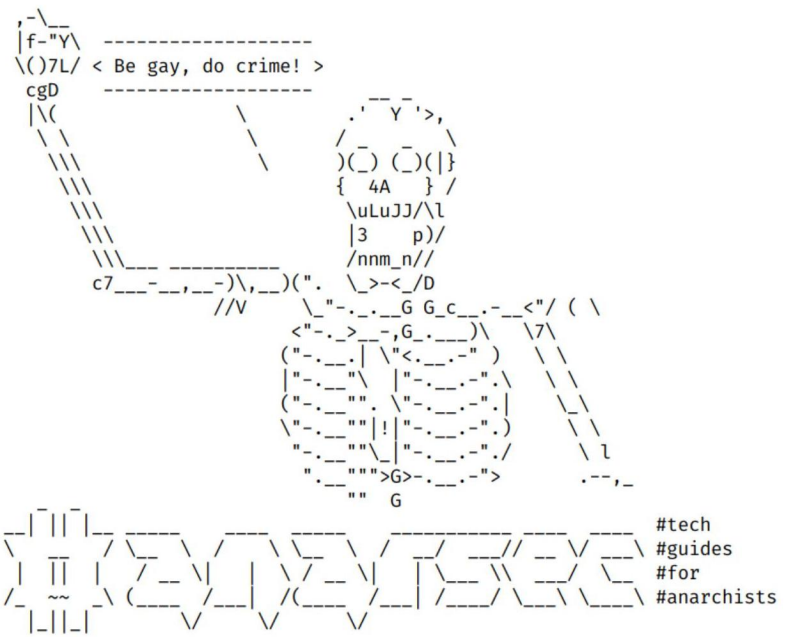
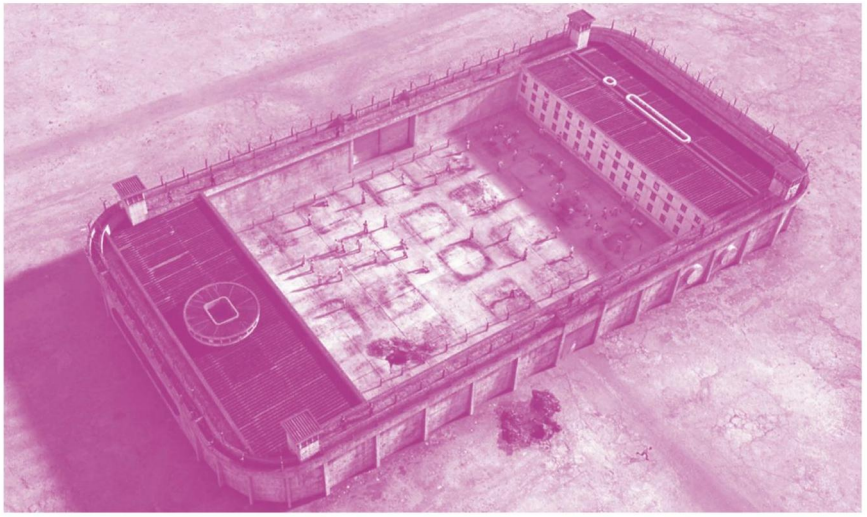
Mate o Policial no seu Bolso

Cultura de segurança e segurança operacional efetivas previnem que forças repressivas descubram sobre nossas atividades criminais específicas, mas também nossas vidas, relacionamentos, padrões de movimento, e tantos outros. Esse conhecimento é uma grande vantagem na hora de chegar a suspeitos e realizar vigilância direcionada. Esse artigo traz algumas estratégias para matar o policial no seu bolso.





Séries: Defensivo

Essa versão do zine foi editada por último em 2024-04-23. Visite anarsec.guide/pt para consultar possíveis atualizações.

O símbolo de adaga † significa que ela tem uma entrada no glossário.
Ai ferri corti.

AnarSec é um material criado para ajudar anarquistes navegarem o terreno hostil da tecnologia — guias defensivos para segurança digital e anonimidade, assim como guias ofensivos para hackeamentos. Todos os guias estão disponíveis em formato de livreto para impressão e serão mantidos atualizados.

Defensivo

Tails

- Tails for Anarchists
- Tails Best Practices

Qubes OS

- Qubes OS for Anarchists

Telefones

- **Mate o Policial no seu Bolso**
- GrapheneOS for Anarchists

Geral

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

Ofensiva

Em Breve

Sumário

Cultura de segurança e segurança operacional efetivas[1] previnem que forças repressivas descubram sobre nossas atividades criminais específicas, mas também nossas vidas, relacionamentos[2], padrões de movimento, e tantos outros. Esse conhecimento é uma grande vantagem na hora de chegar a suspeitos e realizar vigilância direcionada. Esse artigo traz algumas estratégias para matar o policial no seu bolso.

A localização de seu telefone é rastreada a todo o tempo[3], e esses dados são capturados por empresas, permitindo à polícia contornar a necessidade de conseguir um mandato. Os identificadores do hardware e informações de assinatura[4] são registrados por toda e cada uma das torres com as quais seu telefone se conecta. Serviços de raqueamento como Pegasus[5] colocam o comprometimento total de telefones ao alcance mesmo de agências repressivas locais e são "zero click", ou seja, não dependem que você clique em um link ou abra algum arquivo para raquear seu celular. Por outro lado, após mais de 30 incêndios criminosos em uma pequena cidade na França permanecerem sem suspeitos, investigadores reclamaram[6] que "é impossível usar registro de telefone ou veículos porque eles operam sem usar carros ou celulares!".

Em uma recente operação repressiva[7] contra um anarquista, a polícia rastreou em tempo real a geolocalização do celular flip do suspeito e fez uma lista de todos para quem ele ligou. É sabido que vigilância deste tipo não é incomum, e mesmo assim muitos camaradas carregam um celular com eles não importa para onde vão, ou fazem ligações não criptografadas para outros anarquistas. Nós acreditamos que ambas estas práticas deveriam ser evitadas. Não vamos facilitar tanto o trabalho

[1] notrace.how/pt-BR/blog/a-base-to-stand-on/uma-base-onde-se-apoiar.html

[2] notrace.how/threat-library/techniques/network-mapping.html

[3] vice.com/en/article/m7vqkv/how-fbi-gets-phone-data-att-tmobile-verizon

[4] anonymousplanet.org/guide.html#your-imei-and-imsi-and-by-extension-your--phone-number

[5] amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to--catch-nso-groups-pegasus/

[6] actforfree.noblogs.org/post/2022/04/17/grenoblefrance-these-saboteurs-of-the--ultra-left-have-been-elusive-for-five-years/

[7] notrace.how/resources/pt-BR/#ivan

da polícia ou agências de inteligência, entregando nossos círculos sociais e geolocalização para eles em uma bandeja de prata.

Se você deixa seu celular em casa, a polícia vai precisar recorrer a vigilância física para determinar seu paradeiro, algo que consome muito mais recursos e é detectável. Se você for posto sob vigilância física, o primeiro passo dos investigadores é entender seu "perfil de movimento", e o histórico da geolocalização do seu telefone oferece um retrato detalhado de seus padrões diários.

Alguns anarquistas respondem a problemas com smartphones usando celulares flip ou telefones fixos para se comunicarem uns com os outros, mas essas não são boas soluções. Celulares flip e telefones fixos não suportam comunicação criptografada†, então o Estado descobre quem está falando com quem e sobre o que. Um dos principais objetivos da vigilância direcionada é mapear os círculos sociais do alvo para identificar outros alvos. A única forma de evitar entregar estas informações para nossos inimigos é usar somente meios criptografados[8] para comunicação com outros anarquistas, quando ela for mediada por tecnologias.

A normalização da conectividade constante dentro da sociedade dominante levou alguns anarquistas a perceberem corretamente que metadados† são úteis para investigadores. Entretanto, a conclusão a que alguns chegam, de que deveríamos "nunca desligar o telefone"[9], nos leva na direção contrária. A lógica deles é que suas interações com tecnologia formam um padrão básico de metadados, e os momentos que se desviam desta base se tornam suspeitos se coincidem com quando certas ações acontecem, que estes metadados podem ser usados por investigadores para chegar até os suspeitos. Por mais que seja verdade, a conclusão oposta tem muito mais sentido: anarquistas deveriam minimizar a criação de padrões de metadados acessíveis e úteis a investigadores.

---

[8] anarsec.guide/posts/e2ee/

[9] web.archive.org/web/20210126183740/https://325.nostate.net/2018/11/09/never-turn-off-the-phone-a-new-approach-to-security-culture

Nossas conexões com as infraestruturas de dominação devem permanecer opacas e imprevisíveis se pretendemos manter a habilidade de atacar o inimigo. E se reconhecimento de terreno exigido por uma ação envolver um fim de semana inteiro longe de nossos dispositivos eletrônicos? Vamos começar com o simples fato de que celulares devem ser deixados em casa durante uma ação – isso só se torna uma anomalia em um padrão se celulares te acompanham onde quer que você vá. Em uma vida normativamente "sempre conectada", ambas mudanças de metadados se destacariam rapidamente, mas não é o caso se você se recusar a estar constantemente plugado. **Para minimizar suas pegadas de metadados, você deve se acostumar a deixar o celular em casa.**

Celulares colonizaram a vida cotidiana, pois as pessoas foram incutidas com a crença de que elas precisam de comunicação *síncrona* a todo momento. Sincronismo† significa que duas ou mais partes se comunicam em tempo real, em oposição a algo assíncrono† como e-mail, onde mensagens são enviadas em momentos diferentes. Essa "necessidade" foi normalizada, mas vale a pena resistir a ela dentro de espaços anarquistas. O anarquismo só pode ser anti-industrial[10]. Precisamos aprender a viver sem as conveniências vendidas pelas empresas de telecomunicação, devemos defender (ou reavivar) nossa habilidade de viver sem estarmos conectados a Internet a todo momento, sem instruções algorítmicas em tempo real, e em a flexibilidade infinita de mudar de planos no último minuto.

Se você decidir usar um celular, para dificultar o máximo possível que um adversário o geolocalize, intercepte suas mensagens, ou o raqueie, use GrapheneOS[11]. Se conseguirmos concordar em **usar somente comunicação criptografada[12] para nos comunicarmos com outros anarquistas**, isso exclui os celulares de flip e telefones fixos. Graphe-

[10] theanarchistlibrary.org/library/bismuto-beyond-the-moment#toc1
[11] anarsec.guide/posts/grapheneos/
[12] anarsec.guide/posts/e2ee/

qualquer sistema operacional. O sistema operacional do Tails† força todos os programas a usarem a rede Tor quando acessa a Internet.

Para mais informações, veja Tails for Anarchists[45] e Privacy Guides[46]. Para compreender as limitações do Tor, veja a documentação do Whonix[47].

Sistemas Operacionais (OS)

Os sistemas de software que operam seu dispositivo antes de qualquer outro software. Alguns exemplos comuns incluem Windows, macOS, Linux, Android, e iOS. Linux e algumas versões do Android são as únicas opções de código aberto nesta lista.

VoIP (Voice over Internet Protocol)

Google Voice é um serviço VoIP bastante conhecido e pouco seguro; essa tecnologia dirige suas chamadas para internet (como o Signal faz) invés de usar as transmissões normais de torres de celular. Diferente do Signal, o VoIP permite que você receba chamadas de qualquer um, não apenas de outros usuários do Signal. A vantagem de usar VoIP para chamadas, invés de plano de dados, é que você pode criar diferentes números para diferentes atividades (um para contas, um para logar m uma conta do Signal, etc.), e você nunca precisa desligar o Modo Avião. A vantagem de usar plano de dados, é que você pode usá-lo fora do Wi-Fi, às custas da geolocalização (ou seja, será possível que sua operadora e possivelmente outras partes, descubram onde seu serviço está a qualquer momento).

[45] anarsec.guide/posts/tails/#tor
[46] privacyguides.org/en/advanced/tor-overview/
[47] whonix.org/wiki/Warning

Modelagem de Ameaças

Modelagem de ameaças são um conjunto de atividades para melhorar a segurança através da identificação de uma série de adversários e objetivos de segurança[36], e vulnerabilidades[36], e então definindo contramedidas para prevenir ou mitigar os efeitos das ameaças ao sistema. Uma ameaça é um evento indesejável, real ou potencial, que pode sr malicioso (como um ataque DDoS[36]) ou acidental (como a falha de um drive). Modelagem de ameças é a atividade pensada para identificar e acessar ameaças e vulnerabilidades.

Para mais informações, veja a Biblioteca de Riscos do No Trace Project[41], Defend Dissent: Digital Threats to Social Movements[42] e Defending against Surveillance and Suppression[43].

Rede Tor

Tor[44] (sigla para The Onion Router) é uma rede aberta e distribuída que ajuda na defesa ontra anáalise de tráfego. O Tor te protege ao enviar suas comunicações através de uma rede de repetidores de sinais mantidos por voluntários ao redor do mundo: isso previne que alguém monitore sua conexão de Internet para descobrir quais sites você visita, e impede o operador destes sites de descobrirem sua localização física.

Todo site visitado através da rede Tor passa por três repetidores. Repetidores são servidores hospedados por diversas pessoas e organizações ao redor do mundo. Nenhum repetidor sabe de onde a conexão criptografada está vindo ou para onde está indo. Um trecho de um relatório altamente confidencial vazado da NSA, chama o Tor de "o rei da alta segurança, e anonimidade na internet" e "sem competidores para o trono". A rede Tor pode ser acessada através do Navegador Tor em

[41] notrace.how/threat-library/

[42] open.oregonstate.education/defenddissent/chapter/digital-threats/

[43] open.oregonstate.education/defenddissent/chapter/surveillance-and-suppression/

[44] torproject.org/

neOS é o único sistema operacional de smartphone que oferece um nível aceitável de segurança e privacidade.

Para impedir que seus movimentos sejam rastreados, trate o smartphone como uma linha fixa e deixe-o sempre em casa. Mesmo se você usa um cartão SIM comprado de forma anônima, se ele for ligado a sua identidade no futuro, a provedora do serviço pode ser retroativamente consultada por dados de geolocalização. Se você usar o telefone como estamos recomendando (como um dispositivo que só funciona com Wi-Fi[13], mantido a todo tempo em modo avião), ele não vai se conectar com as torres de celular. Não é o bastante apenas deixar o celular em casa quando você estiver indo para uma reunião, manifestação ou ação pois essa será a anomalia em seu padrão de comportamento e serve como indicação de que uma atividade criminal está acontecendo naquela janela de tempo.

Você pode escolher viver totalmente sem telefones, se sentir que não precisa de uma "linha fixa criptografada". As estratégias a seguir servem para minimizar a necessidade de telefones precisarem computadores, onde comunicações síncronas são também possíveis mas mais limitadas.

Burocracia

Muitas instituições burocráticas que somos forçados a conviver, dificultam uma vida sem celulares: planos de saúde, bancos, etc. Comunicação com burocracias não precisam ser criptografadas, então você pode usar um aplicativo de Voice over Internet Protocol (VoIP)†. Isso te permite fazer chamadas telefônicas através da internet, sem usar torres de celular.

Qualquer aplicativo VoIP disponível em um computador é assíncrono pois ele não toca quando o computador está desligado — você precisa do recuro de correio de voz para retornar ligações perdidas. Por exem-

[13] anarsec.guide/posts/grapheneos/#what-is-grapheneos

plo, um serviço como jmp.chat[14] te dá um número VoIP, que você pode pagar com Bitcoin, e você faz chamadas usando um aplicativo XMPP — Cheogram[15] funciona bem.

VoIP geralmente funciona para qualquer autenticação de dois fatores† (2FA) que você precisar (quando um serviço exige que você recebe uma número aleatório para fazer login). Números de telefone online[16] são outra opção.

Apesar de geralmente mais caro do que VoIP, um celular de flip ou linha fixa dedicada exclusivamente a isso também funciona bem para recepção de chamadas "burocráticas", como as mencionadas anteriormente.

Comunicação

Não carregar um telefone para todo lugar que se vai exige uma mudança na forma que você socializa, se você já foi pego na rede[17]. Ser intencional sobre minimizar a mediação das telas em seus relacionamentos é um objetivo valioso por si só.

Usar uma "linha fixa criptografada" para fazer telefonemas e um computador para mensagens criptografadas nos permite evitar o fluxo interminável de notificações em um dispositivo que está sempre ao nosso alcance.

Todos sairíamos ganhando se déssemos uma boa e longe olhada na monocultura de chats em grupo do Signal que foram substituídos por encontros cara a cara em algumas partes dos espaços anarquistas. Essa captura da organização de relacionamentos por celular nos trancafia numa reunião que nunca acaba e é relativamente fácil de se monitorar.

[14] kicksecure.com/wiki/Mobile_Phone_Security#Phone_Number_Registration_Unlinked_to_SIM_Card

[15] cheogram.com/

[16] anonymousplanet.org/guide.html#online-phone-number

[17] theanarchistlibrary.org/library/return-fire-vol-4-supplement-caught-in-the-net

Criptografia de Ponta A ponta

Dados são criptografados[36] conforme viajam de um dispositivo para o outro — de ponta a ponta — e não pode ser descriptografado por nenhum intermediário. A criptografia só pode ser realizada por uma das pontas. Isso é diferente de "criptografia passiva", como a Criptografia Total de Disco[36], onde os dados armazenados no seu dispositivo é criptografado quando seu dispositivo é desligado. Ambos são importantes!

Para mais informações, confira Encrypted Messaging for Anarchists[37], e Defend Dissent: Protecting Your Communications[38].

Metadados

Metadados são dados que oferecem informações sobre outros dados. Por exemplo, um arquivo JPG contém a imagem (JPG) mas pode também conter metadados como a data que o arquivo foi criado, o tipo de câmera, coordenadas de GPS, e afins. Metadados podem ser valiosos para inimigos (para encontrar brechas em softwares desatualizados que o alvo esteja utilizando), agências do governo (para coletar informações sobre pessoas, para criar gráficos estatísticos), e outros grupos (para publicidade direcionada baseada na localização).Toda vez que você está usando um computador. Você provavelmente está deixando metadados para trás.

Para mais informações, veja Remove Identifying Metadata From Files[39] e Defend Dissent: Metadata[40].

[36] anarsec.guide/glossary

[37] anarsec.guide/posts/e2ee

[38] open.oregonstate.education/defenddissent/chapter/protecting-your-communications/

[39] anarsec.guide/posts/metadata

[40] open.oregonstate.education/defenddissent/chapter/metadata/

Mensagens Criptografadas

Veja Encrypted Messaging for Anarchists[34]

Armazenando Dispositivos Eletrônicos

Veja Make Your Electronics Tamper-Evident[35].

Apêndice: Glossário

Autenticação de Dois Fatores (2FA)

A autentificação de dois fatores (ou "2FA") é uma forma do usuário se autoidentificar para um serviço, pedindo a combinação de dois métodos diferentes de autenticação. Estes podem ser algo que o usuário saiba (como uma senha ou PIN) ou algo que o usuário possui (como um token de hardware ou telefone celular).

Comunicação Assíncrona

Diferente da comunicação sincrônica†, ambas as partes não precisam estar online ao mesmo tempo. Isso depende de algum tipo de servidor para armazenar as mensagens até que o recipiente esteja online. A maioria das pessoas conhecem bem este tipo de mensageiro (e-mail, etc.).

Comunicação Sincrônica

Diferente de comunicações assíncronas†, ambas as partes devem estar online ao mesmo tempo. Isso não exige servidores para comunicação e geralmente é chamado de "par a par".

[34]anarsec.guide/posts/e2ee/

[35]anarsec.guide/posts/tamper/

Dito isso, comunicação criptografada pode ser útil para determinar uma data e hora para um encontro, ou para projetos compartilhados através de distâncias. Veja, Encrypted Messaging for Anarchists[18] para várias opções apropriadas para um modelo de ameaça† anarquista.

Chamadas de Emergência

Um transeunte pode te oferecer o telefone dele para uma chamada de emergência, se você disser que o seu está em bateria. Para receber chamadas de emergência, se você não pode ser encontrado por nenhum dos meios descritos anteriormente , nós podemos ir até as casas uns dos outros ou organizar checagens por mensageiros criptografados previamente. Que cenários exigiriam que você estivesse disponível para receber uma chamada a qualquer momento? Se isso de fato existe na sua vida, você se organizar sem projetar aquela urgência em todas outras áreas e momentos.

Direções

Compre um mapa de papel da sua área e ande com ele. Para viagens mais longas ou quando precisar se orientar, use OpenStreetMap[19] para anotá-los com antecedência.

Música e Podcasts

Eles ainda fazem tocadores mp3! Por um preço bem mais em conta, você pode ouvir músicas e podcasts , em um dispositivo que não tem GPS ou hardware de rádio. Entretanto, isso não significa que você não possa ser geolocalizado pro um tocador MP3 . Se ele se conectar com seu Wi-Fi, a localização aproximada de seu aparelho MP3 pode ser determinada pelo seu endereço de IP.

[18]anarsec.guide/posts/e2ee/

[19]openstreetmap.org/

Apêndice: Contra o smartphone

De Fernweh (#24)[20]

Eles está sempre com a gente, não importa onde vamos ou o que estamos fazendo. Ele nos mantém informados sobre tudo e todos: o que nossos amigos estão fazendo, quando o próximo metrô parte, e qual será o clima de amanhã. Ele toma conta de nós, nos acorda pela manhã, nos relembra de encontros importantes, e sempre nos escuta, quando vamos pra cama, quando e onde estivermos, com que nos comunicamos, quem são nossos melhores amigos, o tipo de música que escutamos, e quais são nossos hobbies. E tudo que ele pede é um pouquinho de eletricidade de vez em quando?

Quando eu faço um passeio ou pego o metrô, eu o vejo com quase todos, e ninguém consegue ficar mais do que alguns segundos sem freneticamente buscar pelo que tem no bolso: o celular vem à tona, uma mensagem é enviada, um e-mail é conferido, uma foto recebe um like. Ele é deixado de lado novamente, um peuqeno intervalo, e lá vamos nós de novo, folheando as notícias do dia e checando o que todos seus amigos estão fazendo...

É nosso companheiro quando estamos no banheiro, no trabalho ou na escola, e ele aparentemente serve ara lutar contra o tédio enquanto nós esperamos ou trabalhamos, etc. Essa talvez seja uma das razões do sucesso de todos esses dispositivos tecnológicos, que a vida real é tão absurdamente entediante e monótona que uns poucos centímetros de tela quase sempre é mais interessante do que o mundo e as pessoas a nossa volta? É como um vício (as pessoas definitivamente têm crises de abstinência...) ou ele já se tornou parte do nosso corpo? Sem ele, nós já não sabemos como nos orientar e sentimos que algo está faltando? Então não é apenas mais uma ferramenta ou brinquedo, mas uma parte de nós que também exerce um certo controle sobre nós, ao qual nos adaptamos, por exemplo, não sair de casa antes da bateria estar totalmente

[20] fernweh.noblogs.org/texte/24-ausgabe/gegen-das-smartphone/

Seu computador

Sistema Operacional†: Não há nada que se compare ao **Tails**, para o manejo de informações sensíveis no computador (escrever e enviar comunicados, moderar um site suspeito, pesquisar para ações, ler artigos que talvez venham a ser criminalizados, etc.). O Tails opera a partir de um USB e foi criado com uma propriedade anti-forense que o permite não deixar rastros no seu computador, assim como forçar que todas as conexões da internet aconteçam pela rede Tor†. Veja Tails for Anarchists[29] e Tails Best Practices[30].

Sistema Operacional†: **Qubes OS** para muitos usos de caso, tem uma segurança melhor que o Tails, mas sua curva de aprendizado é mais fechada e nenhuma ferramenta anti-forense. De todo modo é acessível o suficiente para jornalistas e outros usuários não técnicos. Conhecimento básico de Linux é necessário — veja a sessão de Linux Essentials[31]. Qubes OS consegue até mesmo rodar alguns programas do Windows como Adobe InDesign, mas de forma muito mais segura. Vide Qubes OS for Anarchists[32].

Veja quando When to Use Tails vs. Qubes OS[33]. Nós não oferecemos dicas de "redução de danos" para o Windows ou macOS, já que esse tipo de material tende a ser popular e dá a falsa sensação de privacidade e segurança.

[29] anarsec.guide/posts/tails/
[30] anarsec.guide/posts/tails-best/
[31] anarsec.guide/posts/linux
[32] anarsec.guide/posts/qubes/
[33] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

propósitos de incriminação[23] e mapeamento de redes de contatos[24]. Nosso objetivo é atrapalhar a capacidade do Estado de vigiar nossas vidas e projetos. Nossas recomendações são direcionadas a todos anarquistas, e são acompanhadas de guias e conselhos práticos.

Nós concordamos com a conclusão da análise sobre vigilância digital individualizada na França[25]: "Sejamos claros sobre nossas responsabilidades: se nós nós conscientemente levamos um dispositivo equipado com microfone e/ou câmera (celular, babá eletrônica, computador, carro com gps, relógio ligado a internet), mesmo que desligados, para uma conversa na qual 'se fazem comentários e se usam palavras secretas e confidenciais' que devem permanecer secretas, nós nos tornamos possíveis informantes estatais..."

Você talvez se interesse pelas "Boas Práticas Digitais"[26] da nossa Biblioteca de Ameaças.

Seu Telefone

Sistema Operacional†: **GrapheneOS** é a única opção relmente segura para celulares. Veja GrapheneOS for Anarchists[27]. Se você decidir ter um celular, trate-o como uma "linha telefônica criptografada fixa" e deixe-o em casa quando for sair. Vide Mate o Policial no seu Bolso[28].

[23] notrace.how/threat-library/tactics/incrimination.html
[24] notrace.how/threat-library/techniques/network-mapping.html
[25] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive--surveillance-measures-france/
[26] notrace.how/threat-library/mitigations/digital-best-practices.html
[27] anarsec.guide/posts/grapheneos/
[28] anarsec.guide/pt/posts/nophones/

cheia? O smartphone é o primeiro passo em turvar a linha entre o humano e o robô?

Quando vemos oque todos tipo de tecnocrata tem profetizado (Google Glasses, implantes de chips, etc.), é quase como estivéssemos indo em direção a nos tornarmos ciborgues, pessoas com smartphones implantados que controlamos através de nossos pensamentos (até que nossos próprios pensamentos sejam controlados). Não é surpreendente que a mídia, o porta-voz da dominação, nos mostre apenas os aspectos positivos deste desenvolvimento, mas é chocante que quase ninguém questiona esta visão. É possivelmente o sonho mais louco de todo governante: ser capaz de monitorar os pensamentos e ações de todos a todo momento, e ser capaz de intervir imediatamente no caso de qualquer distúrbio. Zangões trabalhadores totalmente controlados que têm alguma diversão (virutal) como recompensa enquanto uns poucos lucram.

Com as vastas quantias de dados agora tão prontamente disponíveis para todos e qualquer um a qualquer hoje do dia, controle social e vigilância também chegaram a um novo patamar. Isso vai muito além de grampear celulares os folhear entre mensagens (como durante as revoltas de 2011 no Reino Unido). Com acesso a uma quantidade incrível de informação, agências de inteligência são capazes de definir o que é "normal". Eles são capazes de determinar que locais são "normais" para nós, quais contatos são "normais", etc. Em resumo, eles podem rapidamente estabelecer e estabelecer praticamente em tempo real se estamos desviando do comportamento que eles estabeleceram como "normal". Isso dá muito poder a certas pessoas, que é usado sempre que há uma oportunidade de tomar vantagem deste poder (ou seja, vigiar pessoas). Tecnologia é parte do poder, ela vem do poder e necessita de poder. É preciso um mundo em que certas pessoas tenham muito poder para permitir a produção de algo como o smartphone. Toda tecnologia é um produto da tendência opressiva do mundo, é parte disso, e serve a ele.

No mundo de hoje, nada é neutro. Até então, tudo que foi ou tem sido desenvolvido é criado para estender o controle e fazer dinheiro. Muitas das inovações das últimas décadas (como GPS, energia nuclear, ou a internet) vem diretamente dos militares. Na maior parte do tempo esses dois aspectos estão de mãos dadas, mas o "bem-estar da humanidade" certamente não é uma motivação, especialmente quando é desenvolvido pelos militares.

Talvez se pegarmos o exemplo da arquitetura podemos ilustrar algo tão complexo quanto a tecnologia: peguemos uma prisão vazia e em desuso, oque poderia ser feito com essa estrutura se não a botar abaixo? Suas própria arquitetura, suas paredes, suas torres de vigilância, suas celas, já contém o propósito da construção: aprisionar pessoas e as destruir psicologicamente. Seria impossível para mim viver dentro de uma prisão, simplesmente porque a construção é opressiva.

É o mesmo com todas as tecnologias de hoje que nos são apresentadas como progresso e como algi que deixa a vida mais fácil. Elas são construídas com a intenção de fazer dinheiro e nos controlar, aqueles que ficam ricos coletando nossos dados e te monitorando sempre vão se beneficiar mais que você.

Se no passado dizíamos que "conhecimento é poder", hoje deveríamos dizer que "informação é poder". Quantos mais os governantes sabem sobre seus súditos, melhor ele pode dominá-los — nesse sentido, tecnologia como um todo é uma poderosa ferramenta de controle para prever e portanto prevenir pessoas de se reunirem para atacar o que as oprime.

Esses smartphones aparentemente precisam mais do que um pouquinho de eletricidade... Na nossa geração, que ao menos conheceu um mundo sem smartphones, ainda deve haver algumas pessoas que ainda abem do que eu estou falando, que ainda sabe o que é ter uma conversa sem estar olhando para seu telefone a cada trinta segundos, para se perder e descobrir novos lugares, ou ter uma discussão sem imediatamente consultar o Google pela resposta. Mas eu não quero voltar ao passado, até porque não seria mais possível, quanto mais a tecnologia

penetra nossas vidas, mais difícil fica de destruí-la. E formos uma das últimas gerações a serem capazes de parar essa evolução de seres humanos em robôs completamente controlados?

E se em algum ponto formos incapazes de reverter essa formação? A humanidade chegou a um novo estágio tecnológico histórico. Um estágio onde é capaz de aniquilar toda vida humana (energia nuclear) ou modificá-la (manipulação genética). Esse fato reforça mais uma vez a necessidade de agirmos hoje para destruir essa sociedade. Pra isso, precisamos encontrar outras pessoas e comunicar nossas ideias.

Não é óbvio que se ao invés de conversamos uns com os outros, nos comunicarmos em mensagens de cinco sentenças ou menos, haverão efeitos de longo termo? Aparentemente não. Primeiro de tudo, o modo como pensamos influencia como falamos, e vice-versa — a forma como falamos e comunicamos influencia a forma que pensamos. Se só formos capazes de trocar mensagens curtas e resumidas, como podemos falar de outro mundo, como podemos criá-lo?

Comunicação direta entre indivíduos autônomos é a base de qualquer rebelião compartilhada, é o ponto de partida de sonhos compartilhados e lutas em comum. Sem comunicações não mediadas, a luta contra esse mundo e por liberdade é impossível.

Então, vamos nos livrar desses telefones e nos encontramos pessoalmente em uma insurgência contra este mundo! Sejamos incontroláveis!

por hiperobjeto.blackblogs.org[21]

Apêndice: Recomendações

Como anarquistas, nós devemos nos defender da polícia e agências de inteligência que conduzem vigilância digital individualizada[22] para os

[21] hiperobjeto.blackblogs.org/2024/09/02/mate-o-policial-no-seu-bolso
[22] notrace.how/threat-library/techniques/targeted-digital-surveillance.html