regionais contra

governos aliados dos EUA em todo o mundo: Cuba, Argélia, Vietnã e Laos, Nicarágua, Guatemala e Líbano. Muitos desses conflitos surgiram de movimentos locais, recrutaram combatentes locais e foram apoiados por populações locais. Contê-los não era algo que uma grande operação militar tradicional ou um ataque nuclear tático poderia resolver.

Dois meses depois de assumir o cargo, o presidente Kennedy enviou uma mensagem ao Congresso defendendo a necessidade de expandir e modernizar a postura militar dos EUA para enfrentar essa nova ameaça. “A segurança do Mundo Livre pode ser ameaçada não apenas por um ataque nuclear, mas também por ser lentamente corroída na periferia, independentemente de nosso poder estratégico, por forças de subversão, infiltração, intimidação, agressão indireta ou não-aberta, revolução interna, chantagem diplomática, guerra de guerrilha ou uma série de pequenas guerras”, disse ele, argumentando energicamente por novos métodos de lidar com insurgências e rebeliões locais. “Precisamos de uma maior habilidade para lidar com as forças de guerrilha, insurreições e subversão. Grande parte do nosso esforço passado para criar forças de guerrilha e anti-guerrilha foi dirigida à guerra geral. Devemos estar prontos agora para lidar com qualquer tamanho de força, incluindo pequenos grupos de homens apoiados externamente; e devemos ajudar a treinar as forças locais para serem igualmente eficazes”.38

O presidente queria uma maneira melhor de combater o comunismo – e a ARPA parecia o veículo perfeito para levar a cabo sua visão.

Pouco depois do discurso, conselheiros da CIA, do Pentágono e do Departamento de Estado elaboraram um plano de ação para um enorme programa de iniciativas secretas de guerra militar, econômica e psicológica para lidar com o que Kennedy via como o maior de todos os problemas: a crescente insurreição no Vietnã e no Laos. O plano incluía a obsessão pessoal de William Godel: o Projeto Agile, um programa de pesquisa e desenvolvimento de contrainsurgência de alta tecnologia.39 Em uma reunião do Conselho de Segurança Nacional em 29 de abril de 1961, o presidente Kennedy assinou no seguinte documento: “Temos que ajudar o GVN [Governo do Vietnã] a estabelecer um Centro de Desenvolvimento e Testes de Combate no Vietnã do Sul para desenvolver, com a ajuda de tecnologia moderna, novas técnicas para uso contra as forças vietcongues.”40

Com essas poucas linhas, nasceu o Projeto Agile da ARPA. Agile foi incorporado em um programa militar e diplomático muito maior iniciado pelo presidente Kennedy e destinado a auxiliar o governo do Vietnã do Sul contra uma crescente ofensiva rebelde. O programa rapidamente se transformaria em uma campanha militar total e, ao fim, desastrosa. Mas para a ARPA, foi uma nova vida. Esse impulso tornou a agência relevante novamente e colocou-a no centro dos acontecimentos.

Godel operou o Agile sem nenhum impedimento e reportava a Edward Lansdale, um oficial aposentado da força aérea que dirigia as operações secretas de contrainsurgência da CIA no Vietnã.41 Devido à necessidade de sigilo – os Estados Unidos não estavam oficialmente envolvidos militarmente no Vietnã -, uma névoa espessa pairava sobre o projeto. “Reportando-se diretamente a Lansdale, ele conduziu um trabalho tão secreto que até os diretores da ARPA, sem falar nos baixos funcionários, desconheciam os detalhes específicos”, escreve Sharon Weinberger em *The Imagineers of War*, sua história da ARPA.42

O foco inicial era o Centro de Testes e Desenvolvimento de Combate, um projeto ultrassecreto da ARPA, composto por um conjunto de edifícios às margens do rio Saigon que Godel ajudou a estabelecer no verão de 1961. O programa começou com um único local e uma missão relativamente direta: desenvolver armas e adaptar dispositivos de campo de batalha de contrainsurgência para uso nas selvas densas e sufocantes do Sudeste Asiático.43 Mas, à medida que a presença militar dos EUA aumentava no Vietnã e, finalmente, se transformava em uma guerra intensa, o projeto cresceu em escopo e ambição.44 Ele acabou abrindo vários outros grandes complexos de pesquisa e desenvolvimento na Tailândia, bem como postos avançados menores no Líbano e no Panamá. A agência não apenas desenvolveu e testou novas tecnologias de armas, mas também formulou estratégias, treinou forças locais e participou de ataques de contrainsurgência e missões de operações psicológicas.45 Cada vez mais, assumiu um papel que caberia muito bem à CIA. Ela também se tornou global, visando revoltas e movimentos políticos de esquerda ou socialistas onde quer que estivessem – incluindo dentro dos Estados Unidos.

A agência testou armas leves de combate para os militares sul-vietnamitas, o que os levou à adoção das AR-15 e M-16 como fuzis

padrão. Ajudou a desenvolver uma aeronave de vigilância leve que planava silenciosamente sobre a floresta. Formulou rações de campo e alimentos adequados ao clima quente e úmido. Financiou a criação de sofisticados sistemas de vigilância eletrônica e financiou esforços elaborados para coletar todo tipo de inteligência relacionada a conflitos. Trabalhou na melhoria da tecnologia de comunicação militar para que funcionasse em florestas densas. Desenvolveu instalações portáteis de radar que poderiam ser colocadas em um balão, uma tecnologia que foi rapidamente implantada comercialmente nos Estados Unidos para monitorar as fronteiras contra travessias ilegais.46 Também projetou veículos que pudessem atravessar melhor um terreno pantanoso, um protótipo de "elefante mecânico" similar aos robôs de quatro patas que a DARPA e a Google desenvolveram meio século depois.47

A ARPA frequentemente ultrapassava as fronteiras do que era considerado tecnologicamente possível e era pioneira em sistemas de vigilância eletrônica que estavam décadas à frente de seu tempo. Ela desempenhou um papel importante em algumas das iniciativas mais ambiciosas da época. Isso incluiu o Projeto Igloo White, uma barreira computadorizada de vigilância que custava bilhões de dólares.48 Operado a partir de uma base secreta da força aérea na Tailândia, o Igloo White envolveu a implantação de milhares de sensores sísmicos controlados por rádio, microfones e detectores de calor e urina na selva. Esses dispositivos de espionagem, em forma de bastões ou plantas e geralmente lançados por aviões, transmitiam sinais para um centro de controle centralizado de computadores, para alertar os técnicos de qualquer movimento na selva.49 Se alguma coisa se movia, um ataque aéreo era acionado e a área coberta com bombas e napalm. O Igloo White era como um gigantesco sistema de alarme sem fio que abrangia centenas de quilômetros de selva. Como a Força Aérea dos EUA explicou: "Estamos, na verdade, grampeando o campo de batalha."50

John T. Halliday, piloto aposentado da Força Aérea, descreveu o centro de operações Igloo White na Tailândia em seu livro de memórias. "Sabe aquelas enormes painéis eletrônicos do filme Dr. Strangelove que mostravam os bombardeiros russos indo para os EUA e os nossos indo contra eles?" escreveu. "Bom, a Força-Tarefa Alpha é muito parecida, exceto pelos monitores coloridos de três andares de altura atualizados

em tempo real – é toda a maldita trilha de Ho Chi Minh, ao vivo e a cores."51

Halliday fazia parte de uma equipe que fazia bombardeios noturnos sobre trilha de Ho Chi Minh, visando comboios de suprimentos com base em informações fornecidas por essa cerca eletrônica. Ele e sua unidade ficaram impressionados com a natureza futurista de tudo aquilo:

> Ao sair da selva e entrar no prédio, você volta para os EUA – mas os EUA quinze anos à frente... talvez 1984. É lindo... um piso de cerâmica reluzente... paredes de vidro por toda parte. Eles têm uma cafeteria completa onde você pode conseguir o que quiser. Eles até têm leite de verdade, não aquela porcaria em pó que pegamos no refeitório. E ar-condicionado? Todo o maldito lugar é climatizado. Tem até uma pista de boliche e um cinema. Era eu e um monte de civis que se pareciam com caras da IBM, correndo de terno e gravata, todos usando óculos... era a "Central dos Nerds". Nós nunca víamos eles em nossa parte da base, então acho que tinham tudo que precisavam lá mesmo.
>
> Aí, tem essa sala de controle principal que se parece com a que vimos na TV durante as cenas da lua da missão Apollo, ou talvez algo saído de um filme do James Bond. Há terminais de computador em todos os lugares. Mas a principal característica é essa enorme tela de três andares representando em cores toda a trilha de Ho Chi Minh com uma representação em tempo real de caminhões descendo a estrada. Era muito foda, cara.52

Igloo White durou cinco anos com um custo total de cerca de US $ 5 bilhões – cerca de US $ 30 bilhões hoje. Embora amplamente elogiado na época, o projeto foi julgado como uma falha operacional. "Os guerrilheiros simplesmente aprenderam a confundir os sensores gringos com ruídos de caminhões gravados em fita, sacos de urina e outros engodos, provocando a liberação de toneladas e mais toneladas de bombas em sendas vazias da selva que eles depois percorriam livremente", diz o historiador. Paul N. Edwards.53 Apesar do fracasso, a tecnologia de "cerca eletrônica" do Igloo White foi implantada alguns anos mais tarde ao longo da fronteira estadunidense com o México.54

O Projeto Agile fez um enorme sucesso com governo sul-vietnamita. O Presidente Diem fez várias visitas ao centro de pesquisa da

ARPA em Saigon e se encontrou pessoalmente com Godel e o restante da equipe da ARPA.55 O presidente tinha apenas uma exigência: o envolvimento gringo deve permanecer secreto. E Godel pensava o mesmo. Lá nos EUA, para justificar a necessidade de uma nova abordagem de contrainsurgência, ele frequentemente repetia o que o presidente Diem lhe disse: “A única forma de perdemos é se os estadunidenses entrarem aqui”.

Conheça o seu inimigo

Para William Godel, a contrainsurgência de alta tecnologia era mais do que apenas desenvolver métodos modernos de matar. Tratava-se também de vigiar, estudar e compreender as pessoas e culturas em que a insurreição estava ocorrendo. Tudo era parte de sua visão para o futuro da guerra: usar a ciência avançada gringa para derrotar as superiores disciplina, motivação e o apoio dos insurgentes locais. A ideia era entender o que os fazia resistir e lutar, e o que seria necessário para fazê-los mudar de ideia.56 O objetivo final era encontrar uma maneira de prever as insurgências locais e detê-las antes que tivessem tempo de amadurecer. O problema no sudeste da Ásia era que os estadunidenses estavam operando em ambientes e culturas que eles não compreendiam. Então, como garantir que os militares estivessem tomando as decisões certas?

No início dos anos 1960, os círculos de defesa e política externa dos EUA receberam uma enxurrada de seminários, reuniões, relatórios e cursos que tentavam estabelecer políticas e doutrinas adequadas de contrainsurgência. Em um influente seminário para múltiplas agências organizado pelo exército dos EUA e com a participação de colegas da ARPA de Godel, um pesquisador militar descreveu a dificuldade de combater contrainsurgências de maneira direta: “O problema é que temos operar em um ambiente cultural estranho e influenciar pessoas com diferentes valores culturais, costumes, crenças e atitudes”. Ele concluiu com uma declaração dura: “A mesma bala matará com a mesma eficácia, seja contra um alvo nos Estados Unidos, na África ou na Ásia. No entanto, a eficácia da arma de contrainsurgência depende de um alvo específico.”57

O Pentágono começou a gastar muito dinheiro com cientistas sociais e comportamentais, contratando-os para garantir que a "arma de contrainsurgência" dos EUA sempre atingisse seu alvo, independentemente da cultura em que estava sendo usada. Sob a direção de William Godel, a ARPA tornou-se um dos principais canais para esses programas, ajudando a transformar a antropologia, a psicologia e a sociologia em armas e colocando-as a serviço da contrainsurgência gringa. A ARPA distribuiu milhões de dólares para estudos sobre camponeses vietnamitas, combatentes norte-vietnamitas capturados e tribos rebeldes das montanhas do norte da Tailândia. Enxames de terceirizados da ARPA – antropólogos, cientistas políticos, linguistas e sociólogos – passaram por aldeias pobres, colocando as pessoas sob um microscópio, medindo, coletando dados, entrevistando, estudando, avaliando e fazendo reportagens.58 A ideia era entender o inimigo, conhecer suas esperanças, seus medos, seus sonhos, suas redes sociais e suas relações com o poder.59

A RAND Corporation, através de um contrato da ARPA, fez a maior parte desse trabalho. Localizada em um prédio com vista para as longas praias de Santa Monica, a RAND era uma poderosa terceirizada militar e de inteligência que havia sido criada pela Força Aérea dos Estados Unidos várias décadas antes como uma agência de pesquisa público-privada.60 Na década de 1950, a RAND era fundamental para a formulação da política nuclear beligerante dos EUA. Na década de 1960, montou uma grande divisão de contrainsurgência e tornou-se uma extensão privatizada de fato do Projeto Agile da ARPA. A ARPA dava as ordens; A RAND contratava as pessoas e fazia o trabalho.

Com grande empenho, os cientistas da RAND estudaram a eficácia da iniciativa Estratégia Hamlet, um esforço de pacificação desenvolvido e impulsionado por Godel e pelo Projeto Agile e que envolveu o reassentamento forçado de camponeses sul-vietnamitas de suas aldeias tradicionais em novas áreas que foram cercadas e tornadas "seguras" contra a infiltração rebelde.61 Em outro estudo encomendado pela ARPA, os contratados da RAND foram encarregados de responder às perguntas que incomodavam os estadunidenses: por que os combatentes norte-vietnamitas não desertaram para o nosso lado? O que a causa deles tinha de mais? Os comunistas não eram brutais com o seu próprio povo? Por que eles não querem viver como nós, na gringolândia? Por que a moral deles era tão alta? E o que poderia ser feito para minar sua

confiança?62 Eles conduziram 2400 entrevistas com prisioneiros e desertores norte-vietnamitas e geraram dezenas de milhares de páginas de inteligência em busca desse objetivo.63

Ao mesmo tempo, a ARPA financiou vários projetos destinados a estudar as populações locais para identificar os fatores sociais e culturais que poderiam ser usados para prever por que e quando as tribos se tornariam insurgentes. Uma iniciativa, contratada pela RAND, enviou uma equipe de cientistas e antropólogos políticos das universidades UCLA e UC Berkeley à Tailândia para mapear "os sistemas religiosos, sistemas de valores, dinâmicas de grupo, relações civis-militares" de tribos de montanhas tailandesas, dando destaque para comportamento preditivo.64 "O objetivo desta tarefa é determinar as fontes mais prováveis de conflito social no nordeste da Tailândia, concentrando-se nos problemas e atitudes locais que poderiam ser explorados pelos comunistas", diz o relatório.65 Outro estudo na Tailândia, realizado para a ARPA pelos Institutos Estadunidenses para Pesquisa (*American Institutes for Research*, AIR), ligados à CIA, teve como objetivo aferir a eficácia das técnicas de contrainsurgência aplicadas contra tribos rebeldes de montanhas – práticas como assassinar líderes tribais, realocar aldeias e usar fome artificialmente induzida para pacificar populações rebeldes.66

Uma investigação de 1970 para a revista Ramparts detalhou os efeitos desses métodos brutais de contrainsurgência ao estilo de campo de concentração sobre uma pequena tribo rebelde de montanha, conhecida como Meo. "As condições nas aldeias de reassentamento de Meo são severas, lembrando fortemente as reservas indígenas estadunidenses do século XIX. As pessoas não têm arroz e água suficientes e os agentes locais corruptos embolsam os fundos destinados a Meo em Bangueco-que." A revista citou um relatório de uma testemunha ocular: "Dificuldades físicas e tensão psicológica causaram um grande impacto nessas pessoas. Elas estão magras e doentes; muitas estão em um estado permanente de semi-abstinência estimulado pela falta de ópio para alimentar hábitos de longa data. No entanto, a decadência do espírito dos meos é ainda mais angustiante do que a deterioração de seus corpos. Eles perderam toda a aparência de força interior e independência: parecem ter murchado, ao mesmo tempo que assumem as maneiras dos humildes".67

Uma dimensão ainda mais perturbadora do trabalho de pacificação dos AIR na Tailândia era que ele deveria servir como um modelo para operações de contrainsurgência em outras partes do mundo – inclusive contra negros que moravam nas cidades estadunidenses, onde tumultos raciais estavam ocorrendo na época. “A potencial aplicabilidade dessas descobertas dentro dos Estados Unidos também receberá atenção especial. Em muitos de nossos principais programas nacionais, especialmente aqueles direcionados a subculturas desfavorecidas, os problemas metodológicos são semelhantes aos descritos nesta proposta”, diz o texto do projeto. “A aplicação das descobertas tailandesas em território nacional constitui talvez a contribuição mais significativa do projeto.”68

E foi justamente o que aconteceu. Depois da guerra, pesquisadores, incluindo um jovem chamado Charles Murray (autor da Curva de Sino), que havia trabalhado em programas de contrainsurgência para a ARPA no Sudeste Asiático, retornaram aos Estados Unidos e começaram a aplicar as ideias de pacificação que desenvolveram na selva em questões domésticas espinhosas relacionadas a classe, raça e desigualdade econômica. Os efeitos foram tão desastrosos em casa quanto no exterior, dando um verniz científico moderno às políticas públicas que reforçavam o racismo e a pobreza estrutural.70

Como a proposta dos AIR não tão sutilmente havia sugerido, os programas de ciência comportamental da ARPA no Sudeste Asiático andaram de mãos dadas com uma política de contrainsurgência mais sangrenta e tradicional: programas secretos de assassinato, terror e tortura que coletivamente passaram a ser conhecidos como o Programa Fênix.

Um dos faróis desse lado obscuro da contrainsurgência foi Edward Lansdale, ex-executivo da Levi Strauss e Cia, que aprendeu o ofício lutando contra a insurgência comunista nas Filipinas após a Segunda Guerra Mundial.71 A estratégia de guerra psicológica de Lansdale era usar mitos e crenças locais para induzir o terror e mexer com os medos mais profundos de seus alvos. Um truque célebre foi o uso de uma crença filipina na existência de vampiros para assustar os guerrilheiros comunistas. “Uma das táticas contraterroristas de guerra psicológica de Lansdale foi pendurar um guerrilheiro comunista capturado de

uma árvore, esfaqueá-lo no pescoço com um estilete e drenar seu sangue", explicou Douglas Valentine, um jornalista que expôs o Programa Fênix. "Os comunistas aterrorizados fugiram da área e os moradores muito assustados, que acreditavam em vampiros, imploraram ao governo por proteção."72 Lansdale, que se tornaria chefe de Godel, replicou a estratégia filipina no Vietnã: assassinatos, esquadrões da morte, tortura e a destruição de aldeias inteiras. Tudo foi feito para "desincentivar" os camponeses a ajudar os rebeldes vietnamitas do norte. Em algum lugar entre quarenta e oitenta mil vietnamitas foram mortos nos assassinatos seletivos do Programa Fênix; a CIA estima que o número esteja em torno de vinte mil.

No final da década de 1960, a Guerra do Vietnã se transformou em um moedor de carne. Em 1967, 11.363 soldados estadunidenses perderam suas vidas. Um ano depois, esse número subiu para quase 17.000. Em 1970, os soldados estadunidenses não queriam mais lutar. Houve caos no campo de batalha e insubordinação nas bases. Havia centenas de casos de "*fragging*", oficiais superiores mortos pelos seus próprios soldados. O uso de drogas era desenfreado. Os soldados estavam acabados – bêbados e chapados de maconha e ópio. O Projeto Agile da ARPA não estava imune a essa transformação, mas conectado a ela. De fato, de acordo com um ex-chefe da ARPA, William Godel esteve pessoalmente envolvido com as missões "Air America" para fornecer meios para a guerra secreta da CIA no Laos, uma operação que, segundo relatos confiáveis, envolvia o contrabando de heroína para financiar milícias anticomunistas.74

Como Saigon se transformou em um campo militar cheio de bebida, heroína, prostituição e adrenalina sem sentido, o centro de pesquisa da ARPA se tornou uma junção bizarra de antropólogos entediantes, espiões, generais, oficiais sul-vietnamitas e soldados sociopatas cruzando o centro de pesquisas indo a caminho de missões terroristas no meio do território controlado pelo inimigo. Uma antiga vila colonial francesa na cidade que abrigava os cientistas da RAND se tornou um centro social para essa cena estranha: de dia um centro de comando em funcionamento, à noite um local para festas e bebedeiras.75

Uma estranha pseudociência surgiu. Combinando economia de livre mercado e teoria da escolha racional, planejadores militares e cien-

tistas viam os vietnamitas como autômatos, nada mais que indivíduos racionais que agiam puramente por interesse próprio. Eles não tinham valores ou ideais orientadores – nenhum patriotismo, nenhuma lealdade a suas comunidades ou tradições ou algum ideal político maior. Eles não estavam interessados em nada além de maximizar resultados positivos para si mesmos. O truque seria afastar os vietnamitas da insurgência através de uma mistura de marketing, incentivos consumistas e um pouco de amor bruto quando nada mais funcionasse. Esmolas em dinheiro, empregos, pequenas melhorias de infraestrutura, esquemas de privatização da terra, propaganda anticomunista, destruição de colheitas, mutilações, massacres, assassinatos – todas essas eram variáveis legítimas para se lançar na equação da coerção.76

Algumas pessoas começaram a duvidar da missão dos EUA no Vietnã e questionaram o propósito da abordagem científica da ARPA à contrainsurgência. Anthony Russo, um contratado da RAND que trabalhou em projetos da ARPA e que mais tarde ajudaria Daniel Ellsberg a vazar os Documentos do Pentágono, descobriu que quando os resultados dos estudos da ARPA contradiziam os desejos militares, seus chefes simplesmente os suprimiam e descartavam.77

"Quanto mais eu admirava a cultura asiática – especialmente a vietnamita", escreveu Russo em 1972, "mais indignado ficava com o horror orwelliano da máquina militar gringa que estraçalhava o Vietnã e destruía tudo em seu caminho. Dezenas de milhares de meninas vietnamitas foram transformadas em prostitutas; ruas que tinham sido ornamentadas com belas árvores foram desnudadas para dar lugar aos grandes caminhões militares. Eu estava farto do horror e enojado pela petulância e mesquinhez com que a RAND Corporation conduziu seus negócios."78

Ele acreditava que todo o aparato do Projeto Agile da ARPA era uma gigantesca falcatrua usada por planejadores militares para dar cara científica a qualquer política de guerra que eles pretendessem conduzir. Esta não era uma ciência militar de ponta, mas um elefante branco e uma fraude. As únicas pessoas beneficiadas pelo Projeto Agile eram as empresas privadas militares contratadas para fazer o trabalho.

Mesmo William Godel, o astro da contrainsurgência que iniciou o programa, foi pego em um esquema ridículo de desvio de dinheiro que

envolveu a apropriação indevida de parte dos US $ 18.000 em dinheiro que ele levou para Saigon em 1961 para criar o Projeto Agile.79 Foi um caso bizarro que envolveu uma soma praticamente insignificante de dinheiro. Alguns de seus colegas sugeriram que ele havia sido politicamente motivado, mas isso não importava. Godel foi finalmente condenado por conspiração por cometer peculato e sentenciado a cinco anos de prisão.80

Outros contratados da ARPA também tinham reservas sobre seu trabalho no Vietnã, mas a missão prosseguiu. Fraudulento ou não, o Projeto Agile transformou o Sudeste Asiático, da Tailândia ao Laos e Vietnã, em um gigantesco laboratório. Todas as tribos, todos os caminhos da selva, todos os guerrilheiros capturados deveriam ser estudados e analisados, monitorados e compreendidos. Enquanto as equipes de assassinato aterrorizavam a população rural do Vietnã, os cientistas da ARPA estavam lá para registrar e medir sua eficácia. Os programas de incentivo foram desenhados e, em seguida, monitorados, analisados, ajustados e monitorados novamente. A ARPA não apenas grampeou o campo de batalha; tentou grampear sociedades inteiras.

Entrevistas, pesquisas, contagens populacionais, estudos antropológicos detalhados de várias tribos, mapas, armamentos, estudos de migração, redes sociais, práticas agrícolas, dossiês – todas essas informações foram extraídas dos centros da ARPA no Vietnã e na Tailândia. Porém, havia um problema. A agência estava se afogando em dados: relatórios datilografados, cartões perfurados, rolos de fita gigantes, cartões de índice e toneladas de impressões de computador. Havia tanta informação chegando que era efetivamente inútil. De que adiantaria toda essa informação se ninguém pudesse encontrar o que precisava? Algo tinha que ser feito.

Capítulo 2

Comando, Controle e Contrainsurgência

> O que separa a inteligência militar nos Estados Unidos de suas contrapartes nos Estados totalitários não são suas capacidades, mas suas intenções. Essa é uma distinção importante, mas que talvez não tranquilize totalmente muitos estadunidenses.-
> *Christopher Pyle, "Vigilância militar de Civis: Uma Análise Documentária", 1973*

Na manhã de 1º de outubro de 1962, segunda-feira, um homem chamado JCR Licklider acordou em um apartamento perto do rio Potomac, em frente à Casa Branca. Tomou café da manhã, despediu-se de sua esposa e suas filhas e dirigiu-se rapidamente até o Pentágono para iniciar seu novo trabalho como diretor das divisões de Ciência Comportamental e de Pesquisa de Comando e Controle da ARPA.

Ao instalar-se em seu modesto escritório, ele examinou a cena. Nos últimos anos, houve muita pressão de quem estava nos círculos de defesa para atualizar os sistemas de comunicação militar e de inteligência dos Estados Unidos. Assim que assumiu o cargo, o Presidente Kennedy se queixou da dificuldade de exercer efetivamente o comando das forças militares dos EUA. Ele se viu cego e surdo nos momentos mais cruciais, incapaz de obter atualizações de inteligência em tempo real ou de comunicar comandos oportunos aos comandantes em campo. Acreditando que os comandantes militares estavam usando a tecnologia ultrapassada como uma desculpa para minar sua autoridade e ignorar instruções, ele exigiu que o secretário de Defesa Robert McNamara investigasse soluções. Ele também discutiu com o Congresso a necessidade de

desenvolver “um sistema verdadeiramente unificado, nacional e indestrutível para garantir comando, comunicação e controle de alto nível”.1

Licklider concordou. Os sistemas de comunicação de defesa dos Estados Unidos estavam de fato pateticamente ultrapassados. Eles simplesmente não conseguiam responder efetivamente aos desafios do dia: dezenas de guerras e insurgências em pequena escala acontecendo em lugares distantes, das quais ninguém sabia nada. Tudo isso combinado com a sempre presente ameaça de ataques nucleares que poderia aniquilar diversos pontos de comando militar. Mas como seria exatamente esse novo sistema? Quais componentes ele teria? Que novas tecnologias precisavam ser inventadas para que funcionasse? Poucas pessoas no Pentágono sabiam as respostas. Licklider era uma delas.

Joseph Carl Robnett Licklider – simplesmente chamado de “Lick” -, usava óculos fundo de garrafa, terno e gravata e era conhecido por seu vício em Coca-Cola. Nos círculos militares mais altos, Lick tinha uma reputação de psicólogo brilhante e visionário da computação, com algumas ideias meio fora da casinha sobre o futuro na era pessoa-máquina.

Ele nasceu em 1915, em Saint Louis, Missouri. Seu pai, ministro batista e chefe da Câmara de Comércio da cidade, era um homem de negócios e crente. Lick deixou seu pai orgulhoso. Em 1937, ele se formou na Universidade de Washington, em Saint Louis, com um triplo diploma em psicologia, matemática e física. Em seguida, passou a estudar como os animais processavam o som, o que envolvia principalmente cortar os crânios de gatos e dar choques em seus cérebros.2 Durante a Segunda Guerra Mundial, Lick foi recrutado para trabalhar no Laboratório Psicoacústico de Harvard, estabelecido com fundos luxuosos da Força Aérea dos EUA para estudar a fala, audição e comunicação humanas.3 Neste laboratório, ele conheceu sua futura esposa, Louise Thomas, que trabalhava como secretária em um centro de pesquisa militar. Ela se considerava socialista e até trazia para o escritório sua cópia do jornal anticapitalista britânico Socialist Worker. Ela deixava-o na beira da mesa para que os homens do laboratório pudessem pegá-lo a caminho do banheiro e ter algo para ler enquanto estavam na privada.

Depois da guerra, Lick deixou Harvard e foi para o Instituto de Tecnologia de Massachusetts (MIT). Lá, entrou em contato com o pri-

meiro sistema de vigilância digital por computador em rede do mundo. Isso mudou a trajetória de sua vida.

Mísseis nucleares soviéticos

Exatamente às 7:00 da manhã de 29 de agosto de 1949, os engenheiros de um *bunker* fortificado nas estepes isoladas da República Socialista Soviética do Cazaquistão acionaram um botão e detonaram a primeira bomba nuclear soviética: *First Lightning*, codinome RDS-1.4 A bomba foi montada em uma torre de madeira cercada por construções falsas e máquinas industriais e militares transportadas para lá para testar os efeitos da explosão: um tanque T-34, prédios de tijolos, uma ponte de metal, um pequeno trecho de uma ferrovia completa com vagões, automóveis, caminhões, artilharia de campanha, um avião e mais de mil animais vivos diferentes – cães, ratos, porcos, ovelhas, porquinhos-da-índia e coelhos – amarrados em trincheiras, atrás de paredes e dentro de veículos.

Era uma bomba bastante pequena, do tamanho da que foi lançada sobre Nagasaki. Na verdade, era quase uma réplica da Fat Man, como essa bomba era conhecida. As fotos anteriores e posteriores do local mostram que os danos foram enormes. Muitos dos animais morreram instantaneamente. Aqueles que sobreviveram foram gravemente queimados e morreram de exposição à radiação. Lavrentiy Beria, notório chefe do NKVD (Comissariado do Povo para Assuntos Internos, uma organização policial soviética), estava lá para observar. Ele telegrafou a Stalin: o teste foi um sucesso.5

As notícias da explosão fizeram os militares estadunidenses entrar em pânico. O domínio nuclear dos EUA não existia mais. A União Soviética agora tinha a capacidade de lançar um ataque nuclear contra os Estados Unidos; o que faltava era um bombardeiro de longo alcance. O problema tinha se tornado muito sério.

O primeiro sistema de alerta por radar dos EUA era escasso e cheio de vazios. O processo de rastreamento de aviões era feito à mão:

militares uniformizados, sentados em salas escuras cheias de fumaça de cigarro, observando telas de radar verdes primitivas. Eles então gritavam coordenadas e anotavam-nas em painéis de vidro para, em seguida, enviar comandos por rádio aos pilotos. O sistema seria inútil diante de um grande ataque nuclear por via aérea.

Um relatório de um órgão especial convocado pela Força Aérea dos EUA recomendou que o sistema de alerta primário por radar fosse automatizado: as informações do radar devem ser digitalizadas, enviadas por cabos e processadas em tempo real por computadores.6 Em 1950, essa recomendação era mais do que ambiciosa – era uma ideia insana. O professor do MIT, George Valley, que liderou o estudo da força aérea, perguntou a várias empresas de computadores se elas seriam capazes de construir um sistema de computadores em tempo real. Todas riram dele. A tecnologia para processamento de dados em tempo real, especialmente a partir de várias instalações de radar, a centenas de quilômetros de distância do computador central, simplesmente não existia. Não havia nada parecido.

Se a força aérea quisesse um sistema de radar automatizado, teria que inventar um computador poderoso o suficiente para lidar com o problema. Felizmente, o Pentágono já era um dos principais impulsionadores nessa área.

Durante a Segunda Guerra Mundial, os militares dos EUA foram a ponta de lança no avanço do estado primitivo da tecnologia digital de computadores. Muitas foram as razões para isso, e todas tinham a ver com guerra. Uma delas foi a criptografia. A divisão de inteligência da Marinha, assim como diversas outras agências predecessoras à Agência Nacional de Segurança, há muitos anos já usavam os tabuladores de cartão perfurado da IBM para realizar análises de criptografia e quebra de códigos. Durante a guerra, tiveram que enfrentar as técnicas avançadas de criptografia nazista e precisaram de máquinas que pudessem trabalhar rápido e com códigos muito complicados. Somente os computadores digitais eram capazes de lidar com o problema.

Outros serviços também estavam desesperados por máquinas que pudessem realizar cálculos matemáticos em alta velocidade, mas por uma razão um pouco diferente. Durante a guerra, novos e poderosos canhões e artilharia de campo saíram das linhas de produção e foram

para áreas de combate da Europa e do Pacífico. Todo esse poder de fogo era inútil se a pontaria não fosse adequada. A artilharia, composta por grandes armas que podiam atingir alvos a dezenas de quilômetros de distância, não dispara em uma trajetória reta, mas lança projéteis com uma leve inclinação para que eles desçam sobre alvos distantes depois de traçar um arco parabólico. Cada arma possui uma tabela de tiro que especifica o ângulo em que o tiro será disparado para que os projéteis atinjam seu alvo. As tabelas de tiro não são simplesmente uma folha, mas apostilas grossas com centenas de variáveis nas equações. O canhão de 155 milímetros "Long Tom", um dos canhões mais populares usados durante a Segunda Guerra Mundial, leva em conta quinhentas variáveis em sua tabela de tiro.7 Temperatura do ar, temperatura da pólvora, altitude, umidade, velocidade e direção do vento e até o tipo de solo – todos são fatores ambientais importantes exigidos nesses cálculos complexos.

Não surpreende que esses gráficos fossem complicados de calcular. Todas as variáveis em centenas de permutações tinham que ser conectadas e elaboradas manualmente. Erros apareciam regularmente e os cálculos eram reiniciados do zero. Uma única tabela de tiro para um tipo de arma podia levar mais de um mês para ser concluída. E houve surpresas: o exército descobriu que as tabelas calculadas para funcionar na Europa não funcionavam na África porque as variáveis do solo eram diferentes; embora as armas estivessem lá, elas eram pouco mais que peso morto até que os dados de disparo pudessem ser recalculados do zero.8 Esquadrões de funcionários – geralmente mulheres – trabalhavam sem parar, usando caneta, papel e ferramentas mecânicas de adição para fazer os cálculos. Essas mulheres eram chamadas de "computadores". Isso foi antes da existência dos computadores digitais e elas eram incrivelmente importantes para o esforço de guerra.9 As tabelas de tiro tinham um significado tão vital que tanto a Marinha quanto o Exército financiaram esforços separados para construir calculadoras automáticas – tudo a serviço da pontaria de máquinas assassinas gigantes – e ajudaram a desenvolver os primeiros computadores digitais durante o caminho. O mais notável dentre eles foi o ENIAC, construído para o Exército por uma equipe de matemáticos e engenheiros da Escola de Engenharia Elétrica Moore da Universidade da Pensilvânia. Instantaneamente, o computador virou uma sensação.

"Calculadora robótica derruba as computadoras como um raio" declarou uma manchete de jornal em 1948 em um artigo que relatava a inauguração do ENIAC:

> Filadélfia, PA – O departamento de guerra divulgou hoje "a máquina de calcular mais rápida do mundo" e disse que o robô possivelmente abriu o caminho matemático para melhorar a vida de todas as pessoas.
>
> Produtos industriais aprimorados, melhor comunicação e transporte, previsão climática superior e outros avanços em ciência e engenharia podem ser possíveis, disse o Exército, a partir do desenvolvimento do "primeiro computador de uso geral totalmente eletrônico".
>
> O Exército descreveu a máquina como mil vezes mais rápida que a mais avançada máquina de calcular construída anteriormente e declarou que o aparelho permite "resolver em horas problemas que levariam anos" em qualquer outra máquina.
>
> Faz-tudo
>
> A máquina, que pode adicionar, subtrair, multiplicar, dividir e calcular raiz quadrada, além de fazer cálculos mais complexos com base nessas operações, é chamada de "ENIAC" – abreviação de "integrador e computador numérico eletrônico". Também foi apelidado de "Einstein mecânico".10

O ENIAC não foi rápido o suficiente para ajudar na guerra, mas permaneceu em operação por quase uma década, calculando tabelas de tiro, executando cálculos de bombas atômicas e construindo modelos climáticos a respeito do clima soviético, incluindo o mapeamento de uma possível propagação de precipitação radioativa como resultado de uma guerra nuclear.11 Por mais poderoso que fosse, o ENIAC não era suficiente.

Para desenvolver as tecnologias de computadores e redes necessárias para alimentar um moderno sistema de defesa por radar, foi criada uma divisão de pesquisa especial conhecida como Laboratório Lincoln. Ligado ao Instituto de Tecnologia de Massachusetts e sediado em um campus de pesquisa a 16 quilômetros a leste de Cambridge, o Lincoln

Lab era um projeto conjunto da Marinha, Força Aérea, Exército e IBM, cujo único objetivo era construir um sistema moderno de defesa aérea. Incontáveis recursos foram usados para o projeto e milhares de terceirizados civis e militares estiveram envolvidos durante um período de dez anos. O software em si levou cerca de mil homens-ano para ser programado.12 Todo o projeto custou mais do que o Projeto Manhattan, aquele dedicado desenvolver a primeira arma atômica.

O Lincoln Lab montou um monstro: o Ambiente Semi-Automático de Solo (Semi-Automatic Ground Environment, SAGE). Foi o maior sistema de computadores da história e a primeira verdadeira rede de computadores. O SAGE era controlado por 24 "Centros de Controle" localizados estrategicamente em todo os EUA. Esses gigantescos bunkers de concreto à prova de bombas nucleares abrigavam dois computadores IBM que, juntos, custam US $ 4 bilhões em dólares de hoje. Eles pesavam seiscentas toneladas e ocupavam um hectare de espaço; um estava sempre em modo de espera, caso o outro falhasse.13 Cada centro de controle empregava centenas de pessoas e estava conectado ao conjunto de radares terrestres e costeiros, silos de mísseis e bases de aeronaves interceptoras próximas. O sistema podia rastrear até quatrocentos aviões em tempo real, ordenar o lançamento de caças e mísseis para abater aeronaves e apontar canhões antiaéreos.14 O SAGE eram os olhos, ouvidos e cérebros de uma arma gigantesca. Foi também a primeira máquina de vigilância computadorizada de abrangência nacional – vigilância no sentido mais amplo: um sistema que coletava informações de sensores remotos, analisava-as e permitia que a inteligência militar agisse segundo seus resultados.

O SAGE era uma máquina incrivelmente sofisticada, mas, na prática, já estava desatualizada antes mesmo de ser ligada. Entrou em operação no início dos anos 1960, mais de três anos após o lançamento do Sputnik pela União Soviética, quando ela demonstrou sua capacidade de lançar mísseis intercontinentais. Os soviéticos podiam atirar uma carga nuclear no espaço e fazê-la descer em qualquer lugar dos Estados Unidos, e nenhum sistema sofisticado de defesa por radar poderia fazer algo a respeito.

Superficialmente, o SAGE era um elefante branco. Mas em um sentido histórico maior, foi um sucesso fenomenal. O Laboratório Lin-

coln do MIT – com seus grandes talentos em engenharia e recursos quase ilimitados direcionados a um conjunto restrito de problemas – tornou-se mais do que apenas um centro de pesquisa e desenvolvimento para um único projeto militar. Era um campo de treinamento para uma nova elite de engenharia: um grupo multidisciplinar de cientistas, acadêmicos, funcionários do governo, empresários e matemáticos que continuariam criando a indústria moderna de computadores e construindo a Internet.

E J. C. R. Licklider estava no centro disso tudo. No Laboratório Lincoln, trabalhou no lado humano desse vasto sistema de computadores por radar e ajudou a desenvolver a parte gráfica do sistema, que precisava integrar dados de vários radares e exibir informações de velocidade e rumo em tempo real que poderiam ser usadas para guiar interceptores de aeronaves. Era um componente pequeno, mas vital, do SAGE, e o trabalho abriu seus olhos para as possibilidades de criar ferramentas que integrassem pessoas e computadores em um sistema contínuo: uma pessoa-máquina que romperia as limitações físicas humanas e criaria novos e poderosos seres híbridos.

Ciborgues e Cibernética

O Instituto de Tecnologia de Massachusetts foi o marco zero para uma nova ciência chamada cibernética. Desenvolvida pelo professor do MIT Norbert Wiener, a cibernética definiu o mundo como uma enorme máquina computacional. Ele bolou uma estrutura conceitual e matemática para pensar e projetar sistemas de informação complexos.

Wiener era um homem estranho e brilhante. Ele era baixo, rechonchudo, com uma cabeça redonda carnuda e óculos grossos. Nos últimos anos, se parecia um pouco com Hans Moleman, dos Simpsons. Ele também era um verdadeiro prodígio. Filho de um acadêmico rigoroso e ambicioso de origem eslava, Wiener foi forçado a memorizar livros inteiros e recitá-los de memória. Além disso, executar álgebra e trigonometria complexas em sua cabeça.15 “Enquanto meu pai fazia em casa seu trabalho para Harvard, eu tinha que ficar ao lado dele e recitar

minhas lições de memória, mesmo em grego, aos seis anos de idade. Ele me ignorava até que eu cometesse um errinho qualquer. Aí, então, ele verbalmente me humilhava", contou em sua autobiografia.16

Com esse tipo de treinamento, Wiener ingressou na faculdade aos onze anos – o "prodígio infantil de Boston", como um jornal o chamava –, obteve um PhD em matemática aos dezoito anos e, rejeitado de um emprego em Harvard, começou a lecionar no MIT. Sua vida de estudo frenético e as críticas impiedosas de seu pai não o prepararam para a dimensão social da vida: ele era desajeitado, não conseguia conversar com as mulheres, tinha poucos amigos de verdade, era depressivo e mal conseguia se cuidar.

Seus pais arranjaram seu casamento com Margaret Engemann, uma imigrante da Alemanha que tinha problemas para encontrar um marido. Eles tiveram duas filhas, e o casamento parecia bom, exceto por um detalhe: Margaret era uma firme defensora de Adolf Hitler e forçou as filhas a lerem Minha Luta. "Um dia, ela nos disse que os membros de sua família na Alemanha haviam sido certificados como Judenrein – 'livres de mácula judaica'. Ela achou que isso nos deixaria alegres", lembrou a filha. "Ela disse que eu não deveria sentir pena dos judeus da Alemanha porque eles não eram pessoas muito agradáveis." Durante uma festa de Natal, tentou convencer os convidados de que a linhagem ariana remonta ao próprio filho de Deus. "Jesus era filho de um mercenário alemão que havia se instalado em Jerusalém, e isso estava cientificamente comprovado." Era uma situação embaraçosa, dado que seu marido era judeu de ascendência alemã e, portanto, suas filhas eram metade judias. Mas este não era um lar comum.

A mente de Wiener estava perpetuamente faminta, devorando tudo em seu caminho. Ele atravessou quase todas as fronteiras disciplinares, estudando filosofia, matemática, engenharia, linguística, física, psicologia, biologia evolutiva, neurobiologia e ciência da computação. Durante a Segunda Guerra Mundial, Wiener encontrou um problema que testava os limites de seu brilhante cérebro multidisciplinar. Ele foi recrutado para trabalhar em um empreendimento quixotesco ultrassecreto que visava construir um mecanismo automático de mira que pudesse aumentar a eficácia dos canhões terrestres antiaéreos. Durante toda a guerra, ele trabalhou na construção de um computador especiali-

zado que usava radar de micro-ondas para observar, localizar e prever a posição futura de um avião com base nas ações de seu piloto, a fim de explodi-lo do céu com mais eficácia. Era uma máquina que estudava as ações de um ser humano e respondia dinamicamente a elas. Ao construí-la, ele percebeu algo profundo sobre a natureza da informação. Notou que a comunicação de informações não era apenas um ato abstrato ou efêmero, mas possuía uma poderosa propriedade física. Como uma força invisível, poderia ser usada para desencadear uma reação. Ele também deu outro salto simples, mas profundo: percebeu que a comunicação e a transmissão de mensagens não se limitavam aos seres humanos, mas permeavam todos os organismos vivos e também podiam ser projetadas no mundo mecânico.

Wiener publicou essas ideias em 1948, num tratado denso chamado Cibernética: Controle e Comunicação nos Animais e nas Máquinas. O que era a cibernética? O conceito era escorregadio e enlouquecedoramente difícil de definir. Em termos simples, ele descreveu a cibernética como a ideia de que o sistema nervoso biológico e o computador ou a máquina automática eram basicamente a mesma coisa. Eles eram "dispositivos que tomam decisões com base nas decisões que tomaram no passado", explicou.17 Para Wiener, as pessoas e o mundo inteiro podiam ser vistos como uma gigantesca máquina de informações interligadas, tudo respondendo a tudo em um intrincado sistema de causa, efeito e retroalimentação. Ele previu que nossas vidas seriam cada vez mais mediadas e aprimoradas por computadores, integradas a tal ponto que deixaria de haver qualquer diferença entre nós e a máquina cibernética maior em que vivíamos.

Apesar de estar cheio de provas e jargões matemáticos incompreensíveis, o livro despertou a imaginação do público e se tornou um best-seller instantâneo. Os círculos militares o receberam como um trabalho revolucionário. O que "O Capital" de Karl Marx fez pelos socialistas do século XIX, a Cibernética de Wiener fez pelos anticomunistas gringos da Guerra Fria. Em um nível muito básico, a cibernética postulava que os seres humanos, como todos os seres vivos, eram máquinas de processamento de informações. Éramos todos computadores – altamente complexos, mas, mesmo assim, computadores. Isso significava que os militares poderiam construir máquinas que pudessem pensar como pessoas e agir como pessoas: procurar aviões e navios inimigos,

transcrever comunicações de rádio inimigas, espionar subversivos, analisar notícias estrangeiras em busca de significado oculto e mensagens secretas – tudo sem precisar dormir, comer ou descansar. Com uma tecnologia de computador como essa, o domínio dos EUA estaria garantido. A cibernética desencadeou uma busca indescritível de décadas pelas forças armadas para cumprir sua visão particular da cibernética, um esforço para criar computadores com o que hoje chamamos de inteligência artificial.18

Os conceitos cibernéticos, apoiados por grandes quantidades de financiamento militar, começaram a permear disciplinas acadêmicas: economia, engenharia, psicologia, ciência política, biologia e estudos ambientais. Economistas neoclássicos integraram a cibernética em suas teorias e começaram a enxergar os mercados como máquinas de informação distribuída.19 Os ecologistas começaram a olhar para a própria Terra como um "sistema biológico computacional" autorregulador. E psicólogos e cientistas da cognição abordaram o estudo do cérebro humano como se fosse literalmente um computador digital complexo.20 Cientistas e sociólogos políticos começaram a sonhar em usar a cibernética para criar uma sociedade utópica controlada, um sistema perfeitamente bem lubrificado em que computadores e pessoas fossem integrados a um todo coeso, gerenciado e controlado para garantir segurança e prosperidade.21 "Colocando com mais clareza: na década de 1950, tanto os militares quanto a indústria nos EUA defendiam explicitamente um entendimento messiânico da computação, no qual ela era a questão subjacente a tudo no mundo social e, portanto, podia ser submetida ao controle militar capitalista de Estado – um controle centralizado e hierárquico", escreve o historiador David Golumbia em "A Lógica Cultural da Computação", um estudo inovador sobre a ideologia computacional.22

Em grande parte, esse entrelaçamento de cibernética e o grande poder foi o que levou Norbert Wiener a se opor à cibernética quase tão logo a apresentou ao mundo. Ele viu cientistas e militares adotando a interpretação mais estreita possível da cibernética para criar melhores máquinas de matar e sistemas mais eficientes de vigilância, controle e exploração. Viu corporações gigantescas usando suas ideias para automatizar a produção e demitir trabalhadores em sua busca por maior riqueza e poder econômico. Ele começou a perceber que, em uma socie-

dade mediada por computadores e sistemas de informação, aqueles que controlavam a infraestrutura possuíam o poder supremo.

Wiener imaginou um futuro sombrio e percebeu que ele próprio era culpado, comparando seu trabalho em cibernética com aquele dos maiores cientistas do mundo que liberaram o poder destrutivo das armas atômicas. De fato, ele viu a cibernética em termos ainda mais sombrios do que as armas nucleares. “O impacto da máquina pensante será certamente um choque de ordem comparável ao da bomba atômica”, disse ele em uma entrevista de 1949. A substituição do trabalho humano por máquinas – e a desestabilização social, o desemprego em massa e a concentração de poder econômico que essas mudanças causariam – é o que mais preocupava Wiener.23 “Lembremos que a máquina automática, não importa o que pensamos sobre qualquer sentimento que ela possa ter ou não, é o equivalente econômico preciso do trabalho escravo. Qualquer trabalho que concorra com o trabalho escravo deve aceitar as condições econômicas deste último. É perfeitamente claro que isso produzirá uma situação de desemprego, em comparação com a qual a atual recessão e até a depressão dos anos trinta parecerão uma piada agradável”, escreveu Wiener em um livro sombrio e presciente, “O Uso Humano de Seres Humanos: Cibernética e Sociedade”.24

A destruição seria política e econômica.

Depois de popularizar a cibernética, Wiener tornou-se uma espécie de ativista trabalhista e antiguerra. Ele procurou os sindicatos para avisá-los do perigo da automação e da necessidade de levar a ameaça a sério. Recusou ofertas de grandes empresas que queriam ajuda para automatizar suas linhas de montagem de acordo com seus princípios cibernéticos, e recusou-se a trabalhar em projetos de pesquisa militar. Ele era contra o enorme acúmulo de armas em tempo de paz que ocorreu após a Segunda Guerra Mundial e atacou publicamente os colegas por trabalharem para ajudar os militares a construir ferramentas de destruição maiores e mais eficientes. Destacou cada vez mais sua percepção de que uma “máquina estatal colossal” estava sendo construída por agências gover-

namentais “para fins de combate e dominação”, um sistema computadorizado de informação “suficientemente extenso para incluir todas as atividades civis durante a guerra, antes da guerra e possivelmente até entre as guerras”, como ele descreveu em “O Uso Humano de Seres Humanos”.

O apoio claro de Wiener aos trabalhadores e sua oposição pública ao trabalho corporativo e militar fizeram dele um pária entre seus colegas engenheiros militares.25 Também lhe valeu um lugar na lista de subversivos sob vigilância de J. Edgar Hoover no FBI. Por anos, dado que era suspeito de ter simpatia comunista, sua vida foi documentada num espesso arquivo do FBI que foi fechado após sua morte em 1964.26

Mouses e teclados

J.C.R. Licklider interagiu com Norbert Wiener no MIT e participou de conferências e jantares em que ideias cibernéticas foram apresentadas, discutidas e debatidas. Ele foi fortemente tocado pela visão cibernética de Wiener. Onde Wiener via perigo, Lick via oportunidade. Ele não teve nenhum escrúpulo em colocar essa tecnologia a serviço do poder corporativo e militar dos EUA.

Embora a maioria dos engenheiros da computação achasse que os computadores eram pouco mais do que calculadoras grandes, Lick os via como extensões da mente humana e ficou obcecado em projetar máquinas que pudessem ser perfeitamente acopladas aos seres humanos. Em 1960, publicou um artigo que descrevia sua visão para a próxima “simbiose pessoa-computador” e descrevia em termos simples os tipos de componentes de computador que precisavam ser inventados para que isso acontecesse. O artigo delineava essencialmente um computador multiúso moderno completo, com tela, teclado, software de reconhecimento de fala, recursos de rede e aplicativos que poderiam ser usados em tempo real para diversas tarefas.27 Isso parece óbvio para nós agora, mas naquela época as ideias de Lick eram visionárias. Seu artigo foi

amplamente divulgado nos círculos de defesa e ele recebeu um convite do Pentágono para fazer uma série de palestras sobre o assunto.28

"Minha primeira experiência com computadores foi ouvir uma conversa do [matemático John] von Neumann, em Chicago, em 1948. Na época, parecia ficção científica: uma máquina capaz de executar algoritmos automaticamente", lembra Charles Herzfeld, físico que atuaria como diretor do ARPA em meados da década de 1960.29 "Entretanto, o choque seguinte que recebi foi Lick: não apenas poderíamos usar essas máquinas para cálculos enormes, mas poderíamos torná-las úteis em nossas vidas cotidianas. Ouvi-o, prestando atenção. Fiquei muito empolgado. E, num sentido muito real, desde então, tornei-me um discípulo dele."

De fato, os trabalhos e entrevistas de Lick mostram que ele achava que quase qualquer problema poderia ser resolvido com a aplicação correta de computadores. Chegou a elaborar um plano para acabar com a pobreza e "estimular jovens negros do gueto", fazendo-os mexer com computadores. Ele chamou o processo de "dinamizações", uma versão dos anos 1960 de uma ideia que é muito popular no Vale do Silício até hoje, cinquenta anos depois: a crença de que ensinar crianças pobres a programar de alguma forma as tirará magicamente da pobreza e aumentará as taxas de alfabetização e educação globais.30 "O que é difícil transmitir em poucas palavras é a visão quase messiânica propagada por Licklider sobre o potencial dos avanços no uso de computadores, a maneira como as pessoas podem se relacionar com eles e o impacto resultante em como elas tomariam decisões", explicou um relatório desclassificado interno da ARPA.31 Lick contageou todo mundo com seu entusiasmo pela próxima revolução dos computadores, incluindo pessoas importantes da ARPA, que também estavam querendo impulsionar o desenvolvimento dos computadores para aumentar a eficácia militar.

Em 1962, após uma breve entrevista de emprego no Pentágono, Lick mudou-se com sua família de Boston para Washington, DC, e começou a trabalhar do zero na construção do programa de Pesquisa de Comando e Controle da ARPA.32

Na época, os computadores eram monstros gigantes de metal que ocupavam porões inteiros e eram assistidos por vários técnicos. Apesar

de sua complexidade e tamanho, eles eram primitivos e tinham menos poder computacional do que uma calculadora gráfica dos anos 1990. Eles também executavam um programa de cada vez, e cada um tinha que ser alimentado manualmente usando cartões perfurados. “Imagine tentar, por exemplo, dirigir uma batalha com a ajuda de um computador com este tipo de cronograma”, explicou Lick em seu artigo de 1960. “Você formula seu problema hoje. Passa o dia seguinte com um programador. Na próxima semana, o computador dedica 5 minutos à montagem do seu programa e 47 segundos ao cálculo da resposta para o seu problema. Você recebe uma folha de papel de 6 metros de comprimento, cheia de números que, em vez de fornecer uma solução final, apenas sugere uma tática que deve ser explorada numa simulação. Obviamente, a batalha terminaria antes que o segundo passo em seu planejamento fosse iniciado.”33

E redes? Elas existiam. Mas, como a rede que unia o SAGE, elas geralmente eram altamente especializadas e construídas para um propósito e função específicos. Uma rede teria que ser projetada e construída sob medida para atender a cada nova situação.

Na opinião de Lick, esse era o caminho errado para lidar com o problema da tecnologia de comando e controle. O que a ARPA precisava era desenvolver uma plataforma universal e padronizada de computador e rede que pudesse ser modificada com o mínimo de esforço para lidar com praticamente qualquer tarefa: rastreamento de mísseis, estudos comportamentais, bancos de dados, comunicação de voz, análises para a inteligência ou funções simples de processamento de texto e correio. Essa estrutura de computador teria alguns componentes básicos subjacentes. Seria fácil de usar e teria uma interface gráfica intuitiva para o usuário, portaria um sistema operacional universal e programas que poderiam ser carregados nele. E, o mais importante, se afastaria do modo de calculadora, permitindo que os usuários trabalhassem em tempo real da mesma maneira que as pessoas interagem umas com as outras. Embora isso possa parecer básico e óbvio, esses tipos de ferramentas de computador não existiam no início dos anos 1960.

“Havia a crença na cabeça de várias pessoas – umas poucas pessoas, na verdade – de que poderíamos nos tornar muito mais eficazes para pensar e tomar decisões se tivéssemos o suporte de um sistema de

computador, boas telas, bases de dados, computação sob comando pessoal, etc. Era o tipo de imagem que buscávamos trazer para a realidade", explicou Lick em um relatório da ARPA.34 "Realmente não era um programa de pesquisa de comando e controle. Era um programa de computação interativa. E minha crença era, e ainda é, que não se pode realmente comandar e controlar sem isso."

Com o estado grosseiro da tecnologia de computadores da época, o objetivo de Lick ainda estava a anos de distância, e uma coisa era certa: não seria aprimorado por si só. Alguém tinha que fazer o trabalho. Na visão de Lick, a principal missão da ARPA era investir dinheiro em engenheiros que pudessem construir os componentes básicos do computador necessários para um sistema moderno de comando e controle. No mínimo, a ARPA colocaria as pessoas para trabalhar em projetos de computador que apontassem na direção certa. Lick viu seu trabalho em termos históricos. Ele usaria o orçamento e a influência da ARPA para empurrar a indústria de computadores para um novo território, alinhado à sua visão e às necessidades do sistema de defesa.

Mas, primeiro, ele queria ter certeza de que as agências de inteligência dos EUA já não haviam desenvolvido secretamente esse tipo de tecnologia de computação interativa. "Fui à CIA e joguei um verde", disse Lick. "Disse a eles: 'Olha, não sei o que vocês estão fazendo sobre isso. Espero que estejam fazendo o seguinte. Mas quero contar o que estou fazendo, e então talvez possamos descobrir uma maneira de conversar como relacionar ambos esforços'". Ele também organizou uma reunião com representantes da NSA e fez o mesmo discurso sobre a beleza de uma plataforma de computador universal e fácil de usar. Nenhuma das agências estava trabalhando em computação interativa, mas, com certeza, elas queriam pôr as mãos nela – "a NSA, eles realmente precisavam do que eu queria", Lick lembrou em uma entrevista anos depois.35 De fato, as agências de inteligência estavam entre os primeiros usuários do programa de ferramentas de comando e controle da ARPA que foi produzido poucos anos depois.

O orçamento inicial da Pesquisa em Comando e Controle da ARPA foi de US $ 10 milhões. Lick espalhou esse dinheiro por suas redes pessoais e profissionais no mundo militar-acadêmico-terceirizado. Ele financiou projetos de computação interativa e colaboração sincroni-

zada, design de interface gráfica, redes de computadores e inteligência artificial em MIT, UC Berkeley, UCLA, Harvard, Universidade Carnegie Mellon, Stanford e RAND Corporation. No MIT, Lick estabeleceu uma de suas maiores e mais importantes iniciativas: o Projeto MAC, abreviação de Cognição Auxiliada por Máquinas, que evoluiu para um ambiente sofisticado de computador interativo completo, com e-mail, quadros de avisos digitais e videogames para vários jogadores. O Projeto MAC do MIT gerou a primeira safra de "hackers", empreiteiros da ARPA que mexeram com esses computadores gigantes em seu tempo livre.

No Instituto de Pesquisa de Stanford, que também estava realizando um trabalho contratado pela ARPA sobre guerra química no Vietnã, Lick financiou o Centro de Pesquisa em Realidade Aumentada de Douglas C. Engelbart. Essa equipe tornou-se lendária nos círculos da computação. Ela desenvolveu links de hipertexto, processamento de texto em tempo real para vários usuários, videoconferência e, principalmente, o mouse de computador. Lick também deu início a toda uma gama de projetos de rede, esforços que levariam diretamente à criação da Internet. Uma delas foi uma iniciativa conjunta de US $ 1,5 milhão entre UCLA – UC Berkeley para desenvolver softwares e hardwares para uma rede que conectaria vários computadores a vários usuários.36 Como uma proposta de financiamento explicava, essa pesquisa seria usada diretamente para melhorar as redes militares, incluindo o Sistema Nacional de Comando Militar, que era, na época, um novo sistema de comunicação que ligava os militares ao presidente.37

Lick trabalhou duro e rápido, e seus esforços na ARPA foram notáveis. Empresas como General Electric e IBM não aceitaram inicialmente suas ideias sobre computação interativa. Mas com sua tenacidade e o financiamento da ARPA, sua visão ganhou força e popularidade e, finalmente, mudou a direção da indústria de computadores. Seu mandato na ARPA também desembocou em outra coisa: a ciência da computação tornou-se mais do que apenas uma subdivisão da engenharia elétrica; desenvolveu-se em um campo próprio de estudo.38 Os contratos de pesquisa de longo prazo da divisão de Pesquisa em Comando e Controle da ARPA, entregue às equipes de pesquisa, ajudaram a semear a criação de departamentos independentes de ciência da computação nas

universidades de todo os EUA e os vincularam estreitamente, através de financiamento e pessoal, aos militares.

Redes: o lado obscuro

Os entusiastas da história da computação consideram Lick uma das personalidades mais importantes no desenvolvimento da ciência da computação e da Internet. Uma biografia de quinhentas páginas, chamada "A Máquina dos Sonhos", de M. Mitchell Waldrop, narra a vida e o trabalho de Lick. O que quase nunca é relatado, mas que aparece através de páginas e mais páginas de arquivos governamentais liberados e desclassificados que cobrem o mandato de Lick na ARPA, é o quanto seus esforços de pesquisa em computação foram permeados pela maior missão de contrainsurgência da instituição.

Lick morreu em 1990, alguns meses antes de completar 75 anos. Em entrevistas, ele se certificou de distanciar seus esforços na ARPA do trabalho menos saudável da agência no combate às insurgências. "Tudo era um tanto misterioso", lembrou em uma entrevista de 1988.39 "Havia um sujeito chamado Bill Godel que, ao que me parecia, estava sempre tentando controlar o que eu estava fazendo. Eu nunca sabia o que ele fazia, então essa parte me deixava nervoso. Eu tinha um projeto que não havia sido esclarecido o suficiente para saber o que era, e isso me também me angustiava." Ele prontamente admitiu que sabia que algo obscuro estava sendo preparado na ARPA e deu a entender que tinha uma participação naquilo tudo, mas afirmou que resistia às tentativas de envolver seu projeto de comando e controle nos esforços desagradáveis de contrainsurgência do Vietnã. "Eu meio que fiquei fora daquilo o melhor que pude", explicou ele.

Porém, a verdade é um pouco mais constrangedora.

O trabalho de Lick era desenvolver a tecnologia básica de computadores e redes necessária para combater as guerras modernas. Naturalmente, isso se aplicava à contrainsurgência de uma maneira muito geral. Mas seu trabalho também foi muito mais específico e direto.

Por exemplo, documentos mostram que, em março de 1962, ele participou de um influente simpósio do Exército dos EUA que se reuniu em Washington, DC, para discutir como a ciência comportamental e a tecnologia de computador poderiam ser usadas para melhor travar "guerras limitadas" e contrainsurgência. Lá, Lick fazia parte de um grupo de trabalho dedicado à elaboração de um programa de pesquisa em contrainsurgência do Exército dos EUA que pudesse enfrentar um "desafio comunista multidimensional – na guerra paramilitar, na guerra psicológica e no campo convencional e nuclear".40 O simpósio aconteceu no momento em que Lick estava começando seu trabalho como chefe das divisões de Ciência Comportamental e Pesquisa de Comando e Controle da ARPA. No futuro, seu trabalho na agência fazia parte dos maiores esforços de contrainsurgência das forças armadas e se sobrepunha diretamente ao Projeto Ágil, de William Godel.41

Naturalmente, muitos dos programas da ARPA no sudeste da Ásia – de drones de controle remoto a cercas eletrônicas de sensores e coleta de inteligência humana em larga escala – estavam todos vinculados de uma maneira ou de outra à coleta e comunicação de dados e, em última análise, dependiam da tecnologia de computadores para organizar e automatizar essas tarefas. Eles precisavam de ferramentas que pudessem ingerir dados sobre pessoas e movimentos políticos, compilar bancos de dados pesquisáveis, vincular comunicações de rádio e satélite, criar modelos, prever o comportamento humano e compartilhar dados de maneira rápida e eficiente em grandes distâncias entre diferentes agências. Construir a tecnologia subjacente que poderia alimentar todas as novas plataformas de comunicação foi o trabalho de Lick. Ele certamente nunca se esquivou de direcionar a pesquisa para aplicações de contrainsurgência. Uma olhada nos contratos daqueles dias mostra-o direcionando fundos para projetos que usavam computadores para tudo, como estudar e prever o comportamento de pessoas e sistemas políticos, modelar processos cognitivos humanos e desenvolver simulações que previam "o comportamento de sistemas internacionais".42 Os registros mostram que, já em 1963, a divisão de Pesquisa em Comando e Controle de Lick estava dividindo e misturando fundos com o Projeto Agile de William Godel.43

De fato, mesmo quando Lick começou na ARPA, o Projeto Agile estava implementando iniciativas de contrainsurgência orientada a dados

em campo. Uma das primeiras ocorreu entre 1962 e 1963 no Centro de Teste de Desenvolvimento de Combate da ARPA, na Tailândia, nos arredores de Bangcoc. Foi chamada de Levantamento Antropométrico das Forças Armadas da Tailândia. Na superfície, foi um estudo bem-intencionado que buscou medir o tamanho do corpo de vários milhares de militares tailandeses para auxiliar no projeto de equipamentos e uniformes. Foram coletados cinquenta e dois pontos de dados diferentes, como a altura dos assentos, o comprimento da nádega ao joelho, a circunferência formada pela virilha e a coxa, e sete medições diferentes da face e da cabeça.

Os pontos de dados da pesquisa tinham a sensação desagradável de um estudo eugênico, mas as medidas físicas eram apenas o nível superficial do estudo. O propósito mais profundo estava enraizado na previsão e controle.44 “Também foram feitas perguntas pessoais aos participantes tailandeses – não apenas onde e quando nasceram, mas quem eram seus ancestrais, qual era sua religião e o que pensavam do rei da Tailândia”, explica Annie Jacobsen no livro “O Cérebro do Pentágono”. Essas perguntas estavam no cerne do verdadeiro objetivo do estudo: criar um perfil de computador de cada militar tailandês e usá-lo para testar modelos preditivos. “A ARPA queria criar um protótipo mostrando como seria possível monitorar os exércitos do terceiro mundo para uso futuro. As informações seriam salvas em computadores instalados em bases militares seguras. Em 1962, a Tailândia era um país relativamente estável, mas estava cercado por insurgências e inquietações por todos os lados. Se a Tailândia se tornasse uma zona de batalha, a ARPA teria informações sobre os soldados tailandeses, cada um dos quais poderia ser rastreado. Informações, como quem abandonou o exército tailandês e se tornou um combatente inimigo, podiam ser apuradas. Usando modelos de computador, a ARPA poderia criar algoritmos descrevendo o comportamento humano em áreas remotas.”45

A ligação entre contrainsurgência e computação não é tão surpreendente. A primeira tecnologia de computador rudimentar foi desenvolvida nos Estados Unidos quase um século antes da Guerra do Vietnã para contar, categorizar e estudar populações. No final da década de 1880, um estadunidense chamado Herman Hollerith inventou, através de um contrato com o governo, uma máquina de tabulação para acelerar o processo de contagem de pessoas para o censo dos EUA. Por causa de

um imenso fluxo de imigração, o censo se tornou tão difícil que a contagem levou uma década para ser terminada manualmente.

Hollerith criou uma solução eletromecânica elegante, uma engenhoca que mais tarde se tornaria a espinha dorsal da International Business Machines, ou IBM, a mais antiga empresa de computadores do mundo. Seu projeto dividiu o processo de cálculo automático de dados em duas etapas gerais. Primeiro, os dados foram digitalizados, ou seja, convertidos em um formato que pudesse ser entendido por uma máquina, através de uma série de furos realizados em um pedaço de papel. A segunda etapa envolveu inserir este papel em um aparelho contendo pinos elétricos que tabularam e classificaram os cartões perfurados com base na posição e disposição dos furos. Hollerith inicialmente pensou em gravar as informações em uma longa tira de papel, como uma fita adesiva. Mas rapidamente abandonou a ideia, porque tornou muito difícil localizar e isolar registros individuais – em um censo, a máquina teria que processar centenas de milhares ou até milhões de indivíduos. “O problema era que, por exemplo, se você queria estatísticas sobre os chineses, teria que correr quilômetros de papel para poder contar alguns”, explicou Hollerith.46

Então, ele teve uma ideia diferente: cada pessoa seria representada por um cartão perfurado separado. A inspiração veio de uma observação que ele fez em um trem. Para impedir que as pessoas passem e reutilizem as passagens de trem, os condutores marcavam com furos a descrição do passageiro em um pedacinho de papel: altura, tipo de penteado, cor dos olhos e tipo de nariz. Era uma solução elegante e poderosa. Cada pessoa tinha seu próprio cartão – e cada cartão tinha um padrão bem definido de buracos que correspondiam às informações coletadas pelos tomadores de censo. Cada cartão codificaria os atributos de uma pessoa: idade, sexo, religião, ocupação, local de nascimento, estado civil, histórico criminal. Depois que um funcionário transferia os dados de um formulário do censo para um cartão perfurado, os cartões alimentavam uma máquina que podia contar e organizá-los de várias maneiras. Ela poderia fornecer totais agregados para cada categoria ou encontrar e isolar grupos de pessoas em categorias específicas. Qualquer característica – nacionalidade, status de emprego, deficiência – poderia ser destacada e classificada rapidamente. Hollerith descreveu seu sistema como se fosse “uma fotografia perfurada de cada pessoa”. E, de

fato, era assim mesmo: um dossiê digital de primeira geração de pessoas e suas vidas.

Usados para fazer o censo em 1890, os tabuladores de Hollerith foram um enorme sucesso, reduzindo o tempo necessário para processar os números de anos para meses. As máquinas também deram aos rastreadores do censo a capacidade de cortar, organizar e extrair os dados de maneiras nunca antes vistas; por exemplo, para encontrar uma determinada pessoa ou grupo de pessoas – digamos, estadunidenses com pelo menos um pai japonês na Califórnia ou todos os órfãos que moram em Nova York que tinham cometido um crime. Esse tipo de análise refinada em escala de massas não tinha precedentes. Da noite para o dia, os tabuladores de Hollerith transformaram o censo de uma contagem simples em algo muito diferente – algo que se aproximava de uma forma inicial de vigilância em massa.

Newton Dexter North, um lobista da indústria da lã, escolhido para liderar o censo de 1900, ficou impressionado com a capacidade dos tabuladores de Hollerith de arranjar tão precisamente os dados raciais. Como muitos estadunidenses da classe alta de sua época, North temia que o influxo maciço de imigrantes da Europa estivesse destruindo o tecido social gringo, causando distúrbios sociais e políticos e ameaçando a pureza racial da nação.47 Esse medo da imigração viria a se misturar com a histeria anticomunista, levando à repressão dos trabalhadores e sindicatos em todo o país. North viu estatísticos como ele como soldados tecnocráticos: a última linha de defesa dos EUA contra uma influência corruptora estrangeira. E ele viu a máquina de tabulação como sua arma mais poderosa. “Essa imigração está afetando profundamente nossa civilização, nossas instituições, nossos hábitos e nossos ideais. Ela transplantou para cá línguas estrangeiras, religiões estranhas e teorias alienígenas de como governar; tem sido uma poderosa influência no rápido desaparecimento da visão puritana da vida”, alertou North. E elogiou o novo dispositivo computacional de Hollerith: “Não consigo descrever minha surpresa com esta invenção: correlacionar dados de elementos individuais da população, em combinação com outros dados, além do alcance da tabulação manual? Algo deveras importante”, explicou. “Sem isso, nunca poderíamos trazer à tona toda a verdade que nos é necessária, se quisermos lidar com sucesso com os problemas decorren-

tes da mistura heterogênea de raças que nossas leis defeituosas de imigração estão empurrando sobre nós.”48

Duas décadas após seu lançamento, a tecnologia de tabulação Hollerith foi absorvida pela IBM. Melhoradas e refinadas ao longo dos anos, as máquinas se tornaram um grande sucesso entre empresas e governo. Elas foram usadas extensivamente pelas forças armadas dos EUA durante a Segunda Guerra Mundial para manter um registro atualizado dos números de tropas e até foram levadas durante a invasão da Normandia. Elas também foram usadas para processar o confinamento de nipo-americanos durante a guerra. E, depois que o presidente Franklin Delano Roosevelt criou o sistema da previdência social, a IBM e seus tabuladores funcionaram como um braço privatizado de facto, que faziam todo o processamento e a contabilização do sistema de pensões dos Estados Unidos.49 Talvez o uso mais infame das máquinas tabuladoras da IBM foi aquele realizado pela Alemanha nazista para administrar campos de trabalho para a morte e instituir um sistema de vigilância racial, permitindo que o regime combinasse dados genealógicos para eliminar as pessoas que tinham traços de sangue judeu.50

Willy Heidinger, chefe de operações da IBM na Alemanha e membro devoto do Partido Nazista, sabia qual era a sua função, com a ajuda dos tabuladores da IBM, no estudo de um povo alemão doente e no projeto de Adolf Hitler para a cura: “Nos parecemos muito com o médico, porque dissecamos, célula por célula, o corpo cultural alemão. Relatamos todas as características individuais... em um pequeno cartão”, disse ele em um discurso ardente dedicando uma nova fábrica da IBM em Berlim. “Temos orgulho de poder ajudar nessa tarefa, uma tarefa que fornece ao médico de nossa nação o material de que ele precisa para seus exames. Nosso médico pode então determinar se os valores calculados estão em harmonia com a saúde de nosso pessoal. Isso também significa que, se esse não for o caso, nosso médico poderá adotar procedimentos corretivos para corrigir as circunstâncias doentias... Salve o nosso povo alemão e o Fuhrer!”51

O uso da tecnologia da IBM na Alemanha nazista é um exemplo extremo, mas ressalta a conexão entre o desenvolvimento da tecnologia da computação inicial e o estudo e gerenciamento de grandes grupos de pessoas. Os tabuladores da IBM permaneceram em operação até os anos

1980. De fato, até J. C. R. Licklider e a ARPA desenvolverem sistemas de computação interativos, os tabuladores e cartões perfurados eram os principais meios pelos quais militares, agências governamentais e corporações escreviam programas e trabalhavam com conjuntos de dados complexos.

Não há dúvidas de que a pesquisa de computadores de Licklider na ARPA estava intimamente ligada à missão de contrainsurgência em expansão da instituição.52 Mas, em discussões internas com seus contratados da ARPA – engenheiros e cientistas sociais das principais universidades de todo os EUA –, Lick procurou enfatizar as aplicações militares de seu projeto de comando e controle, mudando o foco para a necessidade de desenvolver tecnologia de computador para aumentar a produtividade de seus colaboradores civis e seus parceiros.

Em uma carta a seus contratantes, Lick escreveu:

> O fato é que, a meu ver, os militares realmente precisam de soluções para a maioria dos problemas que surgirão se tentarmos fazer bom uso das instalações que estão surgindo. Espero que, em nossos esforços individuais, haja vantagens evidentes suficientes na programação e operação cooperativas para nos levar a resolver tais os problemas e, assim, criar a tecnologia de que os militares precisam. Quando os problemas surgem claramente no contexto militar e parecem não aparecer no contexto da pesquisa, a ARPA pode tomar medidas para lidar com eles de forma ad hoc. Do meu ponto de vista, no entanto, espero que muitos dos problemas sejam essencialmente os mesmos e essencialmente tão importantes no contexto da pesquisa quanto no contexto militar.53

Em um nível fundamental, a tecnologia de computador necessária para alimentar operações militares em curso não era diferente daquela necessária para cientistas e pesquisadores fazerem seu trabalho. Colaboração, coleta e compartilhamento de dados em tempo real, modelagem preditiva, análise de imagem, processamento de linguagem natural, controles e interfaces intuitivos e gráficos de computador – se as ferramentas desenvolvidas pelos terceirizados da ARPA funcionassem para eles e seus colegas acadêmicos, elas também funcionariam para os militares com apenas pequenas modificações. As forças armadas de hoje tomam isso como pressuposto: a tecnologia de computador é sempre de “uso

duplo", serve tanto para aplicações comerciais e militares. Minimizar o objetivo militar da ARPA teve a vantagem de aumentar a moral entre os cientistas da computação, que se empolgariam mais trabalhando numa tecnologia se acreditassem que ela não seria usada para bombardear pessoas.54

Após dois anos de trabalho na ARPA, Lick começou a ver os vários projetos de computação que ele havia implantado em todo o país – em universidades como UCLA, Stanford e MIT – como partes de uma unidade conectada maior: "centros de pensamento" de computadores que em algum momento do o futuro próximo seriam reunidos em uma única máquina de computação distribuída e unificada. Isso refletia a visão de uma sociedade em rede que ele havia esboçado em 1960: primeiro, você conecta os computadores poderosos por meio de uma rede de banda larga. Em seguida, você conecta os usuários a esses computadores com linhas telefônicas, antenas parabólicas ou sinais de rádio – qualquer que seja a tecnologia mais adequada às suas necessidades particulares. Não importa se as pessoas fazem login em casa, no trabalho, em um jipe atravessando as selvas do Vietnã ou em um bombardeiro furtivo que voa 16 quilômetros acima da União Soviética. "Nesse sistema, a velocidade dos computadores seria equilibrada, e o custo das memórias gigantescas e dos programas sofisticados seria dividido pelo número de usuários", escreveu. Em 1963, quatro anos após a publicação desse artigo, Lick começou timidamente a se referir a essa ideia como a "Grande Rede Intergaláctica". Fundamentalmente, sua visão para uma rede de computação interativa distribuída não é muito diferente da cara que a Internet tem hoje.55

Em 1964, dois anos depois de chegar à ARPA, Lick decidiu que havia cumprido sua missão de colocar em funcionamento o programa de Pesquisa de Comando e Controle da agência. Ele mudou sua família para o Condado de Westchester, em Nova York, para iniciar um bico confortável, dirigindo uma divisão de pesquisa na IBM.56 Pessoas mais jovens e enérgicas teriam que terminar o trabalho que havia começado.

A ARPANET

Lawrence Roberts tinha 29 anos quando se apresentou na divisão de Pesquisa de Comando e Controle da ARPA, dentro do Pentágono. O ano era 1966 e ele foi contratado para um grande e importante trabalho: tornar a Grande Rede Intergaláctica de Lick uma realidade.

Tudo estava funcionando novamente. A ARPA tinha uma variedade de projetos de computadores interativos e funcionais, operando em paralelo por todo o país, inclusive nos seguintes centros:

- Laboratório de Inteligência Artificial do MIT
- Projeto MAC do MIT
- Laboratório de Inteligência Artificial de Stanford
- Instituto de Pesquisa de Stanford
- Universidade Carnegie Mellon
- Universidade da Califórnia, em Irvine
- Universidade da Califórnia, em Los Angeles (UCLA)
- Universidade da Califórnia, em Berkeley.
- Universidade da Califórnia, em Santa Bárbara
- RAND Corporation
- Universidade de Utah

Estava na hora de conectar todos esses centros de computadores e fazê-los funcionar como uma unidade. O nome dado a ela foi ARPANET.

Roberts veio do Laboratório Lincoln do MIT, onde trabalhava em sistemas gráficos e de comunicação por computador. Alguns de seus colegas acharam que a atmosfera ali era sufocante. Dois deles ficaram zangados por causa da política do laboratório de proibir animais de estimação. “Eles queriam trazer um gato para o laboratório. O Lincoln não deixaria que eles trouxessem um gato. Aí acharam que isso era injusto; encontrariam, então, algum lugar onde os gatos fossem permitidos”, lembrou, observando ironicamente que os gatos não eram para companhia, mas para experiências abomináveis. “Foi realmente uma briga.

Eles queriam conectar os eletrodos no cérebro e sei lá mais o quê. O laboratório simplesmente não queria nada com isso.57

Mas Roberts não teve esse problema. Ele tinha uma testa larga, orelhas grandes e um jeito severo, porém calmo e medido de falar. Era um cara da matemática e da teoria. Ele avançou no Lincoln Lab, trabalhando em algoritmos inovadores, compactação de imagem e design de rede de dados. Ele conhecia Lick e foi inspirado por sua visão de uma rede universal capaz de reunir todos os tipos de sistemas. De fato, Roberts era um engenheiro de redes eficiente. “Em poucas semanas, ele memorizou o local onde trabalhava – um dos maiores e mais labirínticos edifícios do mundo. Passear pelo prédio era complicado pelo fato de certos corredores serem bloqueados como áreas restritas. Roberts arranjou um cronômetro e começou a cronometrar várias rotas para seus destinos frequentes”, escreveu Katie Hafner e Matthew Lyon em seu livro divertido e esquisito sobre a criação da Internet, “Onde os Magos ficam acordados até tarde”.58 Dentro do Pentágono, as pessoas começaram a chamar o caminho mais eficiente entre dois pontos de “Rota de Larry”.

Roberts gostava de construir redes, mas não do tipo social. Ele era reservado e socialmente avesso ao extremo. Nenhum de seus colegas de trabalho, nem mesmo os mais próximos, sabia muito sobre ele ou qualquer coisa sobre sua vida pessoal. Ele era obcecado por eficiência e gostava muito de ler rapidamente, estudando e aprimorando sua técnica a ponto de ler trinta mil palavras por minuto. “Ele pegava um livro e terminava em dez minutos. Era típico dele”, lembrou um de seus amigos.

A tarefa de Roberts era assustadora: conectar todos os projetos de computadores interativos da ARPA – ou seja, computadores fabricados por meia dúzia de empresas diferentes, incluindo um supercomputador ILLIAC único – em uma única rede. “Quase todos os itens possíveis de hardware e software de computadores estarão na rede. Este é o maior desafio do sistema, bem como sua característica mais importante”, afirmou Roberts.59

Pouco tempo depois de chegar à ARPA, ele convocou uma série de reuniões com um grupo central de terceirizadas e vários consultores externos para elaborar o projeto. As sessões reuniram uma mistura diversa de ideias e pessoas. Uma dos mais importantes foi Paul Baran, que havia trabalhado na RAND projetando sistemas de comunicação

para a força aérea que poderia sobreviver a um ataque nuclear.60 Com o tempo, o grupo chegou a um projeto: o ponto-chave da rede seria o que Roberts chamava de processadores de mensagens de interface, ou IMPs. Estes eram computadores dedicados que formariam o tecido conectivo da rede distribuída. Conectados por linhas telefônicas alugadas da AT&T, eles enviavam e recebiam dados, verificavam erros e garantiam que os dados chegassem ao destino com sucesso. Se parte da rede fosse desativada, os IMPs tentariam retransmitir as informações usando um caminho diferente. Os IMPs eram os gateways genéricos da rede da ARPA, funcionando independentemente dos computadores que os usavam. Diferentes marcas e modelos de computadores não precisavam ser projetados para se entender entre si – tudo o que eles precisavam era se comunicar com os IMPs. De certa forma, os IMPs foram os primeiros roteadores da Internet.

Finalmente, em julho de 1968, Roberts solicitou contrato para mais de cem empresas de computadores e militares. As ofertas voltaram de alguns dos maiores nomes do negócio: a IBM e a Raytheon estavam interessadas, mas o contrato foi finalmente fechado com uma empresa de pesquisa de computadores influente em Cambridge, Massachusetts, chamada Bolt, Beranek e Newman, onde a J. C. R. Licklider era executivo senior.61

O primeiro nó da ARPANET, alimentado pelos IMPs, foi lançado em 29 de outubro de 1969, ligando Stanford à UCLA.62 A primeira tentativa de conexão mal funcionou e caiu após alguns segundos, mas no mês seguinte também foram feitas conexões com a UC Santa Barbara e a Universidade de Utah. Seis meses depois, mais sete nós entraram em operação. No final de 1971, existiam mais de quinze nós. E a rede continuou crescendo.63

Em outubro de 1972, uma demonstração completa da ARPANET foi realizada na primeira Conferência Internacional sobre Comunicações por Computador em Washington, DC. Ela surpreendeu as pessoas. Os contratados da ARPA montaram uma sala com dezenas de terminais de computadores que podiam acessar computadores em todo o país e até um link em Paris. O software disponível para demonstração incluía um programa de simulação de tráfego aéreo, modelos climáticos e meteorológicos, programas de xadrez, sistemas de banco de dados e até um pro-

grama de robô psiquiatra chamado Eliza, que fornecia aconselhamento simulado. Os engenheiros corriam como crianças em um parque de diversões, impressionados com a forma como todas as diferentes partes se encaixavam perfeitamente e funcionavam como uma única máquina interativa.64

"Era difícil para muitos profissionais experientes na época aceitar o fato de que uma coleção de computadores, circuitos variados e nós de comutação de minicomputadores – uma quantidade de equipamentos cujo número passava cem – poderia funcionar em conjunto de maneira confiável. Mas a demonstração da ARPANET durou três dias e mostrou claramente em público que sua operação era confiável", lembrou Roberts. "A rede prestou serviço ultra-confiável a milhares de participantes durante toda a duração da conferência."65

Mesmo assim, nem todo mundo estava empolgado com o que a ARPA estava fazendo.

"O *polvutador* serve à classe dominante"

Era 26 de setembro de 1969, um dia tranquilo de outono na Universidade de Harvard. Mas nem tudo estava bem. Várias centenas de estudantes furiosos se reuniram no campus e marcharam para o escritório do reitor. Eles se amontoaram na entrada e se recusaram a sair. Um dia antes, quinhentos estudantes marcharam pelo campus, e um pequeno grupo de ativistas da organização Estudantes para uma Sociedade Democrática invadiu o Escritório de Relações Internacionais da universidade e forçou os administradores a saírem para a rua.66 Problemas semelhantes estavam acontecendo do outro lado do rio no MIT, onde os estudantes estavam realizando protestos e aulas públicas.67

Panfletos publicados em ambos os campi protestavam contra a "manipulação computadorizada de pessoas" e "a flagrante prostituição da ciência social para atender aos objetivos da máquina de guerra". Um folheto advertia: "Até que o complexo 'militares-ciência social' seja eli-

minado, os cientistas sociais ajudarão na escravização, e não na libertação, da humanidade".68

Contra o que exatamente os estudantes estavam protestando?

A ARPANET

O Vietnã é o exemplo mais flagrante da tentativa dos EUA de controlar os países subdesenvolvidos para seus próprios interesses estratégicos e econômicos. Essa política global, que impede os desenvolvimentos econômicos e sociais do terceiro mundo, se chama imperialismo.

Ao realizar essas políticas, o governo dos EUA não tem escrúpulos em montar um projeto que une MIT, Harvard, o Laboratório Lincoln e todo o complexo de pesquisa e desenvolvimento de Cambridge.69

No início daquele ano, ativistas da Estudantes por uma Sociedade Democrática descobriram uma proposta confidencial da ARPA escrita por ninguém menos que J. C. R. Licklider. O documento tinha quase cem páginas e descrevia a criação pela ARPA de um programa conjunto Harvard-MIT que ajudaria diretamente a missão de contrainsurgência da instituição. Ele foi chamado de Projeto Cambridge. Uma vez concluído, permitiria a qualquer analista de inteligência ou planejador militar conectado à ARPANET subir dossiês, transações financeiras, pesquisas de opinião, registros de bem-estar, históricos de antecedentes criminais e qualquer outro tipo de dados e analisá-los de formas bastante sofisticadas: peneirar toneladas de informações para gerar modelos preditivos, mapear relacionamentos sociais e executar simulações que poderiam prever o comportamento humano. O projeto enfatizou a necessidade do uso de analistas com o poder de estudar países do terceiro mundo e movimentos de esquerda.

Os alunos viram o Projeto Cambridge, e a grande ARPANET que se conectava a ele, como uma arma. Um panfleto distribuído no protesto do MIT explicava: "Toda a instalação de computadores e a rede da ARPA permitirá que o governo, pela primeira vez, consulte os dados relevantes de uma pesquisa com rapidez suficiente para ser usado nas decisões políticas. O resultado líquido disso será tornar o policial internacional de Washington mais eficaz na supressão de movimentos popu-

lares em todo o mundo. A chamada pesquisa básica a ser apoiada pelo Projeto CAM abordará questões como 'por que os movimentos camponeses ou grupos de estudantes se tornam revolucionários?'. Os resultados desta pesquisa também serão usados para suprimir movimentos progressivos." Outro folheto apresentava um anúncio falso que trazia uma representação visual desses receios. Ele apresentava "O polvutador", um computador em forma de polvo que tinha tentáculos atingindo todos os setores da sociedade. "Os braços do polvo são longos e fortes", dizia a cópia do anúncio falso. "Ele fica no meio da sua universidade, do seu país, e lança mãos amigas em todas as direções. De repente, seu império trabalha mais. Cada vez mais os seus agentes usam o computador – resolvendo mais problemas, descobrindo mais fatos."71

Para os ativistas, o Projeto Cambridge da ARPA fazia parte de um sistema em rede de vigilância, controle político e conquista militar, sendo silenciosamente montado por pesquisadores e engenheiros diligentes em campi de faculdades em todo o país. E os universitários tinham razão.

O Projeto Cambridge – também conhecido como Projeto CAM – nasceu de uma ideia proposta em 1968 por Licklider e seu colega de longa data Ithiel de Sola Pool, professor de ciências políticas do MIT e especialista em propaganda e operações psicológicas.

Como chefe do projeto de Pesquisa de Comando e Controle da ARPA e do programa de Ciências do Comportamento, Lick viu como a agência lutava com as montanhas de dados gerados por suas iniciativas de contrainsurgência no sudeste da Ásia. Um dos principais objetivos de seu trabalho durante sua breve passagem pela ARPA foi iniciar um programa que acabaria por construir os sistemas básicos que poderiam tornar a contrainsurgência auxiliada por computador e o comando e controle mais eficientes: ferramentas que ingerem e analisam dados, criam bancos de dados pesquisáveis, constroem modelos preditivos e permitem que as pessoas compartilhem essas informações através de longas distâncias. Pool foi movido pela mesma paixão.

Pool, descendente de uma família rabínica proeminente que tinha suas raízes na Espanha medieval. Ele era um professor do MIT e renomado especialista em comunicação e teoria da propaganda. A partir do final da década de 1950, ele dirigiu o Centro de Estudos Internacionais

do MIT, um prestigiado departamento de estudos de comunicação financiado pela CIA e ajudou a criar o Departamento de Ciência Política do MIT. Era um anticomunista incondicional e pioneiro no uso de pesquisas de opinião e modelagem de computadores para campanhas políticas. Com sua experiência, ele foi escolhido para orientar as mensagens da candidatura presidencial de John F. Kennedy em 1960, analisando os números das pesquisas e realizando simulações sobre questões e grupos de eleitores. A abordagem orientada a dados de Pool para as campanhas políticas estava na vanguarda de uma nova onda de tecnologias eleitorais que buscavam vencer, testando as preferências e os preconceitos das pessoas e depois calibrando a mensagem de um candidato para se adequar a elas. Essas novas táticas de mensagens direcionadas, habilitadas por computadores rudimentares, tinham muitos fãs em Washington e, nas próximas décadas, dominariam a maneira como a política era feita.72 Eles também inspiraram o medo de que o sistema político dos EUA estivesse sendo assumido por tecnocratas manipuladores que se preocupavam mais com o marketing e a venda de ideias do que com o que essas ideias realmente significavam.73

Pool era muito mais que um pesquisador de campanha; ele também era especialista em propaganda e operações psicológicas e tinha laços estreitos com os esforços de contrainsurgência da ARPA no sudeste da Ásia, na América Latina e na União Soviética.74 De 1961 a 1968, sua empresa, a Simulmatics Corporation, trabalhou nos programas de contrainsurgência da ARPA no Vietnã do Sul como parte do Projeto Agile de William Godel, incluindo um grande contrato para estudar e analisar a motivação dos rebeldes vietnamitas capturados e desenvolver estratégias para conquistar a lealdade dos camponeses do Vietnã do Sul. O trabalho de Pool no Vietnã ajudou ainda mais a propagar a ideia de que uma solução puramente técnica poderia acabar com a insurgência. “A Simulmatics dependia muito do trabalho do colega de Pool, Lucian Pye, que havia argumentado desde o início da década de 1950 que o comunismo era uma doença psicológica dos povos em transição. Em sua influente obra ‘Política, Personalidade e Construção da Nação’, explicou que as falhas psicológicas estão na raiz dos esforços de construção da nação”, escreve o historiador Joy Rohde em “The Last Stand of the Psychocultural Cold Warriors”. “Para vencer a guerra por corações e mentes, os estadunidenses precisavam projetar uma infraestrutura política

psicologicamente apropriada para a nação emergente – uma estrutura através da qual os camponeses desenvolveriam os laços psicológicos apropriados com o Estado... A pesquisa militar escreveria o protocolo para algo como uma terapia nacional."75

Ao mesmo tempo em que os contratados da Simulmatics coletavam dados nas selvas sufocantes do Vietnã, a empresa de Pool trabalhava em outra iniciativa da ARPA chamada Projeto ComCom, abreviação de "Communist Communications". Operado fora da base de Pool no MIT, o ComCom foi uma tentativa ambiciosa de construir uma simulação em computador do sistema de comunicações internas da União Soviética. O objetivo era estudar os efeitos que as notícias e transmissões de rádio estrangeiras estavam causando na sociedade soviética, bem como modelar e prever o tipo de reação que uma transmissão em particular – digamos, um discurso presidencial ou um programa de notícias de última hora – teria sobre a União Soviética.76 Sem surpresa, os modelos de Pool mostraram que as tentativas secretas da CIA de influenciar a União Soviética transmitindo propaganda pelo rádio estavam tendo um grande efeito, e que esses esforços precisavam ser intensificados. "A maioria das coisas de caráter positivo que estão acontecendo hoje na União Soviética são explicáveis apenas em termos da influência do Ocidente, para a qual o canal único e muito importante é o rádio", disse Pool num discurso explicando os resultados dos estudos do ComCom. "A longo prazo, aqueles que estão falando com a União Soviética não estarão falando para pessoas que não querem ouvir. Suas vozes serão ouvidas e farão muita diferença."77

Mas Pool nunca ficou satisfeito com o desempenho do ComCom. Mesmo no final da década de 1960, o estado bruto da tecnologia de computadores levou vários meses para ele e sua equipe criarem um modelo para apenas uma situação.78 Foi um trabalho meticuloso que claramente exigia ferramentas de computador mais poderosas – ferramentas que simplesmente não existiam.

Pool considerava os computadores mais do que apenas aparelhos capazes de acelerar a pesquisa social. Seu trabalho foi influenciado por uma crença utópica no poder dos sistemas cibernéticos de gerenciar sociedades. Ele vivia entre um grupo de tecnocratas da Guerra Fria que imaginava a tecnologia da computação e os sistemas de rede implanta-

dos de uma maneira que interferisse diretamente na vida das pessoas, criando um tipo de rede de segurança que abrangia o mundo e ajudava a administrar as sociedades de maneira harmoniosa, gerenciando conflitos e extirpando revoltas. Esse sistema não seria confuso, feito de qualquer jeito ou aberto à interpretação; nem envolveria teorias econômicas socialistas. De fato, não envolveria política de nenhuma maneira, mas seria uma ciência aplicada baseada em matemática, "um tipo de engenharia".

Em 1964, ao mesmo tempo em que sua empresa fazia um trabalho de contrainsurgência para a ARPA no Vietnã, Pool tornou-se um forte defensor do Projeto Camelot, um esforço diferente de contrainsurgência financiado pelo Exército dos EUA e apoiado em parte pela ARPA.79 "Camelot" era apenas um codinome. O título oficial completo do projeto era "Métodos para prever e influenciar mudanças sociais e potencial de guerra interna". Seu objetivo final era construir um sistema de radar para detectar revoluções de esquerda – um sistema informatizado de alerta antecipado que pudesse prever e impedir movimentos políticos antes que eles decolassem.80 "Um dos produtos finais esperados do projeto era um 'sistema de coleta e manuseio de informações' automatizado, no qual pesquisadores sociais podiam fornecer fatos para uma análise rápida. Essencialmente, o sistema de computador verificaria informações de inteligência atualizadas em relação a uma lista de agitadores e pré-condições", escreve o historiador Joy Rohde. "A revolução poderia ser interrompida antes que seus iniciadores soubessem que estavam seguindo o caminho da violência política".81

O Projeto Camelot era uma grande empresa que envolvia dezenas de acadêmicos estadunidenses importantes. Pool tinha um carinho pessoal grande por ele, mas nunca foi muito longe.82 Acadêmicos chilenos convidados a participar do Projeto Camelot denunciaram seus laços com a inteligência militar e acusaram os Estados Unidos de tentarem construir uma máquina de golpes de Estado assistida por computador. O caso explodiu em um enorme escândalo. Uma sessão especial do senado chileno foi convocada para investigar as alegações, e os políticos denunciaram a iniciativa como "um plano de espionagem ianque".83 Com toda essa atenção internacional e publicidade negativa, o Projeto Camelot foi fechado em 1965.

Em 1968, o Projeto Cambridge de Lick no MIT começou de onde Camelot parou.84

Para Lick, o Projeto Cambridge significava trazer para a realidade a tecnologia de computador interativa que ele estava buscando. Finalmente, depois de quase uma década, a tecnologia da computação avançou a um ponto em que poderia ajudar os militares a usar dados para combater insurgências. O Projeto Cambridge incluía vários componentes. Ele administrava um sistema operacional comum e um conjunto de programas padrão personalizados para a "missão científica comportamental" das forças armadas que podiam ser acessados a partir de qualquer computador com uma conexão à ARPANET. Era uma espécie de versão simplificada do Palantir dos anos 1960, o poderoso software de mineração de dados, vigilância e previsão que os planejadores militares e de inteligência usam hoje. O projeto também financiou vários esforços para usar esses programas de maneiras favoráveis aos militares, incluindo a compilação de vários bancos de dados de inteligência. Como bônus, o Projeto Cambridge serviu de campo de treinamento para um novo quadro de cientistas de dados e planejadores militares que aprenderam a ser proficientes na mineração de dados.

O Projeto Cambridge tinha ainda outro lado, menos ameaçador. Analistas financeiros, psicólogos, sociólogos, agentes da CIA – o Projeto Cambridge foi útil para qualquer pessoa interessada em trabalhar com conjuntos de dados grandes e complexos. A tecnologia era de uso universal e duplo. Então, em um nível, o objetivo do Projeto Cambridge era genérico. Ainda assim, ele foi personalizado para as necessidades dos militares, com foco especial no combate às insurgências e na reversão do comunismo. Grande parte da proposta que Lick apresentou à ARPA em 1968 se concentrou nos vários tipos de "bancos de dados" que o Projeto Cambridge compilaria e disponibilizaria para analistas militares e cientistas comportamentais conectados através da ARPANET: 85

• Pesquisas de opinião pública de todos os países

• Padrões culturais de todas as tribos e povos do mundo

• Arquivos sobre comunismo comparado (...) arquivos sobre os movimentos comunistas do mundo contemporâneo

• Participação política de vários países. Isso inclui variáveis como votação, participação em associações, atividade de partidos políticos, etc.

• Movimentos da juventude

• Agitação das massas e movimentos políticos em condições de rápida mudança social

• Dados sobre integração nacional, particularmente em sociedades "plurais"; a integração de minorias étnicas, raciais e religiosas; a fusão ou divisão das unidades políticas presentes

• Produção internacional de propaganda

• Atitudes e comportamento camponeses

• Despesas e tendências internacionais de armamento

Era claro que o Projeto Cambridge não era apenas uma ferramenta de pesquisa, era uma tecnologia de contrainsurgência.

No final dos anos 1960 e início dos anos 1970, grandes protestos contra a guerra eclodiram nos campi universitários de todo os EUA. Ativistas ocuparam prédios, roubaram documentos, publicaram boletins, abstruíram locais sentando no chão, realizaram marchas, entraram em conflito com a polícia e tornaram-se cada vez mais violentos. Na Universidade de Michigan, os estudantes tentaram bloquear o recrutamento no campus pela Dow Chemical, que produziu o napalm que choveu no Vietnã. Alguém explodiu o Centro de Pesquisa em Matemática do Exército na Universidade de Wisconsin.87 O grupo Weather Underground detonou uma bomba dentro do Centro de Relações Internacionais de Harvard. Eles queriam parar a Guerra do Vietnã. Eles também queriam interromper a cooptação da pesquisa acadêmica pelo complexo industrial militar.

Os programas da ARPA eram um alvo constante. Os estudantes protestaram contra o ILLIAC-IV, o supercomputador da ARPA, localizado na Universidade de Illinois.89 Eles tiveram como alvo o Instituto de Pesquisas de Stanford (SRI), um importante contratado da ARPA

envolvido em tudo, desde a pesquisa de armas químicas ao trabalho de contrainsurgência e desenvolvimento da ARPANET. Os estudantes ocuparam o prédio, gritando: “Fora o SRI!” e “Abaixo o SRI!” Alguns terceirizados corajosos ficaram para trás para proteger os computadores da ARPA contra multidão enfurecida,90 dizendo aos manifestantes que os computadores eram “politicamente neutros”.91 Mas eles são mesmo?

As manifestações estudantis contra o Projeto Cambridge fizeram parte dessa onda de protestos que varreram o país. A crença comum entre os estudantes do MIT e Harvard era que o Projeto Cambridge, e mais do que ele, a rede ARPA à qual estava vinculado, eram essencialmente uma frente para a CIA. Até alguns professores começaram a se interessar.92 A linguagem da proposta de Licklider – falar sobre propaganda e monitorar movimentos políticos – era tão direta e tão óbvia que não podia ser ignorada. Na proposta, ele confirmava o medo de estudantes e ativistas em relação a computadores e suas redes e deu-lhes um vislumbre de como os planejadores militares queriam usar essas tecnologias como ferramentas de vigilância e controle social.

Uma equipe de ativistas dos Estudantes para uma Sociedade Democrática produziu um livreto pequeno, mas informativo, que expunha a oposição do grupo à iniciativa: ‘Projeto Cambridge: Ciências Sociais para o Controle Social’. Foi vendido por um quarto de dólar. A capa apresentava uma série de cartões perfurados sendo alimentados em um computador que transformava “Militância Negra”, “Protesto de Estudantes”, “Greves” e “Lutas pelo Bem-Estar” em “Contrainsurgência”, “Pacificação do Gueto” e “Quebra de Greve”.93 A certa altura, os produtores do panfleto se reuniram na Technology Square, nos limites do campus do MIT. Eles obtiveram uma cópia da proposta do Projeto Cambridge de Lick e atearam fogo nela. Lick, sempre entusiasmado e confiante em sua capacidade de convencer as pessoas do seu modo de pensar, encontrou os estudantes que protestavam do lado de fora e tentou tranquilizá-los de que tudo estava bem – que esse projeto da ARPA não era uma iniciativa nefasta criada por espiões e generais. Mas os estudantes não engoliram.

“O grupo era hostil”, disse Douwe Yntema, diretor do Projeto Cambridge, a M. Waldrop.94 “Mas ele [Licklider] estava bem de boa com isso. A certa altura, eles tinham uma cópia da proposta e tentaram

atear fogo nela – sem muito sucesso. Então, depois de alguns minutos, Lick disse: 'Olha, se você quiser queimar uma pilha de papel, não tente acendê-la de uma vez. Espalhe as páginas primeiro.' Aí, ele mostrou a eles como fazer, e realmente queimou muito melhor!"

Mas os estudantes reunidos ali tinham um profundo entendimento das dimensões políticas e econômicas da pesquisa militar da ARPA, e não seriam dispensados como crianças bagunceiras da pré-escola. Eles persistiram. Lick tentou levar na esportiva, mas ficou desapontado.95 Não com o projeto, mas com os estudantes. Ele acreditava que os manifestantes não entendiam o projeto e interpretavam mal suas intenções e os laços militares. Por que os jovens não conseguiam entender que essa tecnologia era completamente neutra? Por que eles tinham que politizar tudo? Por que eles achavam que os EUA sempre eram inimigos e usariam a tecnologia para controle político? Ele viu a coisa toda como um sintoma da degradação da cultura jovem gringa.

As manifestações contra o Projeto Cambridge envolveram centenas de pessoas. Em última análise, eles fizeram parte do maior movimento antiguerra do MIT e de Harvard, que atraiu as principais luzes do movimento antiguerra, incluindo Howard Zinn. Noam Chomsky apareceu para criticar os acadêmicos, acusando-os de encobrir o imperialismo violento "investindo-o na aura da ciência".96 Mas, no final, os protestos não tiveram muito efeito. O Projeto Cambridge prosseguiu conforme o planejado. As únicas mudanças foram que as novas propostas e discussões internas para financiamento omitiam referências claras a aplicações militares e ao estudo do comunismo e das sociedades do terceiro mundo, e os terceirizados do projeto simplesmente se referiam ao que estavam fazendo como "ciência comportamental".

Mas nos bastidores, a dimensão militar e de inteligência do projeto permaneceu em primeiro lugar. De fato, um guia secreto de 1973 encomendado pela ARPA para a Agência Central de Inteligência observou que, embora o Projeto Cambridge ainda fosse experimental, ele era "uma das ferramentas mais flexíveis" disponíveis para dados complexos e análises estatísticas existentes, e recomendava que os analistas de segurança internacional da CIA aprendessem como usá-la.97

O Projeto Cambridge durou um total de cinco anos. Como o tempo provaria, os estudantes estavam certos em temê-lo.

Capítulo 3

Espionando os gringos

A criação de mitos históricos é apenas
possível através do esquecimento.
- *Nancy Isenberg, White Trash (Lixo Branco)*

Em 2 de junho de 1975, o correspondente da NBC Ford Rowan apareceu no noticiário da noite para relatar uma investigação impressionante. Com seu rosto de bebê e olhos azuis claros, ele falou diretamente para a câmera e disse aos espectadores que os militares dos EUA estavam construindo uma sofisticada rede de comunicações por computador e estavam-na usando para espionar os estadunidenses e compartilhar dados de vigilância com a CIA e a NSA.1 Ele estava falando sobre a ARPANET.

"Nossas fontes dizem que as informações do Exército sobre milhares de manifestantes estadunidenses foram dadas à CIA, e algumas delas estão nos computadores da CIA agora. Não sabemos quem deu a ordem para copiar e manter os arquivos. O que sabemos é que, uma vez que os arquivos são informatizados, a nova tecnologia do Departamento de Defesa facilita incrivelmente a movimentação de informações de um computador para outro", relatou Rowan. "Essa rede conecta computadores na CIA, na Agência de Inteligência de Defesa, na Agência de Segurança Nacional, em mais de 20 universidades e em uma dúzia de centros de pesquisa, como a RAND Corporation."

Rowan passou meses reunindo a história de vários "delatores relutantes" – incluindo terceirizados da ARPA que ficaram alarmados com a forma como a tecnologia que estavam construindo estava sendo usada. Por três dias após a história inicial, ele e seus colegas do noticiá-

rio da noite da NBC exibiram vários outros relatórios examinando mais de perto essa misteriosa rede de vigilância e a agência sombria que a construíra.

O principal avanço na nova tecnologia de computador foi realizada em uma unidade pouco conhecida do Departamento de Defesa – a Agência de Projetos de Pesquisa Avançada, ARPA.

Os cientistas da ARPA desenvolveram algo novo no campo das comunicações entre computadores, conhecido como IMP, o processador de mensagens da interface. Computadores diferentes se comunicam em diferentes idiomas. Antes do IMP, era extremamente difícil, em muitos casos impossível, vincular os vários computadores. O IMP, na verdade, traduz todas as mensagens do computador para um idioma comum. Isso torna muito fácil vinculá-los em uma rede.

O governo dos EUA agora está usando essa nova tecnologia em uma rede secreta de computadores que dá à Casa Branca, à CIA e ao Departamento de Defesa acesso aos arquivos de computador do FBI e do Departamento do Tesouro de 5 milhões de estadunidenses.

A rede, e ela é conhecida como “a rede”, está agora em operação... Isso significa que, a partir de terminais de computador atualmente instalados na Casa Branca, na CIA ou no Pentágono, um funcionário pode pressionar um botão e obter qualquer informação que possa existir sobre você nos vastos arquivos de computador do FBI. Esses arquivos incluem registros de agências policiais locais que são conectadas ao FBI por computador.2

A investigação de Rowan foi fenomenal. Baseava-se em fontes sólidas do Pentágono, da CIA e do Serviço Secreto, bem como de membros importantes da ARPANET, alguns dos quais estavam preocupados com a criação de uma rede que pudesse ligar de maneira tão perfeita vários sistemas de vigilância do governo. Na década de 1970, o significado histórico da ARPANET ainda não era aparente; o que Rowan descobriu se tornou mais relevante somente em retrospectiva. Levaria mais de vinte anos para a Internet se espalhar pela maioria dos lares estadunidenses, e quatro décadas se passariam antes que os vazamentos de Edward Snowden fizessem o mundo ciente da enorme quantidade de vigilância governamental que estava acontecendo na Internet. Hoje, as

pessoas ainda pensam que a vigilância é algo estranho à Internet – algo imposto de fora por agências governamentais paranoicas. Os relatórios de Rowan, há quarenta anos, contam uma história diferente. Ele mostra como as agências militares e de inteligência usaram a tecnologia de rede para espionar os estadunidenses na primeira versão da Internet. A vigilância estava lá desde o início.

Este é um fato importante na história da Internet. No entanto, ele desapareceu da memória coletiva. Busque qualquer história popular da Internet e não haverá menção a ele. Até os principais historiadores de hoje parecem não saber que isso ocorreu.3

A contrainsurgência chega em casa

No final da década de 1960, enquanto engenheiros do MIT, da UCLA e de Stanford trabalhavam diligentemente para construir uma rede militar unificada de computadores, o país convulsionava com violência e políticas radicais – muitas delas direcionadas contra a militarização da sociedade estadunidense, exatamente o que a ARPANET representava. Esses foram alguns dos anos mais violentos da história dos EUA. Revoltas raciais, ativismo militante dos negros, poderosos movimentos estudantis de esquerda e atentados quase diários nas cidades de todo o país.4 Os Estados Unidos eram uma panela de pressão e o calor continuava aumentando. Em 1968, Robert Kennedy e Martin Luther King Jr. foram assassinados, sendo que a morte deste último provocou revoltas em todo o país. Protestos contra a guerra varreram os campus universitários. Em novembro de 1969, trezentas mil pessoas foram a Washington, DC, para o maior protesto antiguerra da história dos Estados Unidos.5 Em maio de 1970, a Guarda Nacional de Ohio disparou contra manifestantes da Universidade Estadual de Kent, matando quatro estudantes – episódio que foi chamado de “Massacre de Nixon”, por Hunter S. Thompson.

Para muitos, parecia que os Estados Unidos estavam prestes a explodir. Em janeiro de 1970, um ex-oficial da inteligência militar chamado Christopher Pyle jogou mais lenha na fogueira.

Pyle foi aluno de doutorado em ciências políticas na Universidade de Columbia. Ele usava óculos, tinha uma mecha de cabelo jogada para o lado e se comportava com a maneira meticulosa e atenciosa de um acadêmico. Ele havia sido instrutor da Escola de Inteligência do Exército dos EUA em Fort Holabird, nos arredores de Baltimore. Ali, viu algo que o preocupava o suficiente para que ele tivesse que fazer uma denúncia.6

No início de 1970, ele publicou uma investigação no jornal Washington Monthly que revelou uma operação maciça de vigilância e contrainsurgência, administrada pelo Comando de Inteligência do Exército dos EUA. Conhecido como "CONUS Intel" – Inteligência Continental dos Estados Unidos – o programa envolveu milhares de agentes secretos. Eles se infiltraram em grupos e movimentos políticos antiguerra, espionaram ativistas de esquerda e enviaram relatórios para um banco de dados centralizado de inteligência sobre milhões de estadunidenses.7 “Quando esse programa começou no verão de 1965, seu objetivo era fornecer um alerta sobre possíveis desordens civis para que o Exército pudesse depois ser chamado para reprimi-las”, relatou Pyle. “Hoje, o Exército mantém arquivos sobre os filiação, ideologia, programas e práticas de praticamente todos os grupos políticos ativistas do país.”

O CONUS Intel foi idealizado em parte pelo general William P. Yarborough, o principal oficial de inteligência do exército na época. Ele teve uma longa e distinta carreira em contrainsurgência e operações psicológicas, da Segunda Guerra Mundial aos conflitos na Coreia e no Vietnã. Em 1962, o general Yarborough participou do influente simpósio de contrainsurgência sobre “guerra limitada” do Exército dos EUA, realizado em Washington, DC, ao qual também participou J. C. R. Licklider.8 O medo de uma insurgência doméstica assombrava os círculos militares, e o general não estava imune. Ele chegou a acreditar que existia uma crescente conspiração comunista para fomentar agitações e derrubar o governo dos Estados Unidos por dentro. Qual evidência ele acreditava provar isso? O florescente movimento dos direitos civis e a crescente popularidade de Martin Luther King Jr.

Yarborough olhou para as massas de pessoas que lutavam por igualdade racial e não viu cidadão a se envolver politicamente por causa

de demandas e preocupações legítimas. Ele viu impostores e agentes estrangeiros que, quer eles percebessem ou não, faziam parte de uma sofisticada operação de insurgência financiada e dirigida pela União Soviética. Essa não era a opinião de um único maluco, mas foi compartilhada por muitos colegas de Yarborough no exército.9

Quando tumultos raciais eclodiram em Detroit, em 1967, alguns meses após Martin Luther King proferir um discurso tentando unir os movimentos de direitos civis e antiguerra, Yarborough disse a seus subordinados no Comando de Inteligência do Exército dos EUA: "Homens, peguem seus manuais de contrainsurgência. Temos uma acontecendo debaixo dos nossos narizes".10

William Godel criara o Projeto Agile da ARPA para combater insurgências no exterior. O general Yarborough concentrou-se em uma extensão dessa mesma missão: combater o que via como uma insurgência estrangeira em solo gringo. Assim como no Vietnã, sua primeira ordem de trabalho foi acabar com as bases de apoio locais dos insurgentes. Mas antes que ele pudesse começar a limpar as ervas daninhas, seus homens precisavam de informações. Quem eram esses insurgentes? O que os motivou? Quem deu os tiros? Quem eram seus aliados domésticos? Em quais grupos eles se escondiam?

Para erradicar o inimigo, o general Yarborough supervisionou a criação do CONUS Intel. Padres, funcionários eleitos, instituições de caridade, programas de contra-turno escolar, grupos de direitos civis, manifestantes contra a guerra, líderes trabalhistas e grupos de direita como Ku Klux Klan e a Sociedade John Birch foram alvos. Mas parecia que o foco principal do CONUS Intel era Esquerda: qualquer um que parecesse simpático à causa da justiça econômica e social. Não importava se eram clérigos, senadores, juízes, governadores, radicais de cabelos compridos da organização Estudantes para uma Sociedade Democrática ou membros dos Panteras Negras – todos eram a mesma coisa.11

No final dos anos 1960, o CONUS Intel envolveu milhares de agentes. Eles compareceram em tudo e relataram até o menor dos protestos num momento em que os eles eram tão comuns quanto a venda de pipoca Bilu. Eles monitoraram greves trabalhistas e anotaram grupos e

indivíduos que apoiavam sindicatos. Grampearam o telefone do senador Eugene McCarthy, crítico da Guerra do Vietnã, na Convenção Nacional Democrata de 1968. Eles notaram que o senador havia recebido uma ligação de um "grupo radical conhecido" para discutir a prestação de assistência médica a manifestantes que haviam sido feridos pela polícia de Chicago. No mesmo ano, agentes se infiltraram em uma reunião de padres católicos que protestaram contra a proibição da igreja de controlar a natalidade. Eles espionaram o funeral de Martin Luther King, misturando-se com os enlutados e gravando o que se falou. Se infiltraram no festival do Dia da Terra de 1970, tiraram fotografias e preencheram relatórios sobre o que os ativistas antipoluição estavam discutindo e fazendo.12

Alguns de seus alvos de vigilância eram absolutamente cômicos. Um jovem recruta do Exército do Quinto Destacamento de Inteligência Militar em Fort Carson, Colorado, foi designado para espionar o Projeto Jovens Adultos, criado por grupos da igreja e um clube de esqui que promovia a recreação de "jovens emocionalmente perturbados".13 Qual foi o motivo pelo qual fora designado? Aparentemente, o clero local não gostou da relação do projeto com as ideias hippies e achou que seus líderes estavam levando esses jovens a "drogas, música alta, sexo e radicalismo".14 Quais eram as evidências condenatórias que provavam que esse grupo fazia parte de uma conspiração nefasta para derrubar os Estados Unidos? Um de seus fundadores havia participado de um comício antiguerra na frente da base militar de Fort Carson.15 Em seguida, em 1968, agentes foram obrigados a relatar a Marcha dos Pobres em Washington – e a prestar especial atenção às nádegas das mulas. Os animais da tropa eram usados para puxar carroças cobertas do sul rural, e o exército queria que seus espiões procurassem feridas ou marcas nas peles dos animais que pudessem mostrar sinais de abuso. A ideia era acusar e processar os manifestantes por crueldade com os animais.16

Grande parte da justificativa para a vigilância de suspeitos de serem "agentes estrangeiros" era fraca ou inexistente, mas não importava. Quando os agentes do exército falharam em encontrar evidências de orquestração comunista, seus comandantes disseram-lhes para voltarem lá e se esforçarem mais: "Você não olhou o suficiente. Tem que estar aí".17

Os agentes do CONUS Intel usavam todo tipo de tática para espionar e se infiltrar em grupos considerados ameaças aos EUA. Os agentes deixaram os cabelos crscerem, juntaram-se a grupos e marcharam em movimentos. Eles até criaram uma frente de mídia "legítima": Mid-West News. Usando crachás de imprensa, agentes se apresentaram como repórteres e participaram de protestos, fotografaram participantes e conseguiram entrevistas com manifestantes e organizadores. O exército tinha até seu próprio caminhão de som e TV para filmar protestos.18

Em uma entrevista, quarenta e cinco anos depois de denunciar esse programa de vigilância, Christopher Pyle me disse:

> Os generais queriam ser consumidores das últimas inotícias mais quentes. Durante os distúrbios de Chicago em 1968, o exército tinha uma unidade chamada Mid-West News com agentes do exército a paisana. Eles andaram por aí entrevistando todos os manifestantes antiguerra. Então, enviavam as filmagens para Washington todas as noites em um avião, para que os generais pudessem ver vídeos do que estava acontecendo em Chicago quando chegassem ao trabalho pela manhã. Isso os fez tão felizes. Foi uma perda de tempo total. Você poderia ver a mesma coisa na TV por muito menos, mas eles achavam que precisavam de sua própria equipe de filmagem. A principal coisa que eles investigavam era um porco chamado Pigasus, candidato dos Yippies à presidência. Eles estavam realmente empolgados com o Pigasus."19

A vigilância de ativistas de esquerda e grupos políticos não era novidade. Voltando ao século XIX, as agências policiais, locais e federais, mantinham arquivos sobre líderes trabalhistas e sindicais, socialistas, ativistas de direitos civis e qualquer pessoa suspeita de ter simpatia com a esquerda. O Departamento de Polícia de Los Angeles mantinha um arquivo enorme sobre suspeitos de serem comunistas, organizadores do trabalho, líderes negros, grupos de direitos civis e celebridades. Todas as outras grandes cidades gringas tinham seu próprio "esquadrão vermelho" e extensos arquivos.20 Empresas privadas e grupos de justiceiros de direita como a Sociedade John Birch também mantinham seus próprios arquivos. Na década de 1960, a empresa de segurança privada Wackenhut se gabava de ter dois milhões de estadunidenses sob vigilância.21 Essas informações eram compartilhadas livremente com o FBI e

os departamentos de polícia, mas geralmente eram armazenadas à moda antiga: em papel nos armários de arquivos. O banco de dados do Exército dos EUA era diferente. Tinha o apoio de um orçamento ilimitado do Pentágono e acesso às mais recentes tecnologias de computador.

As denúncias de Pyle revelaram que os dados de vigilância do CONUS Intel foram codificados nos cartões perfurados da IBM e alimentados em um computador digital localizado no centro do Corpor de Contrainteligência do Exército, em Fort Holabird, equipado com um link de terminal que poderia ser usado para acessar quase cem diferentes categorias de informações, bem como imprimir relatórios sobre pessoas individualmente. “Os relatórios de personalidade – a serem extraídos dos relatórios de incidentes – serão usados para suplementar os sete milhões de dossiês secretos de segurança sobre indivíduos, coletados e organizados pelo Exército, e para gerar novos arquivos sobre as atividades políticas de civis totalmente não associados às forças armadas”, escreveu no Washington Monthly.22 “Nesse sentido, o banco de dados do Exército tem tudo para ser único, em termos de valor. Ao contrário de computadores similares atualmente em uso no Centro Nacional de Informações sobre Crimes do FBI em Washington e no Sistema de Identificação e Inteligência do Estado de Nova York em Albany, ele não será restrito ao armazenamento de histórias de casos de pessoas presas ou condenadas por crimes. Em vez disso, se especializará em arquivos dedicados exclusivamente às descrições da atividade política legal dos civis.”

O Totalitarismo de Big Data

A partir do final da década de 1960, iniciou-se a corrida do ouro da informatização nos Estados Unidos, uma época em que departamentos de polícia, agências do governo federal, serviços militares e de inteligência e grandes empresas começaram a digitalizar suas operações. Eles compraram e instalaram computadores, administraram bancos de dados, realizaram cálculos imensos, automatizaram serviços e conectaram computadores via redes de comunicação. Todos estavam com pressa de digi-

talizar, conectar-se e participar da gloriosa revolução dos computadores.23

Bancos de dados digitais do governo surgiram em todo o país.24 Naturalmente, o Escritório Federal de Investigação (Federal Bureau of Investigation, FBI) saiu na frente. Começaram a construir um banco de dados digital centralizado em 1967, por ordem de J. Edgar Hoover. Chamado de Centro Nacional de Informações sobre Crime, ele abrangia todos os cinquenta estados e estava disponível para órgãos estaduais e locais de aplicação da lei. Continha informações sobre mandados de prisão, veículos e propriedades roubados e registros de armas. Ele era acessível através de um serviço de despachante. Em meados da década de 1970, o sistema foi expandido para suportar terminais com teclado instalados em viaturas policiais para busca e consulta imediata de dados.25

À medida que o banco de dados do FBI crescia, ele podia ser acessado e se conectava aos bancos de dados policiais locais que estavam surgindo em todo o país, sistemas como o construído no condado de Bergen, Nova Jersey, no início dos anos 1970. Lá, o xerife e os departamentos de polícia locais reuniram recursos para criar a Rede Regional de Informações para Policiamento, um sistema de banco de dados informatizado que digitalizou e centralizou registros de prisões, acusações, mandados, suspeitos e informações de propriedades roubadas de todo o condado. O banco de dados era executado em um IBM 360/40 e as agências participantes puderam acessá-lo em terminais de computadores locais. O sistema estava vinculado aos bancos de dados da polícia estadual e do FBI, o que permitia às agências locais consultar rapidamente registros do condado, do estado e da base federal.26

Ao mesmo tempo, foram feitas várias tentativas para configurar bancos de dados nacionais que ligassem e centralizassem todos os tipos de dados os mais variados. Eles tinham nomes como “Banco de Dados Nacional” e FEDNET.27 Em 1967, a Receita Federal desejava construir o Centro Nacional de Dados, um banco de dados federal centralizado que reuniria, entre outras coisas, registros de imposto de renda e de prisões, dados sobre saúde, status militar, informações do seguro social e transações bancárias. Tudo isso seria combinado num número exclusivo que serviria como número de identificação vitalício e número de telefone permanente de uma pessoa.28

Não só os policiais locais e federais correram para se informatizar. A empresa Corporate America adotou com entusiasmo os bancos de dados digitais e os computadores em rede para aumentar a eficiência e reduzir os custos de mão de obra. Empresas de cartão de crédito, bancos, agências de classificação de crédito e companhias aéreas começaram a digitalizar suas operações, utilizar bancos de dados centralizados de computadores e acessar as informações por meio de terminais remotos.29

Em 1964, a American Airlines lançou seu primeiro sistema de registro e reserva totalmente informatizado, construído pela IBM. Ele foi modelado com base no SAGE, o primeiro sistema de alerta e defesa aérea dos Estados Unidos, destinado a se proteger contra um ataque nuclear da União Soviética. O sistema da companhia aérea ainda tinha um nome semelhante.30 SAGE significa "Ambiente Semi-Automático no Solo"; o sistema da American Airlines chamava-se SABRE, que significa "Ambiente de Negócios Semi-Automatizado". Ao contrário do SAGE, que estava desatualizado no momento em que foi colocado no ar por não poder interceptar mísseis balísticos soviéticos, o SABRE foi um enorme sucesso. Conectou mais de mil máquinas Teletype ao computador centralizado da empresa, localizado ao norte da cidade de Nova York.31 O sistema prometeu não apenas ajudar a American Airlines a preencher assentos vazios, mas também "fornecer à gerência informações abundantes sobre as operações do dia a dia". E ele conseguiu.

"Desde o primeiro dia de operação, o SABRE começou a acumular centenas de informações, as informações mais detalhadas já compiladas sobre os padrões de viagens de todas as principais cidades – por destino, por mês, por estação, por dia da semana, por hora do dia -, informações que nas mãos certas se tornariam extremamente valiosas na indústria que os gringos procuravam dominar", escreve Thomas Petzinger Jr. no livro "Hard Landing".32 Com o SABRE, a American Airlines estabeleceu o monopólio de reservas informatizadas e, posteriormente, aumentou ainda mais esse poder para esmagar sua concorrência.33 Em dado momento, a American Airlines lançou o sistema como uma empresa independente. Hoje, o SABRE ainda é o sistema número um de reservas de viagens no mundo, com dez mil funcionários e receita de US $ 3 bilhões.34

O crescimento de todos esses bancos de dados não passou despercebido. O medo dominante do público na época era que a proliferação de bancos de dados corporativos e governamentais e computadores em rede criaria uma sociedade de vigilância – um lugar onde todas as pessoas eram monitoradas e rastreadas e onde a dissidência política seria esmagada. Não apenas os ativistas de esquerda e os manifestantes estudantis estavam preocupados.35 Essas questões afligiam quase todas as camadas da sociedade. As pessoas temiam a vigilância do governo e também a vigilância corporativa.

Uma reportagem de capa de 1967 para o jornal Atlantic Monthly exemplifica esses medos. Escrita por um professor de direito da Universidade de Michigan chamado Arthur R. Miller, ele lançou um ataque ao esforço de empresas e agências governamentais para centralizar e informatizar a coleta de dados. A história inclui uma arte de capa incrível, mostrando o tio Sam enlouquecendo na frente dos controles de um computador gigante. Ele se concentra em uma proposta de banco de dados federal em particular: o Centro Nacional de Dados, que centralizaria as informações pessoais e as conectaria a um número de identificação exclusivo para todas as pessoas no sistema.

Miller alertou que esse banco de dados era uma grave ameaça à liberdade política. Uma vez implantado, invariavelmente aumentaria para abranger todas as partes da vida das pessoas:

O computador moderno é mais do que uma sofisticada máquina de indexação ou adição, ou uma biblioteca em miniatura; é a pedra angular de um novo meio de comunicação cujas capacidades e implicações estamos apenas começando a perceber. No futuro previsível, os sistemas de computadores serão interligados pela televisão, satélites e lasers, e moveremos grandes quantidades de informações por vastas distâncias num tempo imperceptível...

A própria existência de um Centro Nacional de Dados pode incentivar certas autoridades federais a se envolverem em táticas questionáveis de vigilância. Por exemplo, escâneres ópticos – dispositivos com capacidade para ler uma variedade de fontes de caracteres ou manuscritos a taxas fantásticas de velocidade – poderiam ser usados para monitorar nossa correspondência. Ao vincular os escâneres a um sistema de computador, as informações extraídas pelo dispositivo seriam

convertidas em um formato legível por máquina e transferidas para o arquivo dedicado a certo sujeito no Centro Nacional de Dados.

Então, com uma programação sofisticada, os dossiês de todos as pessoas com as quais um sujeito sob vigilância se corresponde poderiam ser produzidos com o toque de um botão, e um rótulo apropriado – como "pessoas associadas a criminosos conhecidos" – poderia ser adicionado a todos eles. Como resultado, alguém que simplesmente troca cartões de Natal com uma pessoa cuja correspondência está sendo monitorada pode ficar sob vigilância ou pode ser recusada ao se candidatar a um emprego no governo ou solicitar uma bolsa do governo ou se candidatar a algum outro benefício governamental. Um rótulo de computador não testado, impessoal e errôneo, como "pessoas associadas a criminosos conhecidos", marcou aquela pessoa e ela não pode fazer nada para corrigir a situação. De fato, é provável que ela nem estivesse ciente de que o rótulo existia.36

O Atlantic Monthly não estava sozinho. Jornais, revistas e noticiários de televisão da época estão cheios de reportagens alarmantes sobre o crescimento de base de dados centralizados – ou "bancos de dados", como eram chamados naquela época – e o perigo que representavam para uma sociedade democrática.

Nesse momento de medo, a investigação de Christopher Pyle explodiu como uma bomba atômica. O CONUS Intel era notícia de primeira página. Seguiram-se protestos e editoriais indignados, assim como as matérias de quase todas as principais revistas de notícias dos EUA. As redes de televisão acompanharam a de reportagens e realizaram suas próprias investigações aprofundadas. Houve consultas no Congresso para chegar ao fundo das acusações.37

A investigação mais contundente foi liderada pelo senador Sam Ervin, um democrata da Carolina do Norte, um sujeito careca, com sobrancelhas grossas e grossas e mandíbulas carnudas de buldogue. Ervin era conhecido como um democrata moderado sulista, o que significava que ele consistentemente defendia as leis de Jim Crow e a segregação racial de moradias e escolas e lutava contra tentativas de garantir direitos iguais para as mulheres. Ele era frequentemente chamado de racista, mas se via como um constitucionalista estrito. Odiava o governo

federal, o que também significava que odiava programas de vigilância doméstica.38

Em 1971, o senador Ervin convocou uma série de audiências sobre as revelações de Pyle e recrutou-o para ajudar na iniciativa. Inicialmente, a investigação concentrou-se no programa CONUS Intel do exército, mas se expandiu rapidamente para abranger uma questão muito maior: a proliferação de bases de dados digitais governamentais e corporativas e de sistemas de vigilância.39 “Essas audiências foram convocadas porque fica claro pelas queixas recebidas pelo Congresso que os estadunidenses em todas as esferas da vida estão preocupados com o crescimento dos registros governamentais e privados de indivíduos”, disse o senador Ervin diante do Senado na dramática declaração de abertura à sua investigação. “Eles estão preocupados com a crescente coleta de informações sobre eles, que não é da conta de quem as coleta. Uma grande rede de telecomunicações está sendo criada pelas transmissões entre computadores que atravessam nosso país todos os dias... Liderados pelos analistas de sistemas, os governos estaduais e locais estão pensando em maneiras de conectar seus bancos de dados e computadores a suas contrapartes federais, enquanto autoridades federais tentam ‘capturar’ ou incorporar dados estaduais e locais em seus próprios sistemas de dados”.40

O primeiro dia das audiências – intitulado “Bancos de Dados Federais, Computadores e a Declaração de Direitos” – atraiu uma enorme cobertura da mídia. “Os senadores ouvem sobre a ameaça de uma ‘ditadura de dossiês’”, declarou uma manchete de primeira página do New York Times; a história dividia espaço com uma reportagem sobre o bombardeio do Vietnã do Sul ao Laos.41 “A vida privada de um estadunidense comum é objeto de 10 a 20 dossiês de informações pessoais nos arquivos e bancos de dados de computadores do governo e de agências privadas... a maioria dos estadunidenses tem apenas uma vaga noção do quanto estão sendo vigiados”.

Nos vários meses seguintes, o senador Ervin criticou o Pentágono sobre o programa, mas esbarrou em forte resistência. Os oficiais de defesa fincaram pé, ignoraram os pedidos de testemunhas e se recusaram a desclassificar as evidências.42 Os confrontos passaram de um pequeno aborrecimento para um escândalo total, e o senador Ervin ame-

açou denunciar publicamente o programa de vigilância do exército como inconstitucional e usar seu poder para conseguir, via intimação judicial, as evidências necessárias e obrigar legalmente o testemunho se os representantes do Pentágono continuassem não cooperando. No final, os esforços do senador Ervin conseguiram esclarecer o alcance do aparato de vigilância doméstica computadorizado das forças armadas. Seu comitê descobriu que o Exército dos EUA acumulou uma presença poderosa de inteligência doméstica e "desenvolveu um sistema massivo para monitorar praticamente todos os protestos políticos nos Estados Unidos". Havia mais de 300 "centros de registros" regionais em todo o país, muitos deles contendo mais de 100.000 cartões sobre "personalidades de interesse". No final de 1970, um centro nacional de inteligência de defesa possuía 25 milhões de arquivos sobre indivíduos e 760.000 arquivos sobre "organizações e incidentes". Esses arquivos estavam cheios de detalhes obscuros – preferências sexuais, casos extraconjugais e uma ênfase particular na suposta homossexualidade – coisas que não tinham nada a ver com a tarefa em questão: reunir evidências sobre os supostos laços das pessoas com governos estrangeiros e sua participação em planos criminosos.43 E, como o comitê desvelou, o Comando de Inteligência do Exército possuía várias bases de dados que podiam fazer referência cruzada a essas informações e mapear as relações entre pessoas e organizações.

O comitê do senador Sam Ervin também confirmou outra coisa: o programa de vigilância do exército era uma extensão direta da maior estratégia de contrainsurgência dos Estados Unidos, que havia sido desenvolvida para uso em conflitos estrangeiros, mas que foi imediatamente trazida de volta e usada na frente doméstica. "Os homens que dirigiam a sala de guerra doméstica mantinham registros não muito diferentes dos mantidos por seus colegas nas salas de guerra computadorizadas de Saigon", observou um relatório final sobre as investigações do senador Ervin.44

De fato, o exército se referiu a ativistas e manifestantes como se fossem combatentes inimigos organizados, incorporados à população nativa. Eles "agitaram", planejaram ataques a "alvos e objetivos" e até tiveram um "corpo organizado de franco-atiradores". O exército usou cores padrão dos jogos de guerra: azul para as "forças amigas" e vermelho para os "bairros negros". No entanto, como o relatório deixou bem

claro, as pessoas que estavam sendo observadas não eram combatentes, mas pessoas comuns: “a inteligência do exército não estava apenas reconhecendo cidades para montar acampamento, rotas de aproximação e arsenais dos Pantera Negra. Ele estava coletando, disseminando e armazenando quantidades de dados sobre assuntos pessoais e particulares de cidadãos cumpridores da lei. Comentários sobre os assuntos financeiros, vidas sexuais e histórias psiquiátricas de pessoas não afiliadas às forças armadas aparecem nos vários sistemas de registros.” Ou seja, o exército estava espionando uma grande parte da sociedade estadunidense sem uma boa razão para isso.

“A hipótese de que grupos revolucionários pudessem estar por trás dos movimentos de direitos civis e antiguerra se tornou uma pressuposição que contaminou toda a operação”, explicou o senador Ervin em um relatório final que sua equipe produziu com base em sua investigação. “Manifestantes e amotinados não eram vistos como cidadãos gringos com possíveis demandas legítimas, mas como ‘forças dissidentes’ mobilizadas contra a ordem estabelecida. Dada essa concepção de dissidência, não surpreende que a inteligência do exército colete informações sobre a vida política e privada dos dissidentes. As doutrinas militares que governavam as operações de contrainteligência, contrainsurgência e assuntos civis exigiam isso. ”45

As audiências do senador Ervin chamaram muita atenção e lançaram luz sobre a proliferação de bases de dados de vigilância federal reunidas por trás dos panos sem restrições. O exército prometeu destruir os arquivos de vigilância, mas o Senado não pôde obter prova definitiva de que os arquivos foram totalmente eliminados. Pelo contrário, aumentaram as evidências de que o exército havia escondido deliberadamente e continuado a usar os dados de vigilância coletados.46 De fato, enquanto os generais prometiam destruir os arquivos que haviam acumulado em centenas de milhares de estadunidenses, os contratados da ARPA os alimentaram com um novo sistema de análise e pesquisa de dados em tempo real conectado à ARPANET.47

A Vigilância da ARPANET

Foi em 1975 quando a NBC transmitiu a reportagem de Ford Rowan expondo que a ARPANET estava sendo usada para espionar estadunidenses. Três anos se passaram desde a investigação do senador Ervin sobre a operação de espionagem CONUS Intel do exército, e o escândalo havia se tornado notícia antiga, eclipsada pela investigação de Watergate que derrubou o presidente Richard Nixon. Mas os relatórios de Rowan trouxeram o sórdido caso CONUS Intel de volta aos holofotes.48

"No final dos anos 1960, no auge das manifestações contra a guerra, o Presidente Johnson ordenou à CIA, ao FBI e ao Exército que descobrissem quem estava por trás dos protestos. O que se seguiu foi uma grande campanha de infiltração e vigilância de grupos antiguerra", Rowan disse aos telespectadores da NBC em 2 de junho de 1975. "Em 1970, o senador Sam Ervin expôs a extensão da espionagem do Exército. Ele conseguiu que o Pentágono prometesse interromper seu programa de vigilância e destruir os arquivos. Mas quatro anos após a promessa feita a Sam Ervin, os arquivos de vigilância doméstica do Exército ainda existem. A NBC News descobriu que uma nova tecnologia de computador desenvolvida pelo Departamento de Defesa permitiu ao Pentágono copiar, distribuir e atualizar secretamente os arquivos do Exército."

Dois dias depois, Rowan entregou um segmento de acompanhamento:

> A rede secreta de computadores foi possível graças a avanços dramáticos na técnica de conectar diferentes marcas e modelos de computadores, para que eles pudessem conversar entre si e compartilhar informações. É uma tecnologia totalmente nova que poucas pessoas conhecem. Se você pagar impostos ou usar um cartão de crédito, se estiver dirigindo um carro, ou já serviu no exército, se você já foi preso, ou mesmo investigado por uma agência de polícia, se você teve grandes despesas médicas ou contribuiu para um partido político nacional, há informações sobre você em algum lugar de algum computador. O Congresso sempre teve medo de que os computadores, quando conectados,

> pudessem transformar o governo em ‘irmão mais velho’ dos computadores, tornando perigosamente fácil manter o controle da população.

Ele então foi específico com relação ao que aconteceu com os arquivos de vigilância que o exército deveria destruir: “Segundo fontes confidenciais, grande parte do material que foi informatizado foi copiado e transferido, e grande parte foi compartilhado com outras agências onde foi integrado a outros arquivos de inteligência... Em janeiro de 1972, pelo menos parte dos arquivos computadorizados de vigilância doméstica do Exército foram armazenados no computador Harvest da NSA em Fort Meade, Maryland. Com o uso de uma rede de computadores do departamento de defesa, os materiais foram transmitidos e copiados em Massachusetts no MIT e armazenados no Centro de Pesquisa Natick do Exército.”

O primeiro nó da ARPANET entre a UCLA e Stanford entrou em operação em 1969 e a rede expandiu-se nacionalmente no mesmo ano. Agora, com a exposição de Rowan, seis anos depois, essa rede militar inovadora teve seu primeiro grande momento no centro das atenções do público.

Quando finalmente localizei Rowan, ele ficou surpreso ao me ouvir falar daquela transmissão antiga da NBC. Ninguém havia discutido isso com ele há décadas. “Não ouvi ninguém falar sobre isso durante muito tempo. Estou honrado por você ter desenterrado tudo”, disse.

Ele então me contou como conseguiu a história.49 No início dos anos 1970, ele estava trabalhando no tema de Washington. Cobriu Watergate e as Audiências do Comitê de Church, conduzidas pelo senador Frank Church, que continuam sendo a investigação mais minuciosa e condenatória do governo sobre as atividades ilegais das agências de inteligência gringas, incluindo a CIA, a NSA e o FBI. Foi durante o Comitê de Church que ele tropeçou na história da ARPANET e começou a montá-la. “Isso foi pós-Watergate, pós-Vietnã. Este também foi o momento em que estavam investigando os assassinatos de Kennedy, o assassinato de Martin Luther King e, posteriormente, o assassinato de Robert Kennedy. Em seguida, surgiram histórias sobre espionagem

doméstica em massa pelo FBI e pelo Departamento de Defesa sobre manifestantes que eram contra a guerra. Essas investigações eram coisas que eu estava cobrindo e, portanto, conversava com pessoas que habitavam naquele mundo – o FBI, a CIA e o Departamento de Defesa -", explicou Rowan. A operação de vigilância da ARPANET estava intimamente ligada às revoltas políticas ocorridas nos Estados Unidos na época, e ele soube de sua existência aos poucos enquanto procurava outras histórias. "Não foi algo fácil de encontrar. Não havia um informante importante. Ninguém que sabia de tudo. Você realmente tinha que cavar."

Sua investigação sobre a ARPANET levou meses para ser concluída. A maioria das fontes não queriam ser gravadas, mas uma delas aceitou.50 Ela era um técnico de informática do MIT chamado Richard Ferguson, que estava lá em 1972 quando o Pentágono transferiu os dados de vigilância para seu laboratório. Ele decidiu apresentar as informações e apareceu pessoalmente na NBC para fazer a acusação. Ele explicou que os arquivos eram de fato dossiês que continham informações pessoais e crenças políticas. "Vi a estrutura de dados que eles usaram e ela diz respeito à ocupação de uma pessoa, sua política, seu nome", disse ele à NBC. Ele explicou que foi demitido de seu emprego por se opor ao programa.

Várias fontes de inteligência e pessoas envolvidas na transferência dos arquivos de espionagem corroboraram as alegações de Ferguson, mas não quiseram ser gravadas. Com o tempo, outros jornalistas verificaram as reportagens de Rowan.51 Não havia dúvida: a ARPANET estava sendo usada para monitorar a atividade política doméstica. "Eles enfatizaram que o sistema não realizou nenhuma vigilância real, mas foi projetado para usar dados coletados no 'mundo real' para ajudar a construir modelos preditivos que pudessem avisar quando os distúrbios civis eram iminentes", escreveu mais tarde na Technospies, um livro pouco conhecido que expandiu sua investigação sobre a tecnologia de vigilância de rede criada pela ARPA.52 Pelo menos parte do trabalho de escrever o "programa de manutenção" do banco de dados para os arquivos de vigilância ilegal do exército parecia ter sido realizado no MIT. Isso foi feito através do Projeto Cambridge, aquela grande iniciativa de J. C. R. Licklider para criar ferramentas computadorizadas para análise de dados

de contrainsurgência.53 Eles possivelmente foram transferidos para outros sites da ARPANET.

Os estudantes de Harvard e do MIT que protestaram contra o Projeto Cambridge da ARPA em 1969 viram a ARPANET como uma arma de vigilância e uma ferramenta de controle social e político. Eles tinham razão. Apenas alguns anos depois que seus protestos falharam em interromper o projeto, essa nova tecnologia foi lançada contra eles e o povo estadunidense.

As reportagens de Ford Rowan e as revelações de que o exército não havia destruído seus arquivos ilegais de vigilância desencadearam outra rodada de investigações do Congresso. O senador John Tunney, democrata da Califórnia, liderou a maior delas. Em 23 de junho de 1975, ele convocou uma sessão especial do Comitê do Judiciário para investigar a tecnologia de vigilância e abordar especificamente o papel que a tecnologia de rede do ARPA desempenhou na disseminação dos arquivos de vigilância doméstica do exército.

O senador Tunney abriu as audiências com uma condenação: “Acabamos de passar por um período da história dos EUA chamado Watergate, em que vimos certos indivíduos que estavam preparados para usar qualquer tipo de informação, classificada ou não, para seus próprios propósitos políticos, e de formas muito prejudiciais para os interesses dos Estados Unidos e de cidadãos individuais”, afirmou. “Sabemos que o Departamento de Defesa e o Exército violaram seus poderes estatutários. Sabemos que a CIA violou seu poder estatutário ao se envolver com a coleta de informações sobre cidadãos particulares e à sua colocação em computadores.”

Ele prometeu chegar ao fundo do escândalo de vigilância da época para impedir que esse tipo de abuso acontecesse outras vezes. Durante três dias, o senador Tunney interrogou os principais funcionários da defesa. Mas, assim como o senador Sam Ervin, ele encontrou resistência.54

O Subsecretário Adjunto de Defesa David Cooke, um homem corpulento, com a cabeça raspada e um jeito escorregadio, foi um dos principais oficiais que representaram o Pentágono. Ele havia servido sob o Secretário de Defesa Neil McElroy, o homem que criou a ARPA, e ele

exigiu respeito e obediência à autoridade. Em seu depoimento, Cooke negou que os bancos de dados de vigilância doméstica do exército ainda existissem e duplamente negou que a ARPANET tivesse algo a ver com a transferência ou utilização desses arquivos de vigilância inexistentes. "Funcionários do MIT e da ARPA afirmam que nenhuma transmissão de dados sobre distúrbios civis pela ARPANET foi autorizada e que não há evidências de que isso tenha ocorrido", testemunhou. Ele também fez o possível para convencer o senador Tunney de que o Pentágono não tinha necessidade operacional da ARPANET, que ele descreveu como uma pura rede acadêmica e de pesquisa. "A própria ARPANET é um sistema totalmente não classificado, desenvolvido e amplamente utilizado pela comunidade científica e tecnológica dos Estados Unidos", disse ele ao comitê. "Nem a Casa Branca nem nenhuma das agências de inteligência têm um computador conectado à ARPANET."

Como Cooke explicou, os militares não precisavam da ARPANET porque já possuíam seu próprio banco de dados seguros e sua rede de comunicação e inteligência: o Sistema de Inteligência Comunitária Online, conhecido simplesmente como COINS. "É um sistema seguro, que conecta bancos de dados selecionados de três agências de inteligência: a Agência de Inteligência de Defesa, a Agência de Segurança Nacional e o Centro Nacional de Interpretação de Fotos. Ele foi projetado para trocar dados de inteligência estrangeiros classificados e altamente sensíveis entre essas agências de inteligência e dentro do Departamento de Defesa. A Agência Central de Inteligência e o Departamento de Estado podem acessar o sistema", explicou ele, e acrescentou enfaticamente:"A COINS e a ARPANET não estão vinculadas e não virão a ser".

Ou ele estava mal-informado, ou distorcendo a verdade.

Quatro anos antes, em 1971, o diretor da ARPA, Stephen Lukasik, que dirigia a agência durante a criação da ARPANET, explicou muito claramente em seu testemunho ao Senado que o objetivo da ARPANET era integrar redes governamentais – ambas classificadas (como a COINS) e não classificados – em um sistema de telecomunicações unificado.55 "Nosso objetivo é projetar, construir, testar e avaliar uma rede de computadores confiável, de alto desempenho e baixo custo para atender aos crescentes requisitos do Departamento de Defesa para comunicações entre computadores", afirmou. Ele acrescentou que os militares

haviam acabado de começar a testar a ARPANET como uma maneira de conectar sistemas operacionais de computadores.56

De acordo com Lukasik, a beleza da ARPANET era que, embora fosse tecnicamente uma rede não classificada, poderia ser usada para fins sigilosos porque os dados podiam ser criptografados digitalmente e enviados por cabos, sem a necessidade de proteger fisicamente as linhas e equipamentos reais. Era uma rede de computadores de uso geral que podia se conectar a redes públicas e ser usada para tarefas classificadas e não classificadas.57

Lukasik estava certo. Entre 1972 e 1975, várias agências militares e de inteligência não apenas se conectaram diretamente à ARPANET, mas também começaram a construir suas próprias sub-redes operacionais baseadas no design da ARPANET e que poderiam se interconectar com ela. A marinha tinha várias bases aéreas ligadas à rede. O exército usou a ARPANET para conectar centros de supercomputadores. Em 1972, a NSA contratou Bolt, Beranek e Newman – empresa de J. C. R. Licklider e principal terceirizada da ARPANET – para construir uma versão atualizada da ARPANET para o seu sistema de inteligência COINS, o mesmo sistema que Cooke prometeu três anos depois que nunca seria conectado à ARPANET. Esse sistema acabou sendo conectado à ARPANET para fornecer serviços operacionais de comunicação de dados para a NSA e o Pentágono por muitos anos depois.58

Mesmo que Cooke negasse ao senador Tunney que a ARPANET era usada para comunicações militares, a rede apresentava várias conexões do exército, da marinha, da NSA e da força aérea – e muito provavelmente continha nós não listados mantidos por agências de inteligência como a CIA.59 Mas a questão logo se tornou discutível. Algumas semanas após o testemunho de Cooke, a ARPANET foi oficialmente absorvida pela Agência de Comunicações de Defesa, que administrava os sistemas de comunicações de todo o Pentágono. Em outras palavras, ainda que experimental, a ARPANET era a definição de uma rede militar operacional.60

Internet militar

No verão de 1973, Robert Kahn e Vint Cerf se trancaram em uma sala de conferências no sofisticado hotel Hyatt Cabana El Camino Real, a apenas dois quilômetros ao sul de Stanford. O Cabana era o hotel mais glamoroso de Palo Alto, tendo recebido os Beatles em 1965, entre outras celebridades.

Kahn era atarracado e tinha cabelos pretos grossos e costeletas. Cerf era alto e magro, com uma barba despenteada. Os dois poderiam ter sido uma dupla de música folk de passagem em turnê. Mas Kahn e Cerf não estavam lá para brincar, socializar ou festejar. Eles não tinham nenhuma bebida ou drogas. Eles não tinham muito mais do que alguns lápis e blocos de papel. Nos últimos meses, eles tentaram criar um protocolo que pudesse conectar três tipos diferentes de redes militares experimentais. No Cabana, sua missão era finalmente colocar suas ideias no papel e elaborar o projeto técnico final de uma "inter-rede".61

"Você quer começar ou eu começo?" perguntou Kahn.

"Não, ficarei feliz em começar", respondeu Cerf, e então ficou lá, olhando para um pedaço de papel em branco. Após cerca de cinco minutos, ele desistiu: "Não sei por onde começar".62

Kahn assumiu o controle e rabiscou, anotando trinta páginas de diagramas e projetos de redes teóricas. Cerf e Kahn estavam envolvidos na construção da ARPANET: Cerf fazia parte de uma equipe da UCLA responsável por escrever o sistema operacional dos roteadores que formavam a espinha dorsal da ARPANET, enquanto Kahn trabalhava na Bolt, Beranek e Newman ajudando a projetar os protocolos de roteamento da rede. Agora eles estavam prestes a ir para um novo nível: ARPANET 2.0, uma rede de redes, a arquitetura do que chamamos agora de "Internet".

Em 1972, depois que Kahn foi contratado para chefiar a divisão de comando e controle da ARPA, ele havia convencido Cerf a deixar um emprego onde recém-começara a dar aulas em Stanford e vir trabalhar novamente para a ARPA.63 Um dos principais objetivos de Kahn era expandir a utilidade da ARPANET em situações militares do mundo

real. Isso significava, em primeiro lugar, estender o projeto de rede baseada em pacotes para redes de dados sem fio, rádio e satélite. As redes de dados sem fio eram cruciais para o futuro do comando e controle militares, porque permitiam que o tráfego fosse transmitido por grandes distâncias: embarcações navais, aeronaves e unidades móveis de campo poderiam se conectar a computadores no continente por meio de unidades sem fio portáteis. Era um componente obrigatório do sistema global de comando e controle que a ARPA foi encarregada de desenvolver.64

Kahn dirigiu o esforço para construir várias redes experimentais sem fio. Uma delas se chamava PRNET, abreviação de "rede de pacotes via rádio". Ela tinha a capacidade de transmitir dados através de computadores móveis instalados em furgões usando uma rede de antenas localizadas nas cadeias de montanhas em torno das cidades de San Bruno, Berkeley, San Jose e Palo Alto. O projeto foi realizado pelo Instituto de Pesquisa Stanford. Ao mesmo tempo, Kahn desenvolvia a rede de pacotes por satélite, montando uma rede experimental chamada SATNET que ligava Maryland, Virgínia Ocidental, Inglaterra e Noruega; o sistema foi inicialmente projetado para transportar dados sísmicos de instalações remotas configuradas para detectar testes nucleares soviéticos. A tecnologia de pacotes de dados da ARPANET funcionou notavelmente bem em um ambiente sem fio. Mas havia um problema: embora eles fossem baseados nos mesmos projetos fundamentais de troca de pacotes de dados, PRNET, SATNET e ARPANET usavam protocolos ligeiramente diferentes e, portanto, não podiam se conectar entre si. Para todos os fins práticos, eram redes independentes, que contrariavam todo o conceito de rede e minimizavam sua utilidade para os militares.

A ARPA precisava das três redes para funcionar como uma.65 A pergunta era: como reunir todas elas de uma maneira simples? Era isso o que Kahn e Cerf estavam tentando descobrir na sala de conferências do Cabana. Eventualmente, eles estabeleceram um plano básico para uma linguagem de rede flexível que pudesse conectar vários tipos de redes. Chamava-se TCP / IP – Protocolo de Controle de Transmissão (Transmission Control Protocol) / Protocolo de Internet (Internet Protocol), a mesma linguagem básica de rede que alimenta a Internet atualmente.66

Em uma entrevista sobre os anos 1990, Cerf, que hoje trabalha como evangelista-chefe da Google, descreveu como os seus esforços e os de Kahn para criar um protocolo de uma inter-rede estavam inteiramente enraizados nas necessidades dos militares:

Tínhamos muitas ligações com os militares. Por exemplo, queríamos absolutamente ter comunicações de dados para o campo, que é o objetivo dos projetos de pacotes de rádio e de satélite; ou seja, como alcançar áreas imensas, como alcançar pessoas nos oceanos. Não é possível fazer isso arrastando fibra, e não dá para fazer muito bem com o rádio terrestre de armazenamento e envio, porque o sinal não funciona muito bem em um vasto oceano. Então, você precisa de satélites para isso. Portanto, tudo foi fortemente motivado pelo esforço de levar os computadores para o campo para as forças armadas e, em seguida, possibilitar a comunicação entre eles e também com os agentes que estavam na retaguarda das áreas de operações. Então, todas as demonstrações que fizemos mostravam também aplicações militares.67

Até mesmo o primeiro teste bem-sucedido da rede TCP / IP, tipo Internet, realizado em 22 de novembro de 1977, simulou um cenário militar: uso de rádio, satélite e redes cabeadas para se comunicar com uma unidade móvel ativa que lutava contra uma invasão soviética da Europa. Uma velha van GMC equipada pela SRI com vários equipamentos de rádio representou o papel de uma divisão motorizada da OTAN, subindo e descendo a estrada perto de Stanford, transmitindo dados pela rede de rádio da ARPA. Os dados foram então encaminhados pela rede de satélites da ARPA para a Europa – através da Suécia e de Londres – e depois enviados de volta aos Estados Unidos para a UCLA via satélite e por conexões cabeadas da ARPA.68 “Então, o que estávamos simulando era uma situação em que alguém estava em uma unidade móvel em campo, digamos na Europa, no meio de algum tipo de ação em que tentava se comunicar por meio de uma rede de satélites com os Estados Unidos. A informação, então, atravessava os EUA para obter algum comando estratégico de computação que estava deste lado do oceano”, lembrou Cerf. “E houve várias simulações ou demonstrações como essa, algumas das quais extremamente ambiciosas. Numa delas, até o Comando Aéreo Estratégico estava envolvido. Colocamos rádios de pacotes aéreos no campo se comunicando entre si e com o solo usando os sistemas de comunicação dos aviões para costurar fragmentos

da Internet que haviam sido segregados por um ataque nuclear simulado."

Cerf contou como trabalhava em estreita colaboração com os militares a cada passo do caminho e, em muitos casos, ajudando a encontrar soluções para necessidades específicas. "Nós implantamos um monte de equipamentos de rádio e terminais de computador e pequenos processadores em Fort Bragg com o 18º Corpo de Bombardeiros e, por vários anos, fizemos vários exercícios de campo. Também montamos esses equipamentos para o Comando Aéreo Estratégico em Omaha, Nebraska, e fizemos uma série de exercícios com eles. Em alguns casos, o resultado das aplicações que usamos foi tão bom que eles se tornaram parte da operação diária normal."

Obviamente, Vint Cerf não foi o único a elaborar aplicações militares práticas para a ARPANET. Os relatórios do Congresso e os documentos internos da ARPA da década de 1970 estão cheios de exemplos de operativos do exército colocando a rede em uso de várias maneiras, desde a transmissão sem fio de dados de sensores de localizadores submarinos até o fornecimento de comunicação portátil em campo, teleconferência, manutenção remota de computadores equipamentos, e cadeia de suprimentos militar e gerenciamento de logística.69 E, é claro, tudo isso foi entrelaçado com o trabalho da ARPA em "sistemas inteligentes" – a construção de análises de dados e as tecnologias preditivas que Godel e Licklider iniciaram uma década antes.70

Essa foi a grande vantagem da tecnologia ARPANET: era uma rede de uso geral que podia transportar todo tipo de tráfego. Foi útil para todos os envolvidos.

"Aconteceu que eu estava correto", disse-me Ford Rowan, quarenta e um anos depois de contar a história de vigilância do exército da ARPANET na NBC. "As preocupações que muitas pessoas tinham eram em grande parte com relação ao fato de o governo federal estar fabricando um grande computador que teria de tudo. Uma das novidades que surgiu foi que você não precisava de um grande computador. Você podia conectar muitos computadores. Esse foi o salto que ocorreu no início dos anos 1970, quando eles estavam fazendo essa pesquisa. Por fim, descobriram uma maneira de compartilhar informações pela rede sem precisar ter um computador grande que saiba tudo."71

Parte II

Falsas Promessas

Capítulo 4

Utopia e privatização

> Prontos ou não, os computadores estão chegando
> às pessoas. Uma ótima notícias, talvez a melhor
> desde as drogas psicodélicas.
> *- Stewart Brand, "SPACEWAR", 1972*

Se você fosse atropelado por um ônibus e entrasse em coma em 1975 e depois acordasse duas décadas depois, pensaria que os gringos enlouqueceram ou se juntaram a um culto milenar em massa. Provavelmente ambos.

Nos anos 1990, os EUA estavam em chamas com amplas proclamações religiosas sobre a Internet. As pessoas falavam de um grande nivelamento – um incêndio incontrolável que atravessaria o mundo, consumindo burocracias, governos corruptos, elites empresariais mimadas e ideologias difíceis, abrindo caminho para uma nova sociedade global mais próspera e livre em todas as formas possíveis. Era como se o fim dos tempos tivesse chegado. A utopia estava próxima.

Louis Rossetto, fundador de uma nova revista de tecnologia moderna chamada Wired, comparou os engenheiros de computação a Prometeu: eles trouxeram presentes dos deuses para nós mortais, coisas que estimularam "mudanças sociais tão profundas que seu único paralelo é provavelmente a descoberta do fogo", escreveu Rossetto na edição inaugural de sua revista.1 Kevin Kelly, um cristão evangélico barbudo e editor da Wired, concordou com seu chefe: "Ninguém pode escapar do fogo transformador das máquinas. A tecnologia, que antes progredia na periferia da cultura, agora envolve nossas mentes e nossas vidas. Como cada domínio é ultrapassado por técnicas complexas, a

ordem usual é invertida e novas regras são estabelecidas. Os poderosos sucumbem, os que antes eram confiantes, ficam desesperados por orientação, e os ágeis têm a chance de prevalecer."2

Não foi apenas a criançada da tecnologia que impôs essas visões. Não importava quem você fosse – republicano, democrata, liberal ou libertarianista – todos pareciam compartilhar essa convicção única e inabalável: o mundo estava à beira de uma revolução tecnológica que mudaria tudo e mudaria para melhor.

Poucos encarnaram melhor os primeiros anos deste novo Grande Despertar do que George Gilder, um especialista em Reaganomics da velha escola que, no início dos anos 1990, se reinventou como tecnoprofeta e guru do investimento. Em seu livro Telecosmo, ele explicou como as redes de computadores combinadas com o poder do capitalismo estadunidense estavam prestes a criar um paraíso na terra. Ele chegou a ter um nome para essa utopia: o telecosmo. "Todos os monopólios, hierarquias, pirâmides e redes de energia da sociedade industrial se dissolverão diante da pressão constante de distribuir inteligência às margens de todas as redes", escreveu, prevendo que o poder da Internet destruiria a estrutura física da sociedade. "O telecosmo pode destruir cidades, porque assim você pode obter toda a diversidade, toda a serendipte, toda a variedade exuberante que se pode encontrar em uma cidade em sua própria sala de estar."3 O vice-presidente Al Gore concordou, dizendo a quem quisesse ouvir que o mundo estava nas garras de uma "revolução tão abrangente e poderosa quanto qualquer revolução na história".4

De fato, algo estava acontecendo. As pessoas estavam comprando computadores pessoais e conectando-os com modems estridentes a um lugar novo e estranho: a World Wide Web. Um labirinto de salas de bate-papo, fóruns, redes corporativas e governamentais e uma coleção interminável de páginas da web. Em 1994, uma start-up chamada Netscape apareceu com um novo e empolgante produto, um navegador da web. Um ano depois, a empresa foi aberta e subiu para um valor de mercado de US $ 2,2 bilhões até o final do primeiro dia de negociação. Foi o início de uma nova corrida do ouro na área da baía de São Francisco. As pessoas aplaudiram e comemoraram quando empresas obscuras de tecnologia foram abertas ao mercado de ações, com o preço de suas ações dobrando, até mesmo triplicando no primeiro dia. E o que essas

empresas faziam? O que elas produziam? Como elas ganhavam dinheiro? Poucos investidores realmente sabiam. O mais importante era: ninguém se importava! Elas estavam inovando. Elas estavam nos levando para o futuro! As ações estavam em alta, sem previsão de mudança. De 1995 a 2000, a NASDAQ aumentou de 1.000 para 5.000, quintuplicando sua pontuação antes de cair sobre si mesma.

Eu ainda era criança, mas me lembro bem desses tempos. Minha família acabara de emigrar da União Soviética para os Estados Unidos. Saímos de Leningrado em 1989 e passamos seis meses percorrendo uma série de campos de refugiados na Áustria e na Itália até finalmente chegarmos a Nova York. Logo depois, nos mudamos rapidamente para São Francisco, onde meu pai, Boris, usou seu incrível talento para idiomas. Lá conseguiu um emprego como tradutor de japonês. Minha mãe, Nellie, reformulou seu doutorado pedagógico soviético e começou a ensinar física no Colégio Galileo, enquanto meu irmão Eli e eu tentávamos nos adaptar e nos encaixar da melhor maneira possível. No momento em que nos orientamos, a área da baía estava no auge da histeria ponto-com. Todo mundo que eu conhecia estava entrando no ramo de tecnologia e parecia estar prosperando como um bandido. A cidade estava cheia de garotos espinhentos dirigindo carros conversíveis, comprando casas e indo em tecno-raves luxuosas. Meu amigo Leo trocou suas habilidades infantis de hacker por um alto salário de cinco dígitos – era muito dinheiro para um adolescente. Outro garoto imigrante que eu conhecia fez uma pequena fortuna especulando sobre nomes de domínio. Meu irmão mais velho conseguiu um ótimo emprego com um ótimo salário em uma start-up misteriosa que tentou meia dúzia de produtos no espaço de alguns anos e depois sucumbiu sem lançar nada viável. “Tivemos alguns investidores do Centro-Oeste que não tinham ideia do que era a Internet. Eles só sabiam que era preciso investir nela”, lembra ele. Jogos de computador, Internet, páginas da web, pornografia interminável, deslocamento remoto, ensino a distância, streaming de filmes e música sob demanda: o futuro estava aqui. Me matriculei em uma faculdade comunitária e me transferi para a UC Berkeley, com a intenção de obter um diploma em ciência da computação.

Duas décadas antes, os estadunidenses temiam os computadores. As pessoas, especialmente os jovens, os viam como uma ferramenta tecnocrática de vigilância e controle social. Mas tudo mudou nos anos

1990. Os hippies que protestaram contra os computadores e a Internet primitiva agora disseram que essa ferramenta de opressão nos libertaria da opressão! Os computadores foram o grande equalizador! Eles tornariam o mundo mais livre, mais justo, mais democrático e igualitário.

Era impossível não acreditar no hype. Olhando para trás agora, com pleno conhecimento da história da Internet, não posso deixar de me maravilhar com a transformação. É tão estranho quanto acordar e ver hippies marchando para o recrutamento militar.

Afinal, o que aconteceu? Como uma tecnologia tão profundamente conectada à guerra e à contrainsurgência se tornou repentinamente uma via de mão única para a utopia global? Essa é uma pergunta importante. Sem ela, não podemos começar a entender as forças culturais que moldaram a maneira como vemos a Internet hoje.

De certa forma, tudo começou com um empresário desiludido chamado Stewart Brand.5

Hippies na ARPA

Outubro de 1972. Era noite e Stewart Brand, um jornalista e fotógrafo freelancer, jovem e magro, estava no Laboratório de Inteligência Artificial (IA) de Stanford, um terceirizado da ARPA, localizado nas montanhas de Santa Cruz, acima do campus. E ele se divertia muito.

Ele estava a mando da Rolling Stone, a nervosa revista da contracultura gringa, festejando com um monte de programadores de computador e nerds de matemática, todos na folha de pagamento da ARPA. Brand não estava lá para inspecionar dossiês digitais ou pressionar os engenheiros a falarem sobre suas sub-rotinas de vigilância de dados. Estava lá por diversão e frivolidade: fora jogar SpaceWar, um troço chamado “videogame de computador”.

Duas dúzias de pessoas estavam amontoadas em uma sala de console a meia luz, perto do salão principal onde estava o enorme computador PDP-10 do laboratório de IA. O Programador-Chefe de Sistemas de

IA e o mais viciado em SpaceWar, Ralph Gorin, estava na frente de uma tela de computador. Os jogadores pegaram os cinco conjuntos de botões de controle, encontraram sua nave espacial na tela e, simultaneamente, viravam e atiravam em direção a qualquer nave espacial próxima indefesa. Apertavam o botão de propulsão para entrar a órbita antes de serem sugados pelo sol assassino e evadiam ou destruíam qualquer torpedo inimigo a caminho ou minas em órbita. Depois que dois torpedos são disparados, a nave fica desarmada e precisa de três segundos para recarregar.6

Jogar um videogame contra outras pessoas em tempo real? Naquela época, isso era coisa alucinante, algo que a maioria das pessoas via apenas em filmes de ficção científica. Brand ficou paralisado. Ele nunca tinha ouvido falar ou experimentado algo assim antes. Foi uma experiência de expansão da mente. Era emocionante, como tomar uma dose gigantesca de ácido.

Ele olhou para seus colegas jogadores, todos espremidos naquele minúsculo escritório monótono e teve uma visão. As pessoas ao seu redor – seus corpos estavam presos na terra, mas suas mentes haviam sido teletransportadas para outra dimensão, “efetivamente fora de seus corpos, projetadas por computador em telas de tubo de raios catódicos, trancadas num combate espacial de vida ou morte, por horas e horas, arruinando os olhos, tendo cãibra nos dedos com o apertar frenético dos botões do controle, matando alegremente os amigos e desperdiçando o valioso tempo no computador do patrão.”7

O restante do Laboratório de Inteligência Artificial de Stanford também tinha saído diretamente de uma ficção científica. Enquanto Brand e seus novos amigos jogavam obsessivamente o videogame, robôs caolhos sobre rodas vagavam autonomamente pelos cantos. Música gerada por computador enchia o ar e luzes estranhas se projetavam nas paredes. Será que aquilo era um laboratório de informática de Stanford, financiado pelos militares, ou um concerto psicodélico de Jefferson Airplane? Para Brand, eram ambos e muito mais. Ele ficou maravilhado com “um circo de quinze anéis em dez direções diferentes” acontecendo ao seu redor. Foi “a cena mais divertida que eu já vivi desde os Testes de Ácido Merry Prankster”.8

Na época, a atmosfera ao redor de Stanford era carregada de um sentimento anti-ARPA. A universidade acabara de sair de uma onda de violentos protestos contra a guerra, contra pesquisas e recrutamentos militares no campus. Ativistas da Estudantes por uma Sociedade Democrática atacaram especificamente o Instituto de Pesquisas de Stanford – um importante contratado da ARPA profundamente envolvido em tudo, desde a ARPANET a armas químicas e contrainsurgência – e forçou a universidade a cortar os laços oficiais.

Para muitos no campus, a ARPA era o inimigo. Brand discordava.

Em um longo artigo que solicitou à Rolling Stone, ele decidiu convencer os leitores jovens e influenciadores da revista de que a ARPA não era uma grande inutilidade burocrática conectada à máquina de guerra estadunidense, mas que fazia parte de um "programa de pesquisa surpreendentemente esclarecido" que por acaso passou a ser dirigido pelo Pentágono. As pessoas com quem ele estava no laboratório de IA de Stanford não eram engenheiros da computação desalmados trabalhando para uma terceirizada militar. Eles eram hippies e rebeldes, sujeitos da contracultura com cabelos compridos e barbas. Eles decoraram seus cubículos com pôsteres e folhetos de arte psicodélicos contra a Guerra do Vietnã. Eles liam Tolkien e fumavam maconha. Eram "hackers" e "vagabundos de computadores... cheios de liberdade e estranheza... São uns cabeções, a maioria deles", escreveu Brand.9

Eles eram legais, apaixonados, tinham ideias, estavam fazendo alguma coisa e queriam mudar o mundo. Podiam estar presos em um laboratório de informática com um salário do Pentágono, mas não estavam lá para servir os militares. Eles estavam lá para trazer a paz ao mundo, não através de protestos ou ações políticas, mas através da tecnologia. Brand estava em êxtase. "Estando pronto ou não, os computadores estão chegando ao povo. São boas notícias, talvez as melhores desde os psicodélicos", disse ele aos leitores da Rolling Stone.

E os videogames, por mais incrivelmente legais que fossem, apenas arranharam a superfície do que esses cientistas legais estavam preparando. Com a ajuda da ARPA, eles estavam revolucionando os computadores, transformando-os de mainframes gigantes operados por técnicos em ferramentas acessíveis que qualquer pessoa podia comprar e usar em casa. E havia algo chamado ARPANET, uma nova rede de com-

putadores que prometia conectar pessoas e instituições em todo o mundo, facilitar a comunicação e a colaboração em tempo real a grandes distâncias, entregar notícias instantaneamente e até tocar música sob demanda. Tocar The Grateful Dead quando você quiser? Imagina! “As lojas de discos que se virem”, previu Stewart Brand.

Da maneira que ele descreveu, daria para pensar que trabalhar para a ARPA era a coisa mais subversiva que uma pessoa poderia fazer.

Cultos e Cibernética

Brand tinha 34 anos e já era uma celebridade da contracultura quando visitou o Laboratório de IA de Stanford. Ele havia sido o editor da Whole Earth Catalog, uma revista de estilo de vida muito popular para o movimento das comunidades. Trabalhou com Ken Kesey e seus Merry Pranksters cheios de LSD, e desempenhou um papel central na criação e promoção do concerto psicodélico onde The Grateful Dead estreou e tocou no festival Summer of Love, em São Francisco.10 Brand estava profundamente enraizado na contracultura da Califórnia e apareceu como personagem principal no The Electric Kool-Aid Acid Test de Tom Wolfe. No entanto, lá estava ele, agindo como um vendedor da ARPA, uma agência militar que, em sua curta existência, já acumulava uma reputação sangrenta – da guerra química à contrainsurgência e vigilância. Não fazia nenhum sentido.11

Stewart Brand nasceu em Rockford, Illinois. Sua mãe era dona de casa; seu pai, um publicitário de sucesso. Depois de se formar em um colégio interno de elite, Brand frequentou a Universidade de Stanford. Seus diários da época mostram um jovem profundamente apegado à sua individualidade e com medo da União Soviética. Seu maior pesadelo era que os Estados Unidos fossem invadidos pelo Exército Vermelho e que o comunismo tiraria seu livre arbítrio para pensar e fazer o que quisesse. “Minha mente não seria mais minha, mas uma ferramenta cuidadosamente modelada pelos descendentes de Pavlov”, escreveu em um diário.12 “Se houver uma luta, eu lutarei. E lutarei com um propósito. Não lutarei pela América, pelo meu lar, pelo Presidente Eisenhower, pelo

capitalismo, nem pela democracia. Vou lutar pelo individualismo e pela liberdade pessoal. Se é para ser um tolo, quero ser meu tipo particular de tolo – completamente diferente de outros tolos. Vou lutar para evitar ser um número – para os outros e para mim mesmo."13

Após a faculdade, Brand se alistou no Exército dos EUA e treinou como paraquedista e fotógrafo. Em 1962, depois de terminar seu serviço, mudou-se para a Bay Area de São Francisco e se lançou para o movimento de contracultura em ascensão. Ele se envolveu com Kesey e os Merry Pranksters, tomou muitas drogas psicodélicas, festejou, fez arte e participou de um programa experimental para testar os efeitos do LSD que, desconhecido para ele, estava sendo secretamente conduzido pela Agência Central de Inteligência como parte de seu programa MK-ULTRA.14

Enquanto a Nova Esquerda protestou contra a guerra, juntou-se ao movimento dos direitos civis e lutou pelos direitos das mulheres, Brand seguiu um caminho diferente. Ele pertencia à ala libertarianista da contracultura, que tendia a menosprezar o ativismo político tradicional e via toda a política com ceticismo e desprezo. Ken Kesey, autor de One Flew Over the Cuckoo's Nest e um dos líderes espirituais do movimento hippie-libertarianista, canalizou essa sensibilidade quando disse a milhares de pessoas reunidas em um comício contra a Guerra do Vietnã na UC Berkeley que sua tentativa de usar a política para parar a guerra estava fadada ao fracasso. "Você quer saber como parar a guerra?" ele gritou. "Basta virar as costas, ela que se foda!"15

Muitos fizeram exatamente isso. Eles deram as costas e disseram "foda-se!" e mudaram-se das cidades para a zona rural dos EUA: norte de Nova York, Novo México, Oregon, Vermont, oeste de Massachusetts. Eles mesclaram espiritualidade oriental, noções românticas de autossuficiência e as ideias cibernéticas de Norbert Wiener. Muitos tendiam a ver a política e as estruturas hierárquicas sociais como inimigos fundamentais da harmonia humana, e procuravam construir comunidades livres de controle vindo de cima para baixo. Como não queriam reformar ou se envolver com o que viam como um antigo sistema corrupto, fugiram para o interior e fundaram comunidades, na esperança de criar do zero um novo mundo baseado em um conjunto melhor de ideais. Eles se

viam como uma nova geração de pioneiros expandindo a fronteira estadunidense.

O historiador da Universidade de Stanford, Fred Turner, chamou essa ala da contracultura de "novos comunalistas" e escreveu um livro que traçava as origens culturais desse movimento e o papel central que Stewart Brand e a ideologia cibernética desempenharam nele. "Se uma cultura do conflito tomou conta da sociedade estadunidense, com tumultos em casa e guerras no exterior, o mundo da comunidade seria de harmonia. Se o Estado empregava sistemas massivos de armas para destruir povos distantes, os novos comunalistas empregariam tecnologias de pequena escala – variando de machados e enxadas a amplificadores, luzes estroboscópicas, projetores de slides e LSD – para reunir as pessoas e permitir que elas experimentassem sua humanidade comum", escreveu no livro From Counterculture to Cyberculture.16

Os comunalistas estavam se mudando para o deserto e fazendo as coisas por conta própria. Para isso, precisavam de mais do que apenas ideias. Eles precisavam de ferramentas e o equipamento de sobrevivência mais avançado que pudessem obter. Brand viu uma oportunidade. Depois de fazer uma grande tour por diversas comunidades com sua esposa, Lious, ele pegou uma parte de sua herança para lançar um guia de consumo e estilo de vida direcionado para esse mundo. Se chamava Catálogo Toda a Terra. Ele apresentou ferramentas, tinha discussões sobre ciência e tecnologia, deu dicas sobre agricultura e construção, publicou cartas e artigos de membros de comunidades em todo o país e sugeriu livros e literatura, misturando títulos pop libertarianistas como Atlas Shrugged de Ayn Rand com a Cibernética de Wiener.17 "Era como o Google em forma de brochura, só que 35 anos antes do Google aparecer", foi como Steve Jobs, um jovem fã da revista, o descreveu mais tarde. "Era idealista, cheia de ferramentas legais e grandes ideias".18

O catálogo L. L. Bean, enviado por correspondência, foi o que inspirou Brand a criar seu Catálogo Toda a Terra. Mas não se tratava apenas de comércio. Como outros novos comunalistas, Brand estava apaixonado por ideias cibernéticas – a noção de que toda a vida na Terra era uma grande e harmoniosa máquina de informações entrelaçadas mexia com suas sensibilidades. Ele viu seus colegas comunalistas como

o início de uma nova sociedade que se encaixava em um ecossistema global maior. Ele queria que o Catálogo Toda a Terra fosse o tecido conjuntivo que unisse todas essas comunas isoladas, uma espécie de rede de informações impressa em formato revista que todos podiam liam e contribuir e que os unisse em um organismo coletivo.19

O Catálogo Toda a Terra foi um enorme sucesso, e não apenas com os hippies. Em 1971, uma edição especial da revista liderou as listas de livros mais vendidos e ganhou o National Book Award. No entanto, apesar do sucesso cultural e financeiro, Brand enfrentou uma crise de identidade. Quando sua revista ganhou o National Book Award, o movimento comunitário ao qual ele se dedicava e celebrava estava em ruínas.

Anos depois, o cineasta Adam Curtis entrevistou ex-membros de comunidades em seu documentário da BBC All Watched Over by Machines of Loving Grace. Ele descobriu que as estruturas cibernéticas que esses grupos impunham a si mesmas, ou seja, as regras que deveriam achatar e igualar as relações de poder entre os membros e levar a uma nova sociedade harmoniosa, produziram o resultado oposto e, por fim, separaram muitas comunidades.20

"Estávamos tentando criar uma sociedade baseada no entendimento de ecossistemas, uma sociedade baseada em inter-relações e equilíbrio – um sistema biológico homem-máquina trabalhando em conjunto", lembrou Randall Gibson, membro da comuna Synergia no Novo México que trabalhava com uma noção cibernética que ele chamou de eco-técnica.21 A comunidade tinha regras estritas contra ação ou organização coletiva. Os membros precisavam resolver problemas e conflitos por meio de "sessões de conexão", nas quais duas pessoas realizavam discussões individuais à vista da comuna, mas não podiam solicitar apoio ou apoio de mais ninguém. "A ideia da eco-técnica era simplesmente que você fazia parte de um sistema em que haveria menos, senão nenhuma hierarquia", disse Gibson. Por fim, essas sessões de conexão tornaram-se algo mais sombrio: exercícios de vergonha, intimidação e controle, onde membros dominantes se aproveitavam de membros mais fracos e submissos. "Na prática, eram sessões de humilhação de 20 a 30 minutos e geralmente eram recebidas em silêncio pelo resto dos colegas."22

Outras comunidades passaram por transformações semelhantes, transformando-se de experimentos juvenis otimistas em ambientes repressivos e, frequentemente, cultos explícitos de personalidade. “Na verdade, havia medo porque as pessoas que dominavam mais – havia raiva. Havia constantemente um pano de fundo de medo na casa – como um vírus no ar. Como um spyware. Você sabe que está lá, mas não sabe como se livrar dele ”, disse Molly Hollenback, membro de uma comuna chamada The Family, em Taos, Novo México.23 Formada por estudantes da UC Berkeley em 1967, a Família rapidamente se transformou em uma hierarquia rígida, com homens sendo chamados de “senhor” e “Lorde”, e mulheres obrigadas a usar saias e designadas a trabalhos conservadoramente separados por gênero: cozinhar, cuidar das crianças e lavar roupa. Um membro fundador que se chamava Lord Byron presidia o grupo e se reservava o direito de fazer sexo com qualquer mulher da comuna.24

A maioria das comunas durou apenas alguns anos, e algumas menos que isso. “O que as despedaçou foi exatamente o que eles deveriam ter banido: o poder”, explicou Adam Curtis. “As personalidades mais fortes passaram a dominar os membros mais fracos do grupo, mas como se viam como um sistema auto-organizado, as regras desse sistema impediam qualquer oposição organizada a essa opressão.” No final, o que deveriam ser experimentos em liberdade e novas sociedades utópicas simplesmente replicaram e ampliaram a desigualdade estrutural do mundo exterior que as pessoas haviam trazido consigo.

Mas Stewart Brand não admitiu a derrota, nem tentou entender por que a ideologia cibernético-libertarianista subjacente ao experimento fracassou de forma tão espetacular. Ele simplesmente transferiu as ideias utópicas da comunidade mítica para algo que o fascinava há muito tempo: a indústria de computadores em rápido crescimento.

Repaginando Stewart Brand

Aparentemente, os mundos da ARPA e da pesquisa militar em computadores e o cenário hippie da comunidade hippie dos anos 1960 não pode-

riam ser mais diferentes. De fato, eles pareciam ocupar diferentes sistemas solares. Um deles usava uniformes, ternos pomposos, protetores de bolso, estava permeado por pensamentos de guerra, cartões perfurados e hierarquias rígidas. O outro tinha cabelos compridos, amor livre, drogas, música maluca, hostilidade à autoridade e uma existência decadente e irregular.

Mas as diferenças eram superficiais. Em um nível mais profundo, as duas cenas operavam no mesmo comprimento de onda cibernético e se sobrepunham em várias frentes. J. C. R. Licklider, Ithiel de Sola Pool e outros engenheiros militares e da ARPA estavam implantando ideias cibernéticas para criar redes de computadores, enquanto sonhavam em construir tecnologia de previsão para administrar o mundo e gerenciar conflitos políticos. Os hippies estavam fazendo o mesmo com suas comunidades cibernéticas. Exceto que, onde a ARPA e os militares eram industriais e globais, as comunas eram pequenas quitandas.

Também havia conexões diretas entre eles. Pegue o Instituto de Pesquisas de Stanford (Stanford Research Institute, SRI), um importante contratado da ARPA que trabalhava em tudo, desde contrainsurgência e guerra química até a administração de um importante nó da rede ARPANET e também um de seus centros de pesquisa. Vários funcionários do SRI eram amigos íntimos de Stewart Brand e contribuintes ativos do Catálogo Toda a Terra.25 Brand frequentava o SRI e até representou o instituto em uma demonstração em 1968 da tecnologia de computador interativa que o Augmentation Research Center de Douglas Englebart desenvolveu sob um contrato da ARPA.26 O evento contou com videoconferência em tempo real e edição colaborativa de documentos usando a ARPANET, que, na época, tinha apenas dois meses de idade.27 E depois havia o próprio Engelbart. O engenheiro e guru da computação interativa era o favorito de Licklider e recebeu milhões em financiamento da ARPA. Ao mesmo tempo, ele fez experiências com LSD administrando doses de ácido em engenheiros de computação para ver se os tornava mais eficientes e criativos. Ele também fez uma turnê por várias comunas e apoiou muito a tentativa do movimento de criar novas formas de sociedades descentralizadas.28

O sentimento era mútuo. A cena da contracultura hippie de Bay Area viveu e respirou as ideias cibernéticas divulgadas pelo complexo

industrial militar dos Estados Unidos. Richard Brautigan, um escritor de cabelos desgrenhados e bigode caído que morava em São Francisco, compôs uma ode à utopia cibernética que demonstra a proximidade espiritual desses dois mundos aparentemente contraditórios. Publicado em 1967 e intitulado "Todos vigiados por máquinas de adorável graça", o poema descreve um mundo no qual os computadores se fundem com a natureza para criar uma espécie de ser divino altruísta que cuidaria de todos nós – um mundo "onde os mamíferos e computadores / convivem em harmonia / mutuamente programada / como água pura / tocando o céu limpo".29 Brautigan entregou seu poema na rua Height, o epicentro do movimento de contracultura. Naturalmente, Brand era fã de Brautigan e publicou seu trabalho no Catálogo Toda a Terra. "Richard não sabia programar. Não sei se ele conhecia alguma coisa de computadores", recordaria Brand mais tarde. Mas você não precisava ser um programador para acreditar.

Havia profunda simpatia e laços estreitos entre os dois mundos, e Stewart Brand levou isso além. No início dos anos 1980, após o colapso do sonho das comunas, ele pegou seu prestígio na contracultura e transformou os ideais utópicos dos novos comunalistas em um veículo de marketing para a crescente indústria de computadores para consumidores. Ele foi fundamental para a causa. Como uma parteira experiente, guiou o nascimento do crescente senso de autoimportância e relevância cultural dessa indústria. Ele era astuto. Brand entendeu que a Bay Area estava no topo de uma importante "crista geológica" econômica e cultural. As placas tectônicas estavam mudando, tremendo e emitindo ondas de choque. Todo o local parecia não estar preparado para um terremoto monstruoso que reestruturaria a sociedade, gerando novas indústrias, novos negócios, uma nova política e uma cultura radicalmente nova. Ele realmente acreditava nisso e ajudou uma nova classe de empresários de computadores a se ver como ele os via – como rebeldes e heróis da contracultura. Ele então os ajudou a vender essa imagem para o resto do mundo.

Nesse novo papel, Brand ainda era um idealista utópico, mas também um empreendedor. "Sou um homem de pequenos negócios que é atingido pelo mesmo tipo de problemas que qualquer pequeno empreendedor enfrenta", disse ele à revista Newsweek.30 Nos anos que viriam, à medida que os computadores pessoais ganharam força, ele reuniu em

torno de si uma equipe de jornalistas, marketeiros, profissionais da indústria e outros hippies que se tornaram empreendedores. Juntos, eles replicaram o marketing e a estética que Brand usara durante seus dias no Catálogo Toda a Terra e venderam computadores da mesma forma que vendiam comunas e drogas psicodélicas: como tecnologias de libertação e ferramentas de empoderamento pessoal. Esse grupo contaria a história dessa mitologia entre as décadas de 1980 e 1990, ajudando a ofuscar as origens militares das tecnologias de computadores e de redes, cobrindo-as com a linguagem da contracultura dos anos sessenta. Nesse mundo repaginado, os computadores eram as novas comunas: uma fronteira digital onde a criação de um mundo melhor ainda era possível.

Na linguagem do atual Vale do Silício, Brand “pivotou”. Ele transformou o Catálogo Toda a Terra no Catálogo Toda a Terra de Softwares e na Revista Toda a Terra – revistas anunciadas como "ferramentas e ideias para a era do computador". Ele também lançou a Rede Bons Negócios, uma empresa de consultoria corporativa que aplicou suas estratégias de relações públicas de contracultura a problemas enfrentados por clientes como Shell Oil, Morgan Stanley, Bechtel e DARPA.31 Também organizou uma influente conferência de computadores que reuniu os principais engenheiros de computação e jornalistas.32 Chamava-se simplesmente de “Conferência dos Hackers” e foi realizada no condado de Marin em 1984. Cerca de 150 dos maiores gênios da computação do país compareceram, incluindo Steve Wozniak, da Apple. Brand inteligentemente gerenciou o evento para oferecer ao grupo o máximo valor cultural. Quando ouvimos ele e outros "crentes" contarem como foi, descrevem-no como o "Woodstock da elite dos computadores!" As matérias dos jornais encantaram os leitores com histórias de nerds estranhos, com visões fantásticas do futuro. “Temos que dar ao computador um mundo seu. O maior de todos os hacks é a consciência artificial ”, disse uma pessoa que participou a um repórter do Washington Post. "Minha visão de hacking é uma criatura pequena e confusa que cresce dentro de cada máquina", brincou outra.33

Uma equipe de filmagem da PBS estava no local para gravar um documentário e registrar o papel de Brand em reunir esses hackers. Ele não era o jovem que lançou o Catálogo Toda a Terra duas décadas antes. Seu rosto mostrava sua idade e ele ostentava uma cabeça brilhante e careca, mas seguia entusiasmado. Usava uma camisa xadrez em preto e

branco sob um colete de pele de carneiro e gravava uma música sobre a natureza rebelde dos que se reuniam em Marin.34 "Eles são tímidos, doces, incrivelmente brilhantes e considero essa imagem mais eficaz no sentido de promover a cultura de uma maneira boa do que quase qualquer grupo em que eu possa imaginar" Fora das câmeras, ele foi para as páginas da Revista Toda a Terra para expor mais a natureza rebelde dos programadores de computador. "Acho que hackers – programadores de computador inovadores e irreverentes – são o corpo de intelectuais mais interessante e eficaz desde os autores da Constituição dos EUA", escreveu em uma introdução a uma foto da Conferência de Hackers de 1984. “Nenhum outro grupo que conheço se propôs a libertar uma tecnologia e conseguiu... A alta tecnologia agora é algo que os consumidores em massa usam, e não apenas ela usa eles, e isso é uma coisa importante no mundo.” E acrescentou: “A sub-subcultura mais silenciosa dos anos 1960 emergiu como a mais inovadora e poderosa – e a que o poder mais desconfia”.35

A Conferência dos Hackers foi um grande momento na história cultural do Vale do Silício. Ajudou a apresentar programadores de computador ao público de uma maneira totalmente diferente. Já não eram engenheiros que trabalhavam para grandes corporações e empreiteiros militares, mas "hackers" – gênios e rebeldes contrários ao sistema. Embora Brand tenha sido uma figura importante que impulsionou essa mudança de percepção, ele não estava operando isoladamente, mas representava uma grande mudança cultural.

O ano de 1984 foi grande e simbólico para a indústria de computadores, para além da Conferência dos Hackers da Brand. Naquele ano, William Gibson publicou o Neuromancer, um romance de ficção científica sobre um hacker viciado em drogas que luta contra um perigoso mundo cibernético de realidade virtual dirigido por empresas assustadoras e seus supercomputadores divinos. Era um mundo sem regras, sem leis, apenas poder e inteligência. Gibson pretendia que fosse uma metáfora para o crescimento do poder corporativo irrestrito no momento em que a pobreza e a desigualdade atingiram o pico sob o mandato de Ronald Reagan. Era um experimento de ficção científica sobre o que aconteceria se essa tendência chegasse à sua conclusão natural. Neuromancer cunhou o termo ciberespaço. Também lançou o movimento cyberpunk, que respondeu à crítica política de Gibson de uma maneira

cardinalmente diferente: aplaudiu a chegada dessa distopia cibernética. Computadores e hackers eram rebeldes contraculturais assumindo o poder. Eles eram fodas.

Nesse mesmo ano, a Apple Computer lançou seu anúncio “1984” para o Macintosh. Dirigida por Ridley Scott, que acabara de impressionar o público com o hit distópico Blade Runner, e foi ao ar durante o Super Bowl, a mensagem da Apple não poderia ter sido mais clara: esqueça o que você sabe sobre a IBM ou computadores mainframes corporativos ou sistemas informáticos militares. Com a Apple no comando, os computadores pessoais são o oposto do que costumavam ser: não se trata de dominação e controle, mas de rebelião e empoderamento individuais. "Em uma saída impressionante da abordagem direta de comprar este produto da maioria das empresas americanas, a Apple Computer apresentou sua nova linha de computadores pessoais com a provocativa alegação de que o Macintosh ajudaria a salvar o mundo da sociedade paralela do romance de George Orwell", relatou o New York Times.36 Curiosamente, o jornal apontou que o anúncio "1984" havia surgido de outra campanha que a empresa abandonara, mas que explicitamente falara sobre a capacidade de usar computadores incorretamente. Um rascunho dessa campanha dizia: “É verdade que existem computadores monstros à espreita em grandes empresas e grandes governos que sabem tudo – coisas como: em que motéis você ficou até quanto dinheiro você tem no banco. Mas, na Apple, estamos tentando equilibrar a balança, dando às pessoas o tipo de poder do computador que antes era reservado às empresas.”

O cofundador e CEO da Apple, Steve Jobs, era um grande fã de Stewart Brand.Ele era apenas uma criança no final dos anos 1960, quando a revista e a cultura das comunidades estavam no auge de popularidade e poder, mas ele leu o Catálogo Toda a Terra e absorveu essa cultura em sua própria visão de mundo. Portanto, não era de surpreender que a campanha publicitária original da Apple, que sugeria computadores como monstros corporativos e governamentais, fosse deixada na lixeira, enquanto a visão de Brand dos computadores pessoais como uma tecnologia de liberdade prevalecia.

Stewart Brand ofereceu uma visão poderosa que foi plantada profundamente na psique estadunidense. O seu esforço para renomear a tec-

nologia militar de computadores como libertação coincidiu com uma força menos visível: a privatização gradual da ARPANET e a criação de uma Internet comercial global.

O homem que privatizou a Internet

Em algum momento de 1986, Stephen Wolff entrou nos escritórios da Fundação Nacional de Ciências, na Wilson Boulevard, em Washington, DC, do outro lado do rio Potomac, da Casa Branca, e depois de virar a esquina do Pentágono.

Como a maioria das pessoas envolvidas no início da Internet, Wolff era um militar. Alto e magro, com uma voz calma e tranquilizadora, ele passou a década de 1970 trabalhando na ARPANET no Laboratório de Pesquisa Balística do Exército dos EUA no Aberdeen Proving Ground, uma área de pântano e floresta luxuriantes que se projetam na Baía de Chesapeake, cerca de 55 quilômetros ao norte de Baltimore. Aberdeen, agora fechado, desfrutou de uma história longa e documentada. Foi estabelecido durante a Primeira Guerra Mundial e destinado a desenvolver e testar artilharia de campo e armas pesadas: canhões, armas de defesa aérea, munição, morteiros e bombas. Norbert Wiener serviu lá como uma calculadora humana pré-computador, elaborando trajetórias balísticas para os canhões enormes que estavam sendo desenvolvidos. Durante a Segunda Guerra Mundial, foi o berço do primeiro computador totalmente digital e eletrônico da América, o ENIAC. Na década de 1960, Aberdeen estava conectado a algo um pouco mais assustador: uma série de experimentos de "laboratório de guerra limitado", nos quais o Corpo de Químicos do Exército dos EUA usava drogas alucinógenas – incluindo LSD e o superalucinogênio conhecido como BZ, que poderia colocar uma pessoa em coma alucinatório que dura dias – como armas químicas.38

O trabalho de Stephen Wolff em Aberdeen, na década de 1970, tinha a ver com a ARPANET e sua ligação à rede de supercomputadores do Exército dos EUA.39 Em 1986, o Escritório de Rede da Fundação Nacional de Ciências contratou-o para fazer a mesma coisa, mas com

uma grande mudança: ele deveria construir uma rede financiada pelo governo que estendesse o design da ARPANET para o mundo civil e, em seguida, passasse essa rede para o setor privado.40 No final das contas, Wolff supervisionou a criação e a privatização da Internet.

Quando falei com Wolff, perguntei: "É certo chamá-lo de o homem que privatizou a Internet?"

"Sim, essa é uma avaliação acertada", respondeu ele.41

Mesmo antes de Stephen Wolff chegar à Fundação Nacional de Ciências, estava claro que os dias da ARPANET estavam contados. Em 1975, o Pentágono havia dispensado oficialmente a ARPA de suas responsabilidades pela administração da rede e a colocou sob o controle direto da Agência de Comunicação de Defesa. O exército, a marinha, a força aérea e a Agência de Segurança Nacional começaram a construir suas próprias redes baseadas na tecnologia ARPANET. Eles mantinham conexões com a infraestrutura original da ARPANET, mas a rede física, com suas limitadas velocidades de modem de 56K, estava começando a capengar. O experimento foi um sucesso, mas, à medida que a década de 1980 se aproximava, parecia que a ARPANET original seria jogado no lixo.

A rede havia se tornado obsoleta, mas a tecnologia e a estrutura em que era executada estavam apenas começando. Muitos dos arquitetos e designers originais da ARPANET ganharam muito dinheiro com sua experiência na ARPA. Vários migraram para empregos lucrativos no setor privado da crescente indústria de redes de computadores; outros permaneceram no Pentágono, pressionando e evangelizando para uma adoção mais ampla do design da rede ARPANET. Muitos estavam ansiosos para ver a ARPANET original crescer além dos círculos militares e entrar em uma rede comercial que todos pudessem usar.42 A Fundação Nacional de Ciências (National Science Foundation, NSF), uma agência federal criada pelo Congresso em 1950 com a missão de "promover o progresso da ciência" e "garantir a defesa nacional", foi o veículo que acabaria por fazer o trabalho.

No início dos anos 1980, a NSF administrava uma pequena rede que conectava um punhado de departamentos de ciências da computação de algumas universidades à ARPANET. Em 1985, os administrado-

res desejavam expandir o projeto em uma rede maior e mais rápida que conectasse um conjunto maior de universidades, estendendo a ARPANET para fora dos círculos militares e da ciência da computação e disponibilizando-a a todos os usuários acadêmicos e educacionais.43 Com base em sua década de experiência conectando supercomputadores do Exército dos EUA à ARPANET em Aberdeen, Wolff foi convidado para criar e gerenciar esse novo projeto de rede educacional – chamado NSFNET.

A primeira versão do NSFNET foi lançada online em 1986. Foi um esforço modesto, conectando centros de supercomputadores de cinco universidades financiadas pela NSF. O objetivo era que pudessem compartilhar dados e conectá-los a um conjunto mais amplo de universidades que já estavam ligadas à antiga ARPANET militar. O alcance da rede era limitado, mas a demanda era tão alta que causou um travamento no sistema. Suas linhas alugadas insignificantes tinham o rendimento combinado de um modem lento e não conseguiam lidar com o aumento de usuários. Claramente, a NSFNET precisava de uma grande atualização e mais largura de banda. A pergunta era: como seria essa nova rede?

A resposta veio rapidamente.

"Começando com a inauguração do programa NSFNET em 1985, tínhamos a esperança de que ele crescesse para incluir todas as faculdades e universidades do país", lembrou Wolff em uma entrevista.44 "Mas a noção de tentar administrar uma rede de três mil nós a partir de Washington – bem, não havia toda essa arrogância em Beltway".

Arrogância, de fato. Este foi o auge da era Reagan, um tempo de privatização e desregulamentação, quando a propriedade pública de infraestrutura vital era considerada uma relíquia bárbara que não tinha lugar no mundo moderno. Tudo estava sendo desregulado e privatizado – do setor bancário aos setores de telecomunicações e transmissão. Wolff e sua equipe na NSF, como os funcionários públicos obedientes que eram, seguiram a linha.

No início de 1987, ele e sua equipe finalmente criaram um design para uma NFSNET aprimorada e atualizada. Essa nova rede, um projeto do governo criado com dinheiro público, conectaria universidades e seria projetada para funcionar como um sistema de telecomunicações

privatizado. Esse era o entendimento implícito que todos na NSF concordavam. Eles viam a natureza pública da NSFNET como um estado transitório: um pequeno girino do governo que faria a transição para um sapo-boi comercial. De acordo com as especificações, a nova NSFNET seria construída como uma rede de duas camadas. A camada superior seria uma rede nacional, uma "espinha dorsal" de alta velocidade que abrangeria todo o país. A segunda camada seria composta de "redes regionais" menores que conectariam as universidades ao backbone (à espinha dorsal). Em vez de construir e gerenciar a própria rede, a NSF terceirizaria a rede para um punhado de empresas privadas. O plano era financiar e nutrir esses provedores de rede até que eles se tornassem autossuficientes. Aí então seriam soltos e permitidos de privatizar a infraestrutura de rede que construíram para a NSFNET.

Mais tarde, em 1987, a NSF firmou contratos pelo seu design atualizado da NSFNET. A parte mais importante do sistema, a espinha dorsal, era administrada por uma nova corporação sem fins lucrativos, um consórcio incluindo IBM, MCI e o estado de Michigan.45 As redes regionais de segundo nível foram criadas por uma dúzia de outros consórcios privados recém-criados. Com nomes como BARRNET, MIDNET, NYSERNET, WESTNET e CERFNET, eles eram administrados por uma mistura de universidades, instituições de pesquisa e terceirizadas militares.46

Em julho de 1988, o backbone da NSFNET entrou online, conectando treze redes regionais e mais de 170 campi diferentes em todo o país.47 A rede física rodava nas linhas T-1 da MCI, capazes de transmitir 1,54 megabits por segundo, e era roteada através de comutadores de dados construídos pela IBM. A rede se estendeu de San Diego a Princeton – percorrendo pontos de troca de redes regionais em Salt Lake City, Houston, Boulder, Lincoln, Champaign, Ann Arbor, Atlanta, Pittsburgh e Ithaca. Também foi lançada uma linha transatlântica internacional até a Organização Europeia de Energia Nuclear em Genebra.48 A rede foi um enorme sucesso na comunidade acadêmica.49

Mesmo com o aumento da demanda, os gerentes da NSF começaram o processo de privatização. “Dissemos a eles: 'Vocês terão que sair e encontrar outros clientes. Não temos dinheiro suficiente para apoiar os regionais para sempre. Então eles foram atrás”, explicou Wolff. “Tenta-

mos ... garantir que os regionais mantivessem seus livros de contabilidade em ordem e que os contribuintes não subsidiassem diretamente as atividades comerciais. Mas, por necessidade, forçamos as regionais a se tornarem fornecedores de redes de uso geral."50

Dizer aos fornecedores da NSFNET para diversificarem sua base de clientes buscando clientes comerciais – até parece uma decisão menor. No entanto, é um detalhe crucial que teve um grande impacto, permitindo que a agência, alguns anos depois, privatizasse silenciosa e rapidamente a Internet, enquanto fazia parecer que a transição era inevitável e até natural. As pessoas de dentro entendiam a gravidade do que Wolff e a NSF estavam fazendo. Eles viram isso como uma espécie de truque inteligente.

Vinton Cerf, que em 1982 havia deixado o emprego na ARPA para chefiar a divisão de redes da MCI, descreveu o esquema de provedor de rede público-privado de Wolff como "brilhante". Ele disse: "A criação dessas redes regionais e a exigência de que elas se tornassem autofinanciadas foram a chave para a evolução da Internet atual".51

Cerf está certo. A Internet é talvez uma das invenções públicas mais valiosas do século XX, e as decisões tomadas por alguns funcionários importantes não eleitos da burocracia federal colocaram a Internet no caminho certo para a privatização. Não houve debate público real, discussão, dissensão e supervisão. Foi apenas revelado, antes que alguém fora dessa bolha burocrática percebesse o que estava em jogo.

A privatização da Internet – sua transformação de uma rede militar para o sistema de telecomunicações privatizado que usamos hoje – é uma história complicada. Mergulhe fundo o suficiente e você se encontrará em um pântano de agências federais de três letras, siglas de protocolos de rede, iniciativas governamentais e audiências do congresso repletas de jargões técnicos e detalhes entorpecedores. Mas, em um nível fundamental, tudo era muito simples: após duas décadas de financiamento, pesquisa e desenvolvimento pródigos no sistema do Pentágono, a Internet foi transformada em um centro de lucro para o consumidor. O setor empresarial demandava uma fatia desse mercado, e uma pequena equipe de gerentes do governo estava muito feliz em atender a essa exigência. Para fazer isso, com fundos públicos, o governo federal criou uma dúzia de fornecedores de rede do nada e depois os transferiu

para o setor privado, construindo empresas que, no espaço de uma década, se tornariam parte integrante dos conglomerados de mídia e telecomunicações que todos nós conhecemos e usamos hoje – Verizon, Time-Warner, AT&T, Comcast.

Mas como isso realmente aconteceu? Para desvendar a história, é necessário olhar para o primeiro provedor privatizado de NSFNET: um consórcio liderado pela IBM e MCI.52

A Fundação Nacional de Ciências funcionava com um mandato educacional e podia apoiar apenas iniciativas que tivessem essa mesma característica. Legalmente, os contratados da NSFNET não tinham permissão para rotear seu tráfego comercial através da rede financiada pelo governo. Esses termos foram incorporados ao contrato da "Política de uso aceitável" da agência federal e eram bastante claros. Como a rede poderia ser privatizada se não conseguia rotear o tráfego comercial? Mais tarde, os gerentes da NSF alegaram que os provedores da NSFNET não violavam esses termos e direcionavam o tráfego comercial por meio de uma infraestrutura de rede separada e privada. Mas um acordo de bastidores que a NSF fez com seu operador de backbone mostra que a verdade é um pouco mais obscura.

Em 1990, o consórcio MCI-IBM, com a aprovação da NSF, se dividiu em duas entidades corporativas: uma organização sem fins lucrativos chamada Serviços de Rede Avançados (Advanced Network Services, ANS) e uma organização com fins lucrativos denominada ANS Sistemas CO + RE. Os Serviços de Rede Avançados continuaram a contratar a NSF para manter e executar o backbone físico da NSFNET. Enquanto isso, sua divisão com fins lucrativos, ANS CO + RE, vendia serviços de rede comercial para clientes em uma nova rede chamada ANSNET.53 É claro que essa nova ANSNET funcionava exatamente na mesma infraestrutura de rede física que alimentava a NSFNET. Legalmente, porém, os dois – NSFNET e ANSNET – foram tratados como entidades completamente separadas pela Fundação Nacional de Ciências, o que significava que, apesar da Política de Uso Aceitável que proibia o tráfego comercial na NSFNET, o consórcio IBM-MCI tinha uma luz verde para fazer exatamente isso por lucro.54 Foi uma manobra inteligente. Em um nível básico, permitiu ao consórcio MCI-IBM contabilizar o mesmo ativo duas vezes, embolsando dinheiro do governo para

administrar a NSFNET e depois vendendo essa mesma rede para clientes comerciais. Mais fundamentalmente, permitiu que uma entidade corporativa com participação direta no negócio de redes de computadores privatizasse um ativo do governo sem fazê-lo explicitamente. Foi exatamente assim que os executivos da recém-formada divisão ANS da MCI-IBM viram: “Nós privatizamos a NSFNET”, o presidente da ANS se gabou em um workshop da indústria de redes em Harvard em 1990.55

Essa mudança público-privada não foi anunciada ao público e também foi ocultada de outros provedores da NSFNET. Quando finalmente descobriram a existência desse acordo astuto, um ano depois, eles deram um alarme e acusaram a agência de privilegiar a privatização a rede para uma corporação. Alguns pediram uma investigação do Congresso sobre o que consideravam má administração e possivelmente fraude. “É como pegar um parque federal e entregá-lo ao K Mart. Não está certo ”, disse um gerente de um grande fornecedor de NSFNET ao New York Times.56

Eles tinham o direito de ficar chateados. Esse acordo de privatização do backbone deu a uma empresa poderosa uma posição privilegiada que lhe permitiu dominar rapidamente o mercado de redes comerciais, frequentemente à custa de outros fornecedores regionais da NSFNET.57 A chave para essa vantagem foi o próprio backbone da NSFNET. Construída e sustentada com fundos do governo, a rede abrangeu o território dos Estados Unidos e tinha conexões com mais de trinta outros países. As redes regionais, por outro lado, eram menores, geralmente restritas a áreas geográficas como a Grande Nova York, o Centro-Oeste ou o norte da Califórnia. Aqueles que se expandiram para o mercado comercial nacional não conseguiram direcionar o tráfego comercial através do backbone da NSFNET, mas tiveram que construir suas próprias redes privadas sem financiamento do governo. Em resumo, a NSF subsidiou diretamente a expansão nacional dos negócios do consórcio MCI-IBM. A empresa usou sua posição privilegiada para atrair clientes comerciais, dizendo que seu serviço era melhor e mais rápido porque tinha acesso direto ao backbone nacional de alta velocidade.58

Stephen Wolff entendeu que apoiar uma empresa de telecomunicações como a MCI poderia levar a uma situação em que um punhado de empresas poderosas acabaria controlando a recém-criada Internet,

mas deixou de lado esses perigos. Como Wolff explicou em uma entrevista na época, seu principal objetivo era criar uma Internet comercial viável. Regular a justiça e as práticas competitivas era o trabalho de outra pessoa.59 Em um nível muito básico, ele estava certo. Seu objetivo era apenas construir uma rede, não regulá-la. O problema era que, ao construir uma rede privatizada, ele também estava construindo uma indústria e, por extensão, estabelecendo as regras básicas que governavam e regulamentavam essa indústria. Essas coisas estavam entrelaçadas.60

O estilo de gerenciamento laissez-faire de Wolff provocou protestos entre os pequenos fornecedores regionais da NSFNET. Houve acusações de conflito de interesses, informações privilegiadas, favoritismo. William Schrader, presidente de um provedor da área de Nova York chamado PSINET, acusou explicitamente a NSF de conceder o monopólio dos ativos do governo a uma única empresa privilegiada. "O governo privatizou a propriedade de um recurso federal", disse ele em uma audiência no Congresso de 1992 realizada para investigar uma possível má administração do governo da NSFNET. "A privatização desnecessariamente forneceu ao contratado [IBM-MCI] uma posição de monopólio exclusivo para usar os recursos federais pagos pelos fundos dos contribuintes".61

O PSINET de Schrader se uniu a outros provedores regionais de NSFNET para pressionar o governo a acabar com os privilégios da MCI-IBM e finalmente abrir a rede para tráfego comercial irrestrito. "É possível criar condições de concorrência equitativas alterando as políticas atuais da NSF que favorecem um concorrente", disse Schrader ao Congresso.62

Schrader não estava contestando a privatização em si. Por que ele o faria? Sua própria empresa, PSINET, também havia sido desmembrada de um provedor regional da NSFNET, semeado com dinheiro federal como uma entidade com fins lucrativos.63 Como a ANS da IBM-MCI, o provedor PSINET representou uma privatização de fato de um ativo subsidiado pelo governo por alguns privilegiados que estavam no lugar certo na hora certa. Schrader não contestou isso. Sua oposição era em relação à NSF dar a um grupo diferente – e talvez mais poderoso – de privilegiados mais vantagens do que sua empresa havia recebido.

Essa era uma briga entre empresas concorrentes de rede subsidiadas pelo governo em um setor criado pelo governo. Não foi uma luta pela privatização. Foi uma disputa sobre como dividir os lucros futuros de bilhões de dólares em um mercado emergente.

Em meados da década de 1980, enquanto Stephen Wolff planejava a atualização da NSFNET, os Estados Unidos enfrentavam dois booms relacionados à tecnologia de computadores: a explosão de computadores pessoais baratos e o fácil acesso às redes de computadores. Primeiro, a IBM lançou um poderoso computador pessoal e licenciou o design para que qualquer fabricante de computadores pudesse fabricar componentes IBM compatíveis. Alguns anos depois, em 1984, a Apple lançou o Macintosh, com uma interface gráfica de usuário e mouse. O sistema operacional DOS da Microsoft para computadores IBM foi seguido por uma versão crua do Windows. De repente, os computadores eram fáceis de usar e acessíveis. Não eram mais apenas empresas gigantes, grandes universidades e agências militares e do governo – empresas menores e entusiastas nerd da classe média poderiam ter seus próprios sistemas. Logo ficou claro que o verdadeiro poder do computador pessoal não era pessoal, mas social. Os computadores permitiam que as pessoas acessassem servidores remotos e se conectassem com outros computadores, comunicando e compartilhando informações com pessoas a centenas e milhares de quilômetros de distância. Centenas de milhares de pessoas levaram computadores para casa, ligaram seus modems e se conectaram a uma forma estranha e primitiva da Internet.

Algumas empresas selecionadas forneciam acesso semelhante à ARPANET a grandes corporações desde a década de 1970. Mas, no final dos anos 1980, diversos tipos de serviços de conexão discada e rede surgiram em todo o país. Havia grandes empresas como CompuServe, Prodigy e America Online, além de centenas de empresas menores. Alguns, não mais do que quadros de mensagens através de conexão discadas, eram executados como hobbies em servidores montados em porões e garagens. Outras eram pequenas empresas que apresentavam uma série de recursos: fóruns, salas de bate-papo, e-mail, jogos rudimentares de computador e notícias. Todos eles eram simples e baseados em texto, uma sombra da Internet real que surgiria mais tarde, mas eram extremamente populares. Até Stewart Brand entrou a bordo. Ele foi cofundador de um painel de mensagens chamado A Fonte, que fornecia

um fórum e um local de encontro on-line para sua vasta rede de parceiros de negócios hippie, artistas, escritores e jornalistas. A fonte se tornou popular muito rapidamente, transformando-se em um centro social para os futuros "digirati" – formadores de opinião da Bay Area, empreendedores, autores, hackers e jornalistas que surgiram na década de 1990 para moldar a cultura digital.

Essa não era a Internet conectada globalmente que conhecemos hoje. Serviços como A Fonte e America Online não estavam conectados um ao outro e permitiam a comunicação apenas entre membros do mesmo serviço. Efetivamente, eles foram isolados, pelo menos por um tempo. Todos na indústria entendiam que essa seria uma indústria enorme e extremamente lucrativa, e que algum tipo de rede nacional conectaria tudo. “Não era segredo que, qualquer que fosse a rede na época, ela se tornaria um grande sucesso comercial em algum momento. Ninguém nunca duvidou disso”, disse Wolff em uma entrevista.65

De fato, os prestadores de serviços da NSFNET começaram a lutar pelo controle desse mercado inexplorado e crescente, assim que Stephen Wolff lhes deu luz verde para privatizar suas operações. Era por isso que acontecia a luta entre fornecedores como PSINET e ANS. Eles estavam se refestelando, felizes por o governo bancar a rede e ainda mais felizes por ele estar prestes a sair do negócio. Havia muito dinheiro a ser ganho. De fato, no final dos anos 1990, o humilde provedor PSINET de Schrader tinha clientes em 28 países e valia US$ 3 bilhões na NASDAQ.66

Perguntei a Stephen Wolff sobre a privatização furtiva da Internet, querendo saber como era possível que uma decisão dessa magnitude fosse executada sem a participação do público ou discussões sobre o que isso implicaria. Foi chocante para mim que uma pessoa, ou mesmo um grupo de pessoas, tivesse tanto poder.

Além das discussões interindustriais, não havia oposição real ao plano de Stephen Wolff de privatizar a Internet – não dos membros da NFSNET, do Congresso e certamente também não do setor privado.67 “Eu tinha pessoas trabalhando para mim e todos concordamos que esse era o caminho a seguir”, disse Wolff. "Não houve nenhum conflito lá."68 De fato, o oposto era verdadeiro. Seja dentro ou fora da NSF, parecia que todos apoiavam esse plano.

As empresas de cabo e telefone pressionaram pela privatização, assim como democratas e republicanos no Congresso.69 “Houve pouco debate público ou oposição à privatização da NSFNET”, escrevem Jay Kesan e Rajiv Shah em sua dissecação detalhada do processo de privatização da Internet: “Engane-nos uma vez, que vergonha de vocês. Engane-nos duas vezes, que vergonha de nós”. “No início dos anos 1990, a política de telecomunicações para ambos os partidos políticos se baseava em noções de desregulamentação e concorrência. Em várias ocasiões anteriores à privatização da NSFNET, políticos e executivos da área de telecomunicações deixaram claro que o setor privado possuiria e operaria a Internet.”70

O senador Daniel Inouye, democrata do Havaí, foi um dos poucos funcionários eleitos em Washington que se opuseram a essa privatização generalizada. Ele queria amenizar a pressão pela privatização com uma proposta que reservaria 20% da capacidade futura da Internet para uso não comercial por organizações sem fins lucrativos, grupos comunitários locais e outros grupos de benefício público.71 Seu raciocínio era que, como o governo federal havia financiado a criação dessa rede, deveria poder reservar uma pequena parte para o público. Mas sua proposta modesta não era párea para o lobby da indústria e o fervor da privatização de seus colegas no Congresso.

Em 1995, a Fundação Nacional de Ciências aposentou oficialmente a NSFNET, entregando o controle da Internet a um punhado de provedores de redes privadas que havia criado menos de uma década antes. Não houve votação no Congresso sobre o assunto.72 Não houve referendo ou discussão pública. Isso aconteceu por decreto burocrático, e o projeto privatizado da rede, financiado pelo governo, por Stephen Wolff, fez com que a privatização parecesse perfeita e natural.

Um ano depois, o presidente Bill Clinton assinou a Lei de Telecomunicações de 1996, uma lei que desregulamentou o setor de telecomunicações, permitindo, pela primeira vez desde o New Deal, uma propriedade cruzada quase ilimitada da mídia: empresas de cabo, estações de rádio, estúdios de cinema, jornais, empresas de telefonia, emissoras de televisão e, é claro, provedores de serviços de Internet.73 A lei desencadeou uma consolidação maciça, culminando em apenas algumas empresas verticalmente integradas que possuíam a maior parte do mercado

estadunidense de mídia. "Esta lei é uma legislação verdadeiramente revolucionária que trará o futuro à nossa porta", declarou o presidente Clinton ao assinar o ato.

Um punhado de poderosas empresas de telecomunicações absorveu a maioria dos provedores privatizados de NSFNET que haviam sido criados com fundos da Fundação Nacional de Ciências uma década antes. O provedor regional da área da baía de São Francisco tornou-se parte da Verizon. O do sul da Califórnia, pertencente à empreiteira militar General Atomics, foi absorvido pela AT&T. O provedor de Nova York tornou-se parte da Cogent Communications, uma das maiores empresas de backbone (espinha dorsal) do mundo. A espinha dorsal da internet dos EUA foi para a Time-Warner. E a MCI, que administrava a espinha dorsal junto com a IBM, se fundiu com a WorldCom, combinando dois dos maiores provedores de serviços de Internet do mundo.74

Todas essas fusões representaram a centralização corporativa de um poderoso novo sistema de telecomunicações criado pelos militares e introduzido na vida comercial pela Fundação Nacional de Ciências.75 Em outras palavras, a Internet nasceu.76

Em meio a toda essa consolidação, surgiu uma nova publicação de tecnologia que enxertou os ideais utópicos das comunidades cibernéticas de Stewart Brand no fervor do mercado livre nos anos 1990. Ela ajudou a vender essa Internet privatizada emergente como uma verdadeira revolução política contracultural: chamava-se Wired.

A Terra Toda 2.0

Louis Rossetto, um graduando esbelto com um corte de cabelo de Patrick Swayze, começou a revista Wired em 1993. Rossetto cresceu em Long Island em uma família católica conservadora. Seu pai, Louis Rossetto Sr., era executivo de uma grande gráfica e trabalhou no desenvolvimento de mísseis e produção de armas durante a Segunda Guerra Mundial.77 O jovem Rossetto se matriculou na Universidade de Columbia no final dos anos 1960 e esteve lá durante os protestos estudantis

contra a Guerra do Vietnã e a militarização da pesquisa acadêmica da ARPA. Observou seus colegas ocuparem prédios e se confrontarem violentamente com a polícia, mas ele não compartilhava suas preocupações.79 Rossetto estava no lado oposto das barricadas. Ele era contra a política anti-guerra de esquerda que dominava os círculos radicais estudantis de Nova York. Foi presidente dos republicanos da faculdade de Columbia e um obstinado defensor de Richard Nixon.

Toda a atividade política no campus e a natureza cada vez mais violenta dos protestos o levaram mais à direita: para Ayn Rand, o anarquismo libertarianista e as idéias dos fundamentalistas antigovernamentais do século XIX e dos darwinistas sociais. Ele foi co-autor de um ensaio na Revista New York Times que explicava a filosofia do libertarianismo e criticava o foco da Nova Esquerda na redistribuição da riqueza e nas reformas democráticas. Para ele, esse tipo de governo expansivo era o inimigo.Entre seus heróis estavam Ayn Rand e Karl Hess III, ex-redator de discurso do senador Barry M. Goldwater, que se autodenominou um libertarianista radical e viu a tecnologia da computação como a principal arma antigovernamental: “Em vez de aprender a fabricar bombas, os revolucionários deveriam dominar a programação de computadores”, disse a um jornalista em 1970.81

Rossetto não seguiu o conselho de Hess. Em vez disso, ele se matriculou em um curso de negócios na Universidade de Columbia e acabou se formando. Sonhava em se tornar um romancista e passou a década seguinte à deriva no mundo. Para um homem com tendências libertarianista de direita, Rossetto certamente tinha uma propensão a aparecer em lugares onde ocorriam insurgências de esquerda: esteve no Sri Lanka durante a rebelião tamil e foi ao Peru a tempo da insurgência maoista do Sendero Luminoso. Ele também conseguiu sair com os mujahedeen no Afeganistão e apresentou relatórios brilhantes no Christian Science Monitor sobre sua luta contra a União Soviética auxiliados com armas estadunidenses.82 Rossetto viajou para a zona de guerra pegando carona em uma caminhonete com combatentes jihadistas.83

Em meio a tudo isso, ganhava dinheiro escrevendo editoriais para uma pequena empresa de investimentos em Paris; conheceu sua futura esposa Jane Metcalfe, que veio de uma família antiga em Louisville, Kentucky; e lançou uma das primeiras revistas de tecnologia chamada

Electric Word, financiada por uma empresa de software de tradução holandesa.84 A revista faliu, mas durante seu tempo lá Rossetto entrou em contato com Stewart Brand e sua equipe de impulsionadores da tecnologia da Bay Area. O contato com essa subcultura influente o fez perceber que o mundo não tinha uma revista de estilo de vida de tecnologia sólida. Era isso que ele queria criar.

Em 1991, Rossetto e Metcalfe se mudaram para Nova York para iniciar a revista, mas todos os seus investidores desapareceram aos poucos. Por alguma razão, eles não conseguiram despertar empolgação. As indústrias de computadores e redes estavam pegando fogo na área da baía de São Francisco, mas ninguém queria apoiar seu projeto. Ninguém, exceto uma pessoa: Nicholas Negroponte, um engenheiro e empresário rico que passou mais de duas décadas trabalhando na ARPA.

Negroponte veio de uma família rica com muitos contatos. Seu pai era um magnata grego da navegação. Seu irmão mais velho, John Negroponte, era um diplomata de carreira e funcionário do governo Reagan que acabara de ser embaixador com práticas altamente controversas em Honduras: foi acusado de participar em uma campanha secreta de contrainsurgência apoiada pela CIA contra o governo sandinista de esquerda na Nicarágua.85

Nicholas Negroponte, como seu irmão mais velho, também estava conectado ao aparato de inteligência militar dos EUA, mas de um ângulo um pouco diferente. Ele era um contratado de longa data da ARPA e havia trabalhado em várias iniciativas militares de computadores no MIT.86 Também havia sido um membro proeminente do Projeto ARPANET Cambridge. No MIT, ele coordenou seu próprio grupo de pesquisa financiado pela ARPA, chamado Machine Architecture Group (MAG).87

O MAG fez todos os tipos de pesquisa para os militares. Ele trabalhou na tecnologia de videoconferência que permitiria ao presidente e seus principais generais, espalhados por todo o país em bunkers subterrâneos, interagir uns com os outros de maneira natural no caso de uma guerra nuclear.88 Desenvolveu um “mapa de vídeo” interativo da cidade de Aspen, no Colorado, que era um ambiente experimental de realidade virtual que poderia ser usado para treinamento de ataques militares.89 Talvez o experimento mais assustador do MAG tenha envolvido a cria-

ção de um labirinto robótico povoado por gerbos (um tipo de roedor). O projeto, chamado SEEK, era uma gaiola gigante cheia de blocos de luz que os animais esbarravam e mudavam de lugar à medida que se moviam pelo ambiente. Um computador observava a cena e utilizava um braço robótico para reorganizar os blocos deslocados e colocá-los em locais que "pensavam" que os animais queriam que eles estivessem. A ideia era criar um ambiente dinâmico mediado por computador – um "modelo mundial cibernético" – que mudasse de acordo com as demandas e desejos dos gerbos.90

Em 1985, Negroponte transformou o Machine Architecture Group em algo mais interessante e mais alinhado com a revolução dos computadores pessoais: o MIT Media Lab, um hub que conectava negócios, contratação militar e pesquisa universitária. Buscou obstinadamente o patrocínio corporativo, tentando encontrar maneiras de comercializar e lucrar com o desenvolvimento da tecnologia de computadores, redes e gráficos que estava desenvolvendo para a ARPA. Por uma pesada taxa anual de associação, os patrocinadores obtinham acesso a toda a tecnologia desenvolvida no Media Lab sem ter que pagar taxas de licenciamento. Foi um grande sucesso. Apenas dois anos depois de abrir suas portas, o Media Lab acumulou uma enorme lista de patrocinadores corporativos. Todas as principais redes de jornais e televisão estadunidenses faziam parte do clube, assim como as principais empresas automobilísticas e de computadores, incluindo General Motors, IBM, Apple, Sony, Warner Brothers e HBO.91 A ARPA, que naquela época havia sido renomeada como DARPA, também era um dos principais patrocinadores.92

O MIT Media Lab foi uma grande sensação na época – tanto que Stewart Brand praticamente implorou a Negroponte por uma chance de aparecer por lá. Em 1986, ele teve a oportunidade de passar um ano no Media Lab como um "cientista visitante". Mais tarde, publicou um livro sobre Negroponte e a tecnologia de ponta que seu laboratório inaugurou no mundo. O livro parece um alegre panfleto de marketing, falando de um mundo de bugigangas de computador, realidade virtual, inteligência artificial e redes de computadores que abarcassem todo o mundo. Brand descreveu Negroponte como um "visionário" singularmente impulsionado a "inventar o futuro", e ele ajudou a consolidar o status de Negroponte como um sacerdote rebelde de alta tecnologia, que atravessou o

mundo das grandes empresas e grandes governos, mas transcendeu os dois.

No início dos anos 1990, quando Rossetto e Metcalfe estavam desesperados por investidores para sua revista de estilo de vida tecnológico, Negroponte era um dos visionários da computação mais respeitados e procurados do mundo. Então, em 1992, armados com uma edição de teste da Wired e um plano de negócios, Rossetto e Metcalfe o encurralaram na Conferência de Tecnologia, Entretenimento e Design, em Monterey, Califórnia – que custava US $ 1.000 por cabeça e hoje é conhecida como TED. Eles fizeram seu discurso e, para sua surpresa, Negroponte ficou impressionado e concordou em ajudá-los a obter financiamento. Ele marcou reuniões com Ted Turner e Rupert Murdoch, mas nenhum dos dois manifestou muito interesse. No final, Negroponte decidiu apoiar o projeto por conta própria. Ele forneceu US $ 75.000 em capital em troca de uma participação de 10%. Era uma quantia insignificante para grande parte dos negócios, mas Rossetto e Metcalfe concordavam. Eles sabiam que ali estava uma oportunidade: Nicholas Negroponte era um grande nome, com profundas conexões com os mais altos escalões dos negócios, da academia e do governo. Eles apostaram que Negroponte ajudaria a impulsionar o fluxo de investimentos, com seu dinheiro e envolvimento, o que atrairia outros grandes atores que estariam dispostos a investir quantias muito maiores na Wired. E eles tinham razão. Depois que Negroponte entrou a bordo, os investimentos começaram a chover.

Para ajudá-lo a criar a nova revista, Rossetto contratou o antigo aprendiz de Stewart Brand como o editor executivo fundador da Wired: Kevin Kelly. Rechonchudo, com uma barba no estilo Amish, Kelly havia trabalhado para Stewart Brand no final dos anos 1980, no momento em que o promotor da contracultura estava começando a afastar seu negócio editorial das comunas em direção à crescente indústria de computadores pessoais. Kelly era um acólito enérgico e ansioso, um homem maduro para uma missão justa.

Filho de um executivo da revista Time, Kelly passou a maior parte da década de 1970 viajando de mochila pelo mundo. Em 1979, enquanto esteve em Israel, ele teve uma visão divina. Por decisão própria, trancou-se para fora do seu hotel e forçou-se a passear por Jerusa-

lém à noite. Adormeceu em uma laje de pedra dentro da Igreja do Santo Sepulcro e, ao acordar, teve uma visão religiosa na qual percebeu que Jesus era o filho de Deus e havia retornado dos mortos como salvador da humanidade. “No final, tudo se resume a uma decisão que se toma. Você segue uma estrada e, dentro dela, tudo faz absoluto sentido”, disse Kelly mais tarde sobre sua experiência de conversão. “Acho que foi isso que fiz. Foi preciso ir a Jerusalém na manhã de Páscoa até os túmulos vazios para realmente desencadear uma aceitação dessa visão alternativa. Depois que aceitei, apareceu uma lógica, um conforto, um impulso que me acompanha por causa dessa visão.”93

Impulso é uma boa palavra para a súbita inspiração religiosa de Kelly. Sua fé em Deus combinava com sua fé no poder do progresso tecnológico, que ele via como parte do plano divino para o mundo. Ao longo dos anos, ele desenvolveu a crença de que o crescimento da Internet, a proliferação de bugigangas eletrônicas e a informatização de tudo ao nosso redor, a fusão definitiva da carne com os computadores, e o upload de seres humanos em um mundo virtual de computadores eram parte de um processo que fundiria as pessoas com Deus e permitiria que nos tornássemos deuses, criando e governando nossos próprios mundos digital e robótico, da mesma forma que o nosso criador. “Eu tive essa visão de Deus, sem limites, se ligando à sua criação. Quando criarmos esses mundos virtuais no futuro – mundos cujos seres virtuais terão autonomia para cometer maldades, assassinar, machucar e destruir – não me parece impensável que o criador do jogo tente consertar o mundo por dentro. Essa, para mim, é a história da redenção de Jesus. Temos um Deus ilimitado que entra neste mundo da mesma maneira que você entraria na realidade virtual e se ligaria a um ser limitado e tentaria redimir as ações dos outros seres, uma vez que são suas criações”, explicou Kelly em entrevista à revista Cristianismo Hoje.

Na Wired, Kelly injetou essa teologia em todas as partes da revista, imprimindo ao texto uma crença inquestionável na bondade e retidão dos mercados e na tecnologia de computador descentralizada, não importava como ela fosse usada.

A primeira edição da Wired chegou às bancas em janeiro de 1993. Ela foi impressa em papel brilhante com tintas neon e apresentava layouts dissonantes que copiaram deliberadamente a estética caótica de

zines DIY usada pelo Catálogo Toda a Terra de Stewart Brand. Assim como a Toda a Terra, a Wired se posicionou como uma publicação para e por uma contracultura digital nova e radical que vivia na vanguarda de um novo mundo em rede. Era também um guia para pessoas de fora que queriam fazer parte deste futuro emocionante, ensinando os leitores a falar e pensar sobre a revolução da tecnologia.94 “Existem muitas revistas sobre tecnologia”, explica Rossetto na edição inaugural da revista. “A Wired não é uma delas. A Wired é sobre as pessoas mais poderosas do planeta atualmente – a Geração Digital. Essas são as pessoas que não apenas previram como a fusão de computadores, telecomunicações e mídia está transformando a vida na chegada do novo milênio, como estão fazendo isso acontecer.”95

A Wired foi um sucesso financeiro e crítico imediato. Tinha trinta mil assinantes até o final de seu primeiro ano. Em seu segundo ano de publicação, conquistou o prestigioso prêmio National Magazine e acumulou duzentos mil assinantes. Lançou uma subsidiária de televisão e um mecanismo de busca chamado HotBot. Em 1996, Louis Rossetto estava pronto para lucrar com o boom e levar a empresa a público. Ele recrutou Goldman Sachs para isso, o que deu à Wired um valor estimado de US $ 450 milhões. A revista foi o rosto do boom das pontocom e a evangelista da Nova Economia, um momento revolucionário da história em que o progresso tecnológico deveria reescrever todas as regras e tornar irrelevante e desatualizado tudo o que havia chegado antes.

A imprensa da indústria de computadores dos EUA datava da década de 1960. Não era chamativa ou moderna, mas abrangia muito bem os negócios emergentes de computadores e redes – não evitava reportagens críticas. Publicações como a ComputerWorld estavam na vanguarda da cobertura do debate sobre privacidade e o perigo de bancos de dados centralizados de computadores na década de 1970 e forneceram uma cobertura aprofundada dos escândalos de privatização da NSFNET nos anos 1990. A Wired era diferente. Assim como o Toda a Terra, a Wired não era exatamente uma empresa jornalística; nem era uma publicação da indústria.96 Parecia mais um centro para fazer contatos e um veículo de marketing para a indústria, um impulsionador destinado a criar uma marca em torno do culto à tecnologia e às pessoas que a criaram e a venderam e depois a reembalaram para a cultura convencional. Ela continuava uma tradição que Stewart Brand havia começado,

cobrindo uma indústria de computadores cada vez mais poderosa com imagens da contracultura para dar a ela uma cara provocativa e revolucionária.

Isso não era apenas uma pose. Nesses primeiros anos, a energia e o evangelismo encharcaram todas as páginas da Wired em cores neon. A revista abordou a tecnologia de ponta do campo de batalha de realidade virtual do Pentágono.97 Criava perfis de criptografadores e empresários marginais que se rebelavam contra o governo federal. Ela fez a cobertura de uma nova classe de capitalistas da computação que construíram um novo mundo tecnológico entre as ruínas da União Soviética. Ela aplaudiu o boom das ponto-com e o mercado de ações em alta, argumentando que não se tratava de uma bolha especulativa, mas de uma nova fase na civilização, quando os avanços tecnológicos fizeram finalmente com que o mercado de ações nunca mais caísse.98 Apresentou resenhas de livros e filmes, exibiu os mais recentes aparelhos de computador, apresentou entrevistas com músicos como Brian Eno e contratou autores de ficção científica como William Gibson para fazer reportagens investigativas. E, é claro, Stewart Brand frequentemente adornava as páginas da revista, começando com a edição inaugural. No mundo da Wired, os computadores e a Internet estavam mudando tudo. Governos, exércitos, propriedade pública de recursos, alinhamento tradicional esquerda-direita de partidos políticos, dinheiro fiduciário – todas essas eram relíquias do passado. A tecnologia de redes de computadores estava varrendo tudo e criando um novo mundo em seu lugar.

O impacto da Wired não foi apenas cultural, mas também político. O fato de a revista ter abraçado e propagandeado um mundo digital privatizado tornou-a uma aliada natural dos poderosos interesses comerciais que pressionavam para desregular e privatizar a infraestrutura de telecomunicações estadunidense.

Entre o panteão de tecno-heróis promovidos nas páginas da revista estavam políticos e especialistas de direita, magnatas das telecomunicações e lobistas corporativos que rodeavam Washington para aumentar a empolgação e pressionar por uma infraestrutura de Internet e telecomunicações privatizada e dominada por empresas. O congressista republicano Newt Gingrich e o guru econômico de Ronald Reagan, George Gilder, enfeitaram a capa da revista, fizeram uma matéria sobre

seus esforços para construir um sistema de telecomunicações privatizado – e suas visões retrógradas sobre os direitos das mulheres, o aborto e os direitos civis foram diminuídas e acabaram sendo ignoradas.99 John Malone, o bilionário monopolista de cabos à frente da TCI e um dos maiores proprietários de terras nos Estados Unidos, também esteve presente. A Wired o colocou na capa como um rebelde punk da contracultura por sua luta contra a Comissão Federal de Comunicações, que estava travando a fusão multibilionária de sua empresa de TV a cabo com a Bell Atlantic, uma gigante telefônica. Ele é visto andando por uma estrada rural vazia com um cachorro ao lado, vestindo uma jaqueta de couro esfarrapada e segurando uma espingarda. A referência é clara: ele era Mel Gibson, do filme Road Warrior (Mad Max), lutando para proteger sua cidade de ser invadida por um grupo selvagem de desajustados que, para estender a metáfora, eram os reguladores da FCC. Qual era a razão pela qual esse bilionário era tão legal? Ele teve a coragem de dizer que atiraria na cabeça da FCC se o governo não aprovasse sua fusão rápido o suficiente.100

A promoção que a Wired fez de empresários de telecomunicações, políticos republicanos e outros atores desse mercado não é tão surpreendente. Louis Rossetto era, afinal, um republicano que se tornou um libertarianista que acreditava na primazia dos negócios e no livre mercado. Não havia discordância ideológica aqui.

Um grupo que frequentou as páginas da Wired e que mais tarde ganhou destaque, foi a Fundação da Fronteira Eletrônica (Electronic Frontier Foundation, EFF).101 Fundada em São Francisco em 1990 por três milionários que participavam do quadro de mensagens A Fonte de Stewart Brand, a EFF começou a fazer lobby para a indústria de provedores de serviços da Internet.102 Em 1993, o cofundador da EFF Mitch Kapor escreveu um artigo para a Wired que expunha a posição dele e da EFF sobre a futura Internet: “Privada, não pública ... a vida no ciberespaço parece estar se moldando exatamente como Thomas Jefferson desejaria: fundada na primazia da liberdade individual e com um compromisso com o pluralismo, a diversidade e a comunidade.”103

A Wired apoiou a visão privatizante da EFF, dando à organização um espaço na revista para expor seus pontos de vista, além de oferecer uma cobertura bajuladora das atividades do grupo. Ela comparou o tra-

balho de lobby que a EFF estava fazendo em nome de seus poderosos doadores de telecomunicações com o cenário da contracultura da área da baía de São Francisco dos anos 1960. “De certa forma, eles são os Merry Pranksters, os apóstolos do LSD, que tropeçaram nos anos 1960 em um ônibus psicodélico chamado Furthur, liderado pelo romancista Ken Kesey e narrado por Tom Wolfe no The Electric Kool-Aid Acid Test”, escreveu para a Wired o jornalista Joshua Quittner em um perfil contando a mudança da EFF para Washington, DC.104 “Mais velhos e mais sábios agora, eles estão na estrada novamente, sem o ônibus e o ácido, mas distribuindo muitos brometos com sons semelhantes: ligue, plugue, conecte-se. Alimente sua cabeça com o rugido de bits pulsando pelo cosmos e aprenda algo sobre quem você é.”

Escrever sobre lobistas corporativos que trabalhavam em nome das telecomunicações para desregular a Internet como se fossem rebeldes e doidões? Pode parecer cínico, até gauche. Mas a Wired era séria e genuína, e de alguma forma se encaixava, e as pessoas acreditavam nisso. Porque no mundo que a Wired construía para seus leitores, qualquer coisa ligada à Internet era diferente e radical. Fazia sentido. A Wired e a EFF eram extensões da mesma grande rede e ideologia de contracultura comercial da nova-direita que emergiram da revista Toda a Terra de Stewart Brand. É aí que reside o verdadeiro poder cultural da Wired: usar os ideais cibernéticos da contracultura para vender a política corporativa como um ato revolucionário.

A revista Wired era apenas mais jovem e moderna, representando uma tendência cultural e política maior na sociedade estadunidense. Nos anos 1990, parecia que onde quer que você olhasse – o jornal Wall Street, a Forbes, o New York Times – especialistas, jornalistas, economistas e políticos previam uma era de abundância em que quase tudo mudaria.105 Antigas regras – escassez, trabalho, riqueza e pobreza, poder político – não se aplicariam mais. Computadores e tecnologia de rede estavam inaugurando a Era da Informação, onde a raça humana seria finalmente libertada: de governos e fronteiras, libertada até de sua própria identidade.106

Em 1996, no mesmo ano em que a Lei de Telecomunicações foi aprovada, Louis Rossetto fez uma previsão ousada: a Internet iria mudar tudo. Tornaria obsoletos até os militares. "Quero dizer, tudo – se você tem um monte de ideias preconcebidas sobre como o mundo funciona, é melhor reconsiderá-las, porque as mudanças que estão acontecendo são

instantâneas", disse ele.107 “E você não precisa de exércitos pesados em uma aldeia global. Talvez precise de uma força policial no máximo, e de boa vontade da parte dos habitantes, mas, caso contrário, não precisará desses tipos dessas estruturas que que estão aí agora.”

Em 1972, Stewart Brand tentou convencer os leitores da Rolling Stone de que os jovens terceirizados do Pentágono escondidos em um laboratório de Stanford, jogando videogame e construindo poderosas ferramentas de computador para a ARPA, não estavam realmente trabalhando a serviço da guerra. Eles estavam invadindo o sistema, usando a tecnologia militar de computadores para acabar com os militares. "O [jogo] Spacewar serve à Paz na Terra [Earthpeace]", escreveu na época. "E assim é também com qualquer brincadeira divertida com computadores, qualquer busca computadorizada de seus próprios objetivos peculiares, e especialmente qualquer uso de computadores para impulsionar outros computadores". Brand viu os computadores como um caminho em direção a uma ordem mundial utópica onde o indivíduo exercia o poder supremo. Tudo o que veio antes – militares, governos, grandes corporações opressivas – desapareceria e um sistema igualitário surgiria espontaneamente. "Quando os computadores se tornarem disponíveis para todas as pessoas, os hackers assumirão o controle: somos todos vagabundos computadorizados, todos mais capacitados como indivíduos e como cooperadores".108

Vinte e quatro anos depois, Rossetto canalizou o mesmo sentimento, promovendo computadores pessoais e a Internet como ferramentas que empoderariam radicalmente o indivíduo e eliminariam os exércitos da existência. Era uma visão deslumbrada e, talvez, egoísta para um homem cuja fama e fortuna repousavam no apoio de Nicholas Negroponte, um terceirizado militar de carreira cujo MIT Media Lab recebeu financiamento da DARPA, enquanto Rossetto pronunciava essas palavras.

Não é de surpreender que o futuro não deu certo de acordo com o sonho de Rossetto. A vila se tornou global, é verdade. Mas os grandes exércitos do passado não desapareceram; de fato, como o tempo mostrou, as redes de computadores e a Internet apenas expandiram o poder das agências militares e de inteligência estadunidenses, tornando-as globais e onipresentes.

Capítulo 5

Vigilância S.A.

O mecanismo de busca perfeito seria como a mente de Deus.
- Emery Brin, no livro
"O que vem a seguir para o Google"

Todo mundo nos EUA se lembra de onde estava na manhã de 11 de setembro de 2001, quando dois aviões derrubaram o World Trade Center.

Eu estava mudando meus pertences para uma sala no lado sul do campus da Universidade da Califórnia, em Berkeley, onde acabava de me transferir de uma faculdade comunitária em San Mateo. Eu não tinha televisão ou computador, e espertofones não existiam. Para receber as notícias, via a CNN o dia todo com um amigo em uma pizzaria suja na Telegraph Avenue, mordiscando fatias frias, bebendo cerveja e geralmente me sentindo confuso e desamparado.

O cofundador da Google, Sergey Brin, também se lembra de onde estava no 11 de setembro. Mas, diferentemente da maioria de nós, ele tinha o poder de fazer alguma coisa. Algo que impactasse.

Naquela manhã, Brin entrou na sede da Google na Bayshore Avenue, em Mountain View. Ele silenciosamente convocou um pequeno grupo de seus engenheiros e gerentes mais confiáveis e encarregou-os de uma tarefa secreta: vasculhar os registros de pesquisa do Google por qualquer coisa que pudesse ajudar a descobrir a identidade das pessoas envolvidas no ataque daquela manhã.

"O Google é grande o suficiente, a essa altura, e é perfeitamente possível que os terroristas o tivessem usado para ajudar a planejar o ataque", disse Brin ao grupo antiterror de mineração de dados reunido ao seu redor. "Podemos tentar identificá-los com base em conjuntos de consultas de pesquisa realizadas durante o período anterior aos sequestros". Para começar, ele reuniu uma lista de possíveis termos de pesquisa, como "Boeing", "capacidade de combustível", "escola de aviação".1 Se eles descobrissem várias palavras-chave relacionadas ao ataque vindas do mesmo computador, Brin instruiu-os a tentar fazer engenharia reversa na pesquisa para revelar a identidade do usuário e possivelmente interromper o próximo ataque.

O plano tinha uma boa chance de sucesso.

Três anos se passaram desde que Brin e seu parceiro, Larry Page, usaram US $ 25 milhões em capital de risco para transformar seu projeto de pós-graduação em Stanford em uma lucrativa empresa de pesquisa. A Google ainda não era a presença onipresente que é hoje, e seu nome ainda não era sinônimo de "pesquisa". De fato, mal estava ganhando dinheiro. Mas a Google estava no caminho de se tornar o mecanismo de pesquisa mais popular do mundo e estava no topo de uma mina de ouro de dados comportamentais. A empresa processava 150 milhões de buscas todos os dias.2 Cada um desses registros continha uma consulta de pesquisa, o local de sua origem, a data e a hora em que foi inserido, o tipo de computador usado e o link do resultado da pesquisa no qual o usuário finalmente clicou. Tudo isso estava vinculado a um arquivo de "cookie" de rastreamento que o Google colocava em todos os computadores que usavam seus serviços.

Individualmente, essas consultas de pesquisa eram de valor limitado. Mas, coletivamente, quando exploradas por padrões de comportamento por longos períodos de tempo, elas poderiam pintar um retrato biográfico rico, incluindo detalhes sobre os interesses, trabalho, relacionamentos, hobbies, segredos, idiossincrasias, preferências sexuais, doenças médicas e visões políticas e religiosas de uma pessoa. Quanto mais uma pessoa digitasse na caixa de pesquisa do Google, mais refinada seria a imagem que apareceria. Multiplique isso por centenas de milhões de pessoas em todo o mundo, cada uma usando o site o dia

todo, e você começará a ter uma ideia dos insondáveis estoques de dados à disposição da Google.

A riqueza das informações nos registros de pesquisa da Google surpreendeu e encantou os engenheiros obcecados por dados da empresa. Era como uma pesquisa contínua de interesses e preferências públicas, uma imagem do que as pessoas se preocupavam, cobiçavam e que tipo de gripe estava se espalhando em suas comunidades. "O Google pode ser um amplo sensor do comportamento humano", foi como um funcionário da Google a descreveu.3

Os dados podem ser extremamente específicos, como um toque no cérebro, permitindo que a Google analise indivíduos com detalhes sem precedentes. As pessoas tratavam a caixa de pesquisa como um oráculo imparcial que aceitava perguntas, cuspia respostas e seguia em frente. Poucas perceberam que ele registrava tudo o que era escrito nele, desde detalhes sobre problemas de relacionamento até – esperava Brin – planos para futuros ataques terroristas.

A equipe de experts caçadores de terroristas que Brin reuniu naquela manhã sabia tudo sobre o tipo de informação contida nos registros de pesquisa; muitos deles passaram os últimos três anos construindo o que em breve se tornaria um negócio de publicidade direcionada de vários bilhões de dólares. Então eles foram procurar suspeitos.

"Em uma primeira execução, a equipe de registros encontrou cerca de cem mil consultas por dia que atendiam a alguns de seus critérios", lembrou Douglas Edwards, primeiro diretor de marketing da Google, em suas memórias "Estou com sorte: as confissões dos funcionários do Google"59. Ele estava lá para a caçada e lembrou-se de que uma análise mais profunda dos registros se mostrou decepcionante. “A busca em nossos registros pelos terroristas do 11 de setembro não revelou nada de interessante. O mais próximo que chegamos foi de um cookie que procurara tanto pelo 'World Trade Center' quanto pelo 'Egypt Air Hijack'. Se os terroristas usaram o Google para planejar seu ataque, eles o fizeram de uma maneira que não conseguimos descobrir."4

Nunca ficou claro se Brin estava revistando os registros exclusivamente por sua própria iniciativa ou se era um pedido não divulgado do FBI ou de outra agência policial. Mas seu esforço de mineração de

dados precedeu mais de um mês a assinatura da Lei Patriota pelo presidente George W. Bush, que daria à Agência Nacional de Segurança ampla autoridade para extrair e minerar dados de registros de pesquisa de maneira muito semelhante.

"Essa nova lei que assino hoje permitirá a vigilância de todas as comunicações usadas por terroristas, incluindo e-mails, Internet e telefones celulares. A partir de hoje, seremos capazes de enfrentar melhor os desafios tecnológicos impostos por essa proliferação das tecnologias de comunicações", disse o presidente Bush em 26 de outubro de 2001, no dia em que assinou a lei. "O povo estadunidense precisa saber que estamos coletando muitas informações e estamos gastando muito tempo tentando reunir o máximo de inteligência possível, para perseguir todas as pistas, verificar todas as dicas para que nós possamos manter os EUA seguros. E isso está acontecendo."5

Em um nível, a busca de Brin para encontrar terroristas era compreensível. Foi uma época aterrorizante. Os Estados Unidos foram dominados pelo medo de que mais ataques terroristas fossem iminentes. Mas, dada a fome do governo por informações – qualquer informação – sobre terroristas em potencial e seus cúmplices, o esforço teve uma dimensão perturbadora. Logo após o 11 de setembro, a CIA pegou dezenas de suspeitos de serem agentes da Al-Qaeda no Afeganistão e no Paquistão e os jogou na Baía de Guantánamo, em muitos casos agindo com informações de segunda mão pelas quais pagaram milhões de dólares. No final, 731 dos 780 detidos, mais de 90%, foram libertados sem serem acusados.6 Uma série de pesquisas como "Boeing", "capacidade de combustível", "escola de aviação" e "morte aos EUA" pode parecer incriminatória, mas dificilmente eram prova de cumplicidade em atos terroristas. Se um adolescente em Islamabad tivesse pesquisado esses termos no Google, e a empresa tivesse entregue essas informações ao governo, é possível que ele fosse jogado num saco preto no meio da noite e enviado a Guantánamo.

Mas o esforço vigilante de Brin foi eficaz? Quais foram os resultados?

Na verdade, não, e não muito. Para Douglas Edwards, que relatou essa história em suas memórias, o episódio serviu como uma anedota de advertência. Ele estava na empresa quase desde o início, mas apenas em

11 de setembro finalmente começou a compreender quanta energia a Google – e, por extensão, o restante do Vale do Silício – havia colocado em seus arquivos. “Não havia como evitar o fato de estarmos tentando filtrar usuários específicos com base em suas pesquisas. Se os encontrássemos, tentaríamos determinar suas informações pessoais a partir dos dados sobre eles em nossos registros", escreveu Edwards. "Tínhamos os pensamentos mais íntimos das pessoas em nossos arquivos de registro e, em breve, as pessoas perceberiam isso".7

Comecei a usar o Google em 2001, quando Sergey Brin iniciou sua caçada aos terroristas. Para mim, como para muitas pessoas que atingiram a maioridade no início dos anos 2000, a Google foi a primeira empresa de Internet em que realmente confiei. Não exigiu dinheiro meu dinheiro. Não me bombardeou com anúncios desagradáveis. Tinha um design limpo, com uma simples caixa de pesquisa centralizada em um fundo em branco. Funcionou como nada havia funcionado na Internet, ajudando você a navegar por um mundo novo, caótico e maravilhoso. Colocou bibliotecas inteiras na ponta dos dedos, permitiu que você traduzisse idiomas estrangeiros rapidamente, e colaborasse em tempo real com pessoas no outro lado do planeta. E você tinha tudo isso de graça. Parecia desafiar as leis da economia.

Mesmo quando se expandiu para uma corporação transnacional de bilhões de dólares, a Google conseguiu manter sua imagem de nerd inocente, com os dizeres "Não seja malvado". Convenceu seus usuários de que tudo o que fazia era movido por um desejo de ajudar a humanidade. Essa é a história que você encontrará em quase todos os livros populares sobre a Google: uma história sobre dois nerds brilhantes de Stanford que transformaram um projeto de faculdade em um dínamo da Nova Economia. Uma empresa que incorporava todas as promessas utópicas do sociedade em rede: empoderamento, conhecimento, democracia. Por um tempo, pareceu verdade. Talvez este realmente tenha sido o começo de uma nova ordem mundial altamente conectada em rede, onde as antigas estruturas – os militares, as corporações, os governos – eram impotentes diante do poder nivelador da Internet. Como Louis Rossetto da Wired escreveu em 1995, “Tudo o que sabemos será diferente. Não apenas uma mudança de um presidente para outro, mas não saberemos sequer se haverá presidente algum."8

Naquela época, qualquer pessoa que sugerisse que a Google fosse o arauto de um novo tipo de distopia, em vez de uma tecno-utopia, teria sido ridicularizada. Era praticamente impensável.

Biblioteca Digital

Lawrence Page era uma criança socialmente desajeitada, nascida e criada em torno de computadores. Em 1978, quando tinha cinco anos, seu pai, Carl, passou um ano trabalhando como pesquisador no Centro de Pesquisas de Ames, da NASA em Mountain View, Califórnia. O centro era um local da ARPANET que a Google arrendaria anos depois, ao expandir seu campus corporativo.9 A mãe de Page, Gloria, ensinava programação de computadores na Universidade Estadual de Michigan. Seu irmão mais velho, Carl Page Jr., foi um empreendedor pioneiro da Internet que fundou uma empresa de quadro de mensagens mais tarde comprada pela Yahoo! por quase meio bilhão de dólares.

Page cresceu escrevendo software.10 Quando tinha doze anos, leu uma biografia de Nikola Tesla, o brilhante inventor sérvio-estadunidense que havia desenvolvido tudo, desde motores elétricos, rádio e luzes fluorescentes a correntes alternadas, tudo antes de morrer na pobreza, sozinho e fora de si, enquanto escrevia cartas para um pombo que morava no peitoril da sua janela.11 Page devorou o livro, e Tesla permaneceu uma inspiração duradoura. Não apenas as invenções de Tesla obcecavam Page, mas também seu repetido fracasso em monetizar suas ideias. “Ele teve todos esses problemas para comercializar seu trabalho. É uma história triste. Percebi que Tesla era o maior inventor de todos, mas ele não conseguiu tanto quanto deveria”, disse Page ao jornalista John Battelle. “Percebi que queria inventar coisas, mas também queria mudar o mundo. Eu queria colocá-las lá fora, colocá-las nas mãos das pessoas para que elas pudessem usá-las, porque é isso que realmente importa.”12

Riqueza, fama, deixar uma marca no mundo – essas eram as coisas que o jovem Page fantasiava. A Universidade de Stanford, e um programa de pesquisa financiado pela Agência de Projetos de Pesquisa

Avançada em Defesa (anteriormente conhecida como ARPA), permitiriam que ele alcançasse seus sonhos.13

Stanford fica na beira da Baía de São Francisco, 85 quilômetros ao sul da cidade. Foi fundada por Leland Stanford, um magnata ferroviário local eleito como governador do estado e depois tornou-se senador.14 Quando a universidade abriu em 1891, o jornal Mail and Express de Nova York zombou do projeto, escrevendo: "a necessidade de outra universidade na Califórnia é tão grande quanto a de um asilo para os marinheiros da Suíça".15 Mas a instituição e a área circundante floresceram em conjunto. No início do século XX, a Bay Area desenvolveu uma próspera indústria de rádio e eletrônica, emergindo como o centro da fabricação de tubos de vácuo. Durante a Segunda Guerra Mundial, a área cresceu novamente, impulsionada pela necessidade de tecnologia de rádio e design avançado de tubo de vácuo para apoiar a tecnologia de radar militar. Após a guerra, a Universidade de Stanford tornou-se a resposta da Costa Oeste ao Instituto de Tecnologia de Massachusetts, a universidade de elite de engenharia intimamente ligada ao complexo industrial militar dos EUA.16 A área em torno do campus era o epicentro do desenvolvimento de computadores e microprocessadores.

William Shockley era um químico do MIT e eugenista notório que fez seu nome como parte da equipe do Bell Labs que inventou o transistor de estado sólido. Em 1956, ele retornou à sua cidade natal, Palo Alto, para iniciar a Shockley Semiconductor dentro da universidade, no seu Parque Industrial Stanford.17 Sua empresa gerou várias outras empresas de microchip, incluindo a Intel, e deu o nome ao Vale do Silício. A Hewlett-Packard, a Eastman Kodak, a General Electric, a Xerox PARC e a Lockheed Martin também instalaram escritórios no Parque Industrial de Stanford na mesma época. Havia tanto trabalho militar em andamento no Vale do Silício que, durante a década de 1960, a Lockheed era o maior empregador da área da baía.

A ARPA também teve uma presença enorme no campus. O Instituto de Pesquisas de Stanford fez um trabalho de contrainsurgência e guerra química para a agência como parte do Projeto Agile de William Godel. Também abrigava o Augmentation Research Center, um laboratório da ARPANET administrado por Douglas Engelbart, que fazia testes com LSD. De fato, a ARPANET nasceu em Stanford.18

Nos anos 1990, a Universidade de Stanford não havia mudado muito. Ainda era o lar de pesquisas de ponta em computadores e redes e ainda estava inundada de dinheiro militar e de utopismo cibernético. Talvez a maior mudança tenha ocorrido nos subúrbios em torno da universidade – Mountain View, Cupertino, San Jose – que cresceu com investidores e empresas iniciantes na Internet: eBay, Yahoo! e Netscape. Stanford foi o epicentro do boom das pontocom da Bay Area quando o jovem Larry Page caiu de paraquedas no vórtice.

Page iniciou o programa de doutorado em ciência da computação em Stanford no outono de 1995. Ele estava em seu elemento e imediatamente começou a procurar um tópico de pesquisa digno de uma dissertação. Brincou com várias ideias, incluindo um carro autônomo, no qual a Google mais tarde investiria pesadamente. Eventualmente, ele optou pela pesquisa na Internet.19

Em meados dos anos 1990, a Internet estava crescendo exponencialmente. O cenário era caótico: uma confusão de sites aleatórios, páginas pessoais, sites de universidades, sites de notícias e de corporações. Páginas estavam aparecendo por todo o lugar. Mas não havia um bom diretório central ou com autoridade que pudesse ajudar as pessoas a navegar para onde queriam ir ou encontrar uma música, um artigo ou uma página da web específica. Motores de busca e portais de diretórios como Yahoo!, AltaVista e Excite eram brutos e, às vezes, precisavam ser selecionados manualmente. Os algoritmos de pesquisa eram extremamente primitivos, correspondendo pesquisas palavra por palavra sem a capacidade de encontrar os resultados mais relevantes. Apesar de sua tecnologia primitiva e resultados terríveis de pesquisa, esses primeiros sites de pesquisa atraíram enormes quantidades de tráfego e investimento. Os jovens programadores que os iniciaram ficaram absolutamente ricos.

No jargão do Vale do Silício, era um mercado propenso a reviravoltas. Encontrar uma maneira de melhorar os resultados da pesquisa não era apenas intelectualmente desafiador, mas também podia ser extremamente lucrativo.

Com o fantasma de Nikola Tesla pairando sobre si, Page abordou a questão com seu cérebro matemático. Os ajustes de Page foram encorajados por seu orientador de pós-graduação, Terry Winograd, pioneiro

em inteligência artificial linguística que havia trabalhado na década de 1970 no Laboratório de Inteligência Artificial do MIT, uma parte do grande projeto da ARPANET. Na década de 1990, Winograd era responsável pelo projeto Bibliotecas Digitais de Stanford, um componente da Iniciativa Biblioteca Digital de vários milhões de dólares patrocinada por sete agências federais civis, militares e policiais, incluindo NASA, DARPA, FBI e a Fundação Nacional de Ciências.20

A Internet se transformou em um vasto e labiríntico ecossistema, abrangendo todos os tipos de redes de computadores e tipos de dados imagináveis: documentos, bancos de dados, fotografias, gravações sonoras, textos, programas executáveis, vídeos e mapas.21 O objetivo da Iniciativa Biblioteca Digital era encontrar uma maneira de organizar e indexar essa bagunça digital. Embora o projeto tivesse um amplo mandato civil, também estava ligado às necessidades das agências de inteligência e de aplicação da lei. Cada vez mais, a vida acontecia online. As pessoas estavam deixando rastros de informações digitais: diários, blogs, fóruns, fotografias pessoais, vídeos. As agências de inteligência e aplicação da lei queriam uma maneira melhor de acessar esse ativo valioso.

Fazia sentido. Na década de 1960, quando os militares estavam lidando com uma avalanche de dados e precisavam de novas ferramentas para digerir e analisar as informações, a ARPA foi incumbida da tarefa de encontrar uma solução. Três décadas depois, a Iniciativa Biblioteca Digital evoluiu para uma extensão do mesmo projeto, impulsionada pelas mesmas necessidades. E, como nos velhos tempos, a DARPA esteve envolvida.22 De fato, em 1994, apenas um ano antes de Page ter chegado a Stanford, o financiamento da DARPA para a Iniciativa Biblioteca Digital na Carnegie Mellon University produziu um sucesso notável: o Lycos, um mecanismo de busca cujo nome se refere a Lycosidae, o nome científico da família das aranhas-lobo.23

O interesse de Larry Page em busca digital se alinhava perfeitamente com os objetivos da Iniciativa Biblioteca Digital, e sua pesquisa foi realizada sob seu guarda-chuva.24 Quando ele finalmente publicou seu primeiro artigo em 1998, apresentava uma frase familiar: “financiado pela DARPA”. A agência que criou a Internet continuava sendo um ator central.

Larry Page conheceu Sergey Brin em seu primeiro dia em Stanford, na reunião de orientação de pós-graduação. Os dois eram ao mesmo tempo semelhantes e completos opostos. Rapidamente se tornaram amigos.

Page era reservado e quieto; algumas pessoas pensaram que talvez ele fosse um pouco autista. Ele falava com um estranho suspiro que algumas pessoas confundiram com um sotaque do Leste Europeu.25 Brin era o oposto. Ele era social e falador, e gostava de esportes. Quando seus colegas pensam no seu tempo em Stanford, eles se lembram de Brin andando de patins pelos corredores e constantemente passando pelos escritórios de seus professores para jogar conversa fora. Ao contrário de Page, Brin vinha realmente do leste europeu. Um grande interesse uniu os dois futuros bilionários: suas primeiras experiências com computadores e a Internet.

A família de Sergey Brin emigrou de Moscou para os Estados Unidos na década de 1970 e se integrou com muito sucesso ao mundo acadêmico de engenharia. Sua mãe, Eugenia, era uma cientista da NASA. Seu pai, Michael, era um professor titular de matemática na Universidade de Maryland.

Brin era um prodígio da matemática. Quando tinha nove anos, descobriu aquela Internet incipiente e passava seu tempo nas salas de chat e jogando jogos de fantasia medieval multiusuário, ou MUDs.26 Passou horas imerso nessa nova tecnologia de comunicação, acabando por irritar-se quando percebeu que estava cheia de pessoas como ele, “garotos de dez anos tentando falar sobre sexo”.27

Brin terminou o ensino médio em 1990, um ano antes do esperado, e se matriculou na Universidade de Maryland com especialização em matemática e ciências da computação. Ele se formou com honras em 1993 e mudou-se para Palo Alto para continuar seus estudos em Stanford com uma bolsa de pesquisa de pós-graduação da Fundação Nacional de Ciências.28 Em Stanford, interessou-se pela mineração de dados: construiu algoritmos de computador que poderiam prever o que as pessoas fariam com base em suas ações passadas. O que elas comprariam? Quais filmes elas se interessariam?29 Ele até fundou um grupo de estudantes chamado MIDAS: "Mining Data at Stanford". Mais recentemente, a mineração comportamental de dados provaria ser o toque de

Midas da Google. Mas isso estava bem além no futuro. Como Brin ficou entediado com o foco restrito de sua pesquisa de mineração de dados, decidiu se juntar a um novo projeto com seu amigo, Larry Page. "Conversei com muitos grupos de pesquisa, e esse foi o projeto mais empolgante, tanto por abordar a Web, que representa o conhecimento humano, quanto por gostar de Larry", lembrou Brin numa entrevista.30

O principal problema da pesquisa era a relevância. Algumas páginas da web eram mais importantes e tinham mais autoridade do que outras, mas os primeiros mecanismos de pesquisa não sabiam identificar essa diferença. O ponto central, entendeu Page, era encontrar uma maneira de incorporar um sistema de classificação nos resultados da pesquisa. Era uma ideia simples, mas poderosa, baseada no mundo acadêmico, onde a importância de um trabalho de pesquisa era medida por quantas vezes ele havia sido citada por outros trabalhos de pesquisa. Um artigo citado mil vezes era considerado mais importante do que um artigo citado apenas dez vezes. Devido ao seu design com hiperlinks – com todas as páginas vinculadas a outras páginas -, a Internet era essencialmente uma máquina gigante de citações. Esta foi a inovação de Page. Ele chamou o projeto experimental resultante de “PageRank” e, com a ajuda de Brin, começou a costurar tudo.

Eles primeiro programaram um bot para rastrear toda a Internet, vasculhar seu conteúdo e salvar tudo em seu servidor em Stanford. Eles então refinaram o algoritmo PageRank para produzir resultados relevantes. Como links diferentes carregavam valores diferentes – um link de um jornal como o New York Times tinha muito mais autoridade do que um link da página pessoal de alguém – eles ajustaram seus cálculos para que as páginas fossem pontuadas pelo número de links e pela pontuação dos próprios links. No final, a classificação de qualquer página da web seria a soma total de todos os links e seus valores que apontam para ela. Depois que os valores de algumas páginas da web iniciais entraram no algoritmo PageRank, novas classificações propagaram-se recursivamente por toda a web. "Convertemos toda a web em uma grande equação com várias centenas de milhões de variáveis, que são as classificações de todas as páginas da web", explicou Brin pouco depois de lançar o Google.31 Era um modelo matemático dinâmico da Internet. Se um valor fosse alterado, tudo teria que ser recomputado.32

Eles juntaram isso num mecanismo de pesquisa experimental chamado "BackRub" e o colocaram na rede interna de Stanford. O logotipo do BackRub era assustador: mostrava uma foto em preto e branco de uma mão presa a um braço peludo esfregando as costas nuas. Mas não importava. À medida que a notícia se espalhou, os alunos começaram a usá-lo – e ficaram surpresos. Esse projeto estudantil era melhor do que qualquer mecanismo de pesquisa comercial disponível na época, como Excite ou AltaVista. As empresas de busca dominantes foram avaliadas em bilhões de dólares, mas não entendiam seus próprios negócios. "Eles estavam olhando apenas para o texto e não considerando esse outro sinal", disse Page.33

O mecanismo de busca, que rapidamente foi renomeado para Google, tornou-se tão popular que sobrecarregou a largura de banda da conexão de rede de Stanford. Brin e Page perceberam que tinham encontrado algo muito especial. O Google era muito maior que um projeto de pesquisa.

Mesmo no estágio inicial, eles percebiam que o algoritmo de busca do Google não era apenas matemática abstrata. Ele catalogou e analisou páginas da web, leu seu conteúdo, analisou links de saída e classificou as páginas por importância e relevância. Como as páginas da Web foram escritas e construídas por pessoas, os dois criadores do Google entenderam que seu sistema de indexação dependia essencialmente de um tipo de vigilância da Internet pública. “O processo pode parecer completamente automatizado, mas, em termos de quanta contribuição humana entra no produto final, há milhões de pessoas que passam o tempo projetando suas páginas da Web, determinando a quem vincular e como, e esse elemento humano faz parte do mecanismo, Disse Brin.34

Mas houve mais coisas envolvidas.

Brin ficou profundamente fascinado pela arte e ciência de extrair informações do comportamento das pessoas, a fim de prever suas ações futuras. Catalogar o conteúdo da Internet foi apenas o primeiro passo. O próximo foi entender a intenção da pessoa que pesquisava. Era adolescente? Um cientista da computação? Masculino, feminino ou trans? Onde moravam? Onde eles compraram? Se eles procuravam por "filhotes", eram amantes da natureza ou fãs de beisebol? Quando digitaram "comprar roupas íntimas", estavam interessados em calcinhas rendadas

ou cuecas boxer? Quanto mais o Google soubesse de alguém, melhores seriam os resultados da pesquisa.

Enquanto Page e Brin trabalhavam para aperfeiçoar o algoritmo de relevância do Google, começaram a pensar em como personalizar os resultados da pesquisa para os interesses e hábitos de uma pessoa. Algumas de suas ideias iniciais foram rudimentares, incluindo a digitalização dos marcadores de navegador de uma pessoa ou a leitura do conteúdo de sua página inicial acadêmica, que geralmente listava interesses pessoais e também uma história acadêmica e profissional. "Esses mecanismos de busca podem economizar uma grande quantidade de dificuldades aos usuários, adivinhando eficientemente uma grande parte de seus interesses", escreveram os dois no artigo original de 1998 que descrevia os métodos de busca do Google.35

Esta frase curta definiria a futura empresa. A coleta de dados e a criação de perfis de usuários tornaram-se uma obsessão para os dois. Isso os tornaria absurdamente ricos e transformaria o Google de um mero mecanismo de pesquisa em uma ampla plataforma global, projetada para capturar o máximo de informações possível sobre as pessoas que entrarem em contato com ela.

Garimpando o cérebro

Em 1998, Larry Page e Sergey Brin se mudaram para a garagem de uma casa de propriedade de Susan Wojcicki, irmã da futura esposa de Brin, Anne Wojcicki. Eles receberam um cheque inicial de US $ 100.000 de Andy Bechtolsheim, co-fundador da Sun Microsystems, uma poderosa empresa de computadores que havia saído de um programa de pesquisa em computação da década de 1970, financiado pela ARPA na Universidade de Stanford.36 O pequeno investimento inicial foi seguido por uma parcela de US $ 25 milhões de duas empresas poderosas de capital de risco, Sequoia Capital e Kleiner Perkins.37

Brin e Page não poderiam estar mais felizes. Cheios de dinheiro, os dois jovens empreendedores contrataram alguns de seus colegas da

Iniciativa Biblioteca DIgital de Stanford e investiram sua energia para melhorar o mecanismo de pesquisa ainda rudimentar do Google.

Todas as primeiras empresas de mecanismos de pesquisa, do Lycos ao Yahoo!, do AltaVista à AOL, perceberam que estavam sentadas em algo novo e mágico. “As pessoas vinham aos nossos servidores e deixavam rastros. Todos os dias podíamos ver exatamente o que as pessoas achavam que era importante na Internet”, disse Tim Koogle, primeiro CEO do Yahoo.38 “A Internet tem tudo a ver com conexão.… Nós sentamos no meio, conectando pessoas.” Yahoo! tentou aproveitar esses dados para obter informações sobre a demanda dos consumidores, mas seus engenheiros mal arranharam a superfície dos dados valiosos que estavam acumulando. Os registros de pesquisa do Google não foram diferentes. O que separou a empresa das outras foi a sofisticação e agressividade que Page e Brin colocaram sobre a mineração e monetização do rastro de dados.

Inicialmente, a equipe do Google focou na mineração do comportamento do usuário para melhorar o mecanismo de pesquisa e adivinhar melhor a intenção dele. “Se as pessoas digitarem algo e depois mudarem sua consulta, você pode dizer que elas não estão felizes. Se elas forem para a próxima página de resultados, é um sinal de que não estão felizes. Você pode usar esses sinais de que alguém não está satisfeito com o que demos a elas para voltar e estudar esses casos e encontrar pontos para melhorar a pesquisa”, explicou um engenheiro da Google.39 Estudando os registros em busca de padrões, os engenheiros da Google transformaram o comportamento do usuário em um sistema de mão de obra gratuita de crowdsourcing. Ele agia como um loop de feedback que ensinava o mecanismo de busca a ser "mais inteligente". Um recurso de verificação ortográfica de sugestão automática permitiu ao Google reconhecer peculiaridades menores, mas importantes, na maneira como as pessoas usavam o idioma para adivinhar o significado do que elas digitaram, em vez de apenas combinar texto com texto. “Hoje, se você digitar 'Gandhi bio', sabemos que 'bio' significa 'biografia'. E se você digitar 'guerra bio', significa 'biológica'”, explicou outro engenheiro da Google.

Steven Levy, um jornalista veterano da área de tecnologia, cuja carreira incluiu uma passagem pelo Catálogo de Softwares A Terra Toda de Stewart Brand na década de 1980, obteve acesso privilegiado sem

precedentes para escrever a história da Google. O resultado foi In the Plex: Como o Google pensa, funciona e molda nossas vidas. Era uma história hagiográfica, mas altamente informativa, da ascensão da Google à posição dominante. O livro demonstra que Page e Brin entenderam desde o início que o sucesso do Google dependia de obter e manter controle proprietário sobre os dados comportamentais que eles capturavam por meio de seus serviços. Este foi o maior patrimônio da empresa. "Ao longo dos anos, o Google tornaria os dados em seus registros a chave para desenvolver seu mecanismo de busca", escreveu Levy. “Ele também usaria esses dados em praticamente todos os outros produtos que a empresa desenvolveria. Não apenas anotava o comportamento do usuário em seus produtos lançados, mas também media esse comportamento em inúmeras experiências para testar novas ideias e várias melhorias. Quanto mais o sistema do Google aprendesse, mais novos sinais poderiam ser incorporados ao mecanismo de busca para determinar melhor a relevância.”40

Melhorar a usabilidade e a relevância do Google ajudou a torná-lo o mecanismo de pesquisa mais popular da Internet. No final de 1999, a empresa recebia em média sete milhões de buscas diárias, um aumento de aproximadamente 70.000% em relação ao ano anterior.41 Agora que o Google dominava o mercado, era hora de ganhar dinheiro. Não demorou muito tempo para a empresa descobrir como.

No ano 2000, logo após mudar para seu novo escritório expandido no número 2400 da Bayshore em Mountain View, ao lado do Centro Ames NASA e a uma curta distância do campus de Stanford, Page e Brin lançaram o primeiro gerador de dinheiro do Google. Chamava-se AdWords, um sistema de publicidade direcionada que permite ao Google exibir anúncios com base no conteúdo de uma consulta de pesquisa. Era simples, mas eficaz: um anunciante selecionava palavras-chave e, se essas palavras-chave aparecessem em uma sequência de pesquisa, o Google exibia o anúncio ao lado dos resultados da pesquisa e só seria pago se um usuário clicasse no link.

Os registros de pesquisa do Google foram vitais para o Google AdWords. A empresa descobriu que, quanto melhor conhecia a intenção e os interesses dos usuários quando pressionavam o botão de pesquisa, mais efetivamente a empresa podia alinhá-los com um anunciante rele-

vante, aumentando assim a chance de os usuários clicarem em links de anúncios. O Google AdWords foi inicialmente rudimentar, correspondendo palavra-chave a palavra-chave. Nem sempre era possível adivinhar os interesses de uma pessoa com precisão, mas estava quase lá. Com o tempo, o Google melhorou em atingir a meta, resultando em anúncios mais relevantes, mais cliques e mais lucros para o Google. Multiplicado por centenas de milhões de pesquisas por dia, até um pequeno aumento na probabilidade de um usuário clicar em um link de publicidade aumentou drasticamente a receita da empresa. Nos anos seguintes, a Google sentiu fome de mais e mais dados para refinar a eficácia do programa de anúncios. "Os registros de busca eram dinheiro – recebíamos dos anunciantes com base nos dados desses registros", explicou Douglas Edwards.42

De fato, o dinheiro começou a chover do céu. Em 2001, a Google contratou Sheryl Sandberg, ex-chefe de gabinete do secretário do Tesouro do presidente Bill Clinton, Larry Summers. Ela foi incumbida de desenvolver e administrar o lado dos negócios de publicidade e conseguiu superar as expectativas de todo mundo. Com um sistema direcionado baseado no comportamento do usuário, a receita de publicidade aumentou de US $ 70 milhões em 2001 para US $ 3,14 bilhões em 2004, a maior parte resultante da simples exibição do anúncio certo no momento certo e para os olhos certos.43 Era como uma nova forma de alquimia: a Google estava transformando fragmentos inúteis de dados em montanhas de ouro.44

Carne de menina assada

Enquanto os engenheiros da Google extraíam informações pessoais de milhões de usuários, os executivos temiam que a menor divulgação sobre essa operação pudesse causar um desastre fatal nas relações públicas da empresa. Pagae percebeu que a Google poderia potencialmente perder usuários se as pessoas entendessem como a empresa usava seus fluxos de pesquisa.45 Proteger esse segredo tornou-se uma política corporativa fundamental.46

Page estava incrivelmente paranoico sobre a possibilidade de vazamento de qualquer informação desse tipo. Por insistência dele, a política de privacidade da empresa foi mantida vaga e breve, lembrou Douglas Edwards no livro I'm Feeling Lucky. “A recusa de Larry em iniciar a discussão de privacidade com o público sempre me frustrou. Eu seguia convencido de que poderíamos começar com informações básicas e depois montar um centro de informações que fosse claro e direto sobre o que os usuários entregavam quando faziam suas consultas no Google ou em qualquer outro mecanismo de pesquisa”, escreveu. “Quem realmente se importava veria que estávamos sendo transparentes. Mesmo que não gostassem das nossas políticas de coleta ou retenção de dados, saberiam o quais eram. Se eles acabassem indo para outro buscador, estariam arriscando que as práticas de nossos concorrentes fossem muito piores que as nossas.”47

Mas Page não via as coisas dessa maneira.

O fundador queria total sigilo. Sua paranoia chegou a tal ponto que ele começou a se preocupar com uma tela de rolagem no lobby do escritório em Mountain View, na Google, que exibia pesquisas aleatórias do Google em todo o mundo em tempo real. “Os jornalistas que vinham à Google ficavam no lobby, hipnotizados por essa espiada na gestalt global e depois imaginavam coisas sobre o impacto internacional do Google e o aprofundamento do papel da pesquisa em todas as nossas vidas. Os visitantes ficavam tão fascinados que olhavam para a tela enquanto assinavam seus crachás temporários, sem se preocupar em ler os acordos restritivos de confidencialidade com os quais concordavam”, escreveu Edwards. “Larry nunca se importou com a tela de consultas do lobby. Ele monitorava constantemente as tendências da paranoia pública sobre abuso informacional, e as consultas que apareciam no lobby dispararam seu alarme. Page acreditava que o letreiro rolante dava aos visitantes muitas informações sobre o que sua empresa realmente estava fazendo.

Ironicamente, a Internet daquela época já proporcionava ao público uma visão rara e inadvertida do tipo de informações íntimas que os mecanismos de busca estavam armazenando em seus registros de pesquisa. Em agosto de 2006, a AOL, a gigante pré-histórica provedora de rede, lançou no domínio público alguns gigabytes de registros de pes-

quisa anônimos: 20 milhões de consultas feitas por 657.000 de seus clientes durante um período de três meses. Os resultados da pesquisa foram baseados no Google, que possuía 5% da AOL e administrava o mecanismo de pesquisa da empresa.48

Page viu esses registros como um ativo lucrativo, mas volátil, que ameaçava o negócio principal da empresa se viesse a se tornar público. Uma equipe de pesquisa da AOL pensou de maneira diferente: eles lançaram o lote de logs como uma boa ação em nome da promoção da pesquisa social. Para o público, foi uma boa ação. Mas para a AOL e, por extensão, à Google, os registros foram um fiasco de relações públicas, iluminando a intromissão maciça e sistêmica da privacidade na qual a economia de buscas se baseava.

Respondendo ao alvoroço, a AOL alegou que seus engenheiros haviam anonimizado os logs, substituindo as informações pessoais da conta de usuário por números aleatórios. Mas os jornalistas descobriram rapidamente que as identidades dos usuários poderiam ser facilmente modificadas com apenas meia dúzia de buscas. Um desses usuários – conhecido nos registros como “4417749” – foi facilmente desmascarado por dois repórteres ousados do New York Times como uma vovozinha da zona rural da Geórgia:

O nº 4417749 realizou centenas de buscas em um período de três meses sobre tópicos que vão de "dedos dormentes" a "60 homens solteiros" a "cães que urinam em tudo". E, pesquisa por pesquisa, clique por clique, tornou-se mais fácil discernir a identidade do usuário da AOL nº 4417749. Há consultas para "paisagistas em Lilburn, Geórgia", várias pessoas com o sobrenome Arnold e "casas vendidas no lago sombreado, subdivisão gwinnett, county georgia". Não demorou muito tempo para investigar essa trilha de dados para Thelma Arnold, uma viúva de 62 anos moradora de Lilburn, Geórgia, que frequentemente pesquisa as doenças médicas de suas amigas e ama seus três cães.49

Os dados de log da AOL revelaram outra coisa. Muitas das consultas de pesquisa eram extremamente privadas, humilhantes, perturbadoras e possivelmente incriminatórias. Intercaladas em pesquisas sobre tópicos mundanos, como restaurantes, programas de televisão e resenhas de câmeras digitais, foram feitas buscas de doenças médicas e conselhos sobre o que fazer "na manhã seguinte ao estupro" e, em alguns casos,

consultas que pareciam mostrar indivíduos instáveis à beira de fazer algo violento e perigoso. Para entender completamente a natureza pessoal das pesquisas agora públicas, eis uma amostra dos registro brutos:

Usuário 2281868

"Como destruir demônios que vivem no apto acima"

"O hip hop e o rap são uma forma de satanismo"

"Os negros são satanás ou demônios ou gremlins?"

"Sexo animal"

"Os negros têm visão de raio-x?"

Usuário 6416389

“Garotas engordadas para abate”

“Carne tenra e cozida de meninas”

“Cortando bifes de nádegas de meninas”

“Garotas estranguladas e comidas”

“Garotas cortadas em bifes”

Usuário 1879967

"Comer minha ejaculação e quanto tempo ela pode permanecer fresca"

"vivendo no limite"

"Eu uso meu esperma como creme pós-barbear"

"É insalubre armazenar semem ou esperma em um copo e beber em uma semana"

“Eu coloco esperma no rosto como perfume para atrair garotas”

Vasculhei os registros e um fluxo de pesquisa chamou minha atenção. Pertencia ao usuário 5342598 e apresentava várias consultas sobre um assassinato não resolvido de uma mulher em San Jose, segui-

das de pesquisas de recursos que poderiam ajudar uma pessoa a determinar se ela era um assassino em série. Aqui está uma amostra do fluxo:

Usuário 5342598
“Assassinatos não resolvidos em san jose”
"Tara marowski"
“Assassinato não resolvido de tara marowski”
“Tara marowski encontrada morta no carro”
“Tara encontrada morta no carro”
“Mistérios não resolvidos tara marowski”
“Departamentos de polícia de san jose casos frios”
“Teste psicológico dado aos prisioneiros”
"Teste para ver se você é um serial killer"

Essa pessoa matou alguém? Será que ela era um assassino em série? O outro pesquisador era canibal? O outro usuário realmente acreditava que os vizinhos eram demônios? Ou essas pessoas estavam apenas procurando coisas estranhas na Internet? É impossível dizer. Quanto às buscas por assassinato, eles eram um assunto para a polícia e, de fato, os registros de buscas se tornaram um componente cada vez mais importante das investigações criminais.

Uma coisa era certa após a AOL publicar os logs: os registros de pesquisa forneceram uma visão não adulterada dos detalhes da vida interior das pessoas, com toda a estranheza, peculiaridades embaraçosas e angústia pessoal que esses detalhes mostravam. E a Google possuía tudo isso.

Email espião

É abril de 2004 e a Google está em modo de crise. Sergey Brin e Larry Page montaram uma sala de guerra e reuniram altos executivos de toda a

empresa para lidar com um desenvolvimento perigoso. Desta vez, não estão caçando terroristas, mas repelindo um ataque em andamento.

Cerca de um mês antes, a Google começou a lançar a versão beta do Gmail, seu serviço de e-mail. Foi um grande negócio para a jovem empresa, representando sua primeira oferta de produtos além da pesquisa. No começo, tudo estava indo bem. Então os eventos rapidamente saíram do controle.

O Gmail visava roubar usuários de provedores de e-mail estabelecidos, como Microsoft e Yahoo. Para fazer isso, a Google chocou todo mundo ao oferecer um gigabyte de espaço de armazenamento gratuito para todas as contas – uma quantidade incrível de espaço na época, considerando que o Hotmail da Microsoft oferecia apenas dois megabytes de armazenamento gratuito. Naturalmente, as pessoas correram para se inscrever. Alguns estavam tão ansiosos para obter suas contas que os convites pré-públicos do Gmail estavam chegando a US $ 200 no eBay.50 “Um gigabyte muda tudo. Você não tinha mais o medo de que alguém lhe enviasse uma foto e excedesse seu limite de dois megabytes. Isso faria com que todas as mensagens subsequentes retornassem aos seus remetentes. Agora, não mais”, escreveu o colunista de tecnologia do New York Times David Pogue. "De fato, a Google afirma que, com tanto espaço de armazenamento, você deve largar o hábito de excluir mensagens".51

O serviço da Google parecia bom demais para ser verdade, mais uma vez subvertendo as leis da economia. Por que uma empresa doaria algo tão valioso? Parecia caridade. Era um exemplo da mágica da Internet acontecendo na nossa frente. Porém, houve uma grande vantagem para a Google.

A caixa de pesquisa onde você digita sua busca era uma coisa poderosa. Isso permitiu que a Google visse a vida, os hábitos e os interesses das pessoas. Mas só funcionava enquanto os usuários permanecessem no site do Google. Assim que clicavam em um link, eles desapareciam e o fluxo de navegação sumia. O que as pessoas faziam depois que saíam do Google.com? Quais sites elas visitaram? Com que frequência? Quando? Sobre o que eram esses sites? Para essas perguntas, os registros de pesquisa do Google ofereciam um silêncio absoluto. Foi aí que entrou o Gmail.

Depois que os usuários acessavam sua conta de e-mail por um navegador da Internet, a Google conseguia rastrear todos os seus movimentos na Internet, mesmo que usassem vários dispositivos. As pessoas poderiam até usar um mecanismo de busca rival, e mesmo assim a Google poderia manter sua mira sobre elas. O Gmail também deu à Google outra coisa.52

Em troca do gigabyte "gratuito" de armazenamento de e-mail, os usuários deram à empresa permissão para ler e analisar todos os e-mails da mesma maneira que a empresa analisava seus fluxos de pesquisa para exibir anúncios direcionados com base no conteúdo. Eles também deram à Google permissão para vincular seu histórico de pesquisa e hábitos de navegação ao endereço de e-mail.

Nesse sentido, o Gmail abriu uma nova dimensão do rastreamento e da criação de perfis de comportamento: capturou correspondência pessoal e comercial, documentos particulares, cartões postais, fotos de férias, cartas de amor, recibos de compras, contas, registros médicos, extratos bancários, registros escolares e qualquer outra coisa que as pessoas rotineiramente enviem e recebam por email. A Google argumentou que o Gmail beneficiaria os usuários, permitindo que a empresa exibisse anúncios relevantes em vez de inundá-los com spam.

Mas nem todo mundo via dessa maneira.

Menos de uma semana após o lançamento público do Gmail, trinta e uma organizações de privacidade e liberdade civil, lideradas pelo Fórum Mundial de Privacidade, publicaram uma carta aberta endereçada a Sergey Brin e Larry Page pedindo que suspendessem imediatamente o serviço de email. “A Google propôs a digitalização do texto de todos os e-mails recebidos para colocação de anúncios. A verificação de email confidencial viola a confiança implícita de um provedor de serviços de email”, escreveram as organizações. “A Google poderá – amanhã – por opção ou por ordem judicial, empregar seu sistema de verificação para uso jurídico-policial. Observamos que em um caso recente, a Polícia Federal (Federal Bureau of Investigation, FBI) obteve uma ordem judicial obrigando um serviço de navegação de automóveis a converter seu sistema em uma ferramenta para monitorar conversas no carro. Quanto tempo levará até a polícia forçar a Google a uma situação semelhante? ”53

A imprensa, que até então não tinha nada a dizer sobre a Google, se tornou crítica. A empresa foi atacada por jornalistas por sua digitalização "assustadora" de e-mails. Um repórter da revista Maclean do Canadá relatou sua experiência no uso do sistema de anúncios direcionados do Gmail: “Descobri recentemente o quão relevante é o sistema de anúncios da Google quando escrevi um email para um amigo usando minha conta do Gmail. A mensagem mencionava uma mulher grávida cujo marido teve um caso. Os anúncios da Google não divulgaram artigos para bebês e livros para pais. Em vez disso, o Gmail entendeu que 'grávida' nesse caso não era uma coisa boa porque estava associada à palavra 'caso'. Então, me ofereceu os serviços de um detetive particular e um terapeuta matrimonial. ”54

Mostrar anúncios de serviços de espionagem para mães traídas? Isso não cairia bem para uma empresa que ainda se vestia com uma imagem progressista que dizia "Não Seja Malvado".

Fiel à paranoia de Larry Page sobre privacidade, evitando falar sobre o assunto, a Google permaneceu rígida quanto ao funcionamento interno do seu programa de verificação de e-mail diante das críticas. Mas uma série de perfis e patentes de tecnologia de publicidade direcionada registradas pela empresa naquele ano oferecia um vislumbre de como o Gmail se encaixava no sistema de rastreamento e criação de perfis multiplataforma da Google.55 Essas patentes revelavam que toda a comunicação por email estava sujeita a análise e garimpada por significado; os nomes foram relacionados a identidades e endereços reais usando bancos de dados de terceiros (outras empresas de perfilamento), bem como informações de contato armazenadas no catálogo de endereços do Gmail do usuário; foram extraídos dados demográficos e psicográficos, incluindo classe social, tipo de personalidade, idade, sexo, renda pessoal e estado civil; os anexos de email foram vasculhados para obter informações; até o status de residência de uma pessoa nos EUA foi estabelecido. Tudo isso foi cruzado e combinado com dados coletados pelos registros de pesquisa e navegação do Google, além de provedores de dados de terceiros e, então, adicionados a um perfil de usuário. As patentes deixaram claro que esse perfil não se restringia a usuários registrados do Gmail, mas aplicava-se a qualquer pessoa que enviasse email para uma conta do Gmail.

Em conjunto, esses documentos técnicos revelaram que a empresa estava desenvolvendo uma plataforma que tentava rastrear e criar um perfil de todas as pessoas que entrassem em contato com um produto da Google. Era, em essência, um sistema elaborado de vigilância privada.

Havia ainda outro detalhe. A linguagem nos registros de patentes – as descrições do uso de "informações psicográficas", "características da personalidade" e "níveis de educação" para traçar um perfil e prever os interesses das pessoas – tinha uma estranha semelhança com as primeiras iniciativas de contrainsurgência baseada em dados financiadas pela ARPA nas décadas de 1960 e 1970. Naquela época, a agência havia experimentado mapear os sistemas de valores e as relações sociais de tribos e grupos políticos rebeldes, na esperança de isolar os fatores que os levaram à revolta e, finalmente, usar essas informações para criar modelos preditivos para interromper as insurgências antes que elas acontecessem. O abortado Projeto Camelot foi um exemplo desse esforço. Outro foi o Projeto Cambridge, também da ARPA, de 1969, de J. C. R. Licklider e Ithiel de Sola Pool, que teve como objetivo desenvolver um conjunto de ferramentas de computador que permitisse que pesquisadores militares construíssem modelos preditivos usando dados complexos, incluindo fatores como "participação política de vários países", "filiação em associações", "movimentos juvenis" e "atitudes e comportamentos de camponeses".

O Projeto Cambridge foi uma primeira tentativa de construir uma base tecnológica para possibilitar previsão e análise de massas de dados. Naturalmente, o sistema preditivo da Google, que apareceu trinta anos depois, era mais avançado e sofisticado do que as ferramentas brutas de banco de dados de primeira geração da ARPA. Mas também era muito parecido. A empresa queria ingerir dados de pesquisa, histórico de navegação e email para criar perfis preditivos capazes de adivinhar os interesses e o comportamento futuros de seus usuários. Havia apenas uma diferença: em vez de impedir insurgências políticas, a Google queria que os dados vendessem produtos e serviços com anúncios direcionados. Um era militar, o outro comercial. Mas, em sua essência, ambos os sistemas foram dedicados à criação de perfil e previsão. O tipo de dados conectado a eles era irrelevante.

O professor de direito da Universidade de Berkeley, Chris Hoofnagle, especialista em direito da privacidade da informação, argumentou perante o Senado da Califórnia que a diferença entre perfis militares e comerciais era ilusória. Ele comparou a digitalização de e-mails pela Google com o projeto de vigilância e previsão do programa Atenção Informacional Total (Total Information Awareness, TIA) da DARPA, uma tecnologia de policiamento preditivo inicialmente financiada pela DARPA e entregue à Agência de Segurança Nacional (NSA) após os ataques terroristas de 11 de setembro em Nova Iorque.56

Um ano após a Google lançar o Gmail, Hoofnagle testemunhou sobre e-mail e privacidade em audiências realizadas pelo Comitê Judiciário do Senado da Califórnia. "A perspectiva de que um computador pudesse, em massa, visualizar dados transacionais e de conteúdo e tirar conclusões era o plano da Atenção Informacional Total (TIA) de John Poindexter", disse ele, referindo-se ao consultor de segurança nacional do presidente Ronald Reagan que, sob o mandato do presidente George W. Bush, foi encarregado de ajudar a DARPA a combater o terrorismo.57 “A TIA propôs examinar uma ampla variedade de informações pessoais e fazer inferências para a prevenção do terrorismo ou crime em geral. O Congresso rejeitou o plano de Poindexter. A extração de conteúdo do Google é diferente da TIA, pois foi projetada para divulgar publicidade em vez de capturar criminosos.” Para Hoofnagle, a mineração de dados da Google não era apenas tecnicamente semelhante ao que o governo estava fazendo; era uma versão privatizada da mesma coisa. Ele previu que as informações coletadas pelo Gmail seriam eventualmente exploradas pelo governo dos EUA. Não havia dúvidas. “Permitir a extração desse conteúdo de mensagens de email provavelmente terá consequências profundas para a privacidade. Primeiro, se as empresas podem visualizar mensagens privadas para divulgar anúncios, é uma questão de tempo até que a polícia requira acesso para detectar conspirações criminais. Com frequência, em Washington, ouve-se os políticos perguntando: 'se as empresas de cartão de crédito podem analisar seus dados para vender seu cereal matinal, por que o FBI não pode extrair seus dados para investigar terrorismo?'”58

A linguagem das patentes da Google enfatizou as críticas de Hoofnagle de que havia pouca diferença entre a tecnologia comercial e a militar. Também trouxe a conversa de volta aos medos da década de

1970, quando a tecnologia de computadores e redes estava se tornando comum. Naquela época, havia um amplo entendimento de que os computadores eram máquinas criadas para espionagem: coleta de dados sobre usuários para processamento e análise. Não importava se eram dados do mercado de ações, clima, condições de tráfego ou histórico de compras de uma pessoa.59

Para o Centro de Informações de Privacidade Eletrônica, o Gmail apresentou desafios éticos e legais.60 A organização acreditava que a intercepção de comunicação digital privada feita pela Google era uma violação potencial das leis de escutas telefônicas da Califórnia. A organização pediu ao procurador-geral do estado para investigar a empresa.

O primeiro desafio político da Google veio de uma fonte improvável: a senadora estadual da Califórnia Liz Figueroa, cujo distrito abrange uma enorme faixa do Vale do Silício e inclui o QG da Google em Mountain View. Preocupada com a verificação de e-mail do Google, a senadora apresentou um projeto de lei para proibir os provedores de e-mail de coletar informações de identificação pessoal, a menos que recebessem consentimento explícito de todas as partes em uma conversa por e-mail. Seu escritório a descreveu como uma lei pioneira de privacidade para a era da Internet: “Seria a primeira lei do país a exigir que a Google obtivesse o consentimento de todos os indivíduos antes que suas mensagens de email fossem digitalizadas para fins de publicidade direcionada.

"Dizer às pessoas que seus pensamentos mais íntimos e privados enviados por e-mail para médicos, amigos, amantes e familiares são apenas mais uma mercadoria de marketing direto não é o caminho para promover o comércio eletrônico", explicou a senadora Figueroa, quando anunciou o projeto de lei em 21 de abril de 2004. "No mínimo, antes que os pensamentos mais íntimos e privados de alguém sejam convertidos em uma oportunidade de marketing direto para a Google, a empresa deve obter o consentimento informado de todos."61

A lei proposta deixou Page e Brin em pânico. No momento em que os dois se preparavam para abrir o capital da empresa, eles enfrentaram uma legislação que ameaçava seu modelo de negócios. Obter o consentimento das pessoas – informando-as com antecedência sobre a maneira invasiva que a Google as rastreava – era o cenário de pesadelo de Page de uma divulgação pública das práticas de coleta de dados da

empresa; poderia desencadear um desastre de relações públicas e outras coisas piores.

Os executivos da Google montaram uma sala de guerra para lidar com a crescente avalanche de críticas. Brin comandou o esforço.62 Ele ficou furioso com os críticos da Google: eles eram ignorantes; eles não entendiam de tecnologia; eles não tinham ideia de nada. "Bastardos, bastardos!" ele gritou.63 Page fez ligações pessoais para jornalistas de tecnologia simpáticos à empresa, explicando que não havia problema de privacidade e que a Google realmente não espionava os usuários. Ele também organizou uma reunião frente a frente com a senadora Figueroa e seu chefe de gabinete.64

“Entramos nesta sala e estamos eu e dois de meus funcionários – meu chefe de gabinete e um de meus advogados. E à nossa frente estavam Larry, Sergey e o advogado deles”, contou a senadora. Brin imediatamente lançou uma longa explicação das políticas de privacidade da empresa, argumentando que as críticas de Figueroa eram infundadas.

“Senadora, como você se sentiria se um robô entrasse em sua casa e lesse seu diário e lesse seus registros financeiros, lesse suas cartas de amor, lesse tudo, mas antes de sair de casa, ele implodisse? Isso não está violando a privacidade." "É claro que sim", ela respondeu.

Mas Sergey insistiu: “Não, não está. Nada é mantido. Ninguém sabe disso."

“Esse robô leu tudo. Esse robô sabe se estou triste ou se estou com medo, ou o que está acontecendo? ela respondeu, ainda desafiadora e sem vontade de se curvar.

Brin olhou diretamente para ela e respondeu enigmaticamente: “Ah, não. Esse robô sabe muito mais do que isso."

Quando a tentativa de Brin de convencer a senadora não funcionou, a empresa reuniu uma equipe de lobistas poderosos e pessoas de relações públicas para açucarar a mensagem e restaurar a imagem correta da Google. À frente do grupo estava Andrew McLaughlin, estrategista-chefe de relações públicas da Google, alegre e sorridente, que mais tarde atuaria como vice-diretor de tecnologia do presidente Barack

Obama. Ele sabia exatamente como neutralizar a senadora Liz Figueroa: Al Gore. "Mobilizei o Big Al", ele se gabou mais tarde.65

Depois de perder a eleição presidencial de 2000 para George Bush, o vice-presidente Gore se dedicou a uma carreira lucrativa como capitalista de risco de tecnologia. Como parte dessa empreitada, ele aceitou a oferta da Google de ser um "membro virtual do conselho", o que significa que de tempos em tempos ele usava seu poder e conexões para resolver os problemas políticos da Google. Agora, a pedido de McLaughlin, Gore convocou a inconveniente senadora para suas suítes no Ritz-Carlton, no centro de São Francisco. Lá, ele falou-lhe severamente, ensinando-a sobre algoritmos e análise robótica. "Ele foi incrível", contou McLaughlin. "Ele se levantou e estava desenhando gráficos e fez essa longa analogia com o peso do ICBM, o míssil Minuteman".66

O que quer que ele tenha feito naquela sala, funcionou. A senadora Figueroa abandonou sua oposição e o primeiro desafio legal ao modelo de negócios de vigilância da Google desapareceu. E pelo menos um jornalista se alegrou: “A única população que provavelmente não ficará encantada com o Gmail é a que ainda se sente desconfortável com esses anúncios gerados por computador. Essas pessoas são livres para ignorar ou mesmo falar mal do Gmail, mas não devem tentar impedir a Google de oferecer o Gmail para o resto de nós”, declarou o jornalista de tecnologia do New York Times David Pogue em maio. "Sabemos que uma coisa boa quando a vemos."67

Alguns meses depois, em 19 de agosto de 2004, a Google abriu suas ações. Quando a campainha tocou naquela tarde para fechar as negociações da NASDAQ, a Google valia US $ 23 bilhões.68 Sergey Brin e Larry Page alcançaram o status de oligarcas no espaço de um único dia de trabalho, enquanto centenas de seus funcionários se tornaram multimilionários instantâneos, incluindo o cozinheiro da empresa.

Mas as preocupações com o modelo de negócios da Google continuariam assombrando a empresa. O tempo provou que Hoofnagle estava certo. Não havia muita diferença entre a abordagem da Google e a tecnologia de vigilância implantada pela NSA, CIA e Pentágono. De fato, às vezes eram idênticos.

Relatório minoritário

É 6 de outubro de 2014. Estou no escritório do professor da UCLA Jeffrey Brantingham. Está quente e ensolarado, e os alunos se sentam na grama do lado de fora das salas. Lá dentro, nós dois nos inclinamos sobre a tela do computador, inspecionando um mapa interativo de crimes. Ele dá um zoom na praia Venice.

“Essa costumava ser a capital da heroína em Los Angeles. Grande parte do tráfico de heroína está acontecendo aqui. Você pode ver como isso muda”, ele diz, alternando entre os padrões de crime diurno e noturno no oeste de Los Angeles. “Então, se você olhar mais longe na costa do Pacífico, você consegue diz o que está acontecendo com alguns desses outros lugares? Como aqui. Essa é a Playa Vista. Aqui em cima, Palms."69

Brantingham, esbelto e de fala mansa, com barba grisalha curta e cabelos espetados, é professor de antropologia. Ele também é co-fundador da PredPol Inc., uma nova e importante start-up de policiamento preditivo que surgiu de pesquisas de contrainsurgência financiadas pelo Pentágono para prever e impedir ataques a soldados estadunidenses no Iraque.70 Em 2012, os pesquisadores trabalharam com o Departamento de Polícia de Los Angeles para aplicar sua modelagem algorítmica na previsão de crimes. Assim, nasceu a PredPol.

O nome da empresa evoca o livro "Relatório Minoritário" de Philip K. Dick, mas a própria empresa possui uma taxa de sucesso espetacular: reduzir o crime em até 25% em pelo menos uma cidade que o implantou.71 Ele funciona ingerindo décadas de dados criminais, combinando-os com dados sobre o ambiente local – fatores como a localização de lojas de bebidas, escolas, rampas de rodovias – e rodando todas as variáveis por meio de um algoritmo proprietário que gera pontos críticos onde criminosos são mais propensos a vir a atacar.

"O software foi adaptado e modificado a partir de algo que previa terremotos", explica Brantingham enquanto tomamos café. “Se você pensa em Los Angeles e terremotos, para qualquer terremoto que ocorra, você pode realmente atribuir com boa precisão de onde ele vem, em ter-

mos de suas causas. Depois que um terremoto ocorre em uma dessas falhas geológicas, você recebe tremores secundários, que ocorrem perto de onde o choque principal ocorreu e cada vez mais rápidos.

"Com o crime é exatamente o mesmo", continua ele. “Nosso ambiente possui muitos recursos construídos que são geradores de crimes e que não vão a lugar algum. Um ótimo exemplo é uma escola secundária. As escolas secundárias não vão a lugar algum na maior parte do tempo. É um recurso construído que é parte do ambiente. E o que as escolas secundárias têm? Muitos jovens de quinze a dezessete ou quinze a dezoito anos, e não importa para onde você vá no planeta, os jovens de quinze a dezessete anos se metem em confusão. Se metem, sim. Sempre será assim, por causa da testosterona ou das meninas ou o que quer que seja. É a nossa herança dos primatas.”

Coço minha cabeça, concordando. Mas ainda não faz muito sentido para mim. Certamente, é preciso explicar o fato de que os seres humanos têm livre-arbítrio. Certamente, será que eles resistiriam a serem tratados como lajes gigantes de rocha de lava flutuante, esfregando violentamente uma contra a outra? Não havia causas sociais e políticas mais profundas do crime além da simples infraestrutura – coisas como pobreza e dependência de drogas? No que diz respeito às escolas secundárias e às crianças sendo crianças, não deveria haver outras maneiras de lidar com os adolescentes problemáticos além da criminalização e do policiamento concentrado?

Brantingham responde que a PredPol não está tentando consertar a sociedade, mas apenas ajudar a polícia a prevenir o crime. "A PredPol não tem a ver com combater as causas do crime", diz ele. “A PredPol busca conseguir que o policial seja a ferramenta para dificultar a ocorrência desse crime. Isso não quer dizer que que não precisamos consertar o vício em metanfetamina. Precisamos consertar o vício em metanfetamina."Em resumo: alguém tem que fazer o trabalho duro de melhorar a sociedade, lidando com as causas sociais e econômicas do crime. A PredPol está simplesmente ajudando os policiais a conter com mais eficiência a bagunça que existe hoje.

Em 2014, a PredPol era uma das muitas empresas competindo por um mercado incipiente, mas em rápida expansão, em tecnologias de policiamento preditivo.72 Empresas grandes e estabelecidas, como

IBM, LexisNexis e Palantir, ofereciam produtos que previam o crime.73 A PredPol, embora pequena, assinou contratos com departamentos de polícia de todo o país: Los Angeles; Condado de Orange, no centro da Flórida; Reading, Pensilvânia; Tacoma, Washington. Jornais e emissoras de televisão locais adoraram a história da PredPol: a cura milagrosa de alta tecnologia que os departamentos de polícia estavam esperando. Permitiu aos policiais reduzir o crime a baixo custo. Com um preço de US $ 25.000 a US $ 250.000 por ano, dependendo da população de uma cidade, a PredPol parecia uma pechincha.

O policiamento preditivo estava engatinhando, mas já era criticado por ativistas e cientistas sociais que o viam como uma nova marca da tática milenar de criação de perfil racial e econômico reforçada com um brilho objetivo e orientado por dados.74 Áreas e indivíduos ricos nunca pareciam ser alvo de policiamento preditivo, nem a técnica se concentrou em criminosos de colarinho branco. Jornalistas e criminologistas criticaram a PredPol, em particular por alegar que ela simplesmente não podia ser respaldada.75

Apesar desses choques, a PredPol tinha partidários e apoiadores no Vale do Silício. Seu conselho de administração e conselho consultivo incluíam figurões: executivos do Google, Facebook, Amazon e eBay, além de um ex-diretor da In-Q-Tel, a empresa de capital de risco da CIA que opera no Vale do Silício.76

De volta ao seu escritório, Brantingham oferece pouco sobre os laços da empresa com esses gigantes da Internet. Outro executivo da PredPol me informou que, nos bastidores, a Google era uma das maiores impulsionadoras e colaboradoras da PredPol. "Na verdade, a Google veio até nós", disse-me por telefone Donnie Fowler, diretor de desenvolvimento de negócios da PredPol.77 “Esse não é o caso de uma pequena empresa minúscula indo a uma gigante como a Google e dizendo que a única maneira de sobrevivermos é pegando carona em você. É um relacionamento mutuamente benéfico.”

Ele se gabou de que, ao contrário de outras empresas, a PredPol fez mais do que simplesmente pagar a licença da tecnologia da Google para incorporar o sistema de mapeamento em seu produto, mas também trabalhou com a Google para desenvolver funcionalidades personalizadas, incluindo “construir sinos e assobios adicionais e até ferramentas

adicionais para aplicação da lei". " Ele foi direto sobre o motivo pelo qual a Google era tão proativa em trabalhar com sua empresa. "A última fronteira deles é vender sua tecnologia aos governos. Eles os tornaram consumidores. É com eles que rolam os negócios." E a PredPol era um suporte de vendas perfeito – um exemplo poderoso dos departamentos de polícia que aproveitavam a tecnologia da Google para manter as pessoas seguras. "Um desses caras da Google me disse: 'Vocês nos completam'", disse Fowler com um ar de satisfação.

Policiais? Empreiteiros do governo? Tecnologia de contrainsurgência propulsionada por dados? Previsão de crime alimentada por uma plataforma onipresente da Internet? Ele estava falando sobre a Google? Ou foi um daqueles sistemas de contrainsurgência cibernética da Guerra Fria que o Pentágono sonhou por tanto tempo? Havia alguma diferença?

Aperto a mão de Brantingham e saio de seu escritório. Enquanto atravesso o campus da UCLA em direção ao meu carro, penso na nossa conversa. Com base no que já descobri investigando os negócios de vigilância privada do Vale do Silício, não me surpreendo ao saber que a Google está na cama com uma empresa de previsão de crimes iniciada pela pesquisa de contrainsurgência.

A Internet percorreu um longo caminho desde que Larry Page e Sergey Brin converteram o buscador Google de um projeto de doutorado em Stanford em uma empresa multibilionária. Mas, sob muitos aspectos, não mudou muito desde os dias da ARPANET. Apenas ficou mais poderosa.

O desenvolvimento da parte direcionada ao consumidor foi a mudança mais dramática. A Internet comercial que conhecemos hoje se formou no início dos anos 1990, quando a National Science Foundation privatizou a NSFNET. No espaço de duas décadas, a rede cresceu de um simples meio de dados e de telecomunicações para uma vasta rede global de computadores, smartphones, aplicativos, cabos de fibra ótica, redes celulares e data centers em depósitos tão grandes que cabiam bairros inteiros de Manhattan neles. Hoje, a Internet nos rodeia. Medeia a vida moderna. Lemos livros e jornais na Internet; usamos o banco, compramos e jogamos videogame na Internet. Conversamos por telefone, frequentamos a faculdade, encontramos empregos, paqueramos, trabalhamos, ouvimos música e assistimos a filmes, marcamos consultas com

dentistas e obtemos aconselhamento psicológico na Internet. Aparelhos de ar condicionado, telefones, relógios, distribuidores de alimentos para animais de estimação, babás eletrônicas, carros, geladeiras, televisões, lâmpadas – todos esses objetos também se conectam à Internet. Os lugares mais pobres do mundo podem não ter encanamento e eletricidade, mas eles, com certeza, têm acesso à Internet.

A Internet é como uma bolha gigante e invisível que envolve o mundo moderno. Não há escapatória e, como Page e Brin astutamente entenderam quando lançaram a Google, tudo o que as pessoas fazem online deixa um rastro de dados. Se salvos e usados corretamente, esses traços compõem uma mina de ouro com informações cheias de insights sobre as pessoas em um nível íntimo, além de uma leitura valiosa sobre macro tendências culturais, econômicas e políticas.

A Google foi a primeira empresa de Intenet a aproveitar totalmente esse insight e construir um negócio com base nos dados que as pessoas deixam para trás. Mas não ficou sozinha por muito tempo. Algo na tecnologia levou outras empresas na mesma direção. Aconteceu em quase todos os lugares, desde o menor aplicativo até a plataforma mais ampla.

O Netflix monitorou os filmes que as pessoas assistiram para sugerir outros filmes, mas também para orientar o licenciamento de conteúdo e a produção de novos programas.78 Angry Birds, o jogo da Finlândia que se tornou viral, pegou dados dos smartphones das pessoas para criar perfis, com informações como idade, sexo, renda familiar, estado civil, orientação sexual, etnia e até alinhamento político, e transmiti-los para empresas de publicidade direcionada de terceiros.79 Os executivos do Pandora, o serviço de streaming de música, construíram um novo fluxo de receita, analisando seus setenta e três milhões de ouvintes, captando suas crenças políticas, etnia, renda e até status parental, para depois vender essas informações para anunciantes e empresas de campanhas políticas. A Apple extraiu dados dos dispositivos das pessoas – fotos, emails, mensagens de texto e locais – para ajudar a organizar as informações e antecipar as necessidades dos usuários. Em seus materiais promocionais, divulgou isso como uma espécie de assistente pessoal digital que poderia "fazer sugestões proativas para onde você provavelmente irá".

O eBay de Pierre Omidyar, o maior site de leilões on-line do mundo, implantou software especializado que monitorava os dados dos usuários e combinava-os com as informações disponíveis on-line para desmascarar vendedores fraudulentos.81 Jeff Bezos sonhava em transformar sua varejista on-line Amazon na “loja de tudo”, uma plataforma global de vendas que anteciparia todas as necessidades e desejos dos usuários e entregaria produtos sem ser solicitada.82 Para fazer isso, a Amazon implantou um sistema para monitoramento e criação de perfil. Ele registrava os hábitos de compra das pessoas, suas preferências de filmes, os livros nos quais estavam interessados, a rapidez com que liam livros em seus Kindles e os destaques e notas de margem que eles faziam. Também monitorou os trabalhadores dos depósitos, rastreando seus movimentos e cronometrando seu desempenho.83 A Amazon exige um poder de processamento incrível para administrar um negócio de dados tão grande, uma necessidade que gerou um negócio paralelo lucrativo de alugar espaço em seus servidores enormes para outras empresas. Hoje, a empresa não é apenas a maior varejista do mundo, mas também a maior empresa de hospedagem na Internet, recebendo US $ 10 bilhões por ano com o armazenamento de dados de outras empresas.84

O Facebook, que começou como um jogo que classificava estudantes mulheres entre "gostosa ou não" em Harvard, transformou-se em uma plataforma global de mídia social alimentada por um modelo de publicidade direcionada semelhante à Google. A empresa engoliu tudo o que seus usuários fizeram: postagens, textos, fotos, vídeos, gostos e desgostos, solicitações de amigos aceitas e rejeitadas, conexões familiares, casamentos, divórcios, locais, opiniões políticas e até postagens excluídas que nunca foram publicadas. Tudo isso foi introduzido no algoritmo secreto de criação de perfis do Facebook, que transformou os detalhes da vida privada em mercadorias privadas. A capacidade da empresa de vincular opiniões, interesses e afiliações de grupos e comunidades tornou-a favorita de empresas de publicidade e marketing de todos os tipos.

As campanhas políticas, em particular, adoraram o acesso direto oferecido pelo Facebook. Em vez de cobrir as ondas de rádio com um único anúncio político, eles poderiam usar perfis comportamentais detalhados para segmentar suas mensagens de forma micro-segmentada,

mostrando anúncios que apelavam especificamente para indivíduos e para os problemas que eles consideravam caros. O Facebook até permitiu campanhas para carregar listas de eleitores e apoiadores em potencial diretamente no sistema de dados da empresa e, em seguida, usar as redes sociais dessas pessoas para extrapolar outras pessoas que podem apoiar um candidato.85 Era uma ferramenta poderosa e lucrativa. Uma década depois que Mark Zuckerberg transfigurou a empresa a partir de um projeto de Harvard, 1,28 bilhão de pessoas em todo o mundo usavam a plataforma diariamente, e o Facebook cunhava US $ 62 em receita para cada um de seus usuários nos EUA.86

A Uber, empresa de táxi na Internet, implantou uso de dados para evitar a regulamentação e a supervisão do governo em apoio à sua expansão agressiva nas cidades onde operava ilegalmente. Para fazer isso, a empresa desenvolveu uma ferramenta especial que analisou as informações do cartão de crédito, os números de telefone, os locais e os movimentos dos usuários, e a maneira como os usuários usavam o aplicativo para identificar se eram policiais ou funcionários do governo que poderiam estar chamando um Uber, apenas para multar motoristas ou apreender seus carros. Se o perfil correspondesse, esses usuários seriam silenciosamente incluídos na lista negra do aplicativo.87

Uber, Amazon, Facebook, eBay, Tinder, Apple, Lyft, Four-Square, Airbnb, Spotify, Instagram, Twitter, Angry Birds. Se você diminuir o zoom e olhar para o quadro maior, poderá ver que, juntas, essas empresas transformaram nossos computadores e telefones em esccutas espiãs conectadas a uma vasta rede de vigilância de propriedade corporativa. Para onde vamos, o que fazemos, sobre o que falamos, com quem falamos e nos encontramos – tudo é gravado e, em algum momento, transformado em valor. Google, Apple e Facebook sabem quando uma mulher visita uma clínica de aborto, mesmo que ela não conte a mais ninguém: as coordenadas GPS no telefone não mentem. Transas de uma noite e casos extraconjugais são muito fáceis de descobrir: dois smartphones que nunca se conheceram de repente se cruzam em um bar e depois se dirigem a um apartamento do outro lado da cidade, ficam juntos durante a noite e se separam pela manhã. Eles nos conhecem intimamente, até as coisas que escondemos das pessoas mais próximas a nós. E, como o programa Greyball da Uber mostra tão claramente, ninguém escapa – nem mesmo a polícia.

Em nosso moderno ecossistema da Internet, esse tipo de vigilância privada é a norma. É tão despercebido e normal quanto o ar que respiramos. Mas mesmo nesse ambiente sofisticado e esfomeado por dados, em termos de escopo e onipresença, a Google reina suprema.

À medida que a Internet se expandia, a Google cresceu junto com ela. Cheia de dinheiro, a Google começou a fazer compras vertiginosamente. Comprou empresas e startups, absorvendo-as em sua crescente plataforma. Ela foi além da pesquisa e do email, expandiu-se para processamento de texto, bancos de dados, blogs, redes de mídia social, hospedagem na nuvem, plataformas móveis, navegadores, auxiliadores de navegação, laptops baseados na nuvem e toda uma gama de aplicativos de escritório e produtividade. Pode ser difícil acompanhar todos eles: Gmail, Google Docs, Google Drive, Google Maps, Android, Google Play, Google Cloud, YouTube, Google Translate, Google Hangouts, Google Chrome, Google+, Google Sites, Google Developer, Google Voz, Google Analytics, Android TV. A empresa ultrapassou os serviços puramente voltados para a Internet e investiu em sistemas de telecomunicações de fibra ótica, tablets, laptops, câmeras de segurança doméstica, carros autônomos, entrega de compras, robôs, usinas elétricas, tecnologia de extensão de vida, segurança cibernética e biotecnologia. Ela chegou a lançar um poderoso banco de investimento interno que agora rivaliza com as empresas de Wall Street, investindo dinheiro em tudo, desde Uber até obscuras startups de monitoramento de culturas agrícolas, ambiciosas empresas de sequenciamento de DNA humano como 23andME e um centro de pesquisa secreto para a extensão de vida chamado Calico .88

Independentemente do serviço implantado ou do mercado em que entrou, a vigilância e a previsão foram incorporadas aos negócios. Os dados que fluem pelo sistema da Google são surpreendentes. Até o final de 2016, o Android da Google estava instalado em 82% de todos os novos smartphones vendidos em todo o mundo, com mais de 1,5 bilhão de usuários de Android no mundo todo.89 Ao mesmo tempo, a Google processava bilhões de pesquisas e o YouTube era reproduzido diariamente e tinha um bilhão de usuários ativos do Gmail, o que significava que ela tinha acesso à maioria dos emails do mundo.90 Alguns analistas estimam que 25% de todo o tráfego da Internet na América do Norte

passa pelos servidores da Google.91 A empresa não está apenas conectada à Internet, é a Internet.

A Google foi pioneira em todo um novo tipo de transação comercial. Em vez de pagar pelos serviços da Google com dinheiro, as pessoas pagam com seus dados. E os serviços que oferece aos consumidores são apenas as atrações – usados para capturar os dados das pessoas e dominar sua atenção, atenção contratada pelos anunciantes. A Google usou dados para aumentar seu império. Em 2017, tinha US $ 90 bilhões em receitas e US $ 20 bilhões em lucros, com setenta e dois mil funcionários em período integral trabalhando em setenta escritórios em mais de quarenta países.92 Tinha uma capitalização de mercado de US $ 593 bilhões, tornando-a a segunda empresa pública mais valiosa do mundo – perdendo apenas para a Apple, outra gigante do Vale do Silício.93

Além disso, outras empresas de Internet dependem da Google para sobreviver. Snapchat, Twitter, Facebook, Lyft e Uber – todos construíram negócios de bilhões de dólares sobre o onipresente sistema operacional móvel da Google. Como guardiã, a Google também se beneficia do sucesso deles. Quanto mais pessoas usam seus dispositivos móveis, mais dados eles recebem.

O que a Google sabe? O que ela pode adivinhar? Bem, parece quase tudo. "Uma das coisas que eventualmente acontece ... é que não precisamos que você digite", disse Eric Schmidt, CEO da Google, em um momento de sinceridade em 2010. “Porque nós sabemos onde você está. Sabemos onde você esteve. Podemos adivinhar mais ou menos o que você está pensando." 94 Mais tarde, acrescentou: “Um dia tivemos uma conversa em que pensávamos que poderíamos apenas tentar prever o mercado de ações. E então decidimos que era ilegal. Então paramos de fazer isso.”

É um pensamento assustador, considerando que a Google não é mais uma startup atraente, mas uma poderosa corporação global com sua própria agenda política e uma missão para maximizar os lucros para os acionistas. Imagine se Philip Morris, Goldman Sachs ou um empreiteiro militar como a Lockheed Martin tivessem esse tipo de acesso.

O Governo da Google

Pouco depois de Sergey Brin e Larry Page terem tornada a Google uma corporação, começaram a ver sua missão em termos maiores. Eles não estavam apenas construindo um mecanismo de pesquisa ou um negócio de publicidade direcionada. Eles estavam organizando as informações do mundo para torná-las acessíveis e úteis para todos. Foi uma visão que também abrangeu o Pentágono.

Mesmo quando a Google cresceu para dominar a Internet do consumidor, surgiu um segundo lado da empresa, que raramente recebia muita atenção: a Google, a contratada pelo governo. Acontece que as mesmas plataformas e serviços que a Google implementa para monitorar a vida das pessoas e coletar seus dados podem ser usados a serviço de grandes áreas do governo dos EUA, incluindo militares, agências de espionagem, departamentos de polícia e escolas. A chave para essa transformação foi uma pequena start-up agora conhecida como Google Earth.

Em 2003, uma empresa de São Francisco chamada Keyhole Incorporated estava nas últimas. Tendo recebido o mesmo nome que o programa secreto de espiões por satélite "Keyhole" da CIA dos anos 1960, a empresa havia sido lançada dois anos antes como derivada de um equipamento de videogame. Seu CEO, John Hanke, veio do Texas e trabalhou por um tempo na Embaixada dos EUA em Mianmar. Ele disse aos jornalistas que a inspiração para sua empresa veio de Snow Crash, de Neal Stephenson, um romance de ficção científica em que o herói utiliza um programa criado pela "Central Intelligence Corporation" chamado Planet Earth, uma realidade virtual projetada para "rastrear todas as informações espaciais que possui – todos os mapas, dados meteorológicos, planos arquitetônicos e equipamentos de vigilância por satélite. ”95

A vida imitaria a arte.96

A Keyhole derivou da tecnologia de videogame, mas a implantou no mundo real, criando um programa que costurava imagens de satélite e fotografias aéreas em modelos tridimensionais de computador da Terra

que poderiam ser explorados como se estivessem em um mundo de realidade virtual. Era um produto inovador que permitia a qualquer pessoa com conexão à Internet voar virtualmente sobre qualquer lugar do mundo. O único problema da Keyhole foi uma questão de assincronia. Ela foi lançado no momento em que a bolha pontocom explodiu no rosto do Vale do Silício. O financiamento secou e a Keyhole se viu lutando para sobreviver.97 Por sorte, a empresa foi salva a tempo pela própria entidade que a inspirou: a Agência Central de Inteligência (CIA).

Em 1999, no auge do boom das pontocom, a CIA lançou o In-Q-Tel, um fundo de capital de risco do Vale do Silício cuja missão era investir em start-ups alinhadas às necessidades de inteligência da agência.98 A Keyhole parecia se encaixar perfeitamente.99

Não se conhece a quantia que a CIA investiu na Keyhole; o número exato permanece classificado. O investimento foi finalizado no início de 2003 e foi realizado em parceria com a Agência Nacional de Inteligência Geoespacial, uma importante organização de inteligência com 14.500 funcionários e um orçamento de US $ 5 bilhões cujo trabalho era fornecer inteligência via satélite à CIA e ao Pentágono. Conhecido por seu acrônimo "NGA", o lema da agência de espionagem era: "Conheça a Terra ... Mostre o caminho... Entenda o mundo.”100

A CIA e a NGA não eram apenas investidores; elas também eram clientes e se envolveram na personalização do produto de mapa virtual da Keyhole para atender às suas próprias necessidades.101 Meses após o investimento da In-Q-Tel, o software Keyhole já estava integrado ao serviço operacional e implantado para apoiar as tropas estadunidenses durante a Operação Liberdade do Iraque, a campanha de choque e pavor para derrubar Saddam Hussein.102 Funcionários da inteligência ficaram impressionados com a simplicidade “semelhante a um videogame” de seus mapas virtuais. Eles também apreciaram a capacidade de colocar informações visuais sobre outras informações.103 As possibilidades eram limitadas apenas por quais dados contextuais podiam ser alimentados e enxertados em um mapa: movimentos de tropas, esconderijos de armas, condições climáticas e do oceano em tempo real, e-mails interceptados e informações de telefonemas, localizações de telefones celulares. A Keyhole deu a um analista de inteligência, um comandante em

campo ou um piloto da força aérea no ar o tipo de capacidade que agora assumimos como evidente: usar serviços de mapeamento digital em nossos computadores e telefones celulares para procurar restaurantes, cafés, museus, condições de tráfego e rotas de metrô. "Poderíamos fazer essas sobreposição de informações e mostrar as fontes de dados herdadas existentes em questão de horas, em vez de semanas, meses ou anos", disse um funcionário da NGA alguns anos depois.104

Os comandantes militares não eram os únicos que gostavam do software Keyhole. Sergey Brin também. Ele gostou tanto que insistiu em demonstrar pessoalmente o aplicativo para executivos da Google. Em um relato publicado na Wired, ele invadiu uma reunião da empresa, digitou o endereço de todas as pessoas presentes e usou o programa para voar virtualmente sobre suas casas.105

Em 2004, no mesmo ano em que a Google se tornou pública, Brin e Page compraram a empresa, investidores da CIA e tudo.106 Eles absorveram a empresa na crescente plataforma de aplicativos da Internet da Google. O Keyhole renasceu como Google Earth.

A compra da empresa Keyhole foi um marco importante para a Google, atestando o momento em que a empresa deixou de ser uma empresa de Internet voltada para o consumidor e começou a se integrar ao governo dos EUA. Quando a Google comprou a Keyhole, também adquiriu um executivo da In-Q-Tel chamado Rob Painter, que vinha com profundas conexões com o mundo da inteligência e contratações militares, incluindo Operações Especiais dos EUA, CIA e grandes empresas de defesa como Raytheon, Northrop Grumman e Lockheed Martin.107 Na Google, Painter foi instalado em uma nova divisão de vendas e lobby chamada Google Federal, localizada em Reston, Virgínia, a uma curta distância da sede da CIA em Langley. Seu trabalho na Google era ajudar a empresa a conquistar uma fatia do lucrativo mercado de inteligência militar. Ou, como Painter descreveu na linguagem empreiteiro-burocrática, ele estava lá para "evangelizar e implementar soluções da Google Enterprise para um grande número de usuários nas Comunidades de Inteligência e Defesa".

A Google havia fechado alguns acordos anteriores com agências de inteligência. Em 2003, assinou um contrato de US $ 2,1 milhões para equipar a NSA com uma solução de pesquisa personalizada que poderia

digitalizar e reconhecer milhões de documentos em vinte e quatro idiomas, incluindo suporte técnico de plantão caso algo desse errado. Em 2004, ao lidar com as consequências do bisbilhotamento de e-mails do Gmail, a Google firmou um contrato de pesquisa com a CIA. O valor do acordo não é conhecido, mas a CIA pediu permissão à Google para personalizar a página de pesquisa interna do Google, colocando o selo da CIA em um dos sistemas operacionais da Google. “Eu disse ao nosso representante de vendas que aceitasse se eles prometessem não contar a ninguém. Eu não queria que isso apavorasse os defensores da privacidade”, escreveu Douglas Edwards no livro I'm Feeling Lucky.108 Negócios como esses ficaram cada vez mais comuns e aumentaram em escopo após a aquisição da Keyhole.

Em 2006, a Google Federal de Painter começou a contratar, recrutando gerentes e vendedores do exército, força aérea, CIA, Raytheon e Lockheed Martin.109 Ele injetou esteroides nos seus músculos de lobby e reuniu uma equipe de agentes democratas e republicanos. A Google até pegou o velho figurão da ARPA: Vint Cerf, que, como vice-presidente da Google e principal evangelista da Internet, serviu como uma ponte simbólica entre a Google e os militares.

Enquanto a equipe de relações públicas da Google fazia o possível para manter a empresa envolvida por uma falsa aura de altruísmo nerd, os executivos da empresa seguiam uma estratégia agressiva para se tornar a Lockheed Martin da Era da Internet.110 “Funcionalmente, mais do que triplicamos a equipe a cada ano”, disse Painter em 2008.111 Era verdade. Com a ajuda de atores de dentro daquele mercado, a expansão da Google no mundo dos contratos militares e de inteligência decolou.

Em 2007, a Google fez uma parceria com a Lockheed Martin para projetar um sistema de inteligência visual para a NGA que exibia bases militares dos EUA no Iraque e marcava bairros sunitas e xiitas em Bagdá – informações importantes para uma região que havia sofrido uma insurgência sectária sangrenta e uma campanha de limpeza étnica entre os dois grupos.112 Em 2008, a Google ganhou um contrato para rodar os servidores e a tecnologia de pesquisa que alimentava o Intellipedia da CIA, um banco de dados de inteligência aos moldes da Wikipedia que era editado colaborativamente pela NSA, CIA, FBI e outras

agências federais.113 Pouco tempo depois, a Google foi contratada pelo Exército dos EUA para equipar cinquenta mil soldados com um conjunto personalizado de serviços da Google para smartphone.114

Em 2010, como um sinal de quão profundamente a Google havia se integrado às agências de inteligência dos EUA, ela ganhou um contrato exclusivo de US $ 27 milhões para oferecer à NGA "serviços de visualização geoespacial", tornando efetivamente a gigante da Internet os "olhos" dos aparelhos de defesa e inteligência estadunidenses. Os concorrentes criticaram a NGA por não abrir o contrato ao processo habitual de licitação, mas a agência defendeu sua decisão, dizendo que não tinha escolha: passou anos trabalhando com a Google em programas secretos e ultrassecretos para construir a tecnologia do Google Earth de acordo com sua necessidades e não poderia ir com nenhuma outra empresa.115

A Google foi minuciosa sobre os detalhes e o escopo de seus negócios de contratação. Ela não lista essa receita em uma coluna separada nos relatórios trimestrais de ganhos aos investidores, nem fornece a soma aos repórteres. Porém, uma análise do banco de dados de contratação federal mantido pelo governo dos EUA, combinado com informações obtidas dos pedidos da Lei da Liberdade de Informação e relatórios periódicos publicados sobre o trabalho militar da empresa, revela que a Google tem feito negócio vendendo o Google Search, Google Earth e Produtos da Google Enterprise (agora conhecido como G Suite) para praticamente todas as principais agências de inteligência e militares: marinha, exército, força aérea, Guarda Costeira, DARPA, NSA, FSA, FBI, DEA, CIA, NGA e Departamento de Estado.116 Às vezes, a Google vende diretamente ao governo, mas também trabalha com empresas contratadas como a Lockheed Martin, Raytheon, Northrop Grumman e SAIC (Science Applications International Corporation), um megacontratado de inteligência da Califórnia que tem tantos ex-funcionários da NSA trabalhando nele que é conhecido no meio empresarial como a "NSA do Oeste".117

A entrada da Google nesse mercado faz sentido. Quando o Google Federal entrou na Internet em 2006, o Pentágono estava gastando a maior parte de seu orçamento em empresas privadas. Naquele ano, do orçamento de US $ 60 bilhões em inteligência dos EUA, 70% ou US $

42 bilhões, foram destinados a empresas. Isso significa que, embora o governo pague a conta, o trabalho real é realizado pela Lockheed Martin, Raytheon, Boeing, Bechtel, Booz Allen Hamilton e outros contratados poderosos.118 E isso não é apenas no setor de defesa. Em 2017, o governo federal gastava US $ 90 bilhões por ano em tecnologia da informação.119 É um mercado enorme – no qual a Google procura manter uma forte presença. E seu sucesso foi praticamente garantido. Seus produtos são os melhores do mercado.120

Eis um sinal de quão vital a Google se tornou para o governo dos EUA: em 2010, após uma invasão desastrosa em seu sistema pelo que a empresa acredita ser um grupo de hackers do governo chinês, a Google firmou um acordo secreto com a Agência de Segurança Nacional.121 "De acordo com funcionários que estavam a par dos detalhes dos acordos da Google com a NSA, a empresa concordou em fornecer informações sobre o tráfego em suas redes em troca de informações da NSA sobre o que sabia de hackers estrangeiros", escreveu o repórter de defesa Shane Harris no livro @War, uma história sobre guerra. “Era um quid pro quo, informação por informação. E da perspectiva da NSA, informações em troca de proteção. ”122

Isso fez todo o sentido. Os servidores da Google forneceram serviços críticos ao Pentágono, à CIA e ao Departamento de Estado, apenas para citar alguns. Fazia parte da família militar e era essencial para a sociedade estadunidense. Logo, a Google também precisava ser protegido.

A Google não trabalhou apenas com agências de inteligência e militares, mas também procurou penetrar em todos os níveis da sociedade, incluindo agências federais civis, cidades, estados, departamentos de polícia locais, equipes de emergência, hospitais, escolas públicas e todos os tipos de empresas e organizações sem fins lucrativos. Em 2011, a Administração Nacional Oceânica e Atmosférica, a agência federal que pesquisa tempo e meio ambiente, passou para a Google.123 Em 2014, a cidade de Boston implantou a Google para administrar a infraestrutura de informações de seus oitenta mil funcionários – de policiais a professores – e até migrou seus e-mails antigos para a nuvem da Google.124 O Serviço Florestal e a Administração Federal de Rodovias usam o Google Earth e o Gmail. Em 2016, a cidade de Nova York cha-

mou a Google para instalar e operar estações Wi-Fi gratuitas por toda a cidade.125 Califórnia, Nevada e Iowa, enquanto isso, dependem da Google para plataformas de computação em nuvem que preveem e detectam fraudes no sistema de bem-estar social.126 Enquanto isso, a Google medeia a educação de mais da metade dos alunos das escolas públicas dos Estados Unidos.127

"O que realmente fazemos é permitir que você agregue, colabore e realize", explicou Scott Ciabattari, representante de vendas do Google Federal, durante uma conferência de contratação do governo em 2013 em Laramie, Wyoming. Ele estava montando uma sala cheia de funcionários públicos, dizendo a eles que a Google tinha tudo para fazer com que eles – analistas de inteligência, comandantes, gerentes de governo e policiais – acessassem as informações certas no momento certo.128 Ele examinou alguns exemplos: rastreio surtos de gripe, monitoramento de inundações e incêndios florestais, cumprimento de mandados criminais com segurança, integração de câmeras de vigilância e sistemas de reconhecimento facial e até ajuda a policiais a responder a tiroteios em escolas. "Estamos começando a ter, infelizmente, com alguns dos incidentes que acontecem nas escolas, a capacidade de montar uma planta baixa desses eventos", disse ele. “Estamos recebendo esse pedido com cada vez mais frequência. 'Você pode nos ajudar a publicar todas as plantas/mapas do nosso distrito escolar. Se houver um desastre, Deus o livre, queremos saber onde estão acontecendo as coisas.' E ter essa capacidade usando um smartphone. Ser capaz de ver essas informações rapidamente no momento certo salva vidas.” Alguns meses após essa apresentação, Ciabattari se reuniu com autoridades de Oakland para discutir como a Google poderia ajudar a cidade da Califórnia a construir seu centro de vigilância policial.

Essa mistura de sistemas militares, policiais, governamentais, educação pública, negócios e voltados para o consumidor – todos canalizados pela Google – continua despertando alarmes. Os advogados se preocupam com a possibilidade de o Gmail violar os a privacidade entre advogado e cliente.129 Os pais se perguntam o que a Google faz com as informações coletadas sobre os filhos na escola. O que a Google faz com os dados que fluem pelo seu sistema? Tudo isso alimenta a máquina de vigilância corporativa da Google? Quais são os limites e

restrições da Google? Existe alguma? Em resposta a essas perguntas, a Google oferece apenas respostas vagas e conflitantes.130

Obviamente, essa preocupação não se restringe apenas à Google. Sob o manto da maioria das outras empresas de Internet que usamos todos os dias, existem vastos sistemas de vigilância privada que, de uma maneira ou de outra, trabalham e fortalecem o Estado.

O eBay criou uma divisão policial interna chefiada por veteranos da Agência de Repressão às Drogas e do Departamento de Justiça. Possui mais de mil investigadores particulares, que trabalham em estreita colaboração com as agências de inteligência e policiais em todos os países onde opera.131 A empresa realiza seminários e sessões de treinamento e oferece pacotes de viagens para policiais de todo o mundo.132 O eBay se orgulha de seu relacionamento com as autoridades policiais e se orgulha de que seus esforços levaram à prisão de três mil pessoas em todo o mundo – aproximadamente três por dia desde o início da divisão.133

A Amazon executa serviços de computação e armazenamento em nuvem para a CIA.134 O contrato inicial, assinado em 2013, valia US $ 600 milhões e posteriormente foi expandido para incluir a NSA e uma dúzia de outras agências de inteligência dos EUA.135 O fundador da Amazon, Jeff Bezos, usou sua fortuna para lançar a Blue Origin, uma empresa de mísseis que faz parceria com a Lockheed Martin e a Boeing.136 A Blue Origin é uma concorrente direta da SpaceX, uma empresa espacial criada por outro magnata da Internet: o cofundador do PayPal, Elon Musk. Enquanto isso, outro fundador do PayPal, Peter Thiel, transformou o sofisticado algoritmo de detecção de fraudes do PayPal na Palantir Technologies, uma importante empresa militar que fornece serviços avançados de mineração de dados para a NSA e a CIA.137

O Facebook também é acolhedor com os militares. Ele levou a ex-chefe da DARPA, Regina Dugan, a administrar sua secreta divisão de pesquisa “Building 8”, que está envolvida em tudo, desde inteligência artificial a redes de Internet sem fio baseadas em drones. O Facebook está apostando muito na realidade virtual como a interface do usuário do futuro. E o Pentágono também. Segundo relatos, o headset de realidade virtual Oculus do Facebook já foi integrado ao Plano X da

DARPA, um projeto de US $ 110 milhões para construir um ambiente de realidade totalmente imersivo e totalmente virtual para combater ciberguerras.138 Parece algo direto do Neuromancer de William Gibson, e parece que funciona. Em 2016, a DARPA anunciou que o Plano X seria transferido para uso operacional pelo Comando Cibernético do Pentágono dentro de um ano.139

Olhando mais de cima, não há diferença real entre o relacionamento da Google com o governo dos EUA e o de outras empresas de Internet. É apenas uma questão de grau. A grande amplitude e escopo da tecnologia da Google a tornam um substituto perfeito para o restante do ecossistema comercial da Internet.

De fato, o tamanho e a ambição da Google a tornam mais do que uma simples terceirizada. Frequentemente, é uma parceira igual que trabalha lado a lado com agências governamentais, usando seus recursos e domínio comercial para trazer empresas com forte financiamento militar ao mercado. Em 2008, lançou um satélite espião privado chamado GeoEye-1 em parceria com a Agência Nacional de Inteligência Geoespacial.140 Ela comprou a Boston Dynamics, uma empresa de robótica da DARPA que produzia mulas robótica experimentais para os militares, apenas para vendê-la depois que o Pentágono determinou que não colocaria esses robôs em uso ativo.141 Investiu US $ 100 milhões na CrowdStrike, uma importante empresa de defesa cibernética militar e de inteligência que, entre outras coisas, liderou a investigação sobre os supostos hacks do governo russo em 2016 do Comitê Nacional Democrata.142 E também administra a JigSaw, uma incubadora híbrida de tecnologia de think tank destinada a alavancar a tecnologia da Internet para resolver problemas complicados de política externa, desde terrorismo a censura e guerra cibernética.143

Fundada em 2010 por Eric Schmidt e Jared Cohen, um garoto de 29 anos do Departamento de Estado, que serviu tanto para o presidente George W. Bush quanto para o presidente Barack Obama, a JigSaw lançou vários projetos com implicações de política externa e segurança nacional.144 Ela fez uma pesquisa para o governo dos EUA para ajudar a Somália devastada pela guerra a redigir uma nova constituição, desenvolveu ferramentas para rastrear as vendas globais de armas e trabalhou com uma *startup* financiada pelo Departamento de Estado para ajudar as

pessoas no Irã e na China a contornar a censura na Internet .145 Ela também criou uma plataforma para combater o recrutamento e a radicalização de terroristas on-line, que funcionava identificando usuários do Google interessados em tópicos extremistas islâmicos e desviando-os para páginas e vídeos do Departamento de Estado desenvolvidos para dissuadir as pessoas de seguir esse caminho.146 A Google chama isso de "Método de redirecionamento", que parte da ideia mais ampla de Cohen de usar plataformas da Internet para pagar "contrainsurgência digital".147 E, em 2012, à medida que a guerra civil na Síria se intensificou e o apoio estadunidense às forças rebeldes de lá aumentou, a Jig-Saw debateu maneiras de ajudar a tirar Bashar al-Assad do poder. Entre elas: uma ferramenta que mapeia visualmente as deserções de alto nível do governo de Assad, que Cohen queria transmitir à Síria como propaganda para dar "confiança à oposição". "Anexei alguns recursos visuais que mostram como será a ferramenta", escreveu Cohen a vários assessores de Hillary Clinton, que na época era secretária de Estado. "Por favor, mantenha esse contato muito próximo e deixe-me saber se há mais alguma coisa que você acha que precisamos explicar ou pensar antes de lançarmos".148 Como mostram os e-mails vazados, a secretária Clinton ficou intrigada, dizendo a seus assessores que imprimissem a maquete de Cohen do aplicativo para que ela pudesse ver por si mesma.149

A JigSaw parecia turvar a linha entre diplomacia pública e corporativa, e pelo menos um ex-funcionário do Departamento de Estado acusou-a de fomentar mudanças de regime no Oriente Médio.150 “A Google está recebendo apoio da [Casa Branca] e do Departamento de Estado e cobertura aérea. Na realidade, eles estão fazendo coisas que a CIA não pode fazer”, escreveu Fred Burton, executivo da Stratfor e ex-agente de inteligência do Serviço de Segurança Diplomático, o ramo de segurança armada do Departamento de Estado.151

Mas a Google rejeitou as alegações de seus críticos. "Não estamos envolvidos em mudanças de regime", disse Eric Schmidt à Wired.152 “Não fazemos essas coisas. Mas se capacitar os cidadãos com smartphones e informações causa mudanças em seu país, então... isso provavelmente é uma coisa boa, não acha?”

Mediando Tudo e Todos

O trabalho da JigSaw com o Departamento de Estado levantou sobrancelhas, mas sua função é uma mera demonstração do futuro se a Google conseguir o que quer. Enquanto a empresa faz novos acordos com a NSA e continua sua fusão com o aparato de segurança dos EUA, seus fundadores a veem desempenhando um papel ainda maior na sociedade global.

"O objetivo da sociedade é nosso objetivo principal. Sempre tentamos dizer isso na Google. Eis algumas das questões mais fundamentais em que as pessoas não estão pensando: como organizamos as pessoas, como motivamos as pessoas. É um problema realmente interessante: como organizamos nossas democracias?" ruminou Larry Page durante uma rara entrevista em 2014 com o Financial Times. Ele olhou cem anos no futuro e viu a Google no centro do progresso. "Nós provavelmente poderíamos resolver muitos dos problemas que temos como humanos".153

Gaste tempo ouvindo e lendo as palavras dos executivos da Google, e você rapidamente perceberá que eles não veem linha clara separando governo e Google. Eles olham para o futuro e vêem empresas da Internet se transformando em sistemas operacionais para a sociedade. Para eles, o mundo é grande demais e se move rápido demais para os governos tradicionais o acompanharem.154 O mundo precisa da ajuda da Google para liderar o caminho, fornecer ideias, investimentos e conhecimento técnico. E, de qualquer maneira, não há como impedir a expansão da tecnologia.155 Transporte, entretenimento, usinas e redes de energia, departamentos policiais, empregos, transporte público, saúde, agricultura, moradia, eleições e sistemas políticos, guerra e até exploração espacial – tudo está conectado à Internet e empresas como a Google não podem deixar de estar no centro. Não há escapatória.

Algumas pessoas na Google falam sobre a construção de uma nova cidade a partir da "Internet", usando a arquitetura de dados da Google como base, livre de regulamentos governamentais que restringem a inovação e o progresso.156 Esse mundo novo e corajoso, cheio de biossensores da Google e piscando com fluxos de dados ininterrup-

tos, é realmente apenas o velho mundo dos sonhos ciber-libertarianistas, visto pela primeira vez no Catálogo Toda a Terra e a poesia utópica de Richard Brautigan, um mundo onde “mamíferos e computadores / moram juntos em harmonia / de programação mútua... uma floresta cibernética ... onde veados passeiam pacificamente, / passam por computadores ... e todos vigiados por máquinas de amorosa graça." Exceto que na versão deste futuro da Google, as máquinas da graça amorosa não são uma abstração benevolente, mas uma poderosa corporação global.157

O paralelo não inspira confiança. Na década de 1960, muitos dos novos comunalistas de Brand construíram microcomunidades baseadas em ideias cibernéticas, acreditando que hierarquias planas, transparência social e interconectividade radical entre indivíduos aboliriam a exploração, a hierarquia e o poder. No final, a tentativa de substituir política por tecnologia foi a falha fatal: sem proteção organizada para os fracos, essas pretensas utopias se transformaram em cultos controlados por líderes carismáticos e dominadores que governavam seus feudos por meio de humilhação e intimidação. "Havia constantemente um pano de fundo de medo na casa – como um vírus correndo no fundo. Como spyware. Você sabe que está lá, mas não sabe como se livrar dele”, lembra uma membro de uma comuna do Novo México que caiu num mundo de pesadelos de abuso e exploração sexual.

Um *spyware* sendo executado em segundo plano.

É uma curiosa escolha de palavras para explicar como foi viver em uma utopia cibernética dos anos 1970 que deu errado. É também uma descrição precisa do mundo atual que a Google e a Internet construíram.

Capítulo 6

A Corrida armamentista de Edward Snowden

Um espectro está assombrando o mundo moderno,
o espectro da anarquia criptográfica.
- Timothy C. May,
Manifesto Criptográfico Anarquista, 1988

Em junho de 2013, manchetes surgiram em todo o mundo: um funcionário da Agência de Segurança Nacional (dos EUA) havia fugido do país com uma enorme quantidade de documentos ultrassecretos e estava denunciando o aparelho de vigilância global dos Estados Unidos. A princípio, a identidade desse vazador da NSA permaneceu envolta em mistério. Jornalistas chegaram a Hong Kong, vasculhando os saguões de hotéis procurando desesperadamente por pistas. Finalmente, surgiu uma fotografia: um jovem magro e pálido, com cabelos desgrenhados, óculos de aro e uma camisa cinza aberta na gola, sentado no sofá de um hotel – calmo, mas parecendo que não dormia há dias.

O nome dele era Edward Snowden – "Ed", como ele queria que as pessoas o chamassem. Ele tinha 29 anos. Seu currículo era assustador: Agência Central de Inteligência (EUA), Agência de Inteligência de Defesa dos EUA e, mais recentemente, Booz Allen Hamilton, empreiteiro de defesa que dirigia operações de vigilância digital para a Agência de Segurança Nacional.1

Sentado em seu quarto no Hotel Mira, cinco estrelas, em Hong Kong, Snowden disse a jornalistas do Guardian que assistir ao sistema de vigilância global operado pela NSA havia forçado sua mão e o obrigou a se tornar um denunciante. "A NSA construiu uma infraestrutura

que permite interceptar quase tudo", disse ele em uma voz calma e controlada durante uma entrevista em vídeo que apresentou o denunciante e seus motivos ao mundo. “Não quero viver em uma sociedade que faça esse tipo de coisa. Não quero viver em um mundo onde tudo o que faço e digo é gravado. Não é isso que estou disposto a apoiar ou a viver com.”2

Nos meses seguintes, um pequeno grupo de jornalistas revisou e montou matérias os documentos que Snowden havia retirado da NSA. O material amparava suas reivindicações, sem dúvida. O governo dos EUA estava executando um vasto programa de vigilância na Internet, invadindo telefones celulares, entrando em cabos de fibra óptica submarinos, subvertendo protocolos de criptografia e explorando praticamente todas as principais plataformas e empresas do Vale do Silício – Facebook, Google, Apple, Amazon. Mesmo jogos para celular, como o Angry Birds, não escaparam à fome da agência de espionagem. Nada parecia estar fora do seu alcance.

As revelações provocaram um escândalo de proporções globais. Privacidade, vigilância e coleta de dados na Internet não eram mais consideradas questões secundárias relegadas principalmente às margens, mas assuntos importantes que venceram o Pulitzers e mereceram tratamento de primeira página no New York Times, Wall Street Journal e Washington Post. E o próprio Snowden, fugindo do governo dos EUA, tornou-se material de lenda, sua história imortalizada na grande tela: um documentário vencedor do Oscar e um filme de Hollywood dirigido por Oliver Stone, seu papel interpretado por Joseph Gordon-Levitt.

Após as revelações de Snowden, as pessoas ficaram subitamente chocadas e indignadas com o fato de o governo dos EUA usar a Internet para vigilância. Mas, dadas as origens da contrainsurgência da Internet, seu papel em espionar os estadunidenses desde a década de 1970 e os laços estreitos entre o Pentágono e empresas como Google, Facebook e Amazon, essas notícias não deveriam ter sido uma surpresa. Ter chocado tantas pessoas é um testemunho do fato de que a história militar da Internet havia sido lavada da memória coletiva da sociedade.

A verdade é que a Internet surgiu de um projeto do Pentágono para desenvolver sistemas modernos de comunicação e informação que permitiriam aos Estados Unidos derrotar seus inimigos, tanto em casa

quanto no exterior. Esse esforço foi um sucesso, superando todas as expectativas. Então, é claro, o governo dos EUA alavancou a tecnologia que havia criado e a mantém ao máximo. E como poderia ser diferente?

É só plugar

Os governos espionam os sistemas de telecomunicações há muito tempo, remontando aos dias do telégrafo e dos primeiros sistemas telefônicos. No século XIX, o presidente Abraham Lincoln deu a seu secretário de guerra, Edwin Stanton, amplos poderes sobre a rede de telégrafos do país, permitindo espionar as comunicações e controlar a disseminação de informações indesejadas durante a Guerra Civil. No início do século XX, o Federal Bureau of Investigation (FBI) utilizou os sistemas telefônicos com impunidade, espionando contrabandistas, ativistas trabalhistas, líderes de direitos civis e qualquer pessoa que o presidente J. Edgar Hoover considerasse subversiva e ameaçadora para os Estados Unidos. No século XXI, a Internet abriu novas perspectivas e possibilidades.3

A ARPANET foi usada pela primeira vez para espionar os estadunidenses em 1972, quando foi empregada para transferir arquivos de vigilância de manifestantes antiguerra e líderes de direitos civis coletados pelo Exército dos EUA. Naquela época, a rede era apenas uma ferramenta para permitir que o Pentágono compartilhasse rápida e facilmente dados com outras agências.4 Para realmente espionar as pessoas, o exército primeiro teve que reunir as informações. Isso significava enviar agentes ao mundo para assistir pessoas, entrevistar vizinhos, grampear telefones e passar noites vigiando alvos. Foi um processo trabalhoso e, a certa altura, o exército montou sua própria equipe de notícias falsas para que os agentes pudessem filmar e entrevistar manifestantes antiguerra com mais facilidade. A Internet moderna mudou a necessidade de todos esses esquemas elaborados.

E-mail, compras, compartilhamento de fotos e vídeos, namoro, mídias sociais, smartphones – o mundo não se comunica apenas pela Internet, ele vive na Internet. E toda essa vida deixa um rastro. Se as

plataformas gerenciadas pela Google, Facebook e Apple poderiam ser usadas para espionar os usuários, a fim de veiculá-los anúncios direcionados, de identificar preferências de filmes, de personalizar feeds de notícias ou de adivinhar onde as pessoas irão jantar, por que elas também não poderiam ser usadas para combater o terrorismo, prevenir crimes e manter o mundo seguro? A resposta é: é claro que elas podem.

Quando Edward Snowden apareceu em cena, os departamentos de polícia de San Francisco a Miami estavam usando plataformas de mídia social para se infiltrar e observar grupos políticos e monitorar protestos. Os investigadores criaram contas falsas e se insinuaram sorrateiramente na rede social de seus alvos, depois conseguiram mandados para acessar mensagens privadas e outros dados subjacentes não disponíveis publicamente. Alguns, como o Departamento de Polícia de Nova York, lançaram divisões especializadas que usavam as mídias sociais como uma ferramenta central de investigação. Os detetives podem passar anos monitorando a atividade na Internet dos suspeitos, compilando postagens do YouTube, Facebook e Twitter, mapeando relacionamentos sociais, decifrando gírias, rastreando movimentos e correlacionando-os com possíveis crimes.5 Outros, como o estado de Maryland, criaram soluções personalizadas que incluíam software de reconhecimento facial para que os policiais pudessem identificar as pessoas fotografadas em protestos, combinando as imagens retiradas do Instagram e do Facebook com as do banco de dados da carteira de motorista do estado.6 Uma indústria editorial que ensinou policiais a conduzir investigações usando a Internet floresceu, com títulos de manuais de treinamento como "O Grampo do Policial Fuleiro: Transformando um Celular em uma Ferramenta de Vigilância Usando Aplicativos Gratuitos" e a "Linha do Tempo do Google: Investigações de Localização envolvendo Dispositivos Android".7

Naturalmente, as agências de inteligência federais foram pioneiras nesse campo.8 A Agência Central de Inteligência (CIA) foi uma grande fã do que chamou de "inteligência de código aberto" – informações que poderiam ser obtidas da Web pública: vídeos, blogs pessoais, fotos e postagens em plataformas como YouTube, Twitter, Facebook, Instagram e Google+.9 Em 2005, a agência fez uma parceria com o Escritório do Diretor de Inteligência Nacional para lançar o Centro de Código Aberto, dedicado à construção de ferramentas de coleta de

código aberto e o seu compartilhamento com outras agências federais de inteligência.10 Por meio do seu fundo de capital de risco In-Q-Tel, a CIA investiu em todos os tipos de empresas que exploravam a Internet para obter informações de código aberto.11 Investiu na Dataminr, que comprou acesso aos dados do Twitter e analisou os tweets das pessoas para identificar possíveis ameaças.12 Apoiou uma empresa "de mídia social de inteligência" chamada PATHAR que monitorava as contas do Facebook, Instagram e Twitter em busca de sinais de radicalização islâmica. E apoiou um produto popular chamado Geofeedia, que permitia que seus clientes exibissem postagens de mídia social do Facebook, YouTube, Twitter e Instagram de locais geográficos específicos, até o tamanho de um quarteirão. Os usuários podem assistir em tempo real ou voltar o relógio para tempos anteriores.13 Em 2016, a Geofeedia possuía como clientes quinhentos departamentos de polícia e divulgou sua capacidade de monitorar “ameaças manifestas”: sindicatos, protestos, tumultos e grupos ativistas.14 Todas essas empresas apoiadas pela CIA pagaram ao Facebook, Google e Twitter por acesso especial aos dados de mídia social – adicionando outro fluxo de receita lucrativa ao Vale do Silício.15

A vigilância é apenas o ponto de partida. Voltando ao sonho original da Guerra Fria de construir sistemas preditivos, oficiais militares e de inteligência viram plataformas como Facebook, Twitter e Google como mais do que apenas ferramentas de informação que poderiam ser vasculhadas em busca de informações sobre crimes ou eventos individuais. Elas poderiam ser os olhos e os ouvidos de um vasto sistema de alerta antecipado interconectado, prevendo o comportamento humano – e, finalmente, mudar o curso do futuro.

Quando Edward Snowden denunciou a NSA no verão de 2013, pelo menos uma dúzia de programas públicos divulgados publicamente pelo governo dos EUA estavam aproveitando a inteligência de código aberto para prever o futuro. A Força Aérea dos EUA tinha uma iniciativa de "Radar Social" para extrair informações provenientes da Internet, um sistema explicitamente padronizado com base nos sistemas de radar de alerta antecipado usados para rastrear aviões inimigos.16 A Agência de Projetos de Pesquisa Avançada de Inteligência (ARPA), administrada pelo Escritório do Diretor de Inteligência Nacional, possuía vários programas de pesquisa de "inteligência antecipatória", que envolviam desde

mineração de vídeos do YouTube em busca de ameaças terroristas até previsão de instabilidade, verificando feeds e blogs do Twitter e monitorando a Internet para prever futuros ataques cibernéticos.17 A DARPA também executou um projeto de radar humano: o Sistema Integrado Global de Alerta Pré-Crise, ou ICEWS. Iniciado em 2007 e construído pela Lockheed Martin, o sistema acabou se transformando em uma máquina operacional militar de previsão que possuía módulos que ingeriam todo tipo de dados de rede de código aberto – notícias, blogs, mídias sociais e postagens no Facebook, várias conversas na Internet e "outras fontes de informação" – e direcioná-la através da "análise de sentimentos", na tentativa de prever conflitos militares, insurgências, guerras civis, golpes e revoluções.18 O ICEWS da DARPA provou ser um sucesso. Sua tecnologia principal foi transformada em uma versão operacional classificada do mesmo sistema chamado ISPAN e absorvida pelo Comando Estratégico dos EUA.19

O sonho de construir um sistema global de computadores que pudesse assistir ao mundo e prever o futuro tinha uma história longa e documentada nos círculos militares. E, como mostraram os documentos divulgados por Snowden, a NSA desempenhou um papel central na construção das ferramentas de interceptação e análise que trariam esse sonho à realidade.20

A Agência de Segurança Nacional (NSA) foi criada por uma ordem executiva classificada, assinada pelo presidente Harry Truman em 1952. Um órgão altamente secreto, cuja própria existência permaneceu oculta por anos após sua criação, a agência tinha um duplo mandato. Um era ofensivo: coletar comunicações eletrônicas e inteligência de sinais no exterior, o que significava capturar transmissões de rádio e satélite, grampear telefones e quebrar a criptografia usada por governos estrangeiros. O outro era defensivo: impedir que sistemas críticos de comunicação do governo dos EUA fossem invadidos por potências estrangeiras. Em meados da década de 1970, quando a existência da NSA chamou a atenção do público pela primeira vez em uma série de audiências no congresso, a agência empregava 120.000 pessoas e tinha 2.000 postos de escuta no exterior com antenas gigantes instaladas em todo o mundo, ouvindo cada alfinete que caída na União Soviética.21

A NSA esteve envolvida com a Internet desde o início da rede como um projeto de pesquisa da ARPA. A partir do início da década de 1970, ela mantinha um nó na incipiente ARPANET e estava diretamente implicada no uso da rede para transferir arquivos de vigilância de manifestantes antiguerra e líderes de direitos civis que o Exército dos EUA havia compilado ilegalmente.22 Em 1972, a NSA contratou a Bolt, Beranek e Newman, uma terceirizada da ARPA, onde J. C. R. Licklider havia atuado como vice-presidente, para construir uma versão atualizada da ARPANET de sua rede de inteligência chamada COINS que eventualmente se conectou à ARPANET, à CIA, ao Departamento de Estado e à Agência de Defesa de Inteligência.23 Ao mesmo tempo, financiou o trabalho em outros projetos classificados da ARPANET que, ao longo das décadas, evoluiriam para sistemas operacionais de rede classificados, incluindo o que a NSA usa hoje: a NSANET.24

Nos anos 2000, quando a Internet se transformou em uma rede comercial de telecomunicações, a missão da inteligência de sinais da NSA também se expandiu. Quando Edward Snowden foi transferido para seu último e derradeiro trabalho de contratação da NSA na Booz Allen Hamilton, no Havaí, em 2013, a agência já sabia tudo o que fluía pela Internet. Fiel à sua natureza espiã, a NSA teve um papel duplo. Por um lado, trabalhou com empresas como Google e Amazon, comprando seus serviços e ajudando a defendê-las de hacks e ciberataques estrangeiros. Por outro lado, a agência invadiu essas empresas pelas costas – fazendo buracos e colocando escutas em todos os dispositivos que podiam penetrar. Ela estava apenas fazendo seu trabalho.

Os vazamentos de Snowden revelaram que a NSA tinha implantes espiões embutidos nos pontos de troca da Internet, onde os backbones, ou seja, a infraestrutura principal da rede de cada país, se encontravam. A empresa administrava uma unidade de operações de acesso sob medida para hackers de elite que fornecia soluções de penetração personalizadas quando as ferramentas de vigilância geral da agência não conseguiam fazer o trabalho. Ela executava programas direcionados a todas as principais plataformas de computadores pessoais: Microsoft Windows, Apple iOS e Google Android, permitindo que os espiões extraíssem tudo e qualquer coisa que esses dispositivos tivessem.25 Em parceria com a agência de espionagem da Sede de Comunicações do Governo do Reino Unido, a NSA lançou um programa chamado MUSCULAR

que secretamente se unia às redes internas de cabos de fibra ótica que conectam um datacenter do Vale do Silício a outro, permitindo que a agência obtenha uma "visão completa" dos dados internos de uma empresa. A Yahoo! era um alvo; a Google também – o que significa que a agência sugou tudo o que a Google tinha, incluindo os perfis e dossiês que a empresa mantinha de todos os seus usuários. Os documentos da NSA mostravam copiosamente a capacidade da agência de fornecer "uma visão retrospectiva das atividades do alvo", significando todos os emails e mensagens enviados, todos os lugares em que ele esteve com um telefone Android no bolso.26

Talvez o programa mais escandaloso da NSA revelado pelas divulgações de Snowden seja o chamado PRISM, que envolve um sofisticado grampo ou acesso de dados sob demanda, alojado nos datacenters dos maiores e mais respeitados nomes do Vale do Silício: Google, Apple, Facebook, Yahoo! e Microsoft. Esses dispositivos permitem que a NSA desvie o que a agência exigir, incluindo e-mails, anexos, bate-papos, catálogos de endereços, arquivos, fotografias, arquivos de áudio, atividades de pesquisa e histórico de localização de telefones celulares.27 Segundo o Washington Post, essas empresas sabiam sobre o PRISM e ajudaram a NSA a criar o acesso especial a seus sistemas de rede que o PRISM requer, tudo sem alarmar o público ou notificar seus usuários. "Os problemas de engenharia são tão imensos, em sistemas de tamanha complexidade e com mudanças frequentes, que seria difícil pressionar o FBI e a NSA para construir portas dos fundos sem a ajuda ativa de cada empresa".28

O Washington Post revelou que o PRISM é administrado para NSA pela secreta Unidade de Tecnologia de Interceptação de Dados do FBI, que também lida com grampos na Internet e no tráfego telefônico que flui através das principais empresas de telecomunicações como AT&T, Sprint e Verizon. O PRISM se assemelha aos acessos físicos tradicionais que o FBI mantinha em todo o sistema de telecomunicações no território dos EUA. Funciona assim: usando uma interface especializada, um analista da NSA cria uma solicitação de dados, chamada de "tarefa", para um usuário específico de uma empresa parceira. “Uma tarefa para a Google, Yahoo, Microsoft, Apple e outros fornecedores é roteada para equipamentos [“unidades de interceptação”] instaladas em cada empresa. Este equipamento, mantido pelo FBI, passa a solicitação

da NSA para o sistema de uma empresa privada."29 A tarefa cria um grampo digital que, em seguida, encaminha a inteligência [os dados] para a NSA em tempo real, tudo sem nenhuma interferência da própria empresa.30 Os analistas podem até optar por receber alertas de quando um determinado alvo efetua login em uma conta.31 "Dependendo da empresa, uma 'tarefa' pode retornar e-mails, anexos, catálogos de endereços, calendários, arquivos armazenados na nuvem, bate-papos de texto ou áudio ou vídeo e 'metadados' que identificam os locais, dispositivos usados e outras informações sobre um alvo."32

O programa, iniciado em 2007 sob o mandato do presidente George W. Bush e expandido pelo presidente Barack Obama, tornou-se uma mina de ouro para os espiões estadunidenses. A Microsoft foi a primeira a ingressar em 2007. A Yahoo! ficou online um ano depois, e o Facebook e a Google se conectaram ao PRISM em 2009. Skype e AOL entraram em 2011. A Apple, a retardatária do grupo, ingressou no sistema de vigilância em 2012.33 Os funcionários da inteligência descreveram o PRISM como o principal sistema de inteligência estrangeira.34 Em 2013, o PRISM foi usado para espionar mais de cem mil pessoas – "alvos" na linguagem da NSA. James R. Clapper, diretor de Inteligência Nacional, descreveu os produtos do PRISM como sendo "as informações de inteligência estrangeira mais importantes e valiosas que coletamos".35

Os documentos da NSA, revelados pelo Washington Post, ofereceram apenas um vislumbre do programa PRISM, mas o suficiente para mostrar que a NSA transformou as plataformas de alcance global do Vale do Silício em um aparato de coleta de inteligência de fato. Tudo com a ajuda da própria indústria. O PRISM ainda apresentava uma interface fácil de usar, com alertas de texto.

Essas foram revelações condenatórias. E, para o Vale do Silício, elas carregavam uma carga de perigo.

Surge uma ameaça

Desde o início, as empresas de Internet apostaram fortemente na promessa utópica de um mundo em rede. Mesmo enquanto elas buscavam contratos com os militares e seus fundadores se juntavam ao grupo das pessoas mais ricas do planeta, eles queriam que o mundo os visse não apenas como os mesmos velhos plutocratas buscando maximizar o lucro dos acionistas e seu próprio poder, mas também como agentes progressistas liderando o caminho para uma brilhante tecno-utopia. Por um longo tempo, eles conseguiram. Apesar de driblarem lentamente as notícias sobre o Vale do Silício fechando acordos com a CIA e a NSA, a indústria conseguiu de alguma forma convencer o mundo de que era diferente, de alguma forma se opunha ao poder tradicional.

Então Edward Snowden estragou tudo.

A divulgação pública do programa PRISM da NSA deu um vislumbre na relação simbiótica entre o Vale do Silício e o governo dos EUA e ameaçou prejudicar a imagem cuidadosamente cultivada da indústria. Isso não era boato ou especulação, mas vinha de documentos primários retirados das profundezas da agência de espionagem mais poderosa do mundo. Eles forneceram a primeira evidência tangível de que as maiores e mais respeitadas empresas de Internet haviam trabalhado em segredo para canalizar dados de centenas de milhares de usuários para a NSA, revelando por extensão a grande quantidade de dados pessoais que essas empresas coletavam sobre seus usuários – dados que elas possuíam e podiam usar da maneira que quisessem.

Você não precisava ser um especialista em tecnologia para ver que a vigilância do governo na Internet simplesmente não poderia existir sem a infraestrutura privada e os serviços ao consumidor fornecidos pelo Vale do Silício. Empresas como Google, Facebook, Yahoo!, eBay e Apple fizeram todo o trabalho pesado: construíram as plataformas que atraíram bilhões de usuários e coletaram uma quantidade espantosa de dados sobre eles. Tudo o que a NSA precisava fazer para obter os dados era conectar alguns fios. E foi o que a agência fez com total cooperação e discrição das próprias empresas.

Nos meses que se seguiram ao vazamento de Snowden, o Vale do Silício e a vigilância subitamente se posicionaram e se entrelaçaram. Argumentos sobre a necessidade de aprovar novas leis que restringiam a coleta de dados na Internet por empresas privadas uniram-se aos apelos

para restringir o programa de vigilância da NSA. Todos agora sabiam que a Google e o Facebook estavam devorando todos os dados possíveis sobre nós. Surgiu um maremoto em torno da ideia de que isso durou tempo demais. Novos controles e limites na coleta de dados teriam que ser implementados.

“A Google pode possuir mais informações sobre mais pessoas do que qualquer entidade na história do mundo. Seu modelo de negócios e sua capacidade de executá-lo demonstram que continuará a coletar informações pessoais sobre o público em um ritmo galopante”, alertou o influente fiscalizador Public Citizen em um relatório que fez manchetes em todo o mundo. “A quantidade de informações e influência que a Google acumulou está ameaçando ganhar tanto domínio sobre especialistas, reguladores e legisladores que poderia deixar o público sem poder de agir se decidisse que a empresa se tornou muito difundida, onisciente e muito poderosa."36

As empresas de Internet responderam com proclamações de inocência, negando qualquer papel no programa PRISM da NSA. “O Facebook não é e nunca fez parte de nenhum programa para dar aos EUA ou a qualquer outro governo acesso direto aos nossos servidores. Nunca recebemos uma solicitação geral ou ordem judicial de qualquer agência governamental que solicite informações ou metadados em massa, como o que a Verizon recebeu. E se o fizéssemos, lutaríamos agressivamente. Nunca ouvimos falar do PRISM antes de ontem”, escreveu Mark Zuckerberg em um post no Facebook. Ele culpou o governo e posicionou o Facebook como vítima. “Liguei para o presidente Obama para expressar minha frustração pelos danos que o governo está causando para todo o nosso futuro. Infelizmente, parece que vai demorar muito tempo para que haja uma verdadeira reforma total.” Apple, Microsoft, Google e Yahoo!, todas reagiram da mesma maneira, negando as acusações e se pintando como vítimas do excesso de governo. “É tremendamente decepcionante que o governo tenha secretamente feito tudo isso e não tenha nos contado. Não podemos ter democracia se tivermos que proteger você e nossos usuários do governo”, disse Larry Page a Charlie Rose em entrevista à CBS.37

Mas suas desculpas soaram vazias. "Apesar das afirmações das empresas de tecnologia de que elas fornecem informações sobre seus

clientes somente quando exigidas por lei – e não conscientemente por uma porta dos fundos – a percepção de que elas permitiram o programa de espionagem permaneceu", relatou o New York Times em 2014.38

Por um momento após os vazamentos de Snowden, o Vale do Silício entrou em um estado de choque, congelado de medo sobre como lidar com o escândalo. Foi um momento surpreendente na história. Você quase podia ouvir as rodas gigantes da máquina de relações públicas do Vale do Silício parar. Enquanto os analistas previam prejuízos de bilhões de dólares para o setor como resultado das revelações de Snowden: um exército de blogueiros amigáveis, acadêmicos, think tanks, ONGs financiadas por empresas (Astroturf groups), lobistas e jornalistas sentaram-se a frente de seus teclados, encarando suas mãos, esperando com expectativa por uma reação.39

Edward Snowden aterrorizou a indústria.

Catapultado para o status de um herói cult, ele agora exercia uma influência maciça. Ele podia facilmente se concentrar no aparato de vigilância privado do Vale do Silício e explicar que era parte integrante da maior máquina de vigilância operada pela NSA – que era uma das duas partes do mesmo sistema. Com apenas algumas palavras, ele tinha o poder de iniciar um movimento político real e estimular as pessoas a pressionar por leis de privacidade reais e significativas. Naquele momento, ele tinha todo o poder. Ele era o pesadelo de Larry Page, a personificação do motivo pelo qual a Google alertou seus investidores de que as leis de privacidade representavam uma ameaça existencial aos seus negócios: “As preocupações com a privacidade relacionadas a elementos de nossa tecnologia podem prejudicar nossa reputação e impedir que usuários atuais e potenciais usem nossos produtos e serviços."40

Mas o Vale do Silício teve sorte. Snowden, que sempre foi um libertarianista, teve outras ideias.

Pronto para atirar

Edward Joseph Snowden nasceu em uma família conservadora em 21 de junho de 1983, em Elizabeth City, Carolina do Norte. Seu pai era oficial da Guarda Costeira. Sua mãe era administradora de um tribunal. Ele se mudou para Maryland na adolescência e abandonou o ensino médio no segundo ano. Foi então que ele começou a aprofundar o interesse infantil em computadores. Ele participou do fórum da Web do Ars Technica, um site de notícias sobre tecnologia com um fórum ativo para geeks com ideias afins. Lá, ele se tornou libertarianista de direita: odiava o New Deal, queria encolher o governo até o tamanho de um amendoim e acreditava que o Estado não tinha o direito de controlar o fornecimento de dinheiro. Ele preferia o padrão ouro. Zombava dos idosos por precisarem de pensões para a velhice. "De alguma forma, nossa sociedade conseguiu passar centenas de anos sem a segurança social", escreveu ele no fórum. "Magicamente, o mundo mudou após o New Deal e os idosos se tornaram pecinhas de vidro". Ele chamou as pessoas que defendiam o sistema de previdência social dos Estados Unidos de "retardados".41

Em 2004, um ano depois que os Estados Unidos invadiram o Iraque, Snowden se alistou no programa das Forças Especiais do Exército. Ele marcou sua religião como "budista". Ao descrever sua decisão de ingressar no exército, disse que sentia uma "obrigação como ser humano de ajudar a libertar as pessoas da opressão" e que acreditava que as Forças Especiais eram um grupo nobre. “Eles estão inseridos atrás das linhas inimigas. É um esquadrão que tem várias especialidades diferentes. E eles ensinam e permitem à população local resistir ou apoiar as forças estadunidenses de uma maneira que permita à população local a chance de determinar seu próprio destino.”42 Snowden nunca chegou ao Iraque (que sempre parecia uma missão estranha para um libertarianista). Ele quebrou as duas pernas em um exercício do exército e não conseguiu concluir o treinamento básico. Sua vida deu uma guinada diferente.

Ele encontrou trabalho como guarda de segurança no Centro de Estudos Avançados de Idiomas da NSA na Universidade de Maryland. Subiu rapidamente a carreira. Em 2006, a CIA o contratou como especialista em segurança da tecnologia da informação, um trabalho que lhe concedeu permissão de segurança ultrassecreta e o enviou a Genebra sob a cobertura do Departamento de Estado. Esta não foi uma tarefa simples de TI. Ele agora era um oficial de campo da CIA que morava na

Europa. “Eu não tenho nenhum tipo de diploma. Nem tenho um diploma do ensino médio”, gabou-se anonimamente para seus amigos online na Ars Technica. Um conhecido de Snowden de seus dias na CIA em Genebra descreveu-o como um "gênio da TI", bem como um lutador de artes marciais. Seu pai se gabava de que seu filho possuía um QI de nível genial de 145.

Em uma nota anexada a seus vazamentos, Snowden deu aos jornalistas um detalhamento de sua experiência de trabalho: 43

Edward Joseph Snowden, SSN: ****

Codinome da CIA "*****"

Número de identificação da agência: *****

Ex-Conselheiro Sênior | Agência de Segurança Nacional dos Estados Unidos, sob cobertura corporativa

Ex-oficial de campo | Agência Central de Inteligência dos Estados Unidos, sob cobertura diplomática

Ex-Professor | Agência de Inteligência de Defesa dos Estados Unidos, sob cobertura corporativa

Apesar de seu trabalho como agente de inteligência no momento exato em que a CIA estava expandindo seus programas globais de vigilância e assassinato por drones, parecia que Snowden de alguma forma continuava inconsciente de que a espionagem estava ocorrendo em toda a Internet. Como ele contou em sua biografia, foi somente em 2009, depois de assumir seu primeiro emprego como contratado particular, trabalhando para a Dell em uma instalação da NSA no Japão, que realmente caiu a ficha. "Vi como Obama avançava as políticas que pensei que seriam freadas", disse ele. O governo dos EUA estava executando uma operação de vigilância global. O mundo precisava saber, e ele começou a se ver como aquele que botaria a boca no trombone.44 “Você não pode esperar que outra pessoa aja. Eu estava procurando líderes, mas percebi que liderança significa ser o primeiro a agir. ”45

Então, começou a se preparar. Em 2012, foi realocado para outra missão da NSA para a Dell, desta vez no Havaí. Lá, trabalhando para o escritório de compartilhamento de informações da NSA em um bunker

subterrâneo que fora usado como instalação de armazenamento, Snowden começou a coletar os documentos que usaria para expor o aparelho de vigilância dos EUA. Ele até solicitou uma transferência para uma divisão diferente da NSA – aquela da terceirizada Booz Allen Hamilton – porque isso lhe daria acesso a um conjunto de documentos sobre operações cibernéticas dos EUA que ele achava que o povo estadunidense deveria conhecer.46 “Minha posição na Booz Allen Hamilton me concedeu acesso a listas de máquinas em todo o mundo que a NSA invadiu. Por isso aceitei essa posição há cerca de três meses”, disse ao South China Morning Post de seu esconderijo em Hong Kong.47

Snowden explicou seu motivo em simples termos morais. Era algo com o qual muitos podiam se relacionar, e ele logo emergiu como um ícone de culto global que eliminava as divisões políticas da esquerda e da direita. Para Michael Moore, ele era o "herói do ano". Para Glenn Beck, ele era um vazador patriótico – corajoso e sem medo de aceitar as consequências.48 Até os colegas denunciantes da NSA ficaram impressionados. "Nunca encontrei alguém como Snowden. Ele é uma raça exclusivamente pós-moderna de denunciantes”, escreveu James Bamford.49 Mas, apesar de todos os elogios que recebeu, este moderno Daniel Ellsberg tinha um perfil político peculiar.

Edward Snowden finalmente escapou para a Rússia, o único país que poderia garantir sua segurança do longo braço dos Estados Unidos. Lá, enquanto vivia sob proteção estatal em um local não revelado em Moscou, ele varreu o papel do Vale do Silício na vigilância da Internet para debaixo do tapete. Questionado sobre isso pelo repórter do Washington Post Barton Gellman, que havia relatado o programa PRISM da NSA, Snowden descartou o perigo representado por empresas como Google e Facebook. O motivo? As empresas privadas não têm o poder de prender, encarcerar ou matar pessoas. "O Twitter não lança ogivas nucleares", brincou.50

Para alguém que passou anos percorrendo a CIA e a NSA, desfrutando do acesso aos segredos mais profundos do Estado de vigilância estadunidense, as visões de Snowden eram curiosamente simples e ingênuas. Ele parecia ignorar os profundos laços históricos entre empresas de tecnologia e as forças armadas dos EUA. Na verdade, ele parecia ignorante sobre os principais aspectos dos mesmos documentos que reti-

rara da NSA, que mostravam como os dados integrais produzidos pelas empresas de tecnologia de consumo serviam para operações governamentais mortais no exterior. Isso incluía o programa global de assassinatos por drones da CIA, que dependia do rastreamento de celulares da NSA dos agentes da Al-Qaeda no Paquistão e no Iêmen e o uso desses dados de geolocalização para realizar ataques com mísseis.51 Até o general Michael Hayden, ex-diretor da CIA e da NSA, admitiu que os dados extraídos de tecnologias comerciais são usados para ataques. "Matamos pessoas com base em metadados", disse ele durante um debate na Universidade Johns Hopkins.52 Em outras palavras, os documentos da NSA de Snowden provaram exatamente o oposto do que Snowden estava argumentando. Involuntariamente ou não, seja para o bem ou para o mal, informações pessoais geradas por empresas privadas – empresas como Twitter, Google e de telecomunicações no Paquistão – de fato ajudaram a lançar mísseis.

As opiniões de Snowden sobre a vigilância privada eram simplistas, mas pareciam estar alinhadas com sua visão política. Ele era libertarianista e acreditava na promessa utópica das redes de computadores. Acreditava que a Internet era uma tecnologia inerentemente libertadora que, se deixada em paz, evoluiria para uma força do bem no mundo. O problema não era o Vale do Silício; era o poder do governo. Para ele, agências de inteligência cínicas como a NSA haviam distorcido a promessa utópica da Internet, transformando-a em uma distopia onde espiões rastreavam cada movimento nosso e registravam tudo o que dizemos. Ele acreditava que o governo era o problema central e desconfiava de soluções legislativas ou políticas para conter a vigilância, o que envolveria ainda mais o governo. Por acaso, sua linha de pensamento acompanhou perfeitamente as iniciativas de privacidade antigovernamentais que empresas de Internet como Google e Facebook começaram a pressionar para desviar a atenção de suas práticas de vigilância privada.

“Precisamos de maneiras de realizar comunicações privadas. Precisamos de mecanismos para associações privadas. E, finalmente, precisamos de formas de realizar pagamentos e remessas particulares, que são a base do comércio”, explicou Snowden a Micah Lee em um elegante hotel de Moscou perto da Praça Vermelha. Lee era um ex-tecnólogo da EFF que, de sua casa em Berkeley, Califórnia, havia trabalhado

em segredo para ajudar Snowden a se comunicar com segurança com jornalistas e realizar seus vazamentos. Ele viajou para Moscou para conversar com Snowden cara a cara sobre o que as pessoas poderiam fazer para "recuperar sua privacidade".

"Acho que a reforma pode ter muitas caras", disse Snowden a Lee. “Isso pode ser através da tecnologia, da política, do voto, do comportamento. Mas a tecnologia é ... talvez o meio mais rápido e promissor pelo qual possamos responder às maiores violações dos direitos humanos de uma maneira que não dependa de cada órgão legislativo do planeta para se reformar ao mesmo tempo, o que provavelmente é um pouco otimista de se esperar. Em vez disso, poderíamos criar sistemas ... que reforçam e garantem os direitos necessários para manter uma sociedade livre e aberta.”53

Para Snowden, a Internet estava quebrada, mas nem tudo estava perdido. Leis, regulamentos, regras – a longo prazo, nada disso serviria. A única solução verdadeiramente permanente era a tecnologia.

Que tipo de tecnologia? O Projeto Tor.

O fim do governo

Em 2011, uma loja misteriosa apareceu na Internet. Chamada Rota da Seda (Silk Road), era uma loja on-line como qualquer outra, com análises de clientes e um sistema de classificação de vendedores. Mas também havia algo único nesse mercado: ali se vendia drogas ilegais e só era acessível através de uma rede chamada Tor, um novo sistema de Internet que supostamente tornava a loja e seus usuários imunes à lei, movendo todas as transações para uma rede anônima paralela que situava-se no topo da Internet real. Tor é agora conhecido como "dark web".

“Conversar com o seu revendedor de maconha é uma droga. Ao comprar cocaína você pode levar um tiro. Pois e se você pudesse comprar e vender drogas on-line, como livros ou lâmpadas? Agora você pode: Bem-vindo à Rota da Seda”, escreveu Adrian Chen, o repórter que

primeiro contou a história para a Gawker. “Por meio de uma combinação de tecnologia de anonimato e um sofisticado sistema de feedback do usuário, a Rota da Seda torna a compra e venda de drogas ilegais tão fácil quanto comprar eletrônicos usados – e aparentemente é tão seguro quanto. É a Amazon – se a Amazon vendesse produtos químicos que alteram a consciência.”54

Construída e operada por uma figura misteriosa chamada Dread Pirate Roberts, a Rota da Seda tinha dois componentes que lhe permitiam operar em total anonimato. Primeiro, todas as compras foram processadas usando uma nova moeda criptográfica digital chamada Bitcoin, criada pelo misterioso criptógrafo pseudônimo Satoshi Nakamoto. Segundo, para usar a Rota da Seda, primeiro os compradores e os vendedores tiveram que baixar um programa chamado Tor e usar um navegador especializado para acessar um endereço URL especial da loja – http: //silkroad6ownowfk.onion – que os retirava da Internet comum e lançava-os na nuvem Tor, também conhecida como dark web.

O Tor era uma ferramenta de anonimato de ponta, criada pelo Tor Project, uma organização sem fins lucrativos criada em 2004 por um criptógrafo fortinho e com rabo de cavalo chamado Roger Dingledine, que na época o administrava de um escritório bagunçado acima de uma YMCA em Cambridge, Massachusetts. Tinha um orçamento anual de US $ 2 milhões, meia dúzia de funcionários em período integral e um pequeno grupo de programadores voluntários ao redor do mundo que ajudavam a desenvolver, testar e lançar seu produto: um aplicativo de camuflagem gratuito que funcionava com base em um técnica chamada "roteamento de cebola". Os usuários baixavam e rodavam um navegador especializado do Tor, que redirecionava seu tráfego para uma rede voluntária paralela ponto a ponto, alternando o caminho dos dados aleatoriamente antes de enviá-lo ao seu destino final. Esse truque desconectava a origem e o destino do fluxo de navegação na Internet de uma pessoa e teoricamente tornava impossível para policiais, espiões, hackers ou qualquer outra pessoa monitorar o tráfego da Internet para observar de onde os usuários vinham e para onde estavam indo. Em termos leigos, o roteamento de cebola é como o jogo da bolinha e três copos com tráfego de rede: as pessoas podem ver a bolinha passar de um copo para o outro, mas nunca sabem onde ela acaba ficando. O Tor alimentou a maior parte da dark web. Basicamente, ele era a dark web.

Graças ao Tor, a Rota da Seda avançou sem problemas. Ela conquistou muitos seguidores e construiu uma comunidade em expansão de traficantes de drogas, como o eBay fez para colecionadores amadores. Antigos traficantes de drogas de fim de semana mudaram suas operações on-line e expandiram suas bases de clientes, que não estavam mais limitadas a conexões pessoais e bairros. Enquanto isso, policiais entraram na Rota da Seda através do Tor como qualquer outra pessoa e acessaram ofertas de PCP, LSD, MDMA, cocaína, metanfetamina e cetamina e leram as opiniões dos clientes, mas não tinham ideia da identidade no mundo real das pessoas que vendiam e compravam as drogas; nem poderiam saber onde requisitar seus mandados de prisão ou quais datacenters invadir. Todo mundo era anônimo e estava trocando dinheiro anônimo. E a própria Rota da Seda funcionava como um "serviço oculto" do Tor, o que significava que poderia ser hospedado em São Francisco ou do outro lado do mundo em Moscou. A única coisa que não era anônima era que as drogas precisavam ser transportadas; portanto, os vendedores desenvolveram rotinas nas quais iriam dirigir por horas às cidades vizinhas para transportar as mercadorias; elas nunca eram enviadas de um local duas vezes seguidas. O FBI e a Agência de Repressão às Drogas observaram a gurizada comprando e vendendo drogas à luz do dia, enquanto o Dread Pirate Roberts arrecadava cerca de 32 milhões de dólares por ano em comissões, mas eles não podiam fazer nada para impedir isso.55 Graças ao Tor, todos eram anônimos e seguros. É assim que a tecnologia deveria ser poderosa. Parecia mágica.

O Tor foi a realização de um sonho de décadas.

Desde o início dos anos 1990, um influente grupo de programadores e hackers que se autodenominavam "cypherpunks" tinham uma ideia política radical. Eles acreditavam que a poderosa tecnologia de criptografia e anonimato, combinada com moedas digitais não rastreáveis, traria uma revolução que acabaria com o poder do governo e estabeleceria uma ordem mundial global descentralizada, baseada em mercados livres e associações voluntárias.56 “É claro que o Estado tentará retardar ou interromper a disseminação dessa tecnologia, citando preocupações de segurança nacional, uso da tecnologia por traficantes de drogas e sonegadores de impostos e temores de desintegração social. Muitas dessas preocupações serão válidas; a anarquia criptográfica permitirá que segredos nacionais sejam negociados livremente assim como materiais

ilícitos e roubados. Um mercado computadorizado anônimo tornará possível mercados abomináveis onde se negociam assassinatos e extorsões", previu Timothy May, engenheiro barbudo e pioneiro da Intel e um dos principais fundadores do movimento cypherpunk, em 1992. May espalhou suas ideias com um zelo messiânico. Em 1994, ele previa que uma revolução global de criptografia estava chegando e que criaria um novo mundo livre de governos e controle centralizado. "Uma fase de mudanças está chegando", escreveu, ecoando a previsão que Louis Rossetto estava fazendo ao mesmo tempo nas páginas da revista Wired, que por si só era uma promotora do movimento cypherpunk e de suas ideias.57

A visão cypherpunk do futuro era uma versão invertida do sonho cibernético-militar perseguido pelo Pentágono e pelo Vale do Silício: em vez de aproveitar os sistemas globais de computadores para tornar o mundo transparente e previsível, os cypherpunks queriam usar computadores e criptografia para tornar o mundo opaco e não rastreável. Era uma força contrária, uma arma cibernética de privacidade e liberdade individual contra uma arma cibernética de vigilância e controle do governo.

O Tor tornava possível a realização desse sonho cripto-cibernético: total anonimato na Internet. A partir de meados dos anos 2000, Tor desenvolveu um grupo de seguidores entre um pequeno, mas influente, grupo de tecno-libertarianistas, hackers e cypherpunks que o viam como uma capa mágica que poderia tornar o governo – policiais, militares, cobradores de impostos, reguladores e espiões – impotente.

O misterioso criador da Rota da Seda, Dread Pirate Roberts, aderiu à ideologia cypherpunk. Ele acreditava na promessa libertadora do Tor e na criptografia. Em suas declarações públicas, Dread Pirate Roberts saiu como um típico libertarianista, não muito diferente de Edward Snowden. Ele seguiu a Escola Austríaca de economia, argumentou contra as regulamentações ambientais e as leis de trabalho infantil, elogiou as fábricas e zombou da necessidade de salário mínimo: "E aquela pessoa cujo trabalho vale menos que o salário mínimo?" Quanto à Rota da Seda, era muito mais que um negócio. De seu esconderijo em algum lugar na dark web, Dread Pirate Roberts viu isso como um ato revolucionário saído diretamente de um romance de Ayn Rand. O

governo era o grande mal político – um parasita, uma forma de escravidão. Tor era a arma que deixava um rapaz como ele revidar. A Rota da Seda era apenas o começo. Ele queria usar o Tor e outras ferramentas de criptografia para ampliar o experimento para abranger todas as partes da vida, não apenas as compras de drogas.

"E se um dia tivéssemos poder suficiente para manter uma presença física no mundo, onde evitávamos os parasitas e defendíamos o estado de direito, onde o direito à privacidade e à propriedade era inquestionável e consagrado na própria estrutura da sociedade. Onde a polícia é nossos servos e protetores em dívida com seus clientes, as pessoas. Onde nossos líderes ganham seu poder e responsabilidade na fornalha dura e implacável do mercado livre e não por trás de uma arma, onde as oportunidades de criar e desfrutar de riqueza são tão ilimitadas quanto a imaginação", escreveu aos usuários da Rota da Seda no sue quadro de mensagens do site. "Depois de ver o que é possível, como você pode fazer o contrário? Como você pode vir a se conectar novamente à máquina comedora impostos, sugadora da vida, violenta, sádica, militar e opressora? Como você pode se ajoelhar quando sente o poder de suas próprias pernas? Sentiu-as esticar e flexionar à medida que você aprendia a andar e pensar como uma pessoa livre? Prefiro viver minha vida em trapos agora do que em correntes de ouro. E agora podemos ter os dois! Agora é rentável se livrar das correntes, com uma incrível tecnologia de criptografia, reduzindo o risco de fazê-lo drasticamente. Quantos nichos ainda precisam ser preenchidos no mundo dos mercados on-line anônimos? A oportunidade de prosperar e participar de uma revolução de proporções épicas está ao nosso alcance!"58

E por que não? Se a Rota da Seda pudesse aguentar o poder do governo estadunidense, tudo parecia possível.

Mais praticamente, Dread Pirate Roberts provou que você poderia usar o Tor para administrar um negócio massivamente ilegal na Internet e manter a polícia sob controle, enquanto arrecada milhões. Seu sucesso gerou uma imensa quantidade de imitadores – empresários da dark web que montaram lojas on-line à imagem de Rota da Seda, permitindo que as pessoas comprassem anonimamente o que quisessem: maconha, ecstasy, cocaína, metanfetamina, armas, granadas e até assassinatos.59 Alguns sites eram possivelmente um engodo, destinado a enganar as

pessoas e pegar suas Bitcoins, mas outros pareciam muito sérios. A dark web de Tor tornou-se um paraíso para a pornografia de abuso infantil, permitindo que fóruns e mercados onde esse material fosse trocado e vendido existissem além do alcance da lei. Também abrigava sites operados por células terroristas, incluindo plataformas de recrutamento administradas pelo Estado Islâmico do Iraque e pelo Levante.60

A facilidade de uso do Tor e o anonimato à prova de balas não apenas capacitaram o lado decadente da Internet. Jornalistas e ativistas políticos o usaram para evitar a vigilância e a repressão do governo em países como China e Irã. Vazadores e denunciantes também usavam a rede. Foi aí que Edward Snowden entrou na história: a capacidade de Tor de esconder as pessoas dos olhares indiscretos da NSA foi um fator-chave em seus vazamentos; ele não poderia ter realizado com sucesso sem ele.

Snowden ♥ Tor

Edward Snowden era um grande fã do Tor Project. Ele, assim como Dread Pirate Roberts, acreditava no poder da criptografia para libertar a Internet do controle do governo. No Havaí, quando trabalhava como contratado pela NSA na Dell e a Rota da Seda estava em expansão, ele controlava um dos nós mais poderosos da rede Tor, executando um servidor físico que ajudava a misturar e anonimizar o tráfego. Ele também se encarregou de educar as pessoas no Havaí sobre como usar a rede Tor para se esconder do governo.

Em novembro de 2012, enquanto estava no meio da sua retirada furtiva de documentos da NSA, Snowden estendeu a mão a Runa Sandvik, uma funcionária do Tor, e pediu alguns adesivos do Tor para entregar aos amigos no trabalho.61 Ele não disse a ela que seu "trabalho" era para a NSA. Mas, no decorrer de suas idas e vindas, ele descobriu que Sandvik estava planejando visitar o Havaí para férias, e ela sugeriu que se encontrassem lá. Na qualidade de embaixadora do Tor, Sandvik ofereceu uma palestra para os locais sobre segurança e criptografia de comunicação. Snowden estava entusiasmado com a ideia e eles concor-

daram em sediar uma CriptoFesta, uma espécie de aula público sobre ferramentas de criptografia. O evento aconteceu no início de dezembro de 2012 em um espaço de arte em Honolulu, onde Snowden e Sandvik ensinaram a cerca de vinte pessoas como usar o Tor e criptografar seus discos rígidos. Snowden organizou pessoalmente uma sessão sobre como configurar e executar um servidor Tor.62

Snowden saindo com funcionários do Tor, executando servidores do Tor e organizando sessões de treinamento do Tor – enquanto planeja o maior roubo de documentos da NSA da história? Parecia um passo imprudente para alguém tão meticuloso quanto ele. Por que se arriscaria se expondo? Para os que estão no mundo da privacidade, o desejo de Snowden de educar as pessoas sobre privacidade, mesmo diante do perigo pessoal, era uma prova de sua crença no poder do Tor e da criptografia e sua dedicação à causa. “Que Snowden tenha organizado esse evento ele mesmo enquanto ainda trabalhava na NSA fala muito sobre seus motivos”, escreveu o repórter da Wired Kevin Poulsen, que contou a história sobre o servidor Tor de Snowden e a criptofesta.

Mas Snowden não era apenas um verdadeiro crente. Ele também era um usuário ativo.

Depois de fugir para Moscou, ele explicou que o Projeto Tor era vital para o cumprimento de sua missão. Ele confiara no Tor para encobrir seus rastros e evitar ser detectado enquanto se comunicava com jornalistas, transferia documentos e planejava sua fuga do Havaí. Ele era tão fã que as primeiras fotografias dele em Hong Kong o mostraram sentado em sua cama de hotel, um laptop preto com um adesivo gigante verde oval do “Projeto Tor” colado em sua tampa. “Acho que o Tor é o projeto de tecnologia mais importante para melhorar a privacidade que está sendo usado hoje. Eu uso o Tor pessoalmente o tempo todo”, disse em uma entrevista em Moscou.

Ao se estabelecer em uma vida no exílio russo, ele desenvolveu uma prática lucrativa de falar, fazendo centenas de milhares de dólares por ano se apresentando remotamente a universidades, conferências de tecnologia e grupos de investidores.63 Em seus discursos e palestras, ele deu voz ao velho sonho cypherpunk, sustentando o Tor como um poderoso exemplo de tecnologia de privacidade popular que poderia derrotar o poder corrupto da vigilância governamental e restaurar o que via como

a promessa utópica original da Internet. Ele convocou seus colegas técnicos – programadores de computador, criptografadores e figuras da segurança cibernética de todas as faixas e classificações – a criar poderosas ferramentas de anonimato e privacidade à imagem de Tor.

Nessas conversas, Snowden retratava a Internet como um lugar assustador e violento, uma paisagem ciber-medieval repleta de bandidos do governo, exércitos hostis e armadilhas. Era um lugar onde pessoas comuns estavam sempre em risco. As únicas ilhas de segurança foram os datacenters privados controlados por empresas privadas – Google, Apple, Facebook. Essas eram as fortalezas cibernéticas e as cidades muradas que ofereciam refúgio às massas. Nesse cenário caótico, engenheiros de computação e criptógrafos desempenharam o papel de cavaleiros altruístas e guerreiros bruxos, cujo trabalho era proteger as pessoas fracas da Internet: a juventude, os idosos e enfermos, as famílias. Era seu dever sair, sacudindo as armas no ar, e transportar pessoas e seus preciosos dados com segurança de fortaleza em fortaleza, não deixando que nenhuma informação caísse nas mãos de espiões do governo. Ele os convocou a iniciar uma guerra de privacidade do povo, reunindo-os para sair e liberar a Internet, para recuperá-la dos governos do mundo.

“A lição de 2013 não é que a NSA seja má. É que o caminho é perigoso. O caminho da rede é algo que precisamos ajudar os usuários a atravessar com segurança. Nosso trabalho como tecnólogos, nosso trabalho como engenheiros, nosso trabalho como qualquer pessoa que se preocupe com a Internet de qualquer forma, que tenha algum tipo de envolvimento pessoal ou comercial, é literalmente fortificar o usuário, proteger o usuário e fazer com que ele consiga passar de um extremo ao outro com segurança, sem interferência", disse ele a um auditório cheio dos principais engenheiros de computadores e de redes do mundo em uma reunião de 2015 da Internet Engineering Task Force em Praga.64 Ele reafirmou sua opinião um ano depois na Real Future Fair de 2016 da Fusion, em Oakland, Califórnia. “Se você deseja construir um futuro melhor, precisará fazer isso você mesmo. Os políticos nos levaram até aqui e, se a história for um guia, eles são os meios menos confiáveis para alcançar a mudança efetiva... Eles não vão aparecer a qualquer momento e proteger seus direitos”, disse. “A tecnologia funciona de maneira diferente da lei. A tecnologia não conhece jurisdição.”

O desprezo de Snowden por soluções políticas e sua total confiança na capacidade da tecnologia de resolver problemas sociais complexos não surpreendiam. Ele estava simplesmente reafirmando o que havia dito aos jornalistas em 2013: "Não falemos mais da fé no homem, mas livremo-lo do mal através da criptografia".65

O chamado às armas de Snowden foi atendido por pessoas de todo o mundo: empresas do Vale do Silício, grupos de privacidade, think tanks e lobistas corporativos, ativistas políticos e milhares de técnicos ansiosos em todo o mundo. Até Sergey Brin, da Google, posou para uma selfie com o infame denunciador – ou o robô de "telepresença" equipado com vídeo que Snowden costumava usar para falar em conferências.66 Graças a Snowden, o movimento pela privacidade estava se tornando popular e o Projeto Tor estava no centro de tudo.

Não importa para onde você fosse no mundo da privacidade, as pessoas se uniram em sua admiração pelo Tor como uma solução para a vigilância na Internet. Isso aconteceu com grupos poderosos como a Electronic Frontier Foundation e a American Civil Liberties Union, jornalistas, hackers e denunciantes vencedores do Prêmio Pulitzer.67 A Google subsidiou o desenvolvimento adicional do Tor, assim como o eBay.68 O Facebook criou suporte para o Tor, permitindo que os usuários acessassem a rede social como se fosse um site da dark web, da mesma maneira que as pessoas acessavam a Rota da Seda. Em pouco tempo, o Facebook se gabou de que mais de um milhão de pessoas acessaram suas contas usando o sistema de camuflagem do Tor.69 Muitos viram a Tor em termos quase sagrados: era a salvação, um exemplo do mundo real de tecnologia que derrota a intrusão do governo na vida privada das pessoas.

Daniel Ellsberg, o lendário denunciante que em 1971 vazou os Documentos do Pentágono, apoiou a Tor como uma arma poderosa do povo.70 “O governo agora possui capacidades que a Stasi não podia imaginar, a possibilidade de um controle autoritário total. Contrariar isso é coragem”, explicou. “E é isso que o Tor facilita. Então, eu diria que o futuro, o futuro da democracia, e não apenas neste país, depende de contrariar as habilidades deste governo e de todos os outros governos deste mundo para saber tudo sobre nossas vidas privadas, enquanto mantêm em segredo tudo sobre o que estão fazendo oficialmente.”

A história do Tor cresceu em apelo. Em pouco tempo, as celebridades de Hollywood se juntaram e ajudaram a promover a causa. "Enquanto a polícia e a mídia pintaram a imagem de que Tor e a darknet são ferramentas nefastas para criminosos, é importante entender que eles são amplamente usados para o bem por agências governamentais, jornalistas e dissidentes ao redor do mundo", disse Keanu Reeves, narrando um documentário chamado Deep Web, um filme feito por Alex Winter, seu antigo colega de aventura de Bill e Ted, que descreveu Tor como resistente ao controle do governo.

Mas e o ventre criminoso de Tor? Para muitos no novo movimento de privacidade, nada disso importava. De fato, as pessoas comemoravam o lado sombrio de Tor. Sua capacidade de proteger os pornógrafos infantis da prestação de contas apenas provou sua eficácia, demonstrando que a tecnologia era realmente a poderosa ferramenta de privacidade que Edward Snowden afirmava ser. Tor era o AK-47 da Internet – uma arma de campo barata e durável que todos os dias as pessoas podiam usar para derrubar o estado de vigilância dos Estados Unidos.

O Tor deveria ser tão radical e tão subversivo que os funcionários do Tor falavam constantemente de seu assédio e intimidação pelas mãos do governo dos EUA. Eles viveram uma existência paranóica, alguns em fuga, buscando refúgio em países estrangeiros. Para eles, não era apenas um emprego, mas uma vida revolucionária. Um proeminente desenvolvedor Tor descreveu seu trabalho como um ato valente, a par da luta com os revolucionários anarquistas que guerreavam contra os fascistas de Franco.71

Tor era apenas o começo. Logo outras organizações populares de criptografia surgiram, lançando tecnologia de criptografia que prometia esconder nossas vidas digitais de olhares indiscretos. A Open Whisper Systems, liderada por um anarquista com dreadlocks, desenvolveu um poderoso aplicativo de texto e chamada de voz criptografado chamado Signal. Um coletivo de comunicação anarquista radical chamado RiseUp ofereceu serviços de e-mail criptografados, enquanto um grupo de técnicos se uniu para criar o melhor sistema operacional criptografado chamado Qubes; supostamente, nem a NSA poderia invadir. Outros formaram grupos de treinamento e realizaram criptofestas espontâneas

para educar as massas sobre como lidar com essas novas e poderosas ferramentas de privacidade.72

A cultura criptográfica chegou até a museus e galerias de arte.73 O Whitney Museum of American Art organizou uma “Vigilância Tech-In”. Trevor Paglen, um artista visual premiado, fez uma parceria com o Tor Project para instalar cubos criptográficos de anonimato em museus e galerias de arte em Nova York, Londres e Berlim. "Como seria a infraestrutura da Internet se a vigilância em massa não fosse seu modelo de negócios?" Paglen perguntou em uma entrevista com a Wired. “Meu trabalho como artista é aprender a ver como é o mundo neste momento histórico. Mas é também tentar fazer coisas que nos ajudem a ver como o mundo pode ser diferente.”74

Sim, de repente, com criptografia, o mundo da arte fez parte da resistência.

Como repórter da Pando, uma revista sediada em São Francisco que cobria o setor de tecnologia, observei esses desenvolvimentos com ceticismo. Rebeldes se armando até os dentes e assumindo o poder de um governo maligno com nada além de seus cérebros e sua tecnologia de criptografia meia boca? Havia algo de errado nessa narrativa. Estava muito limpo. Muito encenado. Muito parecido com um plano de ficção científica barato, ou talvez uma versão na Internet da antiga fantasia da Associação Nacional do Rifle: se todos estivessem armados com uma arma (criptográfica) poderosa, não haveria tirania do governo porque as pessoas seriam capazes de se defender neutralizar a força do governo por conta própria. Era mais uma versão de uma utopia ciber-libertarianista: a ideia de que você poderia igualar os níveis de poder com nada mais que tecnologia.

Eu sabia que a realidade era geralmente mais complicada. E, com certeza, a história do Tor também.

Entrando no buraco do coelho

O ano era 2014. Em uma manhã quente e ensolarada de novembro, acordei, preparei uma xícara de café e sentei-me à minha mesa para ver alguns surfistas descendo para Venice Beach. Acabara de voltar da Ucrânia, onde passei um mês relatando a terrível guerra civil e o colapso econômico brutal que estava destruindo esse país. Eu estava com jet-lag e cansado, minha mente ainda fixa nas imagens horríveis de guerra e destruição em minha terra natal ancestral. Eu esperava um pouco de descanso e silêncio. Mas, então, chequei meu email.

Havia todo um inferno na Internet.

As ameaças e ataques começaram algum dia durante a noite enquanto eu dormia. Pela manhã, eles alcançaram um tom cruel e assassino. Houve pedidos pela minha morte – por fogo, por asfixia, por ter minha garganta cortada com lâminas de barbear. Pessoas que eu nunca conheci me chamavam de estuprador e alegavam que eu tinha prazer em espancar mulheres e forçá-las a fazer sexo comigo. Fui acusado de homofobia. Pessoas anônimas apresentaram queixas falsas ao meu editor. Alegaram que eu era um agente da CIA, assim como que eu trabalhava com a inteligência britânica. O fato de eu ter nascido na União Soviética não me favoreceu; naturalmente, fui acusado de ser um espião do FSB e de trabalhar para o sucessor da KGB na Rússia. Fui informado de que meu nome havia sido adicionado a uma lista de assassinatos na Internet – um site onde as pessoas podiam fazer ofertas anônimas pelo meu assassinato.75 O olhar da máquina de ódio na Internet repentinamente se fixou em mim.

As coisas ficaram ainda mais estranhas quando o movimento Anonymous entrou na briga. O coletivo condenou a mim e a meus colegas, prometendo não descansar até que eu estivesse morto. "Que uma infinidade de insetos venenosos habite no intestino fascista de Yasha Levine", proclamou a conta do Anonymous no Twitter com 1,6 milhão de seguidores.76 Foi uma virada bizarra. O Anonymous era um movimento descentralizado e juvenil de hackers, mais conhecido por perseguir a Igreja da Cientologia. Agora eles estavam atrás de mim – pintando um alvo gigante nas minhas costas.

Andei pela minha sala de estar, nervosamente examinando a rua do lado de fora da minha janela. Reflexivamente, abaixei as persianas, imaginando até onde isso iria. Pela primeira vez, comecei a temer pela

segurança da minha família. As pessoas sabiam onde eu morava. O apartamento que eu e minha esposa, Evgenia, dividíamos na época, ficava no primeiro andar, aberto para a rua, com amplas janelas de todos os lados, como um aquário. Pensamos até em ficar na casa de um amigo do outro lado da cidade por alguns dias até que as coisas esfriassem.

Eu já havia sido alvo de campanhas cruéis de assédio na Internet antes, por eu ser um jornalista investigativo. Mas isso era diferente. Fora além de tudo que eu já havia experimentado. Não apenas a intensidade e crueldade me assustaram, mas também a razão pela qual isso estava acontecendo.

Meus problemas começaram quando comecei a explorar o Projeto Tor. Investiguei o papel central de Tor no movimento pela privacidade depois que Edward Snowden apresentou o projeto como uma panaceia para a vigilância na Internet. Aquilo não havia me convencido e não demorou muito para encontrar fundamentos para minhas suspeitas iniciais.

A primeira bandeira vermelha foi o apoio ao Vale do Silício. Grupos de privacidade financiados por empresas como Google e Facebook, incluindo a Electronic Frontier Foundation e Fight for the Future, foram alguns dos maiores e mais dedicados apoiadores do Tor.77 A Google financiara diretamente seu desenvolvimento, pagando doações generosas a estudantes universitários que trabalhavam no Tor durante as férias de verão.78 Por que uma empresa de Internet cujo todo o seu negócio repousa no rastreamento de pessoas on-line promove e ajuda a desenvolver uma poderosa ferramenta de privacidade? Algo não fechava.

Ao pesquisar os detalhes técnicos de como o Tor funcionava, percebi rapidamente que o Projeto Tor não oferece proteção contra o rastreamento privado e o perfil das empresas da Internet. O Tor funciona apenas se as pessoas se dedicam a manter uma rotina anônima estrita na Internet: usando apenas endereços de e-mail fictícios e contas falsas, realizando todas as transações financeiras em Bitcoin e outras criptomoedas e nunca mencionando seu nome real em e-mails ou mensagens. Para a grande maioria das pessoas na Internet – aquelas que usam o Gmail, interagem com amigos do Facebook e fazem compras na Amazon -, o Tor não faz nada. No momento em que você faz login na sua conta pessoal, seja no Google, Facebook, eBay, Apple ou Amazon, você

revela sua identidade. Essas empresas sabem quem você é. Eles sabem o seu nome, endereço de entrega, informações do cartão de crédito. Eles continuam a verificar seus e-mails, mapear suas redes sociais e compilar dossiês. Com Tor ou sem, depois de inserir o nome e a senha da sua conta, a tecnologia de anonimato do Tor se torna inútil.

A ineficácia de Tor contra a vigilância do Vale do Silício fez dele uma bandeira estranha para Snowden e outros ativistas da privacidade adotarem. Afinal, os documentos vazados por Snowden revelaram que aquilo que qualquer empresa de Internet tinha, a NSA também tinha. Fiquei intrigado, mas pelo menos entendi por que o Tor era apoiado pelo Vale do Silício: ele oferecia uma falsa sensação de privacidade, sem representar uma ameaça ao modelo de negócios de vigilância subjacente do setor.

O que não ficou claro, e o que ficou aparente quando investiguei mais o Tor, foi o motivo pelo qual o governo dos EUA o apoiou.

Uma grande parte da mística e apelo do Tor era que era supostamente uma organização ferozmente independente e radical – um inimigo do Estado. Sua história oficial era que era financiado por uma ampla variedade de fontes, o que lhe dava total liberdade para fazer o que quisesse. Mas, ao analisar os documentos financeiros da organização, descobri que o oposto era verdadeiro. Tor havia saído de um projeto militar conjunto da Marinha dos EUA com a DARPA no início dos anos 2000 e continuou a confiar em uma série de contratos federais depois que foi transformado em uma organização privada sem fins lucrativos. Esse financiamento veio do Pentágono, do Departamento de Estado e de pelo menos uma organização derivada da CIA. Esses contratos somavam vários milhões de dólares por ano e, na maioria dos anos, representavam mais de 90% do orçamento operacional do Tor. Tor era um contratado militar federal. Tinha até seu próprio número de contratação.

Quanto mais fundo eu ia, mais estranho ficava. Descobri que praticamente todas as pessoas envolvidas no desenvolvimento do Tor estavam de alguma forma ligadas ao próprio Estado do qual elas deveriam estar protegendo. Isso incluía o fundador do Tor, Roger Dingledine, que passou um verão trabalhando na NSA e que deu vida ao Tor sob uma série de contratos da DARPA e da Marinha dos EUA.79 Até descobri uma cópia antiga em áudio de uma palestra que Dingledine deu em

2004, exatamente quando ele estava montando o Tor como uma organização independente. "Faço contratos com o governo dos Estados Unidos para construir tecnologia de anonimato para eles e implantá-la", admitiu na época.80

Eu estava confuso. Como uma ferramenta no centro de um movimento global de privacidade contra a vigilância do governo pode obter financiamento do próprio governo dos EUA, do qual deveria escapar? Era um ardil? Uma farsa? Um engodo? Eu estava tendo delírios paranoicos? Embora confuso, decidi tentar entender o melhor que pude.

No verão de 2014, reuni todos os registros financeiros verificáveis relacionados ao Tor, analisei as histórias das agências governamentais dos EUA que o financiaram, consultei especialistas em privacidade e criptografia e publiquei vários artigos no Pando Daily explorando os laços conflitantes entre Tor e o governo. Eles eram diretos e mantinham um velho ditado jornalístico: quando você se depara com um mistério, a primeira coisa a fazer é seguir o dinheiro – ver quem se beneficia. Ingenuamente, pensei que as informações de financiamento em segundo plano do Tor seriam bem-vindas pela comunidade de privacidade, um grupo paranoico de pessoas que estão sempre em busca de bugs e vulnerabilidades de segurança. Mas eu estava enganado. Em vez de dar boas-vindas aos meus relatórios sobre o intrigante apoio governamental do Tor, as principais estrelas da comunidade de privacidade responderam com ataques.

Micah Lee, o ex-tecnólogo da EFF que ajudou Edward Snowden a se comunicar com segurança com jornalistas e que agora trabalha no jornal The Intercept, me atacou como um teórico da conspiração e acusou a mim e aos meus colegas do Pando de serem agressores sexistas; ele alegou que meus relatórios foram motivados não pelo desejo de chegar à verdade, mas por um impulso malicioso de assediar uma desenvolvedora Tor.81 Embora Lee tenha admitido que minhas informações sobre o financiamento do governo de Tor estavam corretas, ele argumentou contra-intuitivamente que isso não importava. Por quê? Porque o Tor era de código aberto e construído em cima da matemática, o que ele alegou torná-lo infalível. “É claro que os financiadores podem tentar influenciar a direção do projeto e da pesquisa. No caso do Tor, isso é atenuado pelo fato de que 100% da pesquisa científica e do código fonte

que o Tor lança é aberto, que a matemática criptográfica é revisada por pares e apoiada pelas leis da física", escreveu ele. O que Lee estava dizendo, e o que muitos outros da comunidade de privacidade acreditavam também, era que não importava que os funcionários de Tor dependessem do pagamento do Pentágono. Eles eram imunes a influências, carreiras, hipotecas, parcelas de carros, relacionamentos pessoais, comida e todos os outros aspectos "moles" da existência humana que silenciosamente dirigem e afetam as escolhas das pessoas. A razão era que o Tor, como todos os algoritmos de criptografia, era baseado em matemática e física – o que o tornava impermeável à coerção.82

Foi um argumento desconcertante. Tor não era "uma lei da física", mas um código de computador escrito por um pequeno grupo de seres humanos. Era um software como qualquer outro, com falhas e vulnerabilidades que eram constantemente descobertas e corrigidas. Os algoritmos de criptografia e os sistemas de computador podem se basear em conceitos matemáticos abstratos, mas traduzidos para o domínio físico real, eles se tornam ferramentas imperfeitas, restringidas por erros humanos e pelas plataformas e redes de computadores em que são executadas. Afinal, mesmo os sistemas de criptografia mais sofisticados acabam falhando e sendo quebrados. E nem Lee nem ninguém poderia responder à grande questão levantada pelos meus relatórios: se Tor era um perigo para o governo dos EUA, por que esse mesmo governo continuaria gastando milhões de dólares no desenvolvimento do projeto, renovando o financiamento ano após ano? Imagine se, durante a Segunda Guerra Mundial, os Aliados financiassem o desenvolvimento da máquina Enigma da Alemanha nazista em vez de montar um esforço maciço para decifrar o código.

Nunca recebi uma boa resposta da comunidade de privacidade, mas o que recebi foram muitas calúnias e ameaças.

Jornalistas, especialistas e tecnólogos de grupos como ACLU, EFF, Fundação Liberdade da Imprensa e The Intercept e funcionários do Projeto Tor se uniram para atacar meus relatórios. Ao contrário de Lee, a maioria não tentou contra-argumentar minhas reportagens, mas empregou uma série de táticas familiares de difamação por relações públicas – táticas que você costuma ver usadas por grupos empresariais, não por ativistas de privacidade cheios de princípios. Eles foram para as mídias

sociais, dizendo a qualquer um que demonstrasse interesse nos meus artigos que deveriam ignorá-los.83 Então, quando isso não funcionou, eles tentaram desacreditar meus relatórios ridicularizando-os, desviando o assunto e lançando insultos grosseiros.

Um respeitado especialista em privacidade da ACLU, que agora trabalha como funcionário do Congresso, me chamou de "um teórico da conspiração que vê helicópteros pretos em toda parte" e comparou minha reportagem sobre Tor aos Protocolos dos Sábios de Sião.84 Como alguém que escapou do antissemitismo patrocinado pelo Estado na União Soviética, achei a comparação extremamente ofensiva, principalmente vinda da ACLU. Os Protocolos foram uma falsificação antissemita disseminada pela polícia secreta do czar russo que desencadeou ondas de pogroms mortais contra judeus em todo o Império Russo no início do século XX.85 Os funcionários do Tor lançaram uma torrente de insultos infantis, chamando-me de "babaca do estado stalinista" e de "filho da puta". Eles me acusaram de ser financiado por espiões para minar a fé na criptografia. Um deles alegou que eu era um estuprador e lançou insultos homofóbicos sobre as várias maneiras pelas quais eu supostamente havia realizado favores sexuais para um colega do sexo masculino.86

Da maneira que essas sessões de trote na Internet ocorrem, a campanha evoluiu e se espalhou. Pessoas estranhas começaram a ameaçar a mim e aos meus colegas nas mídias sociais. Alguns me acusaram de ter sangue nas mãos e de acumular uma "contagem de corpos de ativistas" – que as pessoas estavam realmente morrendo porque meus relatórios minaram a confiança no Tor.87

Os ataques aumentaram para incluir leitores regulares e usuários de mídia social, qualquer um que tivesse a coragem de fazer perguntas sobre as fontes de financiamento do Tor. Um funcionário do Projeto Tor chegou a expor um usuário anônimo do Twitter, desmascarando sua identidade real e entrando em contato com seu empregador na esperança de fazê-lo ser demitido de seu emprego como farmacêutico júnior.88

Foi bizarro. Eu assisti tudo isso se desenrolar em tempo real, mas não tinha ideia de como responder. Ainda mais desconcertante foi que os ataques logo se expandiram para incluir histórias difamatórias colocadas em meios de comunicação respeitáveis. O The Guardian publicou uma

história de um freelancer me acusando de realizar uma campanha online de assédio sexual e bullying.89 The Los Angeles Review of Books, geralmente um bom jornal de artes e cultura, publicou um ensaio de um freelancer, alegando que minhas reportagens foram financiadas pela CIA.90 Paul Carr, meu editor da Pando, apresentou queixas oficiais e exigiu saber como esses repórteres chegaram a suas conclusões. Ambas as publicações finalmente retiraram suas declarações e lançaram correções. Um editor do Guardian pediu desculpas e descreveu o artigo como um "bosta".91 Mas os ataques online continuaram.

Eu não era estranho a intimidações e ameaças. Mas sabia que essa campanha não era apenas para me calar. Ela foi projetada para encerrar o debate em torno da história oficial do Tor. Após o surto inicial, me acalmei e tentei entender por que meus relatórios provocaram uma reação tão cruel e estranha da comunidade de privacidade.

Empreiteiros militares aclamados como heróis da privacidade? Edward Snowden está promovendo uma ferramenta financiada pelo Pentágono como uma solução para a vigilância da NSA? Google e Facebook apoiando a tecnologia de privacidade? E por que os ativistas da privacidade eram tão hostis às informações de que seu aplicativo mais confiável era financiado pelos militares? Era um mundo bizarro. Nada disso fez sentido.

Quando as difamações começaram, pensei que elas poderiam ter sido causadas por um pequeno reflexo defensivo. Muitos dos que me atacaram trabalhavam para Tor ou eram fortes apoiadores, recomendando a ferramenta a outros como proteção contra a vigilância do governo. Eles deveriam ser especialistas na área; talvez minha reportagem sobre os laços em curso de Tor com o Pentágono os tenha pego de surpresa ou os tenha feito se sentirem estúpidos. Afinal, ninguém gosta de ser feito para parecer um otário.

Acontece que não era assim tão simples. Enquanto eu montava a história, pouco a pouco, percebi que havia algo muito mais profundo por trás dos ataques, algo tão assustador e surpreendente que, a princípio, não acreditei.

Capítulo 7

Privacidade na Internet, financiada por Espiões

Isso que chamam de liberdade da Internet,
é na verdade, liberdade sob controle dos EUA.
- *Jornal Global Times da China, 2010*

Era dezembro de 2015, alguns dias depois do Natal em Hamburgo. O termômetro hesita logo acima do ponto de congelamento. Um nevoeiro cinza paira sobre a cidade.

No centro histórico da cidade, vários milhares de pessoas se reuniram dentro de um cubo modernista de aço e vidro conhecido como Centro de Congressos. Os participantes, principalmente homens nerds, estavam ali para a trigésima segunda reunião anual do *Chaos Computer Club*, mais conhecida como 32c3. A atmosfera da conferência era alta e alegre, um contraponto ao tráfego de pedestres cabisbaixos e ao clima sombrio do lado de fora das altas paredes de vidro do centro.

A 32c3 é a Davos do hackativismo, uma extravagância promovida pelo coletivo de hackers mais antigo e mais prestigiado do planeta. Todo mundo que é alguém está aqui: criptografadores, especialistas em segurança da Internet, nerds adolescentes, tecno-libertarianistas, cypherpunks e *cyberpunks*, empresários de Bitcoin, empreiteiros militares, entusiastas de código aberto e ativistas de privacidade de todas as nacionalidades, gêneros, faixas etárias e níveis de classificação dos serviços de inteligência. Eles vão ao evento para fazer rede, programar, dançar

techno, fumar cigarros eletrônicos, saber das últimas tendências de criptografia e consumir oceanos de Club-Mate, a bebida hacker oficial da Alemanha.

Olhando para este lado, vi Ryan Lackey, co-fundador da HavenCo, a primeira empresa extralegal de hospedagem offshore do mundo – ela funcionar numa plataforma de canhões abandonada da época da Segunda Guerra Mundial no Mar do Norte, na costa da Inglaterra. Do outro lado, encontrei Sarah Harrison, membro do WikiLeaks e confidente de Julian Assange, que ajudou Edward Snowden a escapar da prisão em Hong Kong e encontrar segurança em Moscou. Ela ria e se divertia. Acenei quando passei por ela em uma escada rolante. Mas nem todo mundo aqui era tão amigável. De fato, minha reputação como crítico do Tor me precedeu. Nos dias que antecederam a conferência, a mídia social se inundou novamente com ameaças.1 Houve boatos de agressão e de colocar Rohypnol na minha bebida se eu tivesse coragem de aparecer no evento.2 Dado meu confronto anterior com a comunidade de privacidade, não posso dizer que esperava uma recepção particularmente calorosa.

O Projeto Tor ocupa um lugar consagrado na mitologia e na galáxia social do Chaos Computer Club. Todos os anos, a apresentação anual do Tor – "O estado da cebola" – é o evento mais prestigiado do programa. Uma audiência de vários milhares de pessoas lota um auditório enorme para assistir aos desenvolvedores e apoiadores-celebridades do Tor falarem sobre suas lutas contra a vigilância na Internet. No ano passado, o palco contou com Laura Poitras, diretora vencedora do Oscar do documentário Edward Snowden, Citizen Four. Em seu discurso, ela considerou o Tor um poderoso antídoto contra o estado de vigilância dos Estados Unidos. "Quando me comuniquei com Snowden por vários meses antes de conhecê-lo em Hong Kong, conversamos muitas vezes sobre a rede Tor, e é algo que ele realmente considera vital para a privacidade on-line e para derrotar a vigilância. É a nossa única ferramenta capaz de fazer isso", disse ela com aplausos violentos, o rosto de Snowden projetado em uma tela gigante atrás dela.3

Este ano, a apresentação é um pouco mais formal. Tor acaba de contratar uma nova diretora executiva, Shari Steele, ex-chefe da Electronic Frontier Foundation. Ela sobe ao palco para se apresentar aos ativis-

tas da privacidade reunidos no salão e promete sua lealdade à missão principal da Tor: tornar a Internet segura contra a vigilância. Lá em cima, desde o início do evento, está Jacob Appelbaum, "Jake", como todos o chamam. Ele é a verdadeira estrela do show e elogia a nova diretora. "Encontramos alguém que manterá o Projeto Tor por muito tempo depois que todos nós estivermos mortos e enterrados, espero que não em covas rasas", diz ele, em meio aos aplausos.4

Vi-o andando pelos corredores após o evento. Ele estava vestindo jeans e camiseta preta, uma tatuagem aparecia por baixo de uma das mangas. Seus cabelos negros e óculos de armação grossa emolduravam um rosto retangular e carnudo. Ele era uma figura familiar para as pessoas na 32c3. De fato, ele se comportava como uma celebridade, apertando a mão de alegres participantes, enquanto seus fãs se aglomeram nas proximidades para ouvi-lo gabar-se de ousadas façanhas contra governos opressivos em todo o mundo.

Ele entrou em um auditório onde um palestrante estava falando sobre direitos humanos no Equador e imediatamente sequestrou a discussão. “Sou do mundo da criptografia-que-destrói-o-Estado. Quero me livrar do Estado. O Estado é perigoso, tá ligado?”, disso ao microfone. Então, ele abriu um sorriso desonesto, levando algumas pessoas na plateia a gritar e torcer. Em seguida, começou para uma história maluca na qual ele está no centro de uma tentativa de golpe de Estado fracassada, orquestrada pela polícia secreta do Equador contra seu presidente, Rafael Correa. Naturalmente, Appelbaum era o herói da história. O presidente Correa é amplamente respeitado na comunidade internacional de hackers por conceder asilo político a Julian Assange e por lhe dar refúgio na embaixada equatoriana em Londres. Como um moderno Smedley Butler, Appelbaum explicou como ele se recusou a colaborar. Ele não queria usar suas habilidades justas de hacker para derrubar um homem bom e honesto, por isso ajudou a frustrar a trama e salvou o presidente. "Eles me pediram para construir um sistema de vigilância em massa para explorar todo o Equador", disse. “Aí falei pra eles se foderem e os denunciei à presidência. 'Acho que vocês estão propondo um golpe. Tenho seus nomes, vocês tão fodidos'."

Algumas pessoas no palco parecem envergonhadas, sem acreditar em uma palavra. Mas o público se agita. Eles amam Jacob Appelbaum. Todos na 32c3 adoram Jacob Appelbaum.

Appelbaum é o membro mais famoso do Projeto Tor. Depois de Edward Snowden e Julian Assange, ele é provavelmente a personalidade mais famosa no movimento de privacidade na Internet. Ele também é o mais ultrajante. Por cinco anos, ele representou o papel de um nó de mídia auto-facilitador e contracultura chamado Ethan Hunt, uma celebridade hacker que muda constantemente sua aparência, viaja pelo mundo para falar em conferências e pronunciar ensinamentos, e lutar contra a injustiça e a censura onde quer que governos medonhos as promovam. Appelbaum tem poder e influência cultural. Enquanto Assange estava encalhado em uma embaixada de Londres e Snowden preso em Moscou, Appelbaum era o rosto do movimento anti-vigilância. Ele falou por seus heróis. Ele era amigo e colaborador deles. Como eles, ele vivia no limite, uma inspiração para inúmeras pessoas – centenas, senão milhares, se tornaram ativistas da privacidade por sua causa. Ouvia-se repetidamente: "Jake é a razão de eu estar aqui."

Mas a festa do Chaos Computer Club daquele ano representou o auge de sua carreira. Durante anos, rumores se espalharam dentro da comunidade de privacidade na Internet sobre suas histórias de assédio sexual, abuso e bullying. Seis meses após a conferência, o New York Times publicou uma matéria que trouxe à tona essas alegações, revelando um escândalo que viu Appelbaum ser expulso do Projeto Tor e que ameaçava destroçar a organização por dentro.5

Mas tudo isso ainda viria a acontecer. Naquela noite em Hamburgo, Appelbaum ainda estava desfrutando de sua fama e celebridade, sentindo-se confortável e seguro. No entanto, ele estava carregando outro segredo sombrio. Ele era mais do que apenas um lutador de renome mundial pela liberdade na Internet e confidente de Assange e Snowden. Ele também era funcionário de uma terceirizada militar, ganhando US $ 100.000 por ano, mais benefícios, trabalhando em um dos projetos governamentais mais desorientadores da Era da Internet: a armamentização da privacidade.6

A caixa

Algumas semanas depois de ver Jacob Appelbaum na 32c3, cheguei em casa nos Estados Unidos para encontrar uma pesada caixa marrom esperando por mim na minha porta. Ela havia sido enviada pelo Conselho de Governadores de Radiodifusão, uma grande agência federal que supervisiona as operações de radiodifusão nos Estados Unidos e um dos principais financiadores do Projeto Tor.7 A caixa, obtida através da Lei de Liberdade de Informação, continha vários milhares de páginas de documentos internos sobre as relações da agência com o Tor. Eu estava impaciente esperando há meses que ela chegasse.

Até então, eu havia passado quase dois anos investigando o Projeto Tor. Sabia que a organização havia surgido de pesquisas do Pentágono. Também sabia que, mesmo depois de se tornar uma organização privada sem fins lucrativos em 2004, ela dependia quase inteiramente de contratos federais e do Pentágono. Durante minhas reportagens, representantes do Tor admitiram, de má vontade, que aceitavam financiamento do governo, mas permaneceram inflexíveis dizendo que tocavam uma organização independente que não recebia ordens de ninguém, especialmente do temido governo federal, ao qual sua ferramenta de anonimato deveria se opor.8 Eles enfatizaram repetidamente que nunca colocariam backdoors na rede Tor e contaram histórias de como o governo dos EUA tentou, mas não conseguiu, que o Tor grampeasse sua própria rede.9 Eles apontaram para o código-fonte aberto do Tor; se eu estava realmente preocupado com uma porta dos fundos, estava livre para inspecionar o código por mim mesmo.

O argumento de código aberto parecia anular as preocupações da comunidade de privacidade. Mas, com ou sem backdoors, minhas reportagens continuavam esbarrando com a mesma pergunta: se Tor era realmente o coração do movimento moderno de privacidade e uma ameaça real ao poder de vigilância de agências como a NSA, por que o governo federal – incluindo o Pentágono, pai da NSA – continuava a financiar a organização? Por que o Pentágono apoiaria uma tecnologia que subvertia seu próprio poder? Não fazia nenhum sentido.

Os documentos na caixa à minha porta continham a resposta. Combinados com outras informações desenterradas durante minha investigação, eles mostraram que o Tor, assim como o maior movimento de privacidade obcecado por aplicativos que se uniu a ele após o vazamento da NSA de Snowden, não atrapalham o poder do governo dos EUA. Mas, aumentava-o.

As divulgações sobre o funcionamento interno do Tor que obtive do Conselho de Governadores de Radiodifusão nunca foram tornadas públicas antes. A história que eles contam é vital para a nossa compreensão da Internet; eles revelam que os interesses militares e de inteligência estadunidenses estão tão profundamente enraizados na estrutura da rede que dominam as próprias ferramentas de criptografia e organizações de privacidade que deveriam lhe opor resistência. Não havia escapatória.

Espiões precisam de anonimato

A história de como uma terceirizada militar acabou no centro do movimento pela privacidade na Internet começa em 1995 no Laboratório de Pesquisa Naval dentro da base militar Anacostia-Bolling em Potomac, no sudeste de Washington, DC.10 Lá, Paul Syverson, um matemático militar afável, com cabelos compridos e interessado em sistemas seguros de comunicação, decidiu resolver um problema inesperado causado pelo explosivo sucesso da Internet.

Tudo estava sendo conectado à Internet: bancos, telefones, usinas de energia, universidades, bases militares, corporações e governos estrangeiros, hostis e amigáveis. Nos anos 1990, hackers, que alguns acreditavam estar ligados à Rússia e à China, já estavam usando a Internet para investigar a rede de defesa estadunidense e roubar segredos.11 Os Estados Unidos estavam começando a fazer o mesmo com seus adversários: coletando inteligência, grampeando e hackeando alvos e interceptando comunicações. Também estavam usando a infraestrutura comercial da Internet para comunicação secreta.

Porém, o problema era o anonimato. A natureza aberta da Internet, onde a origem de uma solicitação de tráfego e seu destino estavam abertos a qualquer pessoa que estivesse monitorando a conexão, fazia com que trabalhos sigilosos fossem um negócio complicado. Imagine um agente da CIA no Líbano disfarçado secretamente como um empresário tentando verificar seu e-mail de serviço. Ele não podia simplesmente digitar “mail.cia.gov” em seu navegador da sua suíte no hotel Beirut Hilton. Uma análise simples do tráfego acabaria imediatamente com o seu disfarce. Nem um oficial do Exército dos EUA poderia se infiltrar em um fórum de recrutamento da Al-Qaeda sem revelar o endereço IP da base do exército. E se a NSA precisasse invadir o computador de um diplomata russo sem deixar rastros que levassem de volta a Fort Meade, Maryland? Esquece. “Como os dispositivos de comunicação de nível militar dependem cada vez mais da infraestrutura de comunicações públicas, é importante usar essa infraestrutura de maneiras resistentes à análise de tráfego. Também pode ser útil se comunicar anonimamente, por exemplo, ao coletar informações de bancos de dados públicos”, explicaram Syverson e colegas nas páginas de uma revista interna publicada por seu laboratório de pesquisa.12

Espiões e soldados estadunidenses precisavam de uma maneira de usar a Internet que escondesse seus rastros e sua identidade. Era um problema que os pesquisadores da Marinha dos EUA, que historicamente estão na vanguarda da pesquisa em tecnologia de comunicações e na inteligência de sinais, estavam determinados a resolver.

Syverson reuniu uma pequena equipe de matemáticos militares e pesquisadores de sistemas de computador. Eles criaram uma solução: chamava-se "roteador cebola" ou Tor. Era um sistema engenhoso: a marinha montou vários servidores e os vinculou em uma rede paralela que ficava no topo da Internet normal. Todo o tráfego secreto foi redirecionado por essa rede paralela; uma vez lá dentro, ele era embaralhado de maneira a ofuscar para onde estava indo e de onde veio. Era o mesmo princípio da lavagem de dinheiro: transferir pacotes de informações de um nó do Tor para outro até que seja impossível descobrir de onde os dados vieram. Com o roteamento cebola, a única coisa que um provedor de Internet – ou qualquer outra pessoa assistindo a uma conexão – via era o usuário conectado a um computador executando o Tor. Nenhuma indicação de onde as comunicações estavam realmente indo era apa-

rente. E quando os dados saíram da rede paralela e voltaram para a Internet pública do outro lado, ninguém lá poderia ver de onde vinham as informações.

A equipe de cientistas ad Marinha de Syverson trabalhou em várias versões desse sistema. Alguns anos depois, eles contrataram dois programadores novatos, Roger Dingledine e Nick Mathewson, do Instituto de Tecnologia de Massachusetts para ajudar a construir uma versão do roteador que poderia ser usada no mundo real.13

Dingledine, que obteve seu mestrado em engenharia elétrica e ciência da computação e estava interessado em criptografia e comunicações seguras, foi estagiar na Agência de Segurança Nacional. Mathewson tinha interesses semelhantes e havia desenvolvido um sistema de e-mail realmente anônimo que escondia a identidade e a origem de um remetente. Mathewson e Dingledine se conheceram como calouros no MIT e se tornaram grandes amigos, passando a maior parte de seus dias em seus quartos lendo O Senhor dos Anéis e hackeando sem parar. Eles também acreditavam na visão cypherpunk. "Os protocolos de rede são os legisladores não reconhecidos do ciberespaço", gabou-se Mathewson ao jornalista Andy Greenberg. "Acreditávamos que, se mudaríamos o mundo, seria através de código". Na faculdade, os dois se viram em termos românticos, rebeldes hackers tomando o controle do sistema, usando código de computador para combater o autoritarismo do governo. Mas isso não os impediu de ir trabalhar para o Pentágono após a formatura. Como muitos rebeldes hackers, eles tinham uma concepção muito limitada do que era "O Sistema" e o que significaria em termos políticos reais lutar contra "ele".

Em 2002, o par foi trabalhar para o Laboratório de Pesquisa Naval sob um contrato da DARPA.14 Por dois anos, Dingledine e Mathewson trabalharam com Syverson para atualizar os protocolos de roteamento subjacentes da rede de roteadores de cebola, melhorar a segurança e executar uma pequena rede de teste que permitia que os militares experimentassem o roteamento de cebola em campo. Uma equipe militar testou-o para reunir informações de código aberto, o que exigiu que eles visitassem sites e interagissem com pessoas on-line sem revelar sua identidade. Outra equipe o usou para se comunicar durante uma missão no Oriente Médio.15 Em 2004, o Tor, a rede resultante,

estava finalmente pronta para a implantação.16 Bem, exceto por um pequeno detalhe.

Todas as pessoas que trabalhavam no projeto entendiam que um sistema que apenas anonimizava o tráfego não era suficiente – não se fosse usado exclusivamente por agências militares e de inteligência. "O governo dos Estados Unidos não pode simplesmente executar um sistema de anonimato para todos e depois usá-lo apenas para si mesmo", explicou Dingledine em uma conferência de computação em 2004, em Berlim. “Porque então toda vez que uma conexão vinha, as pessoas diziam: 'Oh, é outro agente da CIA', se essas são as únicas pessoas que usam a rede. ”17

Para realmente esconder espiões e soldados, Tor precisava se distanciar de suas raízes no Pentágono e incluir o maior número possível de usuários. Ativistas, estudantes, pesquisadores corporativos, mães do futebol, jornalistas, traficantes de drogas, hackers, pornógrafos infantis, agentes de serviços de inteligência estrangeiros, terroristas. Tor era como uma praça pública – quanto maior e mais diverso o grupo se reunia ali, melhores espiões podiam se esconder na multidão.

Em 2004, Dingledine tomou as rédeas e transformou o projeto militar de roteamento de cebola em uma corporação sem fins lucrativos chamada Projeto Tor e, embora ainda fosse financiado pela DARPA e pela marinha, começou a procurar financiamento privado.18 Ele recebeu ajuda de um aliado inesperado: a Electronic Frontier Foundation (EFF), que deu ao Tor quase um quarto de milhão de dólares para continuar enquanto Dingledine procurava outros patrocinadores privados.19 A EFF até hospedou o site do Tor. Para baixar o aplicativo, os usuários precisavam navegar até tor.eff.org, onde receberiam uma mensagem tranquilizadora da EFF: "Seu tráfego é mais seguro quando você usa o Tor".20

Anunciando seu apoio, a EFF glorificou o Tor. “O projeto Tor é perfeito para a EFF, porque um dos nossos principais objetivos é proteger a privacidade e o anonimato dos usuários da Internet. O Tor pode ajudar as pessoas a exercitarem o seu direito à Primeira Emenda de forma gratuita, através do discurso anônimo on-line”, explicou o gerente de tecnologia da EFF, Chris Palmer, em um comunicado à imprensa de 2004, que curiosamente não mencionou que o Tor foi desenvolvido prin-

cipalmente para uso militar e de inteligência e ainda era financiado ativamente pelo Pentágono.21

Por que a EFF, um grupo de defesa do Vale do Silício que se posicionou como um crítico ferrenho dos programas de vigilância do governo, ajudaria a vender uma ferramenta de comunicação de inteligência militar para usuários inocentes da Internet? Bem, não foi tão estranho quanto parece.

A EFF tinha apenas uma década de idade na época, mas já havia desenvolvido um histórico de trabalho com agências policiais e auxiliado os militares. Em 1994, a EFF trabalhou com o FBI para aprovar a Lei de Assistência às Comunicações para a Aplicação da Lei, que exigia que todas as empresas de telecomunicações construíssem seus equipamentos para que pudessem ser interceptados pelo FBI.22 Em 1999, a EFF trabalhou para apoiar a campanha de bombardeio da OTAN no Kosovo com algo chamado "Projeto de Privacidade do Kosovo", que visava manter o acesso à Internet da região aberto durante ações militares.23 Vender um projeto de inteligência do Pentágono como uma ferramenta de privacidade popular – não parecia tão absurdo assim. De fato, em 2002, alguns anos antes de financiar o Tor, o co-fundador da EFF, Perry Barlow, admitiu casualmente que estava dando consultoria para agências de inteligência há uma década.24 Parecia que os mundos de soldados, espiões e da privacidade não estavam tão distantes quanto pareciam.

O apoio da EFF ao Tor foi um grande negócio. A organização conquistou respeito no Vale do Silício e foi amplamente vista como a ACLU da Era da Internet. O fato de ter apoiado o Tor significava que não seriam feitas perguntas difíceis sobre as origens militares da ferramenta de anonimato durante a transição para o mundo civil. E foi justamente o que aconteceu.25

A liberdade não é livre

Era quarta-feira de manhã, dia 8 de fevereiro de 2006, quando Roger Dingledine recebeu o e-mail que estava esperando. O Conselho de Governadores de Radiodifusão finalmente concordou em apoiar o Projeto Tor.

"Tudo bem, queremos apoiar, Roger. Gostaríamos de oferecer algum financiamento", escreveu Ken Berman, diretor da unidade de Tecnologia da Internet do Conselho de Radiodifusão. "Para esse primeiro esforço, ofereceríamos US $ 80.000 a você, possivelmente mais dependendo de como as coisas evoluem. Dê-nos os detalhes de como estabelecer um relacionamento contratual com você."26

Fazia dois anos que Dingledine tornara o Tor independente, e seu tempo no mundo selvagem de doadores privados e organizações sem fins lucrativos civis não fora muito bem-sucedido.27 Além do financiamento inicial da Electronic Frontier Foundation, Dingledine não conseguiu levantar dinheiro do setor privado, pelo menos não o suficiente para financiar a operação.

O Conselho de Governadores de Radiodifusão, ou BBG, parecia oferecer um acordo. Uma grande agência federal com laços estreitos com o Departamento de Estado, o BBG dirigia as operações de transmissão dos EUA no exterior: Voice of America, Radio Free Europe / Radio Liberty e Radio Free Asia. Era uma agência do governo, então não era o ideal. Mas pelo menos tinha uma missão que soava altruísta: "informar, envolver e conectar pessoas ao redor do mundo em apoio à liberdade e à democracia". De qualquer forma, do governo ou não, Dingledine não teve muita escolha. O dinheiro estava apertado e isso parecia ser o melhor que ele podia conseguir. Ele disse, "Sim".

Foi uma jogada inteligente. Os US $ 80.000 iniciais foram apenas o começo. Dentro de um ano, a agência aumentou o contrato do Tor para um quarto de milhão de dólares e depois aumentou novamente para quase um milhão apenas alguns anos depois. O relacionamento também levou a grandes contratos com outras agências federais, aumentando o escasso orçamento operacional do Tor para vários milhões de dólares por ano.28

Dingledine deveria estar comemorando, mas algo incomodava sua consciência.

Imediatamente após assinar o contrato, ele enviou um e-mail a Ken Berman, seu contato no BBG, para dizer que estava preocupado com a aparência do acordo.29 Dingledine queria fazer todo o possível para manter a imagem independente do Tor, mas como chefe de uma organização sem fins lucrativos isenta de impostos que recebeu financiamento do governo federal, ele foi obrigado por lei a divulgar publicamente suas fontes de financiamento e publicar auditorias financeiras. Ele sabia que, gostando ou não, o relacionamento do Tor com o governo federal apareceria mais cedo ou mais tarde. “Também precisamos pensar em uma estratégia de como manobrar isso para que se alinhe com a visão geral do Tor. Acho que não queremos declarar guerra à China em voz alta, pois isso só prejudicaria nossos objetivos [do Tor] , certo? ” escreveu. “Mas também não queremos esconder a existência de financiamento [do BBG], já que 'eles são pagos pelos federais e não disseram a ninguém' soaria como um péssimo título de matéria para um projeto de segurança. Seria suficiente apenas falar sempre sobre o Irã ou isso não é sutil o bastante? ”30

Na faculdade, Dingledine sonhava em usar a tecnologia para criar um mundo melhor. Agora ele estava subitamente falando sobre se deveriam declarar guerra à China e ao Irã e se preocupando em ser rotulado como um agente federal? O que estava acontecendo?

Berman retornou um e-mail, tranquilizando Dingledine de que ele e sua agência estavam prontos para fazer o que fosse necessário para proteger a imagem independente do Tor. "Roger – faremos qualquer manobra que você queira fazer para ajudar a preservar a independência do TOR", escreveu. "Não podemos (nem devemos) ocultar [o financiamento] pelas razões descritas abaixo, mas também não iremos sair gritando isso por aí."

Berman era um veterano no assunto. Ele passou anos financiando tecnologia anticensura na agência e ofereceu uma solução simples. Recomendou que Dingledine fosse transparente sobre o financiamento governamental do Tor, mas também minimizou o significado desse relacionamento e, em vez disso, se concentrou no fato de que tudo era por uma boa causa: Tor ajudava a garantir a liberdade de expressão na Internet. Foi um conselho sábio. Dizer isso eliminaria qualquer potencial crítica e admitir que Tor recebia um pouco de dinheiro do governo dos

EUA serviria apenas como prova de que o Tor não tinha nada a esconder. Afinal, o que teria de abominável sobre o governo financiar a liberdade de expressão na Internet?

Outros também concordaram dando outros conselhos. Um contratado da BBG respondeu ao tópico do email para dizer a Dingledine para não se preocupar. Ninguém irá se importar. Não haverá retaliação. Ele explicou que, em sua experiência, se as pessoas sabiam sobre o BBG, consideravam-no totalmente inofensivo. "Acho que a maioria das pessoas, especialmente as inteligentes que importam, entende que o governo pode ser bom ou ruim, e os escritórios do governo, como filhotes, devem ser incentivados quando fazem a coisa certa", escreveu ele.31

Apesar das garantias, Dingledine estava certo em se preocupar.

Para ser verdadeiramente eficaz, o Tor não podia ser percebido como um sistema governamental. Isso significava que ele precisava colocar a maior distância possível entre Tor e as estruturas de inteligência militar que o criaram. Mas com o financiamento do BBG, Dingledine trouxe Tor de volta para o centro do monstro. O BBG poderia ter um nome insosso e professar uma missão nobre de informar o mundo e espalhar a democracia. Na verdade, a organização era uma cria da Agência Central de Inteligência.

Operações secretas

A história do Conselho de Governadores de Radiodifusão começa na Europa Oriental em 1948.

A Segunda Guerra Mundial havia terminado, mas os Estados Unidos já estavam ocupados se preparando para a batalha com seu principal inimigo ideológico, a União Soviética. Muitos generais acreditavam que a guerra nuclear era iminente e que o confronto final entre capitalismo e comunismo estava próximo. Eles elaboraram planos engenhosos para a batalha nuclear. Os Estados Unidos derrubariam grandes cidades soviéticas com armas nucleares e enviariam comandantes anticomunistas

recrutados entre as populações locais para assumir o controle e estabelecer governos provisórios. A Agência Central de Inteligência, juntamente com os serviços militares clandestinos, treinou os europeus orientais, muitos dos quais haviam sido colaboradores nazistas, para o fatídico dia em que seriam lançados de paraquedas em suas pátrias para assumir o comando.32

Embora os generais estadunidenses mais agressivos parecessem ansiosos por conflitos nucleares, muitos acreditavam que a guerra aberta com a União Soviética era perigosa demais e, em vez disso, aconselharam por uma abordagem mais comedida. George Kennan – o arquiteto da política de "contenção" pós-Segunda Guerra Mundial – pressionou por expandir o papel de programas secretos para combater a União Soviética. O plano era usar sabotagem, assassinatos, propaganda e financiamento secreto de partidos e movimentos políticos para impedir a propagação do comunismo na Europa pós-guerra, e depois usar essas mesmas ferramentas secretas para derrotar a própria União Soviética. Kennan acreditava que sociedades autoritárias fechadas eram inerentemente instáveis em comparação com sociedades democráticas abertas como os Estados Unidos. Para ele, a guerra tradicional com a União Soviética não era necessária. Dada uma pressão externa suficiente, ele acreditava, o país acabaria em colapso com o peso de suas próprias "contradições internas".33

Em 1948, George Kennan ajudou a elaborar a Diretiva 10/2 do Conselho de Segurança Nacional, que autorizou oficialmente a CIA – com consulta e supervisão do Departamento de Estado – a se envolver em "operações secretas" contra a influência comunista, incluindo desde guerra econômica a sabotagem, subversão e apoio a guerrilhas armadas. A diretiva deu à CIA carta branca para fazer o que fosse necessário para combater o comunismo onde quer que ele levantasse sua cabeça.34 Naturalmente, a propaganda surgiu como parte essencial do arsenal de operações secretas da agência. A CIA estabeleceu e financiou estações de rádio, jornais, revistas, sociedades históricas, institutos de pesquisa de emigrantes e programas culturais em toda a Europa.35 “Esses eram programas muito amplos, projetados para influenciar a opinião pública mundial em praticamente todos os níveis, desde camponeses analfabetos nos campos até os acadêmicos mais sofisticados de universidades de prestígio”, escreveu o historiador Christopher Simpson em Blowback,

um livro sobre o uso de nazistas pela CIA e colaboradores após a Segunda Guerra Mundial. "Eles utilizaram uma ampla gama de recursos: sindicatos, agências de publicidade, professores universitários, jornalistas e líderes estudantis".36

Em Munique, a CIA instalou a Radio Free Europe e a Radio Liberation From Bolshevism (mais tarde renomeada Radio Liberty), que transmitiam propaganda em vários idiomas através de antenas poderosas na Espanha para os estados satélites da União Soviética e da Europa Oriental. Essas estações tinham um orçamento anual combinado da CIA de US $ 35 milhões – uma quantia enorme na década de 1950 -, mas o envolvimento da agência estava oculto ao administrar tudo através de grupos de frente privados.37 Eles transmitem uma variedade de materiais, de notícias diretas e programação cultural a desinformação intencional e boatos destinados a espalhar o pânico e deslegitimar o governo soviético. Em alguns casos, as estações, especialmente as que visavam a Ucrânia, a Alemanha e os Estados Bálticos, eram atendidas por colaboradores nazistas conhecidos e transmitiam propaganda antissemita.38 Embora parciais e politizadas, essas estações acabavam sendo a única fonte de informação externa não autorizada ao povo do bloco soviético. Eles se tornaram altamente eficazes na comunicação dos ideais estadunidenses e na influência de tendências culturais e intelectuais.

Esses projetos não se restringiram à Europa. À medida que a luta dos Estados Unidos contra o comunismo mudou e se espalhou pelo mundo, novas iniciativas de desestabilização e propaganda foram adicionadas. A República Popular da China foi atingida em 1951, quando a agência lançou a Radio Free Asia, que transmitia para a China continental a partir de um escritório em São Francisco por meio de um transmissor de rádio em Manila.39 Na década de 1960, a CIA lançou projetos voltados para movimentos de esquerda na América Central e do Sul. As transmissões voltadas para o Vietnã e a Coreia do Norte também ficaram online.40

Nas palavras da CIA, essas estações estavam liderando uma luta pelas "mentes e lealdades" das pessoas que vivem nos países comunistas. Mais tarde, a agência se gabou de que esses primeiros projetos de rádio da "guerra psicológica" eram "uma das campanhas de ação secreta mais duradouras e bem-sucedidas já montadas pelos Estados Unidos".41

Foi tudo parte de um esforço maior que o professor de Princeton, Stephen Kotkin, chama de esfera pró-ativa de influência cultural e econômica. "Era uma estratégia, e foi assim que a Guerra Fria foi vencida."42

Essa rede global de rádio anticomunista foi exposta em um espetacular programa da CBS de 1967, realizado por Mike Wallace, "In the Pay of the CIA".43 As investigações subsequentes do Congresso levaram o papel da agência a um exame mais aprofundado, mas a exposição não interrompeu os projetos; simplesmente levou a um abalo na administração: o Congresso concordou em assumir o financiamento desse projeto de propaganda e executá-lo a céu aberto.

Nas décadas seguintes, essas estações de rádio foram embaralhadas, reorganizadas e constantemente expandidas. No início dos anos 2000, elas haviam se transformado no Conselho de Governadores de Radiodifusão (BBG), uma agência federal que funcionava como uma holding para reabilitar ativos de propaganda da CIA. Hoje, é uma grande operação que transmite em sessenta e um idiomas e cobre o mundo: Cuba, China, Iraque, Líbano, Líbia, Marrocos, Sudão, Irã, Afeganistão, Rússia, Ucrânia, Sérvia, Azerbaijão, Bielorrússia, Geórgia, Coreia do Norte, Laos e Vietnã.44

A maior parte do BBG não é mais financiada pelo orçamento obscuro da CIA, mas a meta e o objetivo originais da Guerra Fria – operações de subversão e psicológicas dirigidas contra países considerados hostis aos interesses dos EUA – permanecem os mesmos.45 A única coisa que mudou no BBG é que hoje cada vez mais suas transmissões estão ocorrendo on-line.

O relacionamento da agência com o Projeto Tor começou com a China.

Liberdade na Internet

Desde pelo menos 1951, a CIA tinha como alvo a República Popular da China com transmissão secreta, quando a agência lançou a Rádio Livre Ásia. Ao longo das décadas, a agência fechou e relançou o Radio Free

Asia sob diferentes formas e, finalmente, a entregou ao Conselho de Governadores de Radiodifusão.46

Quando a Internet comercial começou a penetrar na China no início dos anos 2000, o BBG e a Radio Free Asia canalizaram seus esforços na programação baseada na Web. Mas essa expansão não foi muito tranquila. Por anos, a China tocava os programas Voice of America e Radio Free Asia junto com ruídos altos ou tocando música de ópera chinesa nas mesmas frequências que eram transmitidos os programas gringos, mas com um sinal de rádio mais poderoso.47 Quando essas transmissões mudaram para a Internet, os censores chineses reagiram, bloqueando o acesso aos sites do BBG e cortando esporadicamente o acesso a serviços privados da Internet, como o Google.48 Não havia nada de surpreendente nisso. As autoridades chinesas viam a Internet apenas como outro meio de comunicação usado pelos EUA para minar seu governo. Ativar esse tipo de atividade era prática padrão na China muito antes da chegada da Internet.49

Esperado ou não, o governo dos EUA não desistiu. As tentativas da China de controlar seu próprio espaço doméstico na Internet e bloquear o acesso a materiais e informações foram vistas como atos beligerantes – algo como um embargo comercial moderno que limitava a capacidade das empresas e agências governamentais dos EUA de operar livremente. Sob o mandato do presidente George W. Bush, os planejadores estadunidenses de política externa formularam políticas que seriam conhecidas na próxima década como "Liberdade na Internet".50 Embora montadas com uma linguagem sublime sobre o combate à censura, a promoção da democracia e a salvaguarda da "liberdade de expressão", essas políticas estavam enraizadas na política das grandes potências: a luta para abrir mercados para empresas gringas e expandir o domínio dos Estados Unidos na era da Internet.51 O programa Liberdade na Internet foi apoiado com entusiasmo por empresas estadunidenses, especialmente gigantes da Internet em ascensão como Yahoo!, Amazon, eBay, Google e, mais tarde, Facebook e Twitter. Elas viam o controle externo da Internet, primeiro na China, mas também no Irã e depois no Vietnã, na Rússia e em Mianmar, como um embargo ilegítimo da sua capacidade de expandir para novos mercados globais e, finalmente, como uma ameaça para seus negócios.

O programa Liberdade na Internet exigia um novo conjunto de armas de “poder brando”: pés de cabra digitais que poderiam ser usadas para abrir buracos na infraestrutura de telecomunicações de um país. No início dos anos 2000, o governo dos EUA começou a financiar projetos que permitiriam que pessoas dentro da China atravessassem por um "túnel" o firewall do governo de seu país.52 A Divisão de Anti-Censura na Internet do BBG liderou o grupo, injetando milhões de dólares em todos os tipos de tecnologias precoces para "contornar a censura". Apoiou o SafeWeb, um proxy da Internet financiado pela empresa de capital de risco da CIA In-Q-Tel. Também financiou várias pequenas mídias dirigidas por praticantes do Falun Gong, um controverso culto anticomunista chinês proibido na China, cujo líder acredita que os seres humanos estão sendo corrompidos por alienígenas de outras dimensões e que pessoas de sangue misto são sub-humanos e impróprios para a salvação.53

O governo chinês viu essas ferramentas anticensura como armas em uma versão atualizada de uma guerra antiga. "A Internet se tornou um novo campo de batalha entre a China e os EUA", declarou um editorial de 2010 da Xinhua News Agency, agência de imprensa oficial da China. “O Departamento de Estado dos EUA está colaborando com a Google, Twitter e outros gigantes de TI para lançar em conjunto softwares que 'permitirão que todos usem a Internet livremente', usando um tipo de software anti-bloqueio fornecido pelo governo dos EUA, na tentativa de espalhar ideologia e valores alinhados às demandas dos Estados Unidos. ”54

A China via o Liberdade na Internet como uma ameaça, uma tentativa ilegítima de minar a soberania do país por meio de uma "guerra de rede" e começou a construir um sofisticado sistema de censura e controle da Internet, que se transformou na infame Grande Firewall da China. O Irã logo seguiu os passos da China.

Foi o início de uma corrida armamentista de censura. Mas havia um problema: as primeiras ferramentas anti-censura apoiadas pelo BBG não funcionavam muito bem. Elas tinham poucos usuários e foram facilmente bloqueadas. Para que o Liberdade na Internet triunfasse, os EUA precisavam de armas maiores e mais fortes. Felizmente, a Marinha dos EUA havia acabado de desenvolver uma poderosa tecnologia de anoni-

mato para esconder seus espiões, uma tecnologia que poderia ser facilmente adaptada à guerra do Liberdade na Internet dos Estados Unidos.

Plano de Implantação na Rússia

Quando o Tor ingressou no Conselho de Governadores de Radiodifusão no início de 2006, Roger Dingledine estava ciente do crescente conflito de liberdade na Internet nos Estados Unidos e aceitou o papel do Tor como uma arma nessa luta. China e Irã estavam lançando técnicas de censura cada vez mais sofisticadas para bloquear a programação dos EUA, e Dingledine falou da capacidade do Tor de enfrentar esse desafio. "Já temos dezenas de milhares de usuários no Irã e na China e em países semelhantes, mas quando ficarmos mais populares, precisaremos estar preparados para começar a corrida armamentista", escreveu ele ao BBG em 2006, descrevendo um plano para adicionar progressivamente recursos à rede Tor que tornariam cada vez mais difícil o bloqueio.55

O Projeto Tor era a arma mais sofisticada do Liberdade na Internet do BBG, e a agência pressionou Dingledine a procurar ativistas políticos estrangeiros e fazê-los usar a ferramenta. Mas, como Dingledine descobriu rapidamente, os laços de sua organização com o governo dos EUA despertaram suspeitas e dificultaram sua capacidade de atrair usuários.

Uma dessas lições veio em 2008. No início daquele ano, o BBG instruiu Dingledine a executar o que ele apelidou de "Plano de Implantação da Rússia", que envolvia adicionar uma opção de idioma russo à interface do Tor e trabalhar para treinar ativistas russos na utilização correta do serviço.56

Em fevereiro de 2008, semanas antes das eleições presidenciais da Rússia, Dingledine enviou uma solicitação por email a um ativista da privacidade russo chamado Vlad. "Um de nossos financiadores ... [o Conselho de Governadores de Radiodifusão] quer que comecemos a procurar usuários de verdade que possam precisar dessas ferramentas em algum momento", explicou Dingledine. “Então escolhemos a Rússia,

que está cada vez mais no radar como um país que pode ter um sério problema de censura nos próximos anos... Então: por favor, não anuncie isso em nenhum lugar ainda. Mas se você quiser se envolver de alguma forma, ou tem algum conselho, por favor me avise.57

Vlad ficou feliz em receber uma mensagem de Dingledine. Ele já conhecia o Tor e era um fã da tecnologia, mas tinha dúvidas sobre o plano. Ele explicou que atualmente a censura não era um problema na Rússia. “O principal problema na Rússia atualmente não é a censura do governo (no sentido do Grande Firewall da China ou de alguns países árabes), mas a autocensura de muitos sites, especialmente de organizações regionais. Infelizmente, não é isso que o Tor pode resolver por si só – ele respondeu. Em outras palavras: por que corrigir um problema que não existe?

Mas uma questão maior pairava sobre o pedido de Dingledine, referente aos laços de Tor com o governo dos EUA. Vlad explicou que ele e outros membros da comunidade de privacidade da Rússia estavam preocupados com o que ele descreveu como "dependência do dinheiro do 'tio Sam'" e que "alguns patrocinadores do projeto Tor estão associados ao Departamento de Estado dos EUA". Ele continuou: "Entendo que essa é uma pergunta ambígua e bastante vaga, mas esse patrocínio traz problemas delicados ao projeto Tor e ao processo de desenvolvimento do Tor?"

Dada a deterioração das relações políticas entre a Rússia e os Estados Unidos, o subtexto da pergunta era óbvio: quão perto Tor estava do governo dos EUA? E, nesse clima geopolítico tenso, será que esses laços causariam problemas a ativistas russos como ele? Essas eram perguntas honestas e relevantes. Os e-mails que obtive através da Lei da Liberdade de Informação não mostram se Dingledine respondeu. Como poderia? O que ele diria?

O Projeto Tor havia se posicionado como uma “organização sem fins lucrativos independente”, mas quando Dingledine procurou Vlad no início de 2008, estava operando como um braço de fato do governo dos EUA.

A correspondência deixou pouco espaço para dúvidas. O Projeto Tor não era uma organização indie radical que lutava contra o sistema.

Para todos os efeitos, ela era parte do sistema. Ou, pelo menos, a mão direita dele. Misturada com atualizações sobre novas contratações, relatórios de status, sugestões de conversas para caminhadas e pontos de férias, e as brincadeiras habituais nos escritórios, a correspondência interna revela a estreita colaboração do Tor com o BBG e várias outras alas do governo dos EUA, em particular aquelas que lidavam com política externa e projeção de "poder brando". As mensagens descrevem reuniões, treinamentos e conferências com a NSA, CIA, FBI e Departamento de Estado.58 Há sessões de estratégia e discussões sobre a necessidade de influenciar a cobertura de notícias e controlar a má imprensa.59 A correspondência também mostra os funcionários do Tor recebendo pedidos de seus "apoiadores" no governo federal, incluindo planos de implantar sua ferramenta de anonimato em países considerados hostis aos interesses dos EUA: China, Irã, Vietnã e, é claro, Rússia. Apesar da insistência pública do Tor, ele nunca colocaria backdoors que concedessem ao governo dos EUA acesso privilegiado secreto à rede do Tor, a correspondência mostra que em pelo menos um caso em 2007, o Tor revelou uma vulnerabilidade de segurança ao seu patrocinador federal antes de alertar o público, potencialmente dando ao governo a oportunidade de explorar a falha para desmascarar os usuários do Tor antes que ela fosse corrigida.60

O registro de financiamento conta a história ainda mais precisamente. Além da Google pagar um punhado de estudantes universitários para trabalhar no Tor por meio do programa Summer of Code da empresa, o Tor subsistia quase exclusivamente em contratos governamentais. Em 2008, isso incluía contratos com a DARPA, a marinha, o BBG e o Departamento de Estado, além do programa de análise de ameaças cibernéticas do Stanford Research Institute. Dirigida pelo Exército dos EUA, essa iniciativa havia saído da divisão de atividades avançadas de pesquisa e desenvolvimento da NSA – James Bamford a descreve como um “tipo de laboratório nacional para grampeamento de comunicações e espionagem” no livro The Shadow Factory.62 E alguns meses depois de entrar em contato com Vlad, Dingledine estava a ponto de fechar outro contrato de US $ 600.000 com o Departamento de Estado,63 desta vez de sua divisão de Democracia, Direitos Humanos e Trabalho, que havia sido criada durante o primeiro mandato do presi-

dente Bill Clinton e era encarregada de distribuir subsídios para "assistência à democracia".64

O que alguém como Vlad pensaria de tudo isso? Obviamente, nada de bom. E isso foi um problema.

O Projeto Tor precisava que os usuários confiassem em sua tecnologia e mostrassem entusiasmo. Credibilidade era a chave. Mas o alcance de Dingledine aos ativistas russos da privacidade foi um lembrete rude de que Tor não podia abalar sua afiliação ao governo e todas as conotações negativas que a acompanham. Foi um problema que Dingledine supôs que assombraria o Tor quando ele aceitasse o primeiro contrato do BBG em 2006.

Claramente, o Tor precisava fazer algo para mudar a percepção do público, algo que poderia ajudar a distanciar o Tor dos patrocinadores do governo de uma vez por todas. Por sorte, Dingledine encontrou o homem perfeito para o trabalho: um jovem e ambicioso desenvolvedor do Tor que poderia ajudar a repaginar o Projeto Tor como um grupo de rebeldes que fazia o tio Sam tremer em suas bases.

Nasce um herói

Jacob Appelbaum nasceu em 1983 no dia da mentira. Cresceu em Santa Rosa, uma cidade ao norte de São Francisco (EUA), em uma família boêmia. Ele gostava de falar sobre sua educação difícil: uma mãe esquizofrênica, um pai músico que virou drogado e uma situação doméstica que ficou tão ruim que ele teve que ficar catando agulhas usadas no sofá quando criança. Mas também era um garoto judeu inteligente de classe média, com um talento especial para programação e hackeio. Frequentou o colégio de Santa Rosa e teve aulas de ciência da computação. Se vestia de preto, no estilo gótico, e brincava com fotografia *steampunk*, tirando fotos retro-futuristas de jovens mulheres usando vestidos da era vitoriana em frente a máquinas a vapor e locomotivas. Politicamente, ele se identificou como libertarianista.

Como a maioria dos jovens libertarianistas, ele ficou encantado com The Fountainhead, de Ayn Rand, que descreveu como um de seus livros favoritos. “Peguei este livro enquanto estava viajando pela Europa no ano passado. A maioria dos meus amigos da extrema esquerda realmente não gosta de Ayn Rand por algum motivo ou outro. Eu não consigo nem começar a entender o porquê, mas é isso, cada um na sua”, escreveu ele em seu diário-blog. “Ao ler The Fountainhead, senti como se estivesse lendo uma história sobre pessoas que conhecia na minha vida cotidiana. Os personagens eram simples. A história também. O que achei atraente foi a moral por trás dela. Imagino que possa ser resumida em uma linha: aqueles que querem juntar pessoas para ações altruístas desejam escravizá-lo para seu próprio ganho. ”66

Ele se mudou para São Francisco e trabalhou em empregos de baixo nível com ênfase em gerenciamento de redes, mas se irritava com empregos regulares em tecnologia e ansiava por algo significativo.67 Tirou uma folga para se voluntariar em Nova Orleans depois do furacão Katrina e de alguma forma acabou no Iraque saindo com um colega de serviço militar que estava instalando serviço de satélite no país devastado pela guerra. Voltou a São Francisco mais determinado do que nunca a viver uma vida empolgante. "A vida é muito curta para desperdiçá-la em empregos que não gosto", disse em uma entrevista em 2005.68 Um dia, ele ingressou em uma empresa iniciante pornô, vestiu-se de preto, pintou o cabelo de vermelho e posou com um vibrador de ferramenta elétrica para a revista Wired.69 No dia seguinte, viajaria para o outro lado do mundo para usar suas habilidades para um bem maior. "Sou um hacker freelancer. Trabalho em grupos que realmente precisam da minha ajuda. Eles vêm até mim e me pedem meus serviços”, disse. “Frequentemente, estou simplesmente configurando suas redes e sistemas em todo o mundo. Isso depende de como me sinto em relação ao trabalho que eles estão fazendo. Tem que ser um trabalho interessante e que visa um resultado interessante.”

Appelbaum também começou a desenvolver uma má reputação na cena hacker de Área da Baía por suas abordagens sexuais agressivas e indesejadas. A jornalista de São Francisco Violet Blue contou como ele passou meses tentando coagir e intimidar as mulheres a fazer sexo com ele, tentou forçar suas vítimas a se isolar com ele em salas ou escadas de festas e recorreu à difamação caso seus avanços fossem rejeita-

dos.70 Esse padrão de comportamento provocaria sua queda quase uma década depois. Mas, por enquanto, ele estava em ascensão. E em 2008, Appelbaum finalmente conseguiu o emprego dos seus sonhos – uma posição que poderia se expandir da mesma forma que seu ego e ambição gigantescos.

Em abril daquele ano, Dingledine o contratou como um terceirizado em tempo integral. Tinha um salário inicial de US $ 96.000 mais benefícios e seu trabalho era tornar o Tor mais fácil de usar. Ele era um bom programador, mas não ficou focado no lado técnico por muito tempo. Como Dingledine descobriu, Appelbaum se mostrou melhor e muito mais útil em outra coisa: propaganda e relações públicas.

Os funcionários do Tor eram engenheiros de computação, matemáticos e viciados em criptografia. A maioria deles era introvertida e socialmente desajeitada. Pior ainda: alguns, como Roger Dingledine, passaram algum tempo nas agências de inteligência dos EUA e exibiram orgulhosamente esse fato em seus currículos on-line – um sinal não tão sutil de falta de radicalidade.72 Appelbaum adicionou um elemento diferente à organização. Ele tinha talento, gosto por drama e hipérbole. Ele estava cheio de histórias grandiosas e vaidade, e tinha um desejo ardente pelos holofotes.

Poucos meses depois de conseguir o emprego, ele assumiu o papel de porta-voz oficial do Projeto Tor e começou a promover o Tor como uma arma poderosa contra a opressão governamental.

Enquanto a Dingledine se concentrava em administrar o negócio, Jacob Appelbaum viajava de avião para locais exóticos ao redor do mundo para evangelizar e espalhar a nova. Esteve em dez países em um mês e não se incomodou: Argentina, Índia, Polônia, Coréia do Sul, Bélgica, Suíça, Canadá, Tunísia, Brasil e até o campus da Google em Mountain View, Califórnia.73 Deu palestras em conferências de tecnologia e eventos de hackers, brigou com executivos do Vale do Silício, visitou Hong Kong, treinou ativistas políticos estrangeiros no Oriente Médio e mostrou a ex-profissionais do sexo no Sudeste Asiático como se proteger on-line. Ele também se encontrou com as agências policiais suecas, mas isso foi feito fora dos olhos do público.74

Ao longo dos anos seguintes, os relatórios de Dingledine para o BBG foram preenchidos com descrições do sucesso do alcance de Appelbaum. "Tem sido feita bastante promoção do Tor", escreveu Dingledine. “Outra caixa de adesivos Tor foi aplicada a muitos laptops. Muitas pessoas estavam interessadas no Tor e muitas instalaram-no em laptops e servidores. Essa promoção resultou em pelo menos dois novos nós de alta largura de banda que ele ajudou os administradores a configurar.”75 Documentos internos mostram que o orçamento proposto para o programa de publicidade global de Dingledine e Appelbaum era de US $ 20.000 por ano, o que incluía uma estratégia de relações públicas.76 “Elaborar uma mensagem que a mídia possa entender é uma parte crítica disso”, explicou Dingledine em uma proposta de 2008. "Não se trata tanto de que a mídia seja favorável ao Tor, mas de preparar jornalistas; se eles veem más notícias e pensam em divulgá-las, eles param e pensam."77

Appelbaum era enérgico e fez o possível para promover o Tor entre ativistas da privacidade, criptografadores e, o mais importante de tudo, o movimento radical do cypherpunk que sonhava em usar a criptografia para assumir o poder dos governos e libertar o mundo do controle centralizado. Em 2010, ele conseguiu o apoio de Julian Assange, um hacker de cabelos prateados que queria acabar com os segredos do mundo.

O Tor fica radical

Jacob Appelbaum e Julian Assange se conheceram em Berlim em 2005, quando o misterioso hacker australiano estava se preparando para colocar o WikiLeaks em movimento. A ideia de Assange para o WikiLeaks era simples: a tirania do governo só pode sobreviver em um ecossistema de sigilo. Retire a capacidade dos poderosos de guardar segredos, e toda a fachada desabará ao seu redor. "Vamos foder com todos eles", escreveu Assange, vertiginosamente, em um servidor de listas secreto, depois de anunciar seu objetivo de arrecadar US $ 5 milhões para o WikiLeaks.

“Vamos abrir o mundo e deixá-lo florescer em algo novo. Se brigar com a CIA vai nos ajudar, então a gente vai fazer isso."78

Appelbaum observou como Assange lentamente erigiu o WikiLeaks do nada, construindo seguidores dedicados dando conferências de hackeio para possíveis vazadores. Os dois se tornaram bons amigos, e Appelbaum mais tarde se gabou para o jornalista Andy Greenberg dizendo que eles eram tão próximos que fodiam garotas juntos. Numa manhã de ano novo, os dois acordaram em um apartamento em Berlim, em uma cama com duas mulheres. "Foi assim que rolamos em 2010", disse ele.

Logo após aquela noite supostamente selvagem, Appelbaum decidiu se juntar à causa do WikiLeaks. Ele passou algumas semanas com Assange e a equipe original do WikiLeaks na Islândia, enquanto preparavam seu primeiro grande lançamento e ajudavam a proteger o sistema de envios anônimos do site usando o recurso de serviço oculto do Tor, que escondia a localização física dos servidores do WikiLeaks e, em teoria, os tornava muito menos suscetível à vigilância e a ataques. A partir de então, o site do WikiLeaks anunciou orgulhosamente o Tor: "uma rede distribuída segura, anônima e para máxima segurança".

A sincronia de Appelbaum não poderia ter sido melhor. No final daquele verão, o WikiLeaks causou sensação internacional ao publicar uma enorme quantidade de documentos secretos do governo roubados e vazados por Chelsea (Bradley) Manning, uma jovem soldado do Exército dos EUA operando no Iraque. Primeiro vieram os registros de guerra do Afeganistão, mostrando como os Estados Unidos subnotificaram sistematicamente as baixas civis e operaram uma unidade de assassinato de elite. A seguir, vieram os registros da Guerra do Iraque, fornecendo evidências irrefutáveis de que os EUA haviam armado e treinado esquadrões da morte em uma brutal campanha de contrainsurgência contra a minoria sunita do Iraque. Isso ajudou a alimentar a guerra sectária xiita-sunita que levou a centenas de milhares de mortes e limpeza étnica em partes. de Bagdá.79 Então vieram os telegramas diplomáticos dos EUA, oferecendo uma visão sem precedentes sobre o funcionamento interno da diplomacia estadunidense: mudança de regime, acordos de bastidores com ditadores, corrupção de líderes estrangeiros por trás dos panos em nome da estabilidade.80

De repente, Assange era uma das pessoas mais famosas do mundo – um radical destemido quebrando o incrível poder dos Estados Unidos. Appelbaum fez o possível para ser o braço direito de Assange. Ele atuou como representante estadunidense oficial da organização e salvou o fundador do WikiLeaks de situações difíceis quando o calor das autoridades gringas era muito alto.81 Appelbaum ficou tão enredado com o WikiLeaks que, aparentemente, alguns funcionários falaram sobre ele acabar liderando a organização se algo acontecesse a Assange.82 Mas Assange manteve o controle firme do WikiLeaks, mesmo depois que foi forçado a se esconder na embaixada do Equador em Londres para escapar da extradição de volta à Suécia, ond enfrentaria uma investigação de acusações de estupro.

Não está claro se Assange sabia que o salário de Appelbaum estava sendo pago pelo mesmo governo que ele estava tentando destruir. O que está claro é que Assange deu amplo crédito a Appelbaum e Tor por ajudar o WikiLeaks. "Jake tem sido um promotor incansável nos bastidores de nossa causa", disse ele a um repórter. "A importância do Tor para o WikiLeaks não pode ser subestimada."83

Com essas palavras, Appelbaum e o Projeto Tor se tornaram heróis centrais na saga do WikiLeaks, logo atrás de Assange. Appelbaum alavancou seu novo status de rebelde por tudo que valia. Ele cevou os repórteres com histórias loucas de como sua associação com o WikiLeaks fez dele um homem procurado. Falou sobre ser perseguido, interrogado e ameaçado por forças sombrias do governo. Descreveu em detalhes arrepiantes como ele e todos que ele conhecia foram jogados em um pesadelo de assédio e vigilância do Big Brother. Alegou que sua mãe foi alvejada. Sua namorada recebia visitas noturnas de homens vestidos de preto. “Eu estava na Islândia trabalhando com um amigo na reforma da constituição deles. E ela viu dois homens do lado de fora de sua casa no quintal, o que significava que eles estavam na propriedade dela dentro de uma cerca. E um deles usava óculos de visão noturna e a observava dormir" contou em uma entrevista de rádio. “Então, ela apenas deitou na cama, em puro terror, pelo período em que eles ficaram ali e a observaram. E, presumivelmente, isso ocorria porque havia uma terceira pessoa na casa colocando uma escuta ou fazendo outra coisa, e eles a vigiavam para garantir que, se ela ouvisse algo ou se levantasse, seriam capazes de alertar essa outra pessoa."84

Ele era um grande artista e tinha o talento de dar a jornalistas o que eles queriam. Contou histórias fantásticas, e Tor estava no centro de todas elas. Os repórteres engoliram tudo. Quanto mais exagerada e heroica sua atuação, mais atenção atraía para si. Artigos de notícias, programas de rádio, aparições na televisão e propagandas de revistas. A mídia não se saciava.

Em dezembro de 2010, a revista Rolling Stone publicou um perfil de Appelbaum como "o homem mais perigoso do ciberespaço". O artigo o retratava como um destemido guerreiro tecno-anarquista que havia dedicado sua vida a derrubar o malvado aparelho de vigilância militar dos Estados Unidos, não importando o custo para sua própria vida. Estava cheio de drama, narrando a vida de Appelbaum na corrida pós-WikiLeaks. Descrições de apartamentos esvaziados às pressas, bolsas Ziploc cheias de dinheiro de locais exóticos e fotos de garotas punk com pouca roupa – presumivelmente os muitos interesses amorosos de Appelbaum. “Appelbaum está fora do radar desde então – evitando aeroportos, amigos, estranhos e locais inseguros, viajando pelo país de carro. Ele passou os últimos cinco anos de sua vida trabalhando para proteger ativistas em todo o mundo contra governos repressivos. Agora está fugindo por conta própria”, escreveu o repórter da Rolling Stone Nathaniel Rich.85

Sua associação com o WikiLeaks e Assange impulsionou o perfil público e as credenciais radicais do Projeto Tor. Receberam apoio e elogios de jornalistas, organizações de privacidade e organizações civis que fiscalizam o governo. A American Civil Liberties Union fez uma parceria com Appelbaum em um projeto de privacidade na Internet, e o Whitney Museum de Nova York – um dos principais museus de arte moderna do mundo – o convidou para um "Curso sobre Vigilância".86 A Electronic Frontier Foundation concedeu ao Tor seu prêmio de pioneiro, e Roger Dingledine fez parte da lista dos 100 pensadores globais da revista Foreign Policy por proteger “qualquer pessoa e todo mundo dos perigos do Big Brother”.87

Quanto aos vínculos profundos e contínuos de Tor com o governo dos EUA? Bom, e daí? Para quem duvida, Jacob Appelbaum era considerado uma prova viva da independência radical do Projeto Tor. "Se os usuários ou desenvolvedores que ele encontra temem que o financia-

mento do governo ao Tor compromete seus ideais, não tem ninguém melhor do que Appelbaum para mostrar que o grupo não recebe ordens dos federais", escreveu o jornalista Andy Greenberg em This Machine Kills Secrets, um livro sobre WikiLeaks. "A melhor evidência de Appelbaum com respeito à pureza do Tor em relação à interferência do Big Brother, talvez, seja sua associação pública ao WikiLeaks, o site menos favorito do governo estadunidense."

Com Julian Assange endossando Tor, os repórteres assumiram que o governo dos EUA via o anonimato sem fins lucrativos como uma ameaça. Mas os documentos internos obtidos através do FOIA do Conselho de Governadores de Radiodifusão (BBG), bem como uma análise dos contratos do TOr com o governo, mostram um quadro diferente. Eles revelam que Appelbaum e Dingledine trabalharam com Assange para a proteção do WikiLeaks com o Tor desde o final de 2008 e mantiveram seus treinadores no BBG informados sobre seu relacionamento e até forneceram informações sobre o funcionamento interno do sistema de envio seguro do WikiLeaks.

"Conversei com o pessoal do WikiLeaks (Daniel e Julian) sobre o uso dos serviços ocultos do Tor e como podemos melhorar as coisas para eles", escreveu Dingledine em um relatório de progresso que enviou ao BBG em janeiro de 2008. “Acontece que eles usam o serviço oculto inteiramente como uma maneira de impedir que os usuários façam bobagem – ou funciona e eles sabem que estão seguros, ou falha, mas de qualquer maneira não revela o que estão tentando vazar localmente. Então, eu gostaria de adicionar um novo recurso de 'serviço seguro' que é como um serviço oculto, mas apenas dá um salto do lado do servidor em vez de três. Um design mais radical seria fazer com que o "nós de entrada" seja o serviço em si, então seria realmente como um enclave de saída".88 Em outro relatório de progresso enviado ao BBG, dois anos depois, em fevereiro de 2010, Dingledine escreveu: “Jacob e o WikiLeaks se reuniram com formuladores de políticas na Islândia para discutir liberdade de expressão, liberdade de imprensa e que a privacidade online deve ser um direito fundamental."

Ninguém no BBG levantou objeções. Pelo contrário, eles pareciam apoiar. Não sabemos se alguém no BBG encaminhou essas informações a algum outro órgão governamental, mas não seria difícil imagi-

nar que as informações sobre a infraestrutura de segurança e o sistema de envio de informações do WikiLeaks fossem de grande interesse para as agências de inteligência dos EUA.

Talvez o mais revelador foi que o apoio do BBG continuou mesmo depois que o WikiLeaks começou a publicar informações confidenciais do governo estadunidense e Appelbaum se tornou o alvo de uma investigação maior do WikiLeaks pelo Departamento de Justiça. Por exemplo, em 31 de julho de 2010, a CNET informou que Appelbaum havia sido detido no aeroporto de Las Vegas e questionado sobre seu relacionamento com o WikiLeaks.89 As notícias da detenção foram manchetes em todo o mundo, mais uma vez destacando os laços estreitos de Appelbaum com Julian Assange. E uma semana depois, o diretor executivo de Tor, Andrew Lewman, claramente preocupado que isso pudesse afetar o financiamento de Tor, enviou um e-mail a Ken Berman no BBG na esperança de amenizar as coisas e responder “quaisquer perguntas que você possa ter sobre as recentes notícias sobre Jake e WikiLeaks." Mas Lewman teve uma agradável surpresa: Roger Dingledine mantinha o pessoal do BBG informado e tudo parecia bem. "Muito bom, obrigado. Roger respondeu a uma série de perguntas quando nos encontramos esta semana em DC”, respondeu Berman.90

Infelizmente, Berman não explicou no e-mail o que ele e Dingledine discutiram sobre Appelbaum e WikiLeaks durante a reunião. O que sabemos é que a associação de Tor com o WikiLeaks não produziu nenhum impacto negativo real nos contratos governamentais de Tor.91

Seus contratos de 2011 chegaram sem problemas – US $ 150.000 do Conselho de Governadores de Radiodifusão e US $ 227.118 do Departamento de Estado.92 O Tor conseguiu até ganhar uma grande parte do dinheiro do Pentágono: um novo contrato anual de US $ 503.706 do Comando de Sistemas Espaciais e Guerra Naval, uma unidade de elite de informações e inteligência que abriga uma divisão secreta de guerra cibernética.93 O contrato da marinha foi aprovado pelo SRI, o antigo contratado militar de Stanford que havia trabalhado com contrainsurgência, rede e armas químicas para a ARPA nas décadas de 1960 e 1970. Os fundos faziam parte de um programa maior da Marinha de “Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento” para melhorar as operações militares.

Um ano depois, Tor veria seus contratos governamentais dobrarem para US $ 2,2 milhões: US $ 353.000 do Departamento de Estado, US $ 876.099 da Marinha dos EUA e US $ 937.800 do Conselho de Radiodifusão.94

Quando fiz essas contas, não pude deixar de conferir com cuidado. Foi incrível. O WikiLeaks havia atingido diretamente os apoiadores do governo de Tor, incluindo o Pentágono e o Departamento de Estado. No entanto, a estreita parceria de Appelbaum com Assange não produziu desvantagens perceptíveis.

Acho que faz sentido, de certa forma. O WikiLeaks pode ter envergonhado algumas partes do governo dos EUA, mas também deu à principal arma de liberdade na Internet dos EUA uma injeção importante de credibilidade, melhorando sua eficácia e utilidade. Na verdade, foi uma boa oportunidade.

Mídias sociais como arma

Em 2011, menos de um ano após o WikiLeaks entrar no cenário mundial, o Oriente Médio e o norte da África explodiram como um barril de pólvora. Aparentemente do nada, grandes manifestações e protestos varreram a região. Tudo começou na Tunísia, onde um pobre vendedor de frutas se incendiou para protestar contra a humilhação de assédio e extorsão realizada pelas mãos da polícia local. Ele morreu de queimaduras em 4 de janeiro, desencadeando um movimento de protesto nacional contra o presidente ditatorial da Tunísia, Zine El Abidine Ben Ali, que governava o país por 23 anos. Em semanas, protestos massivos contra o governo se espalharam para Egito, Argélia, Omã, Jordânia, Líbia e Síria.

A primavera árabe havia chegado.

Na Tunísia e no Egito, esses movimentos de protesto derrubaram ditaduras de longa data. Na Líbia, as forças da oposição depuseram e mataram violentamente Muammar Gaddafi, esfaqueando-o no ânus, após uma extensa campanha de bombardeio das forças da OTAN. Na Síria, os protestos foram enfrentados com uma repressão brutal do

governo de Bashar Assad, e levou a uma guerra prolongada que causaria centenas de milhares de mortes e desencadearia a pior crise de refugiados da história recente, atraindo Arábia Saudita, Turquia, Israel, a CIA, a Força Aérea Russa e suas equipes de operações especiais, Al-Qaeda e ISIS. A Primavera Árabe se transformou em um inverno longo e sangrento.

As causas subjacentes a esses movimentos de oposição eram profundas, complexas e variavam de país para país. O desemprego dos jovens, a corrupção, a seca e os altos preços dos alimentos, repressão política, estagnação econômica e aspirações geopolíticas de longa data foram apenas alguns dos fatores. Para uma safra jovem e com conhecimento digital de funcionários do Departamento de Estado e planejadores de política externa, esses movimentos políticos tinham uma coisa em comum: eles surgiram devido ao poder democratizante da Internet. Eles viam sites de mídia social como Facebook, Twitter e YouTube como multiplicadores democráticos que permitiam às pessoas se desviar das fontes oficiais de informação controladas pelo Estado e organizar movimentos políticos de maneira rápida e eficiente.

"O Che Guevara do século XXI é a rede", disse Alec Ross, funcionário do Departamento de Estado encarregado de política digital da Secretária de Estado Hillary Clinton, elogiado pela revista oficial da Organização do Tratado do Atlântico Norte.95 A referência ao Che cheira a hipocrisia ou talvez ignorância; afinal, Che foi executado por forças bolivianas apoiadas pelos Estados Unidos, em particular pela CIA.

A ideia de que as mídias sociais pudessem ser usadas como armas contra países e governos considerados hostis aos interesses dos EUA não foi uma surpresa. Durante anos, o Departamento de Estado dos EUA, em parceria com o Conselho de Governadores de Radiodifusão e empresas como Facebook e Google, trabalhou para treinar ativistas de todo o mundo sobre como usar ferramentas da Internet e mídias sociais para organizar movimentos políticos da oposição. Países da Ásia, Oriente Médio e América Latina, assim como antigos estados soviéticos como Ucrânia e Bielorrússia, estavam todos na lista. De fato, o New York Times informou que muitos dos ativistas que desempenharam

papeis de liderança na Primavera Árabe – do Egito à Síria e ao Iêmen – haviam participado dessas sessões de treinamento.96

"O dinheiro gasto nesses programas foi minúsculo comparado aos esforços liderados pelo Pentágono", informou o New York Times em abril de 2011. “Mas, enquanto as autoridades estadunidenses e outras pessoas olham para as revoltas da Primavera Árabe, estão vendo que as campanhas de construção da democracia dos Estados Unidos tiveram um papel maior no fomento de protestos do que se sabia anteriormente, com os principais líderes dos movimentos sendo treinados pelos gringos em campanha, organização através de novas ferramentas de mídia e monitoramento de eleições". Os treinamentos eram carregados de conteúdo político e foram vistos como uma ameaça pelo Egito, Iêmen e Bahrein – todos os quais apresentaram queixas ao Departamento de Estado para parar de se intrometer em seus assuntos internos e até impediram as autoridades gringas de entrar em seus países.97

Um líder político jovem egípcio que participou das sessões de treinamento do Departamento de Estado dos EUA e depois liderou protestos no Cairo disse ao New York Times: “Aprendemos a organizar e construir coalizões. Isso certamente ajudou durante a revolução.” Um outro ativista jovem, que havia participado da revolta no Iêmen, estava igualmente entusiasmado com o treinamento em mídia social do Departamento de Estado: "Isso me ajudou muito porque eu costumava pensar que a mudança só poderia ocorrer pela força e pelas armas".

A equipe do Projeto Tor esteve em alguns desses treinamentos, participando de uma série de sessões do Arab Blogger no Iêmen, Tunísia, Jordânia, Líbano e Bahrain, onde Jacob Appelbaum ensinou a ativistas da oposição como usar o Tor para contornar a censura do governo.98 “Hoje foi fantástico... realmente um fantástico encontro no mundo árabe! É esclarecedor e uma honra ter sido convidado. Eu realmente tenho que recomendar visitar Beirute. O Líbano é um lugar incrível. Pessoas amigáveis, boa comida, música intensa, táxis insanos”, tuitou Appelbaum após um evento de treinamento para blogueiros árabes em 2009, acrescentando: “Se você gostaria de ajudar o Tor, inscreva-se e ajude a traduzir o software do Tor para o árabe.”99

Mais tarde, os ativistas colocaram em prática as habilidades ensinadas nessas sessões de treinamento durante a Primavera Árabe, contor-

nando os bloqueios da Internet que seus governos criaram para impedir que usassem as mídias sociais para organizar protestos. “Não haveria acesso ao Twitter ou Facebook em alguns desses lugares se não houvesse o Tor. De repente, apareceram todos esses dissidentes explodindo sob seus narizes e, então, veio uma revolução”, disse mais tarde Nasser Weddady, um importante ativista da Primavera Árabe da Mauritânia, à Rolling Stone. Weddady, que havia participado das sessões de treinamento do Projeto Tor e que havia traduzido para o árabe um guia amplamente divulgado sobre como usar a ferramenta, creditou-a por ajudar a manter vivas as revoltas da Primavera Árabe. “O Tor fez com que os esforços do governo fossem completamente fúteis. Eles simplesmente não sabiam como combater esse movimento. ”100

Pode-se dizer que o Projeto Tor foi um grande sucesso. Ele havia se transformado em uma poderosa ferramenta de política externa – uma arma cibernética de poder brando, com múltiplos usos e benefícios. Escondeu espiões e agentes militares na Internet, permitindo que eles realizassem suas missões sem deixar rastros. Foi usado pelo governo dos EUA como uma arma persuasiva de mudança de regime, um pé de cabra digital que impedia os países de exercer controle soberano sobre sua própria infraestrutura de Internet. Contraintuitivamente, o Tor também surgiu como um ponto focal para organizações e ativistas de privacidade antigovernamentais, um enorme sucesso cultural que tornou o Tor muito mais eficaz para seus apoiadores do governo, atraindo fãs e ajudando a proteger o projeto de qualquer crítica.

Mas o Tor era apenas o começo.

A Primavera Árabe forneceu ao governo dos EUA a confirmação sobre aquilo que estava procurando. As mídias sociais, combinadas com tecnologias como Tor, poderiam ser usadas para trazer grandes massas de pessoas para as ruas e até provocar revoluções. Diplomatas em Washington chamaram isso de "promoção da democracia". Os críticos chamam isso de mudança de regime.101 Mas não importava como é chamado. O governo dos EUA viu que poderia aproveitar a Internet para semear discórdia e inflamar a instabilidade política em países que considerava hostil aos seus interesses. Para o bem ou para o mal, ele poderia fazer das mídias sociais uma arma e usá-las para provocar insurgências. E os EUA queriam mais.102

Após a Primavera Árabe, o governo dos EUA direcionou ainda mais recursos para as tecnologias do projeto Internet Freedom. O plano era ir além do Projeto Tor e lançar todo tipo de ferramentas de criptografia para alavancar o poder das mídias sociais para ajudar ativistas estrangeiros a criar movimentos políticos e organizar protestos: aplicativos de bate-papo criptografados e sistemas operacionais ultrasseguros projetados para impedir que os governos espionassem ativistas, plataformas de denúncias anônimas que podem ajudar a expor a corrupção do governo e redes sem fio que podem ser implantadas instantaneamente em qualquer lugar do mundo para manter os ativistas conectados, mesmo que seu governo desligue a Internet.103

Estranhamente, esses esforços estavam prestes a obter um grande aumento de credibilidade de uma fonte improvável: um contratado da NSA chamado Edward Snowden.

Alianças estranhas

Os anos pós-WikiLeaks foram bons para o Projeto Tor. Com os contratos governamentais em andamento, Roger Dingledine expandiu a folha de pagamento, adicionando uma equipe dedicada de desenvolvedores e gerentes que viram seu trabalho em termos messiânicos: liberar a Internet da vigilância do governo.104

Jacob Appelbaum também estava indo bem. Alegando que o assédio do governo dos EUA era demais para suportar, ele passou a maior parte do tempo em Berlim em uma espécie de exílio auto-imposto. Lá, ele continuou a fazer o trabalho para o qual Dingledine o havia contratado. Viajou pelo mundo treinando ativistas políticos e persuadindo técnicos e hackers a se juntarem como voluntários do Tor. Ele também fez vários projetos paralelos, alguns dos quais obscureceram a linha entre ativismo e coleta de informações. Em 2012, viajou para a Birmânia, país alvo de longa data dos esforços de mudança de regime do governo dos EUA.105 O objetivo da viagem era investigar o sistema de Internet do país e coletar informações sobre sua infraestrutura de telecomunicações, informações que foram então usadas para montar um relatório do

governo para formuladores de políticas e "investidores internacionais" interessados em penetrar no mercado de telecomunicações recentemente desregulamentado da Birmânia.106

Appelbaum continuou a receber um alto salário de cinco dígitos de Tor, um terceirizado governamental financiado quase exclusivamente por subsídios militares e do setor de inteligência. Mas, para o público, ele era um super-herói da vida real fugindo do Estado de vigilância dos EUA – agora escondido em Berlim, o centro nervoso da cena global de hackers, conhecido por sua mistura nerd de machismo, hackathons noturnos, uso de drogas e troca de parceiros. Ele era membro da elite da Liberdade na Internet, defendida pela União Estadunidense das Liberdades Civis e pela Electronic Frontier Foundation, ocupou um assento no conselho da Fundação Liberdade da Imprensa criada pelo fundador do eBay, Pierre Omidyar, e ocupou um cargo consultivo no Centro de Jornalismo Investigativo de Londres. Sua fama e status de rebelde só tornaram seu trabalho como armador do Tor mais eficaz.

Em Berlim, Appelbaum teve outra oportunidade de sorte para o Projeto Tor. Em 2013, sua boa amiga e às vezes amante Laura Poitras, uma documentarista estadunidense que também vivia na capital alemã em exílio auto-imposto, foi contatada por uma fonte misteriosa que lhe disse que tinha acesso às joias da coroa da Agência Nacional de Segurança: documentos que estourariam totalmente o aparato de vigilância dos EUA.107 Poitras aproveitou o conhecimento de Appelbaum sobre sistemas de Internet para elaborar uma lista de perguntas para examinar o possível denunciador e garantir que ele realmente fosse o técnico da NSA que alegava ser. Essa fonte acabou sendo Edward Snowden.108

Desde o início, o Projeto Tor ficou no centro da história de Snowden. O endosso e a promoção do denunciador apresentaram o projeto a uma audiência global, aumentando a base mundial de usuários de Tor de um milhão para seis milhões quase da noite para o dia e injetando-a no coração de um crescente movimento de privacidade. Na Rússia, onde o BBG e Dingledine haviam tentado recrutar ativistas para a implantação do Tor, mas falhado, o uso do software aumentou de vinte mil conexões diárias para algo em torno de duzentos mil.109

Durante uma campanha promocional para o Projeto Tor, Snowden disse:

> Sem o Tor, as ruas da Internet se tornam como as ruas de uma cidade muito vigiada. Há câmeras de vigilância em todos os lugares e, se o adversário simplesmente levar tempo suficiente, ele poderá rebubinar as fitas e ver tudo o que você fez. Com o Tor, temos espaços e vidas particulares, onde podemos escolher com quem queremos nos associar e como, sem ter o medo de como isso poderá ser visto caso seja alvo de abuso por parte do governo. O projeto do sistema Tor é estruturado de tal maneira que, mesmo que o governo dos EUA quisesse subvertê-lo, ele não poderia.

Snowden não falou sobre o contínuo financiamento do Tor por parte do governo, nem abordou uma aparente contradição: por que o governo dos EUA financiaria um programa que supostamente limitava seu próprio poder.111

Quaisquer que fossem os pensamentos particulares de Snowden sobre o assunto, seu endosso deu ao Tor o maior selo de aprovação possível. Era como uma Medalha de Valor de Hacker. Com o apoio de Snowden, ninguém sequer pensou em questionar a boa fé radical do Tor contra o governo.

Para alguns, Edward Snowden era um herói. Para outros, ele era um traidor que merecia ser executado. Funcionários da NSA alegaram que ele havia causado danos irreparáveis à segurança do país, e todas as agências de inteligência e seus contratados passaram a investir em programas dispendiosos de "ameaças internas" projetados para espionar os funcionários e garantir que outro Edward Snowden nunca aparecesse novamente. Alguns pediram para trazê-lo de volta através de um sequestro feito por um esquadrão de elite; outros, como Donald Trump, pediram que ele fosse assassinado. Anatoly Kucherena, a advogada russa de Snowden, alegou que a vida do denunciador estava em perigo. "Existem ameaças muito reais à vida dele", disse ele a um repórter.

De fato, muito ódio e má fé foram apontados na direção de Snowden, mas para aqueles que dirigem a ala do Internet Freedom do aparelho de inteligência militar dos EUA, seu abraço à cultura Tor e de criptografia não poderia ter chegado a um momento melhor.

No início de janeiro de 2014, seis meses após os vazamentos de Snowden, o Congresso aprovou a Lei de Apropriações Consolidadas,

um projeto de lei federal ampla. Escondido nas cerca de mil e quinhentas páginas do projeto, havia uma pequena provisão que dedicou US $ 50,5 milhões à expansão do arsenal do Internet Freedom financiado do governo dos EUA. Os fundos deveriam ser divididos igualmente entre o Departamento de Estado e o Conselho de Governadores de Radiodifusão.113

Embora o Congresso tenha fornecido fundos durante anos para vários programas anticensura, essa foi a primeira vez que orçou dinheiro especificamente para o Internet Freedom. A motivação para essa expansão surgiu na Primavera Árabe. A ideia era garantir que o governo dos EUA mantivesse sua vantagem tecnológica na corrida armamentista de censura que começou no início dos anos 2000, mas os fundos também estavam sendo usados para o desenvolvimento de uma nova geração de ferramentas destinadas a alavancar o poder da Internet para ajudar ativistas estrangeiros de oposição a se organizarem em movimentos políticos coesos.114

O corte de US $ 25,25 milhões do BBG em dinheiro mais que dobrou o orçamento de tecnologia anticensura da agência em relação ao ano anterior, e o BBG canalizou o dinheiro para o Open Technology Fund, 115 uma nova organização criada na Radio Free Asia para financiar as tecnologias de liberdade da Internet em o rastro da primavera árabe.116

Inicialmente lançada pela Agência Central de Inteligência (CIA) em 1951 para atingir a China com transmissões de rádio anticomunistas, a Radio Free Asia havia sido fechada e relançada várias vezes ao longo de sua história.117 Em 1994, após a queda da União Soviética, ela reapareceu, ao estilo "Exteerminador do Futuro", como uma empresa privada sem fins lucrativos, totalmente controlada e financiada pelo Conselho de Governadores de Radiodifusão (BBG).118 Focada em estimular o sentimento anticomunista na Coreia do Norte, Vietnã, Laos, Camboja, Birmânia e China, a Radio Free Asia desempenhou um papel central na corrida armamentista anticensura do governo dos EUA que vinha se formando desde que o BBG começou a promover suas transmissões na China através da Internet. A Radio Free Asia teve problemas em lançar suas táticas secretas da Guerra Fria.119 Na Coreia do Norte, contrabandeava rádios minúsculas e enterrava celulares logo na fronteira do país

com a China, para que sua rede de informantes pudesse relatar as condições dentro do país. Após a morte de Kim Jong Il em 2011, a rádio "entrou em modo de emergência 24 horas por dia, 7 dias por semana" para transmitir sem parar a cobertura das mortes na Coréia do Norte, na esperança de provocar um levante em massa. Os executivos da Radio Free Asia esperavam que, pouco a pouco, o fluxo de propaganda anticomunista direcionada ao país provocasse o colapso do governo.120

Agora, com o Open Technology Fund (OTF), a Radio Free Asia supervisionou o financiamento dos programas estadunidenses do Internet Freedom. Para administrar as operações diárias do OTF, a Radio Free Asia contratou Dan Meredith, um jovem técnico que trabalhava na Al-Jazeera no Catar e que estava envolvido nas iniciativas de anticensura do Departamento de Estado desde 2011.121 Com barba desalinhada e cabelo loiro desarrumado de surfista, Meredith não era uma figura típica do Departamento de Estado. Ele era fluente na linguagem cypherpunk-hacktivista e fazia parte da comunidade de privacidade que procurava conquistar. Em resumo, ele não era o tipo de pessoa que você esperaria executar um projeto do governo com grandes implicações na política externa.

Com ele no comando, o OTF dedicou muito esforço em propaganda. Externamente, parecia uma organização ativista de privacidade, não uma agência governamental. Produziu vídeos do YouTube de 8 bits sobre sua missão de usar "fundos públicos para apoiar projetos de liberdade na Internet" e promover "direitos humanos e sociedades abertas". Seu layout da web mudou constantemente para refletir os padrões de design mais modernos.

Mas, se o OTF parecia mal feito, também era extremamente bem conectado. A organização foi apoiada por uma equipe repleta de estrelas – de autores de ficção científica mais vendidos a executivos do Vale do Silício e célebres especialistas em criptografia. Seu conselho consultivo incluía grandes nomes da Columbia Journalism School, da Electronic Frontier Foundation, da Ford Foundation, da Open Society Foundations, da Google, do Slack e da Mozilla. Andrew McLaughlin, ex-chefe da equipe de relações públicas da Google que contratou Al Gore para convencer um senador do estado da Califórnia a cancelar a legislação que regulamentaria o programa de verificação de e-mail do Gmail, fazia

parte da equipe do OTF. O mesmo aconteceu com Cory Doctorow, uma autora de ficção científica para jovens adultos, que foi sucesso de vendas, cujos livros sobre a vigilância de um governo totalitário foram lidos e admirados por Laura Poitras, Jacob Appelbaum, Roger Dingledine e Edward Snowden.122 Doctorow era uma importante personalidade no movimento de criptografia que podia encher auditórios enormes em conferências sobre privacidade. Ela endossou publicamente a missão do Internet Freedom propagandeada pelo OTF. "Tenho orgulho de ser um consultor voluntário do OTF", ela twittou.

Por trás dessa superfície moderna e conectada, a BBG e a Radio Free Asia construíram uma incubadora verticalmente integrada para as tecnologias desenvolvidas pelo Internet Freedom, despejando milhões em projetos grandes e pequenos, incluindo de tudo, desde escapar da censura até ajudar na organização política, protestos e construção de movimentos. Com seus bolsos cheios de dinheiro e seu recrutamento de grandes ativistas da privacidade, o Open Technology Fund não se inseriu apenas no movimento da privacidade. De muitas maneiras, foi o próprio movimento da privacidade.

Ele estabeleceu programas acadêmicos e bolsas lucrativas, pagando US $ 55.000 por ano para estudantes de graduação, ativistas da privacidade, tecnólogos, criptógrafos, pesquisadores de segurança e cientistas políticos para estudar “o clima de censura da Internet nos antigos estados soviéticos”, investigando a “capacidade técnica” do Grande Firewall da China e acompanhar o "uso de servidores de comando e controle de spyware opressivos por governos repressivos".123

Ele expandiu o alcance e a velocidade da rede do Projeto Tor e direcionou vários milhões de dólares para a criação de nós de saída da rede Tor de alta largura de banda no Oriente Médio e Sudeste Asiático, ambas regiões de alta prioridade para a política externa dos EUA.124 Ele investiu em aplicativos de bate-papo criptografados, sistemas operacionais ultrasseguros supostamente impermeáveis a hackers e iniciativas de e-mail seguro projetadas para dificultar a espionagem dos governos nas comunicações dos ativistas. Ele financiou ferramentas anônimas do tipo WikiLeaks para delatores que denunciavam a corrupção de seus governos. Fez parceria com o Departamento de Estado em vários projetos de "rede de malha" e "Internet-numa-caixa" projetados para manter

os ativistas conectados, mesmo que seu governo tentasse desativar as conexões locais à Internet.125 Forneceu uma infraestrutura de "nuvem segura" com nós de servidores em todo o mundo para hospedar projetos do Internet Freedom, operou um "laboratório jurídico" que oferecia proteção legal aos donatários no caso de surgir algum imprevisto e até criou um "Fundo de Resposta Rápida" para fornecer suporte emergencial a projetos do Internet Freedom considerados vitais e que exigiam implantação imediata.126

O Projeto Tor permaneceu como o aplicativo de privacidade mais conhecido, financiado pelo Open Technology Fund, mas rapidamente se juntou a outro: o Signal, um aplicativo de mensagens criptografadas para celulares iPhone e Android.

O Signal foi desenvolvido pela Open Whisper Systems, uma corporação com fins lucrativos administrada por Moxie Marlinspike, um criptógrafo alto e esbelto com a cabeça cheia de dreadlocks. Marlinspike era um velho amigo de Jacob Appelbaum e jogava um jogo "radical" semelhante. Ele permaneceu enigmático sobre seu nome e identidade reais, contou histórias de ser alvejado pelo FBI e passou seu tempo livre navegando e surfando no Havaí. Ele ganhou um bom dinheiro vendendo sua start-up de criptografia para o Twitter e trabalhou com o Departamento de Estado dos EUA em projetos do Internet Freedom desde 2011. Entretanto, se apresentou como um anarquista agressivo que lutava contra o sistema. Seu site pessoal chamava-se thinkcrime.org – uma referência ao livro "1984" de George Orwell, que parecia um pouco irônico, já que ele estava recebendo muito dinheiro – quase US $ 3 milhões – do Big Brother para desenvolver seu aplicativo de privacidade.127

Sinal foi um enorme sucesso. Jornalistas, ativistas da privacidade e criptógrafos saudaram o Signal como uma ferramenta indispensável para a privacidade na Internet. Foi um complemento para o Tor na era dos telefones móveis. Enquanto o Tor tornava a navegação anônima, o Sinal codificava as chamadas de voz e o texto, impossibilitando os governos de monitorar a comunicação. Laura Poitras deu dois joinhas aprovando sua segurança, indicando-o como uma poderosa ferramenta popular de criptografia e disse a todos para usá-la todos os dias. As pessoas da ACLU alegaram que o Signal fazia agentes federais chorarem.128 A Electronic Frontier Foundation adicionou o Signal ao

lado do Tor ao seu guia de Autodefesa em vigilância. A Fight for the Future, uma organização ativista da privacidade financiada pelo Vale do Silício, descreveu o Signal e o Tor como sendo “à prova de NSA” e instou as pessoas a usá-los.

Edward Snowden foi o maior e mais famoso impulsionador do combo e foi repetidamente ao Twitter para dizer a seus três milhões de seguidores que ele usava Signal e Tor todos os dias, e que eles deveriam fazer o mesmo para se proteger da vigilância do governo. “Use Tor. Use Signal”, ele twittou.129

Com promoções como essas, o Signal rapidamente se tornou o aplicativo preferido por ativistas políticos em todo o mundo. Egito, Rússia, Síria e até os Estados Unidos – milhões baixaram o Signal, e ele se tornou o principal aplicativo de comunicação para aqueles que esperavam evitar a vigilância policial. Coletivos feministas, manifestantes anti-presidente Donald Trump, comunistas, anarquistas, organizações radicais de direitos dos animais, ativistas do Black Lives Matter – todos afluiram para o Signal. Muitos estavam atendendo ao conselho de Snowden: “Organize. Compartimentalize para limitar o comprometimento. Criptografe tudo, desde chamadas de telefone a mensagens de texto (use o Signal como primeiro passo).”130

O Vale do Silício também ganhou dinheiro com os gastos com o OTF do Internet Freedom. O Facebook incorporou o protocolo de criptografia subjacente do Signal no WhatsApp, o aplicativo de mensagens mais popular do mundo. A Google seguiu o exemplo, incorporando a criptografia de Signal aos aplicativos de mensagens de texto e vídeo Allo e Duo.131 Foi uma jogada inteligente porque logo em seguida os elogios pulularam. “Em outras palavras, os novos recursos de segurança de Allo e Duo são os primeiros passos da Google em direção a um futuro totalmente criptografado, não o tipo de movimentos ousados para elevar a privacidade acima do lucro ou da política que alguns de seus concorrentes já adotaram”, escreveu Andy Greenberg da Wired. "Mas para uma empresa criada com base em um modelo de coleta de dados que geralmente é fundamentalmente contrário à privacidade, os pequenos passos são melhores do que nenhum".

Se você recuasse para examinar a cena, todo o cenário desse novo movimento de privacidade, todo ele criado a partir do Internet Freedom,

pareceria absurdo. As organizações da era da Guerra Fria desmembradas da CIA agora financiam o movimento global contra a vigilância do governo? Google e Facebook, empresas que administravam redes privadas de vigilância e trabalhavam lado a lado com a NSA, estavam agora implantando tecnologia de privacidade financiada pelo governo para proteger seus usuários da vigilância governamental? Ativistas da privacidade trabalham com o Vale do Silício e o governo dos EUA para combater a vigilância do governo – e com o apoio do próprio Edward Snowden?

É muito difícil imaginar que, na década de 1960, os estudantes radicais de Harvard e MIT tivessem pensado em fazer uma parceria com a IBM e o Departamento de Estado para protestar contra a vigilância do Pentágono. Se o fizessem, provavelmente teriam sido ridicularizados e escorraçados para fora do campus, tachados de tolos ou – pior – como policiais infiltrados. Naquela época, as linhas eram claras, mas hoje todas essas conexões são obscuras. A maioria das pessoas envolvidas no ativismo pela privacidade não conhece os esforços contínuos do governo dos EUA para armar o movimento pela privacidade, nem avaliam os motivos do Vale do Silício nessa luta. Sem esse conhecimento, é impossível entender tudo. Então, falar sobre o envolvimento do governo no espaço da privacidade parece algo inventado por um paranoico.

De qualquer forma, com o apoio de alguém tão célebre como Edward Snowden, poucos tiveram qualquer motivo para questionar por que aplicativos como Signal e Tor existiam ou qual o objetivo maior que eles serviam. Era mais fácil e simples colocar sua confiança no aplicativo e acreditar na ideia de que os Estados Unidos ainda tinham uma sociedade civil saudável, onde as pessoas poderiam se reunir para financiar ferramentas que contrabalançassem o poder de vigilância do Estado. Isso serviu bem aos patrocinadores do Internet Freedom.

Depois de Edward Snowden, o OTF triunfou. O fundo não mencionou o denunciador pelo seu nome em seus materiais promocionais, mas lucrou com a cultura de criptografia que ele promoveu e se beneficiou com o endosso direto das ferramentas de criptografia que financiava. Ostentava que sua parceria com o Vale do Silício e com os respeitados ativistas da privacidade significava que centenas de milhões de pessoas poderiam usar as ferramentas de privacidade que o governo dos

EUA trouxera para o mercado. E o OTF prometeu que isso era apenas um começo: "Ao alavancar os efeitos das redes sociais, esperamos expandir para um bilhão de usuários regulares, aproveitando as ferramentas apoiadas pela OTF e as tecnologias do Internet Freedom até 2015".132

Um falso senso de segurança

Embora o Projeto Tor, Signal e outros aplicativos de criptografia financiados pelo governo dos EUA tenham sido louvados a torto e a direito, uma análise mais profunda mostrou que eles não eram tão seguros ou impermeáveis à penetração do governo como seus defensores alegavam. Talvez nenhuma história exemplifique melhor as falhas na segurança criptográfica impenetrável do que a de Ross Ulbricht, também conhecido como Dread Pirate Roberts, o arquiteto do Silk Road.

Após sua fundação em 2012, o Silk Road cresceu rapidamente e parecia ser um lugar onde criminosos organizados podiam se esconder à vista de todos – até que não fosse. Em outubro de 2013, quatro meses depois que Edward Snowden saiu do esconderijo e endossou o Tor, um texano nativo de 29 anos chamado Ross Ulbricht foi preso em uma biblioteca pública de São Francisco. Ele foi acusado de ser Dread Pirate Roberts e foi acusado de lavagem de dinheiro, tráfico de narcóticos, hackeamento e, acima de tudo, assassinato.

Quando seu caso foi a julgamento um ano depois, a história do Projeto Tor assumiu um tom diferente, demonstrando o poder do marketing e da ideologia sobre a realidade.

As comunicações internas e os diários recuperados pelos investigadores do laptop criptografado de Ulbricht mostraram que ele tinha certeza de estar totalmente protegido pelo Tor. Ele acreditava no que havia sido dito sobre o Tor, coisas que eram apoiadas por Edward Snowden e promovidas por Jacob Appelbaum. Ele acreditava que tudo o que fazia na obscuridade da dark web não o afetaria no mundo real – ele acreditava tanto que não apenas construiu um negócio ilegal de drogas

em cima dele, mas também encomendou a morte de quem ameaçou seus negócios. Sua crença no poder do Projeto Tor de criar uma ilha cibernética completamente impenetrável à lei persistiu mesmo diante de fortes evidências contrárias.

A partir de março de 2013, o Silk Road foi atingido por vários ataques que travaram o software do servidor oculto do Tor que permitia que ele estivesse na dark web. Repetidamente, o endereço IP real do site vazava para o público, uma falha crítica que poderia ter tornado trivial para a polícia rastrear a identidade real de Dread Pirate Roberts.133 De fato, os atacantes não apenas pareciam saber o endereço IP dos servidores do Silk Road, mas também alegaram ter hackeado os dados dos usuários do site e exigiram que Dread Pirate Roberts os pagasse para ficarem quietos.

Parecia que a festa tinha acabado. O Tor falhou. Se ele não podia proteger sua identidade de um grupo de extorsionistas, como se sairia contra os recursos quase ilimitados da polícia federal? Mas Ulbricht ainda acreditava. Em vez de encerrar o Silk Road, ele assinou um contrato com os Hells Angels para atacar os extorsionistas, pagando aos motoqueiros $ 730.000 para matar seis pessoas. "Pagamento aos Angels para atacarem chantagistas", escreveu em seu diário em 29 de março de 2013. Três dias depois, outra anotação: "soube que os chantagistas foram executados / script para upload de arquivo foi criado".134 Sua indiferença nasceu da rotina. No início daquele ano, ele já havia pago US $ 80.000 para que um ex-administrador do Silk Road, suspeito de roubar mais de US $ 300.000, fosse morto.135

Surpreendentemente, apenas um mês antes de sua prisão, Ulbricht foi contatado pelos criadores da Atlantis, uma das muitas cópias de mercados de drogas da dark web inspiradas no sucesso do Silk Road. Foi um tipo amigável de contato. Disseram-lhe que a Atlantis estava permanentemente fechando as lojas porque receberam a notícia de um grande buraco na segurança do Tor, e sugeriram que ele fizesse o mesmo. "Recebi uma mensagem de um membro da equipe [da Atlantis] que disse que eles desligaram [seu serviço] por causa de um documento do FBI vazado para eles detalhando vulnerabilidades no Tor", escreveu Ulbricht em seu diário. Surpreendentemente, ele continuou a administrar seu site, confiante de que tudo acabaria bem no final. "Tive uma revela-

ção sobre a necessidade de comer bem, dormir bem e meditar para que eu possa permanecer positivo e produtivo", escreveu ele em 30 de setembro. Um dia depois, ele estava sob custódia federal.

Durante seu julgamento, descobriu-se que o FBI e o Departamento de Segurança Nacional (DHS) haviam se infiltrado no Silk Road quase desde o início. Um agente do DHS chegou a assumir uma conta de administrador sênior do Silk Road, que dava aos agentes federais acesso ao sistema, um trabalho pelo qual Ulbricht pagava ao agente do DHS US $ 1.000 por semana em Bitcoins.136 Ou seja, um dos principais funcionários de Ulbricht era um policial e ele não fazia ideia. Mas foi o endereço IP vazado do Silk Road que levou os agentes do DHS a rastrear a conexão de Ulbricht com um café em San Francisco e, finalmente, com ele.137

Ulbricht confessou ser Dread Pirate Roberts e montar Silk Road. Depois de ser considerado culpado de sete crimes, incluindo lavagem de dinheiro, tráfico de drogas, administração de uma empresa criminosa e fraude de identidade, ele deixou a postura de revolucionário para implorar clemência ao juiz. “Mesmo agora eu entendo o terrível erro que cometi. Tive minha juventude e sei que você deve tirar minha meia-idade, mas por favor, deixe-me desfrutar a velhice. Por favor, deixe uma pequena luz no fim do túnel, uma desculpa para se manter saudável, uma desculpa para sonhar com dias melhores pela frente e uma chance de me redimir no mundo livre antes de conhecer meu criador”, disse ele ao tribunal. A juíza não teve piedade. Ela condenou-o a uma sentença de prisão perpétua, sem a possibilidade de liberdade condicional. E mais anos ainda podem ser adicionados caso ele seja condenado por qualquer um de seus assassinatos por aluguel.

A queda do Silk Road furou a invencibilidade do Tor. Mesmo quando Edward Snowden e organizações como a Electronic Frontier Foundation promoveram o Tor como uma ferramenta poderosa contra o Estado de vigilância dos EUA, esse mesmo Estado de vigilância estava esburacando o Tor.138

Em 2014, o FBI, juntamente com o DHS e as agências policiais europeias, caçaram lojas que imitavam o Silk Road, derrubando cinquenta mercados que vendiam de tudo, de drogas a armas, cartões de crédito e pornografia de abuso infantil em uma cooperação internacional

com o nome de Operação Omynous. Em 2015, uma conjunção internacional de polícias junto com o FBI prendeu mais de quinhentas pessoas ligadas ao Playpen, uma notória rede de pornografia infantil que era executada na nuvem do Tor. Setenta e seis pessoas foram processadas nos Estados Unidos e quase trezentas crianças vítimas de todo o mundo foram resgatadas de seus agressores.139 Esses ataques foram direcionados e extremamente eficazes. Parecia que os policiais sabiam exatamente onde acertar e como fazê-lo.

O que estava acontecendo? Como a polícia havia penetrado no que deveria ser o anonimato de ferro do Tor, forte o suficiente para suportar um ataque da NSA?

Foi difícil obter a confirmação, mas Roger Dingledine do Tor estava convencido de que pelo menos algumas dessas batidas policiais estavam usando uma forma de burlar a segurança do Tor, um exploit, desenvolvida por um grupo da Universidade Carnegie Mellon, na Pensilvânia. Trabalhando sob um contrato do Pentágono, os pesquisadores descobriram uma maneira fácil e barata de invadir a rede super-segura de Tor com apenas US $ 3.000 em equipamentos de informática.140 Dingledine acusou os pesquisadores de vender esse método ao FBI.

“O Projeto Tor descobriu mais sobre o ataque do ano passado feito pesquisadores da Carnegie Mellon ao subsistema de serviços ocultos. Aparentemente, esses pesquisadores foram pagos pelo FBI para atacar os usuários de serviços ocultos em uma ampla varredura e, em seguida, vasculhar seus dados para encontrar pessoas a quem eles poderiam acusar de crimes”, Dingledine escreveu em um post agressivo em novembro de 2015, dizendo que tinha sido informado que o FBI pagou pelo menos US $ 1 milhão por esses serviços.141

Era estranho ver Dingledine ficar bravo com os pesquisadores recebendo dinheiro da polícia quando seu próprio salário era pago quase inteiramente por contratos militares e ligados à inteligência. Mas Dingledine fez algo ainda mais estranho. Ele acusou os pesquisadores da Carnegie Mellon de violar os padrões acadêmicos da pesquisa ética, por trabalharem com a polícia. Ele então anunciou que o Projeto Tor publicaria diretrizes para pessoas que gostariam de hackear ou invadir o Tor para fins "acadêmicos" e "pesquisas independentes" no futuro, mas de

maneira ética obtendo primeiro o consentimento das pessoas que estão sendo hackeadas.

"Pesquisa sobre dados humanos é pesquisa humana. Ao longo do século passado, fizemos grandes avanços éticos nas pesquisas que realizamos em pessoas, mas de outros domínios", estava escrito em um rascunho do guia "Pesquisa Ética no Tor". "Devemos garantir que a pesquisa sobre privacidade seja pelo menos tão ética quanto a pesquisa em outros campos". Os requisitos estabelecidos neste documento incluem seções como: "Colete apenas dados aceitáveis para publicação" e "Colete apenas os dados necessários: pratique a minimização de dados".142

Embora demandas como essas façam sentido em um contexto de pesquisa, elas foram desconcertantes quando aplicadas ao Tor. Afinal, Tor e seus patrocinadores, incluindo Edward Snowden, apresentaram o projeto como uma ferramenta de anonimato de fato que resistia aos invasores mais poderosos. Se era tão frágil que exigia que os pesquisadores acadêmicos cumprissem um código de honra ético para evitar a reversão da anonimização do nome de usuários sem o consentimento deles, como poderia dar conta do FBI ou da NSA ou das dezenas de agências de inteligência estrangeiras, da Rússia à China e Austrália, que poderiam quer perfurar seus sistemas de anonimato?

Em 2015, quando li pela primeira vez essas declarações do Projeto Tor, fiquei chocado. Isso foi nada menos do que uma admissão velada de que Tor era inútil para garantir o anonimato e que exigia que os atacantes se comportassem "eticamente" para que continuassem seguros. Deve ter sido um choque ainda maior para os crentes cypherpunk como Ross Ulbricht, que confiavam em Tor para administrar seus negócios na Internet altamente ilegais e que agora está preso pelo resto da vida.

A briga de Tor com os pesquisadores da Universidade Carnegie Mellon revelou outra dinâmica confusa. Enquanto uma parte do governo federal – que incluía o Pentágono, o Departamento de Estado e o Conselho de Governadores de Radiodifusão – financiava o desenvolvimento contínuo do Projeto Tor, outra ala desse mesmo governo federal – que incluía o Pentágono, o FBI e, possivelmente, outras agências – estava trabalhando tão arduamente para quebrá-lo.

O que estava acontecendo? Por que o governo estava trabalhando com propósitos diferentes? Uma parte simplesmente não sabia o que a outra estava fazendo?

Curiosamente, os documentos da NSA de Edward Snowden forneceram o início de uma resposta. Eles mostraram que vários programas da NSA poderiam ultrapassar as defesas de Tor e possivelmente até desvendar o tráfego da rede em "larga escala". Eles também mostraram que a agência de espionagem via o Tor como uma ferramenta útil que concentrava "alvos" em potencial em um local conveniente. 143 Em uma palavra, a NSA via Tor como um engodo.

Em outubro de 2013, o Washington Post informou sobre vários desses programas, revelando que a NSA trabalhava para quebrar o Tor desde pelo menos 2006, no mesmo ano em que Dingledine assinou seu primeiro contrato com o BBG.144 Um desses programas, codinome EGOTISTICALGIRAFFE, foi usado ativamente para rastrear a identidade dos agentes da Al-Qaeda. "Um documento fornecido por Snowden incluía uma troca interna entre hackers da NSA, na qual um deles disse que o Centro de Operações Remotas da agência era capaz de atingir qualquer pessoa que visitasse um site da Al-Qaeda usando o Tor".145 Outro conjunto de documentos, tornado público pelo The Guardian no mesmo mês, mostrou que a agência via o Tor de uma maneira positiva. “A massa crítica de alvos usa Tor. Assustá-los pode ser contraproducente. Nunca obteremos 100% de desanonimização, mas não precisamos fornecer IPs verdadeiros para todos os destinos sempre que eles usarem o Tor”, explicou uma apresentação da NSA em 2012.146 Seu argumento era claro: pessoas com algo a esconder – terroristas, espiões estrangeiros ou traficantes de drogas – acreditavam na promessa de anonimato de Tor e usavam a rede em massa. Ao fazer isso, as pessoas prosseguiram com uma falsa sensação de segurança, fazendo coisas na rede que nunca fariam em campo aberto, enquanto ajudavam a colocar uma marca em si mesmas para uma vigilância adicional.147

Isso não foi surpreendente. A lição maior dos documentos da NSA de Snowden foi que quase nada aconteceu na Internet sem passar por algum tipo de escuta do governo dos EUA. Naturalmente, as ferramentas populares usadas pelo público que prometiam ofuscar e ocultar as

comunicações das pessoas eram alvos, independentemente de quem as financiava.

Quanto às outras ferramentas de criptografia financiadas pelo governo dos EUA? Elas sofreram armadilhas de segurança e engodos semelhantes. Pegue o Signal, por exemplo, o aplicativo criptografado que Edward Snowden disse que usava todos os dias. Comercializado como uma ferramenta de comunicação segura para ativistas políticos, o aplicativo tinha recursos estranhos incorporados desde o início. Exigia que os usuários vinculassem seu número de telefone celular ativo e carregassem todo o seu catálogo de endereços nos servidores do Signal – ambos recursos questionáveis de uma ferramenta projetada para proteger ativistas políticos da polícia em países autoritários. Na maioria dos casos, o número de telefone de uma pessoa era efetivamente a identidade dessa pessoa, vinculada a uma conta bancária e endereço residencial. Enquanto isso, o catálogo de endereços de uma pessoa continha amigos, colegas, ativistas políticos e organizadores, praticamente toda a rede social da pessoa.

Além disso, havia o fato de o Signal ser executado nos servidores da Amazon, o que significava que todos os seus dados estavam disponíveis para um parceiro no programa de vigilância PRISM da NSA. Igualmente problemático, o Signal precisava da Apple e da Google para instalar e executar o aplicativo nos celulares das pessoas. Ambas as empresas também eram e, tanto quanto sabemos, são parceiras do PRISM. "A Google geralmente tem acesso privilegiado [root] ao telefone, por questão de integridade", escreve Sander Venema, desenvolvedor respeitado e instrutor de segurança em tecnologia, em um post no blog explicando por que ele não recomenda mais que as pessoas usem o Signal para bate-papo criptografado. “A Google ainda está cooperando com a NSA e outras agências de inteligência. O PRISM ainda continua operando. Tenho certeza de que a Google poderia fornecer uma atualização ou versão especialmente modificada do Signal para alvos específicos de vigilância, e eles não saberiam que instalaram um malware em seus telefones.”148

Igualmente estranho foi o modo como o aplicativo foi projetado para facilitar a qualquer pessoa que monitora o tráfego da Internet sinalizar as pessoas que usam o Signal para se comunicar. Tudo o que o FBI

ou, digamos, os serviços de segurança egípcios ou russos tinham que fazer era vigiar os telefones celulares que faziam ping em um servidor da Amazon em particular usado pelo Signal, e era trivial isolar ativistas da população geral de smartphones. Portanto, embora o aplicativo tenha criptografado o conteúdo das mensagens das pessoas, também as marcou com um sinal vermelho intermitente: “Siga-me. Eu tenho algo a esconder. (De fato, os ativistas que protestaram na Convenção Nacional Democrata na Filadélfia em 2016 me disseram que ficaram perplexos com o fato de a polícia parecer conhecer e antecipar todos os seus movimentos, apesar de terem usado o Signal para se organizar.)149

O debate sobre o projeto técnico do Signal era discutível de qualquer maneira. Os vazamentos de Snowden mostraram que a NSA havia desenvolvido ferramentas que podiam capturar tudo o que as pessoas faziam em seus smartphones, o que provavelmente incluía textos enviados e recebidos pelo Signal. No início de março de 2017, o WikiLeaks publicou um grande conjunto de documentos sobre ferramentas de hackers da CIA que confirmaram o inevitável. A agência trabalhou com a NSA e com outros "terceirizadas do setor de armas cibernéticas" para desenvolver ferramentas de hackers direcionadas aos smartphones, permitindo que ela contornasse a criptografia do Signal e de outros aplicativos de bate-papo criptografados, incluindo o WhatsApp do Facebook.150 “O ramo de dispositivos móveis (MDB) da CIA desenvolveu vários ataques para invadir e controlar remotamente os smartphones populares. Os telefones infectados podem ser instruídos a enviar à CIA a localização geográfica do usuário, as comunicações de áudio e texto, além de ativar secretamente a câmera e o microfone do telefone”, explicou um comunicado de imprensa do WikiLeaks. "Essas técnicas permitem que a CIA ignore a criptografia do WhatsApp, Signal, Telegram, Wiebo, Confide e Cloackman, invadindo os telefones 'inteligentes' em que eles operam e coletando o tráfego de áudio e mensagens antes do ocorrer a criptografia."

A divulgação dessas ferramentas de hackers mostrou que, no final, a criptografia do Signal realmente não importava, não quando a CIA e a NSA possuíam o sistema operacional subjacente e podiam pegar o que quisessem antes da aplicação dos algoritmos de criptografia ou ofuscação. Essa falha envolvia muito mais do que o Signal e era aplicada a todos os tipos de tecnologia de criptografia em todos os tipos de

sistemas de computadores de consumo. Certamente, os aplicativos de criptografia podem funcionar contra oponentes de baixo nível quando usados por um analista de inteligência do exército treinado como o soldado Chelsea Manning, que usara Tor enquanto estava no Iraque para monitorar fóruns usados por insurgentes sunitas sem revelar sua identidade.151 Esses aplicativos também podem funcionar para alguém com um alto nível de conhecimento técnico – digamos, um hacker astuto como Julian Assange ou um espião como Edward Snowden – que pode usar Signal e Tor combinados com outras técnicas para efetivamente cobrir seus rastros da NSA. Mas, para o usuário médio, essas ferramentas forneciam uma falsa sensação de segurança e ofereciam o oposto de privacidade.

O velho sonho cypherpunk, a ideia de que pessoas comuns podiam usar ferramentas de criptografia populares para criar ilhas cibernéticas livres do controle do governo, estava se mostrando exatamente isso, um sonho.

Guerra de criptografia, quem se beneficia?

Por mais complicado que seja a história, o apoio do governo dos EUA ao projeto Internet Freedom e sua subscrição da cultura de criptografia fazem todo o sentido. A Internet surgiu de um projeto militar da década de 1960 para desenvolver uma arma de informação. Nasceu da necessidade de se comunicar rapidamente, processar dados e controlar um mundo caótico. Hoje, a rede é mais do que uma arma; é também um campo de batalha, um lugar onde operações militares e de inteligência vitais ocorrem. A luta geopolítica mudou para a Internet e o Internet Freedom é uma arma nessa luta.

Se você olhar o todo, o apoio que o Silicon Valley deu ao Internet Freedom também faz sentido. Empresas como Google e Facebook o apoiaram como parte de uma estratégia de negócios geopolítica, uma maneira de pressionar sutilmente os países que fecharam suas redes e mercados para empresas de tecnologia ocidentais. Mas depois que as revelações de Edward Snowden expuseram ao público as práticas desen-

freadas de vigilância do setor privado, o projeto Internet Freedom ofereceu outro benefício poderoso.

Durante anos, a opinião pública se manteve firme contra o modelo de negócios subjacente do Vale do Silício. Pesquisa após pesquisa, a maioria dos estadunidenses manifestou sua oposição à vigilância corporativa e sinalizou apoio ao aumento da regulamentação do setor.152 Isso sempre foi um fator decisivo para o Vale do Silício. Para muitas empresas de Internet, incluindo Google e Facebook, a vigilância é o modelo de negócios. É a base sobre a qual repousa seu poder corporativo e econômico. Separe a vigilância do lucro e essas empresas entrarão em colapso. Limite a coleta de dados e as empresas verão os investidores fugindo e seus preços das ações despencarem.

O Vale do Silício teme uma solução política para a privacidade. O Internet Freedom e a criptografia oferecem uma alternativa aceitável. Ferramentas como Signal e Tor fornecem uma falsa solução para o problema da privacidade, concentrando a atenção das pessoas na vigilância do governo distraindo-as da espionagem privada realizada pelas empresas de Internet que usam todos os dias. O tempo todo, as ferramentas de criptografia dão às pessoas a sensação de que estão fazendo algo para se proteger, criam um sentimento de empoderamento e controle pessoal. E todos esses radicais da criptografia? Bem, eles apenas aprimoram a ilusão, aumentando a impressão de risco e perigo. Com o Signal ou o Tor instalado, de repente o uso de um iPhone ou Android se torna radical. Portanto, em vez de buscarmos soluções políticas e democráticas para a vigilância, terceirizamos nossa política de privacidade para aplicativos com criptografia – softwares criados pelas mesmas entidades poderosas das quais esses aplicativos devem nos proteger.

Nesse sentido, Edward Snowden é como o rosto da marca de uma campanha de estilo de vida consumista rebelde na Internet, como o antigo anúncio da Apple dizendo que ia quebrar o Big Brother. Enquanto bilionários da Internet como Larry Page, Sergey Brin e Mark Zuckerberg criticam a vigilância do governo, defendem a liberdade e adotam Snowden e a cultura de privacidade criptográfica, suas empresas ainda fecham acordos com o Pentágono, trabalham com a NSA e a CIA e continuam a rastrear e perfil de pessoas com fins lucrativos. É o

mesmo velho truque de marketing em tela dividida: a marca pública e a realidade dos bastidores.

O Internet Freedom é vantajoso para todos os envolvidos – todos, exceto os usuários regulares, que confiam sua privacidade a contratados militares, enquanto poderosas empresas do Vale da Vigilância continuam a construir o antigo sonho cibernético militar de um mundo onde todos são observados, previstos e controlados.

Epílogo

Mauthausen, Áustria

A manhã está nítida e ensolarada no final de dezembro de 2015, quando viro à direita em uma pequena estrada rural e entro em Mauthausen, uma pequena cidade medieval no norte da Áustria, a cerca de 50 milhas da fronteira com a República Tcheca. Passo por um aglomerado de prédios baixos e continuo dirigindo por pastos verdes imaculados e lindas fazendas.

Estaciono em uma colina com vista para a cidade. Abaixo está o amplo rio Danúbio. Aglomerados de casas rurais brotam do cume de duas colinas verdes e macias, a fumaça saindo lentamente de suas chaminés. Um pequeno grupo de vacas está pastando, e eu posso ouvir o ruído periódico de um rebanho de ovelhas. Ao longe, as colinas retrocedem em camadas de verde sobre verde, como as escamas de um dragão gigante adormecido. Toda a cena é emoldurada pelos picos brancos e irregulares dos Alpes austríacos.

Mauthausen é um lugar idílico. Calmo, quase mágico. No entanto, dirigi até aqui não para apreciar a vista, mas para me aproximar de algo que só entendi completamente enquanto escrevia este livro.

Hoje, a tecnologia de computadores frequentemente opera sem ser vista, oculta em gadgets, fios, chips, sinais sem fio, sistemas operacionais e softwares. Estamos cercados por computadores e redes, mas mal os notamos. Se pensarmos neles, tendemos a associá-los ao progresso. Raramente paramos para pensar no lado sombrio da tecnologia da informação – todas as maneiras pelas quais ela pode ser usada e abusada para controlar as sociedades, infligir dor e sofrimento. Aqui, neste cenário

bucólico tranquilo, há um monumento esquecido desse poder: o Campo de Concentração de Mauthausen.

Construído em um monte acima da cidade, é surpreendentemente bem preservado: grossas paredes de pedra, torres de guarda, um par de chaminés sinistras ligadas à câmara de gás e ao crematório do campo. Algumas barras de metal pontiagudas ficam penduradas na parede acima dos enormes portões do acampamento, restos de uma águia nazista de ferro gigante que foi derrubada imediatamente após a libertação. Está quieto agora, apenas alguns visitantes solenes. Mas na década de 1930, Mauthausen havia sido um motor econômico vital do plano genocida de Hitler para tornar a Europa e a União Soviética o quintal da sua própria utopia. Começou como uma pedreira de granito, mas rapidamente se transformou no maior complexo de trabalho escravo da Alemanha nazista, com cinquenta subcampos que cobriam a maior parte da Áustria moderna. Aqui, centenas de milhares de prisioneiros – principalmente judeus europeus, mas também ciganos, espanhóis, russos, sérvios, eslovenos, alemães, búlgaros e até cubanos – foram mortos. Eles refinaram petróleo, construíram aviões de combate, montaram canhões, desenvolveram tecnologia de foguetes e foram arrendados para empresas privadas alemãs. Volkswagen, Siemens, Daimler-Benz, BMW, Bosch – todos se beneficiaram da mão-de-obra escrava do campo. Mauthausen, o centro nervoso administrativo, foi dirigido centralmente a partir de Berlim, usando o que havia de mais recente em tecnologia de computadores: tabuladores IBM de cartões perfurados.

Atualmente, nenhuma máquina IBM é exibida em Mauthausen. E, infelizmente, o memorial não faz nenhuma menção a elas. Mas o campo tinha várias máquinas IBM trabalhando horas extras para lidar com a grande rotatividade de reclusos e para garantir que sempre houvesse corpos suficientes para realizar o trabalho necessário.1 Essas máquinas não operavam isoladamente, mas faziam parte de um sistema maior de controle e contabilidade do trabalho escravo que se estendia pela Europa ocupada pelos nazistas, conectando Berlim a todos os principais campos de concentração e de trabalho forçado através de cartão perfurado, telégrafo, telefone e correio humano. Este não era o tipo automatizado de sistema de rede de computadores que o Pentágono começaria a construir nos Estados Unidos apenas uma década depois, mas era uma rede de informação: uma rede eletromecânica que alimentava e sustentava a

máquina de guerra da Alemanha nazista com eficiência impressionante.2 Ela se estendia para além dos campos de trabalho e chegava às cidades e vilas, computando montanhas de dados genealógicos para rastrear pessoas com o mais leve cheiro de sangue judeu ou impureza racial aparente em uma corrida louca para cumprir o esforço de Adolf Hitler de purificar o povo alemão.3 As próprias máquinas IBM não mataram pessoas, mas fizeram com que a máquina de morte nazista funcionasse mais rápida e eficientemente, vasculhando a população e rastreando vítimas de maneiras que nunca seriam possíveis sem elas.

Obviamente, os tabuladores da IBM não foram criados para essa função. Eles foram inventados em 1890 por um jovem engenheiro chamado Herman Hollerith para ajudar o Escritório Estadunidense para o Censo a contar a crescente população de imigrantes dos EUA. Cinquenta anos depois, a Alemanha nazista empregou a mesma tecnologia para realizar sistematicamente o Holocausto.

Esta é, talvez, uma nota sombria para terminar um livro sobre a Internet. Mas para mim, a história de Mauthausen e da IBM traz uma importante lição sobre a tecnologia de computador. Hoje, muitas pessoas ainda veem a Internet como algo exclusivamente especial, algo que não é corrompido por falhas e pecados humanos terrestres. Para muitos, o progresso e a bondade estão embutidos no código genético da Internet: se deixada em paz para evoluir, a rede levará automaticamente a um mundo melhor e mais progressista. Essa crença está profundamente enraizada em nossa cultura, e ela vem resistindo a fatos e evidências. Para mim, Mauthausen é um lembrete poderoso de como a tecnologia de computador não pode ser separada da cultura em que é desenvolvida e usada.

Enquanto eu estava lá, examinando a cena pastoral idílica naquele lugar horrível, pensei na minha conversa com Stephen Wolff, gerente da Fundação Nacional de Ciências dos EUA que ajudou a privatizar a Internet. "Certamente existem valores embutidos [na Internet]", ele me disse. “Se são valores exclusivamente ocidentais ou não, eu não saberia dizer. Não existe uma cultura que eu saiba que se recuse a usar a Internet. Portanto, deve haver algo universal sobre ela. Mas é uma entidade supranacional? Não. A Internet é um pedaço do mundo. É um espelho do mundo, mas é um pedaço do mundo ao mesmo tempo. Ela está

sujeita a todos os males aos quais o resto do mundo está sujeito e participa tanto das coisas boas quanto das coisas ruins."4

Wolff expressa lindamente a questão. A Internet e a tecnologia de microprocessador em rede em que é executada não transcendem o mundo humano. Para o bem ou para o mal, é uma expressão deste mundo e foi inventado e usado de maneiras que refletem as forças e os valores políticos, econômicos e culturais que dominam a sociedade. Hoje, vivemos em um mundo conturbado, um mundo de privação de direitos políticos, pobreza e desigualdade desenfreadas, poder corporativo descontrolado, guerras que parecem não ter fim nem propósito, e um complexo militar e de inteligência privatizado sem regulamentação – e sobre tudo isso pairam as perspectivas de aquecimento global e colapso ambiental. Vivemos tempos sombrios, e a Internet é um reflexo deles: ela é dirigida por espiões e corporações poderosas, assim como nossa sociedade é dirigida por eles. Mas nem tudo está perdido.

É verdade que o desenvolvimento da tecnologia de computadores sempre foi impulsionado pela necessidade de analisar grandes quantidades de dados complexos, monitorar pessoas, criar modelos preditivos do futuro e fazer guerras. Nesse sentido, vigilância e controle estão embutidos no DNA dessa tecnologia. Mas nem todo controle é igual. Nem toda a vigilância é ruim. Sem eles, não pode haver supervisão democrática da sociedade. Garantir que as refinarias de petróleo cumpram os regulamentos de poluição, impedir a fraude de Wall Street, forçar os cidadãos ricos a pagar sua parte justa dos impostos e monitorar a qualidade da comida, do ar e da água – nada disso seria possível. Nesse sentido, vigilância e controle não são problemas por si só. Como eles são usados depende de nossos políticos e da nossa cultura política.

Qualquer que seja a forma da Internet e das redes de computadores no futuro, é seguro dizer que viveremos com essa tecnologia por muito tempo. Ao fingir que a Internet transcende a política e a cultura, deixamos seu potencial interno de vigilância e controle nas mãos das forças mais perversas e poderosas. Quanto mais compreendemos e democratizamos a Internet, mais podemos empregar seu poder a serviço dos valores democráticos e humanísticos, fazendo com que funcione para muitos, e não para poucos.