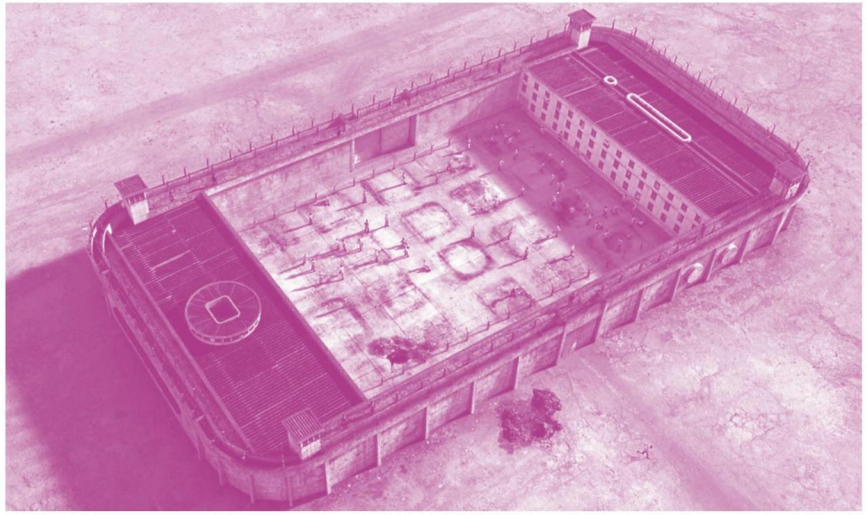
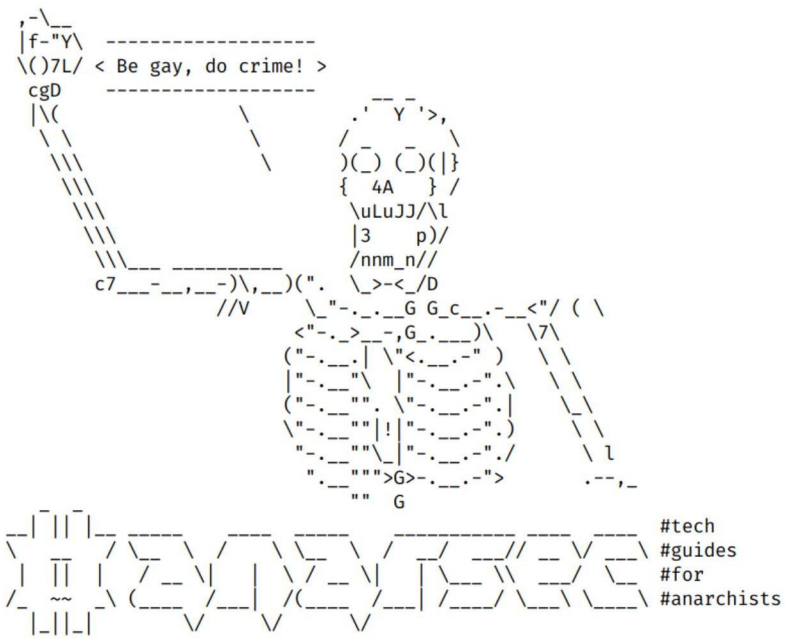
Избавься от шпиона в твоем кармане



Серии: Защита

Эффективная культура безопасности и внимание к безопасности на акциях не позволяют репрессивным структурам узнать не только о нашей конкретной нелегальной деятельности, но и о нашей жизни, взаимоотношениях, схемах передвижения и так далее. Эти знания являются огромным преимуществом при отборе подозреваемых и ведении целенаправленного наблюдения. В этой статье мы рассмотрим несколько стратегий, как убить полицейского в вашем кармане.



Эта версия зина была последний раз обновлена 2024-04-23. Зайдите на сайт anarsec.guide/ru и посмотрите, нет ли более поздних редакций.

Символ † означает, что этот термин есть в словаре. Ai ferri corti.

AnarSec это ресурс который призван помочь анархистам ориентироваться во враждебном мире технологий — подборка пособий по обеспечению цифровой безопасности и анонимности, а также по проведению хакерских атак. Все пособия доступны в виде буклетов, чтобы их можно было распечатать и будут постоянно обновляться.

Защита

Tails

- **Операционная система Tails - для анархистов**
- **Лучшие практики Tails**

Qubes OS

- Qubes OS for Anarchists

Телефоны

- **Избавься от шпиона в твоем кармане**
- GrapheneOS for Anarchists

Общие вопросы

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

Нападение

Скоро ожидается

Содержание

Эффективная культура безопасности[1] и внимание к безопасности на акциях не позволяют репрессивным структурам узнать не только о нашей конкретной нелегальной деятельности, но и о нашей жизни, взаимоотношениях[2], схемах передвижения и так далее. Эти знания являются огромным преимуществом при отборе подозреваемых и ведении целенаправленного наблюдения. В этой статье мы рассмотрим несколько стратегий, как убить полицейского в вашем кармане.

Местоположение вашего телефона отслеживается постоянно[3], и эти данные собираются частными компаниями, что позволяет полиции обходить необходимость получения ордера. Идентификаторы оборудования телефона и информация о соединении[4] регистрируются каждой вышкой сотовой связи, к которой подключается ваш телефон. Такие хакерские сервисы, как Pegasus[5], делают полную компрометацию телефона досягаемой даже для местных правоохранительных органов и являются «zero-click», то есть не зависят от нажатия на ссылку или открытия файла для взлома телефона. С другой стороны, после того как более 30 поджогов в небольшом городке во Франции остались нераскрытыми, следователи пожаловались[6], что «невозможно использовать данные телефонов или регистрационные данные автомобилей, потому что они работают без телефонов и автомобилей!»

В ходе недавней репрессивной операции[7] против анархиста полиция в режиме реального времени отслеживала геолокацию флип-телефона подозреваемого и составила список всех, кому он

[1] notrace.how/blog/a-base-to-stand-on/baza-na-kotoroi-mozhno-stoiat.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/ru/#ivan

for the throne in waiting». The Tor network can be accessed through the Tor Browser on any operating system. The Tails[55] operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists[56] and Privacy Guides[57]. To understand the limitations of Tor, see the Whonix documentation[58].

Two-Factor Authentication (2FA)

Two-factor authentication (or «2FA») is a way for a user to identify themselves to a service provider by requiring a combination of two different authentication methods. These can be something the user knows (such as a password or PIN) or something the user has (such as a hardware token or mobile phone).

VoIP (Voice over Internet Protocol)

Google Voice is a well-known and insecure VoIP service; this technology routes your calls over the Internet (as Signal does) instead of using standard cell tower transmission. Unlike Signal, VoIP allows you to receive calls from anyone, not just other Signal users. The advantage of using VoIP for calls over a data plan is that you can create different numbers for different activities (one for bills, one for signing up for a Signal account, etc.), and you never need to turn off Airplane mode. The advantage of using a data plan instead is that you can use it away from Wi-Fi, at the cost of geolocation (i.e. it will be possible for your service provider and possibly other parties to know where your device is at any given time).

[55] anarsec.guide/glossary/#tails
[56] anarsec.guide/posts/tails/#tor
[57] privacyguides.org/en/advanced/tor-overview/
[58] whonix.org/wiki/Warning

звонил. Хорошо известно, что подобная слежка – не редкость, и все же многие товарищи носят с собой мобильный телефон, куда бы они ни пошли, или делают незашифрованные звонки другим анархистам.

Мы считаем, что обеих этих практик следует избегать. Давайте не будем облегчать работу полиции и спецслужб, вручая им на блюдечке с голубой каемочкой наши социальные сети и историю геолокации. Если вы не выходите из дома с телефоном, полиции придется прибегнуть к физическому наблюдению, чтобы определить ваше местонахождение, что требует значительных ресурсов и может быть обнаружено. Если за вами будет установлено физическое наблюдение, то первым шагом следователя станет изучение вашего «профиля передвижения», а история геолокации вашего телефона дает подробное представление о ваших ежедневных маршрутах.

Некоторые анархисты отвечают на проблемы со смартфонами тем, что используют для общения друг с другом флип-телефоны (обычные мобильные телефоны, не смартфоны) или стационарные телефоны, но это не лучшее решение. Флип-телефоны и стационарные телефоны не поддерживают шифрованную связь†, поэтому государство узнает, кто с кем и о чем разговаривает. Основная цель целенаправленной слежки – составить карту социальной сети цели, чтобы выявить другие цели. Единственный способ избежать передачи этой информации нашим врагам – использовать только зашифрованные средства[8] для общения с другими анархистами с помощью технологий.

Нормализация постоянной связи в доминирующем обществе привела к тому, что некоторые анархисты правильно отмечают, что метаданные† телефонных разговоров полезны для следователей. Однако вывод, который некоторые делают из этой мысли –

[8] anarsec.guide/posts/e2ee/

что мы должны «никогда не выключать телефон»[9] , – ведет нас в неверном направлении. По их логике, ваше взаимодействие с технологией формирует базовую модель метаданных, а моменты, отклоняющиеся от этой базовой модели, становятся подозрительными, если они совпадают с моментом совершения действия, которое может быть использовано следователями для выявления подозреваемых. Хотя это и верно, гораздо более логичен противоположный вывод: анархистам следует минимизировать создание шаблонов метаданных, к которым могли бы получить доступ следователи.

Наши связи с инфраструктурами господства должны оставаться непрозрачными и непредсказуемыми, если мы хотим сохранить способность наносить удары по врагу. Что, если разведка, необходимая для проведения акции, занимает целый уик-энд?

Или давайте начнем с простого факта, что телефоны нужно оставлять дома во время действия – это становится исключением из шаблона, если в остальном телефоны сопровождают нас везде, куда бы мы ни пошли. В нормативной жизни «всегда на связи» любое из этих изменений метаданных будет бросаться в глаза, но это не так, если вы отказываетесь быть постоянно подключенным к сети. **Чтобы минимизировать свой метаданный след, вы должны по умолчанию оставлять телефон дома.**

Телефоны колонизировали повседневную жизнь, потому что людям внушили, что они нуждаются в *синхронном* общении в каждый момент времени. *Синхронная*† означает, что две или более стороны общаются в режиме реального времени, в отличие от *асинхронной*†, например электронной почты, где сообщения отправляются в разное время. Эта «потребность» стала нормой, но ей стоит противостоять в анархистском пространстве. Анархия может быть только антииндустриальной[10]. Мы должны научить-

[9] a2day.org/nikogda-ne-vyiklyuchay-telefon-novyiy-podhod-k-kulture-bezopasnosti/

[10] theanarchistlibrary.org/library/bismuto-beyond-the-moment#toc1

Threat model

Threat modeling is a family of activities for improving security by identifying a set of adversaries, security goals[48], and vulnerabilities[49], and then defining countermeasures to prevent or mitigate the effects of threats to the system. A threat is a potential or actual undesirable event that can be malicious (such as a DDoS attack[50]) or accidental (such as a hard drive failure). Threat modeling is the deliberate activity of identifying and assessing threats and vulnerabilities.

For more information, see the No Trace Project Threat Library[51], Defend Dissent: Digital Threats to Social Movements[52] and Defending against Surveillance and Suppression[53].

Tor network

Tor[54] (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet connection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor «the King of high secure, low latency Internet anonymity» with «no contenders

[48] anarsec.guide/glossary/#security-goal

[49] anarsec.guide/glossary/#vulnerability

[50] anarsec.guide/glossary/#ddos-attack

[51] notrace.how/threat-library/

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

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

[54] torproject.org/

For more information, check out Encrypted Messaging for Anarchists[43], and Defend Dissent: Protecting Your Communications[44].

Metadata

Metadata is data that provides information about other data. For example, a JPG file contains the actual image (data) but it may also contain metadata such as the date the file was created, the type of camera, GPS coordinates, and so on. Metadata can be valuable to attackers (to find appropriate exploits for outdated software the target is using), government agencies (to collect information about people to create social graphs), and other parties (to target location-based advertising). Whenever you use a computer, you are likely leaving metadata behind.

For more information, see Remove Identifying Metadata From Files[45] and Defend Dissent: Metadata[46].

Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android, and iOS. Linux and some versions of Android are the only open-source options on this list.

Synchronous communication

Unlike asynchronous communication[47], both parties must be online at the same time. This does not require servers for the communication and is often referred to as «peer to peer».

[43] anarsec.guide/posts/e2ee

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

[45] anarsec.guide/posts/metadata

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

[47] anarsec.guide/glossary/#asynchronous-communication

ся жить без удобств, продаваемых нам телекоммуникационными компаниями, мы должны защитить (или возродить) нашу способность жить без постоянного подключения к Интернету, без алгоритмических указаний в реальном времени и без бесконечной гибкости, позволяющей менять планы в последнюю минуту.

Если вы решили использовать телефон, чтобы максимально затруднить противнику его геолокацию, перехват сообщений или взлом, используйте GrapheneOS[11]. Если мы договоримся **использовать только зашифрованные средства связи[12] для общения с другими анархистами**, то это исключит использование флип-телефонов и стационарных телефонов.

GrapheneOS – единственная операционная система для смартфонов, которая обеспечивает разумную конфиденциальность и безопасность.

Чтобы предотвратить отслеживание ваших перемещений, обращайтесь со смартфоном как со стационарным телефоном и оставляйте его дома, когда вас нет дома. Даже если вы используете анонимно приобретенную SIM-карту, если в будущем она будет связана с вашей личностью, у поставщика услуг можно будет задним числом запросить данные о геолокации. Если вы используете телефон так, как мы рекомендуем (как устройство, работающее только через Wi-Fi[13] и постоянно находящееся в авиарежиме), он не будет подключаться к вышкам сотовой связи. Недостаточно оставлять телефон дома только тогда, когда вы собираетесь на встречу, демонстрацию или мероприятие, потому что это будет отклонением от вашей обычной модели поведения и послужит признаком того, что в это время происходит преступная деятельность.

Если вы не считаете, что вам нужен «зашифрованный стационарный телефон», вы можете жить совсем без телефона. Следую-

[11] anarsec.guide/posts/grapheneos/

[12] anarsec.guide/posts/e2ee/

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

щие стратегии минимизации потребности в телефонах основаны на использовании компьютеров, где синхронная связь также возможна, но более ограничена.

Бюрократия

Многие бюрократические учреждения, с которыми нам приходится иметь дело, не позволяют жить без телефона: здравоохранение, банковское дело и т. д. Общение с бюрократией не обязательно должно быть зашифровано, поэтому вы можете использовать приложение Voice over Internet Protocol (VoIP)†. Это позволит вам совершать телефонные звонки через Интернет, а не через сотовые вышки.

Любое приложение VoIP, доступное на компьютере, является асинхронным, потому что оно не звонит, когда компьютер выключен – вы полагаетесь на функцию голосовой почты для возврата пропущенных звонков. Например, такой сервис, как jmp.chat[14], предоставляет вам VoIP-номер, который вы можете оплатить в биткойнах, и вы совершаете звонки с помощью XMPP-приложения – Cheogram[15] работает хорошо.

VoIP обычно подходит для любой двухфакторной аутентификации† (2FA), которая вам нужна (когда сервис требует получить случайный номер для входа в систему). Еще одним вариантом являютсяонлайн-телефонные номера[16].

Хотя обычно это дороже, чем VoIP, выделенный телефон или стационарный телефон также хорошо подходит для совершения и приема «бюрократических» звонков из дома, как, например, упомянутых выше.

[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

See When to Use Tails vs. Qubes OS[37]. We do not offer «harm reduction» advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

Encrypted Messaging

See Encrypted Messaging for Anarchists[38]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[39].

Приложение: Словарь

Asynchronous Communication

Unlike synchronous communication[40], both parties do not need to be online at the same time. This relies on some sort of server to store messages until the message recipients come online. This is the type of messaging that most people are familiar with (email, Signal, etc.).

End-to-end encryption (e2ee)

Data is encrypted[41] as it travels from one device to another — endpoint to endpoint — and cannot be decrypted by any intermediary. It can only be decrypted by the endpoints. This is different from «encryption at rest», such as Full Disk Encryption[42], where the data stored on your device is encrypted when the device is turned off. Both are important!

[37] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

[38] anarsec.guide/posts/e2ee/

[39] anarsec.guide/posts/tamper/

[40] anarsec.guide/glossary/#synchronous-communication

[41] anarsec.guide/glossary/#encryption

[42] anarsec.guide/glossary/#full-disk-encryption-fde

«encrypted landline» and leave it at home when you are out of the house. See Kill the Cop in Your Pocket[29].

Your Computer

Operating system[30]: Tails is unparalleled for sensitive computer use (writing and sending communiques, moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network[31]. See Tails for Anarchists[32] and Tails Best Practices[33].

Operating system[34]: Qubes OS has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials[35]. Qubes OS can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists[36].

[30] anarsec.guide/glossary#operating-system-os
[31] anarsec.guide/glossary#tor-network
[32] anarsec.guide/posts/tails/
[33] anarsec.guide/posts/tails-best/
[34] anarsec.guide/glossary#operating-system-os
[35] anarsec.guide/posts/linux
[36] anarsec.guide/posts/qubes/

Связь

Чтобы не носить с собой телефон повсюду, необходимо изменить способ общения, если вы уже попали в сети[17]. Намеренное сведение к минимуму посредничества экранов в наших отношениях – ценная цель сама по себе.

Использование «зашифрованного стационарного телефона» для совершения телефонных звонков и компьютера для обмена зашифрованными сообщениями позволяет нам избежать нескончаемого потока уведомлений на устройстве, которое всегда находится под рукой.

Нам всем не помешало бы внимательно посмотреть на монокультуру групповых чатов Signal, которая заменила личные встречи в некоторых частях анархистского пространства. То, что культура смартфонов захватила организацию отношений, принуждает нас к бесконечным встречам, за которыми относительно легко наблюдать.

Тем не менее, зашифрованные сообщения могут быть полезны для определения даты и времени встречи или для проектов, выполняемых на расстоянии. См. «Encrypted Messaging for Anarchists»[18], где описаны различные варианты, подходящие для анархистской модели угроз[†].

Экстренные звонки

Прохожий на улице часто одолжит вам свой телефон, чтобы сделать срочный звонок, если вы скажете ему, что в вашем разрядилась батарея. Для получения экстренных звонков, если вы не можете дозвониться, как описано выше, мы можем заходить друг к другу в гости или заранее договариваться о встрече с помощью шифрованных сообщений. Какие сценарии требуют, чтобы вы

[17] theanarchistlibrary.org/library/return-fire-vol-4-supplement-caught-in-the-net
[18] anarsec.guide/posts/e2ee/

были готовы принять звонок в любой момент? Если они действительно существуют в вашей жизни, вы можете организовать их, не проецируя эту срочность на все остальные сферы и моменты.

Направления

Купите бумажную карту вашего района и носите ее с собой. Для длительных поездок или поездок, в которых вам нужны указания, используйте OpenStreetMap[19], чтобы отметить их заранее.

Музыка и подкасты

До сих пор выпускают MP3-плееры! За гораздо меньшую цену вы можете слушать музыку и подкасты, но в устройстве нет GPS и радио. Однако это не значит, что MP3-плеер не сможет определить ваше местоположение. Если он подключается к Wi-Fi, приблизительное местоположение MP3-плеера можно определить по его IP-адресу.

Приложение: Против смартфона

Om Fernweh (#24)[20]

Телефон всегда с нами, всегда включен, независимо от того, где мы находимся и что делаем. Он держит нас в курсе всего и всех: что делают наши друзья, когда отправляется следующее метро и какая погода будет завтра. Он заботится о нас, будит по утрам, напоминает о важных встречах и всегда слушает нас. Он знает о нас все: когда мы ложимся спать, где мы находимся и когда, с кем общаемся, кто наши лучшие друзья, какую музыку мы слу-

[19] openstreetmap.org/

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

Приложение: Рекомендации

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[22] for the purposes of incrimination[23] and network mapping[24]. Our goal is to obscure the State's visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France[25]: «So let's be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which "private or confidential words are spoken» and must remain so, even if it's switched off, we become a potential state informer…"

You may also be interested in the Threat Library's «Digital Best Practices»[26].

Your Phone

> **Operating system**[27]: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[28]. If you decide to have a phone, treat it like an

[22] notrace.how/threat-library/techniques/targeted-digital-surveillance.html

[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/glossary#operating-system-os

[28] anarsec.guide/posts/grapheneos/

[29] anarsec.guide/posts/nophones/

ний, способных остановить эволюцию человека в полностью контролируемого робота?

И что если в какой-то момент мы окажемся не в состоянии обратить это развитие вспять? Человечество достигло исторически нового этапа развития технологий. Этап, на котором оно способно уничтожить всю человеческую жизнь (ядерная энергия) или модифицировать ее (генетические манипуляции). Этот факт еще раз подчеркивает необходимость действовать уже сегодня, чтобы уничтожить это общество. Для этого нам нужно встречаться с людьми и доносить до них свои идеи.

Разве не очевидно, что если вместо того, чтобы разговаривать друг с другом, мы будем общаться только сообщениями из пяти предложений или меньше, то это приведет к долгосрочным последствиям? Судя по всему, нет. Прежде всего, то, как мы думаем, влияет на то, как мы говорим, и наоборот – то, как мы говорим и общаемся, влияет на то, как мы думаем. Если мы можем обмениваться только самыми короткими и лаконичными сообщениями, как мы можем говорить о совершенно другом мире? А если мы даже не можем говорить о другом мире, как мы можем к нему приблизиться?

Прямое общение между автономными личностями – основа любого совместного восстания, это отправная точка общих мечтаний и общей борьбы. Без непосредственного общения борьба против этого мира и за свободу невозможна.

Так давайте же избавимся от смартфонов и встретимся лицом к лицу в восстании против этого мира! Давайте станем неуправляемыми!

с a2day.org[21]

[21] a2day.org/izbavsya-ot-shpiona-v-tvoem-karmane

шаем и чем увлекаемся. И все, о чем он просит, – это немного электричества время от времени?

Когда я прогуливаюсь по району или еду в метро, я вижу это почти у всех, и никто не может продержаться дольше нескольких секунд без того, чтобы судорожно не потянуться к карману: достать мобильный телефон, отправить сообщение, проверить электронную почту, поставить лайк фотографии. Его снова убирают, короткий перерыв, и вот мы уже снова просматриваем сегодняшние новости и проверяем, чем занимаются все друзья...

Это наш спутник в туалете, на работе или в школе, и, очевидно, он помогает бороться со скукой во время ожидания, работы и т. д. Возможно, это одна из причин успеха всех этих технологических устройств: реальная жизнь настолько чертовски скучна и однообразна, что несколько квадратных сантиметров экрана почти всегда оказываются более захватывающими, чем мир и люди вокруг нас?

Это как зависимость (у людей определенно бывают симптомы отмены...) или это даже стало частью нашего тела? Без телефона мы уже не знаем, как сориентироваться, и чувствуем, что чего-то не хватает? То есть это уже не просто инструмент или игрушка, а часть нас, которая также осуществляет над нами определенный контроль, к которому мы приспосабливаемся, например, не выходя из дома до полной зарядки аккумулятора? Является ли смартфон первым шагом к стиранию грани между человеком и роботом?

Когда мы видим, что пророчат технократы всех мастей (очки Google Glass, вживленные чипы и т. д.), кажется, что мы движемся к тому, чтобы стать киборгами, людьми с вживленными смартфонами, которыми мы управляем с помощью наших мыслей (пока наши мысли сами не станут окончательно управляемыми). Неудивительно, что средства массовой информации, выразители господства, показывают нам только положительные стороны этого развития, но шокирует то, что почти никто не ста-

вит под сомнение эту точку зрения. Это, наверное, самая смелая мечта каждого правителя: иметь возможность постоянно следить за мыслями и действиями каждого и немедленно вмешиваться в случае любого нарушения. Полностью контролируемые и управляемые рабочие пчелы, которым в качестве вознаграждения разрешено немного (виртуально) развлечься, пока несколько человек получают прибыль.

С огромными объемами данных, которые теперь так легко получить от всех и каждого в любое время суток, социальный контроль и слежка также вышли на совершенно новый уровень. Теперь это выходит далеко за рамки прослушивания мобильных телефонов или просмотра сообщений (как во время беспорядков в Великобритании в 2011 году).

Имея доступ к невероятному количеству информации, спецслужбы способны определить, что является «нормальным». Они могут определить, какие места являются «нормальными» для нас, какие контакты являются «нормальными» и т. д. Короче говоря, они могут быстро и почти в режиме реального времени установить, отклоняются ли люди от своего «нормального» поведения. Это дает некоторым людям огромную власть, которая используется при каждом удобном случае (например, для слежки за людьми). Технология – это часть власти, она исходит от власти и нуждается в ней. Чтобы создать что-то вроде смартфона, нужен мир, в котором люди обладают огромной властью. Все технологии являются продуктом нынешнего угнетающего мира, его частью и будут усиливать его.

В современном мире ничто не является нейтральным. На сегодняшний день все, что было или разрабатывается, направлено на расширение контроля и зарабатывание денег. Многие инновации последних десятилетий (такие как GPS, ядерная энергетика или интернет) даже исходят непосредственно от военных. Чаще всего эти два аспекта идут рука об руку, но «благосостояние человечества», конечно, не является мотивацией, особенно когда

это разрабатывается военными. Возможно, пример архитектуры может лучше проиллюстрировать столь сложную технологию: возьмем пустую и неиспользуемую тюрьму, что можно сделать с этим сооружением, кроме как снести его? Сама ее архитектура, ее стены, сторожевые башни, камеры уже содержат в себе назначение этого здания: заключать людей в тюрьму. Сама его архитектура, его стены, его сторожевые башни, его камеры уже содержат в себе цель этого здания: заключать людей в тюрьму и уничтожать их психологически. Для меня было бы невозможно жить там, просто потому что здание угнетает.

То же самое происходит со всеми современными технологиями, которые преподносятся нам как прогресс и то, что облегчает жизнь. Они были созданы с целью зарабатывания денег и контроля над нами, и так будет всегда. Сколько бы преимуществ ни давал вам смартфон, те, кто богатеет, собирая ваши данные и следя за вами, всегда будут получать больше выгоды, чем вы. Если раньше говорили, что «знание – сила», то сегодня следует говорить, что «информация – сила». Чем больше правители знают о своей пастве, тем лучше они могут над ней властвовать – в этом смысле технология в целом является мощным инструментом контроля, позволяющим предсказывать и тем самым препятствовать объединению людей для нападения на то, что их угнетает.

Этим смартфонам, кажется, нужно немного больше, чем просто немного электричества… В нашем поколении, которое, по крайней мере, знало мир без смартфонов, возможно, еще есть люди, которые понимают, о чем я говорю, которые все еще знают, каково это – вести дискуссию, не глядя на телефон каждые тридцать секунд, заблудиться и открыть для себя новые места, или поспорить о чем-то, не обращаясь за ответом к Google. Но я не хочу возвращаться в прошлое, хотя это было бы невозможно.

Но чем больше технологии проникают в нашу жизнь, тем сложнее их уничтожить. Что, если мы – одно из последних поколе-