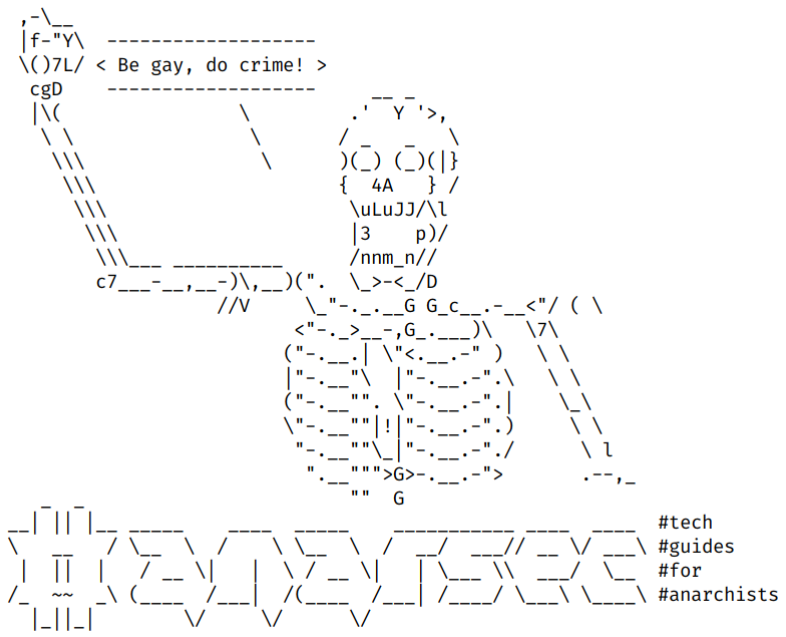
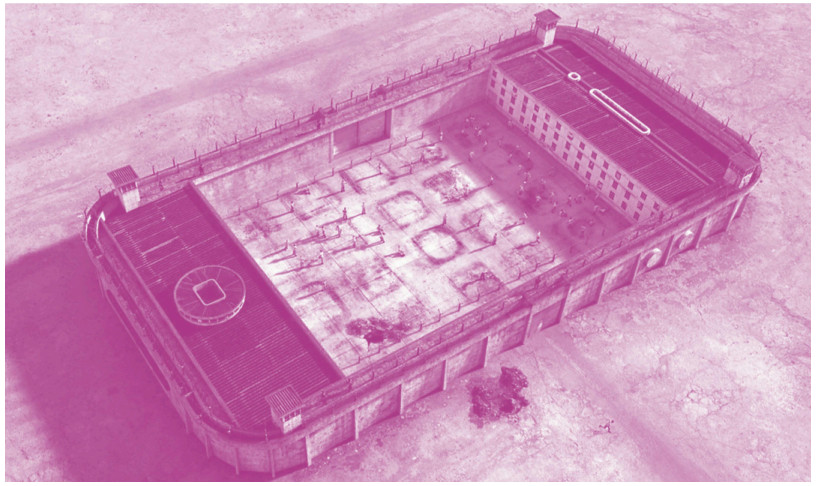
Η αποτελεσματική κουλτούρα ασφάλειας και η επιχειρησιακή ασφάλεια εμποδίζουν τις δυνάμεις καταστολής να γνωρίζουν για τις συγκεκριμένες εγκληματικές μας δραστηριότητες, αλλά και για τη ζωή μας, τις σχέσεις μας, τα μοτίβα μετακίνησής μας και ούτω καθεξής. Αυτή η γνώση είναι ένα τεράστιο πλεονέκτημα για τον περιορισμό των υπόπτων και τη διεξαγωγή στοχευμένης παρακολούθησης. Αυτό το άρθρο θα περιγράψει μερικές στρατηγικές για να σκοτώσετε τον μπάτσο στην τσέπη σας




# Σκότωσε τον μπάτσο στην τσέπη σου



Σειρά: Άμυνα

Αυτή η έκδοση της μπροσούρας τροποποιήθηκε τελευταία φορά στις 2024-04-23. Επισκέψου το anarsec.guide/el για να δεις εάν έχει ενημερωθεί από τότε.

Το σύμβολο στιλέτο † σε μια λέξη σημαίνει ότι υπάρχει μια καταχώριση στο γλωσσάρι για αυτήν. Ai ferri corti.

Το AnarSec είναι ένα νέο βοήθημα που έχει σχεδιαστεί για να βοηθήσει τους αναρχικούς να πλοηγηθούν στο εχθρικό έδαφος της τεχνολογίας — αμυντικοί οδηγοί για ψηφιακή ασφάλεια και ανωνυμία, καθώς και επιθετικοί οδηγοί για χάκινγκ. Όλοι οι οδηγοί διατίθενται σε μορφή booklet για εκτύπωση και θα ενημερώνονται.

# Άμυνα

### *Tails*

- Tails for Anarchists
- Tails Best Practices

### *Qubes OS*

- Qubes OS for Anarchists

### *Τηλέφωνα*

- **Σκότωσε τον μπάτσο στην τσέπη σου**
- GrapheneOS for Anarchists

### *Γενικά*

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

# Επίθεση

*Προσεχώς*

# Contents

Η αποτελεσματική κουλτούρα ασφάλειας και η επιχειρησιακή ασφάλεια[1] εμποδίζουν τις δυνάμεις καταστολής να γνωρίζουν για τις συγκεκριμένες εγκληματικές μας δραστηριότητες, αλλά και για τη ζωή μας, τις σχέσεις μας[2], τα μοτίβα μετακίνησής μας και ούτω καθεξής. Αυτή η γνώση είναι ένα τεράστιο πλεονέκτημα για τον περιορισμό των υπόπτων και τη διεξαγωγή στοχευμένης παρακολούθησης. Αυτό το άρθρο θα περιγράψει μερικές στρατηγικές για να σκοτώσετε τον μπάτσο στην τσέπη σας

Η τοποθεσία του τηλεφώνου σας παρακολουθείται ανά πάσα στιγμή[3] και αυτά τα δεδομένα συλλέγονται από ιδιωτικές εταιρείες, επιτρέποντας στην αστυνομία να παρακάμψει την ανάγκη έκδοσης εντάλματος. Τα αναγνωριστικά υλικού και οι πληροφορίες συνδρομής[4] του τηλεφώνου καταγράφονται από κάθε πύργο κινητής τηλεφωνίας στον οποίο συνδέεται το τηλέφωνό σας. Υπηρεσίες hacking, όπως η Pegasus[5], θέτουν τον πλήρη συμβιβασμό των τηλεφώνων σε απόσταση αναπνοής ακόμη και από τις τοπικές αρχές επιβολής του νόμου και είναι "μηδενικό κλικ", που σημαίνει ότι δεν εξαρτώνται από το αν κάνετε κλικ σε έναν σύνδεσμο ή ανοίξετε ένα αρχείο για να χακάρουν το τηλέφωνό σας. Από την άλλη πλευρά, αφού περισσότεροι από 30 εμπρησμοί σε μια μικρή πόλη της Γαλλίας έμειναν ανεξιχνίαστοι, οι ερευνητές παραπονέθηκαν[6] ότι «είναι αδύνατο να χρησιμοποιηθούν δεδομένα τηλεφώνου ή οχήματος επειδή λειτουργούν χωρίς τηλέφωνα ή αυτοκίνητα!»

[1] notrace.how/blog/a-base-to-stand-on/mia-base-gia-na-statheis.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/



## 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).

## 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 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).

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



# Κρυπτογράφηση και γεωεντοπισμός

Σε μια πρόσφατη κατασταλτική επιχείρηση[7] εναντίον ενός αναρχικού, η αστυνομία παρακολούθησε τη γεωγραφική θέση του flip phone του υπόπτου σε πραγματικό χρόνο και έφτιαξε μια λίστα με όλους όσους είχε καλέσει ο ύποπτος. Είναι γνωστό ότι τέτοιες παρακολουθήσεις δεν είναι ασυνήθιστες, και όμως πολλοί σύντροφοι έχουν μαζί τους ένα κινητό τηλέφωνο όπου κι αν πάνε, ή κάνουν μη κρυπτογραφημένες κλήσεις σε άλλους αναρχικούς. Πιστεύουμε ότι και οι δύο αυτές πρακτικές πρέπει να αποφευχθούν. Ας μην κάνουμε τη δουλειά της αστυνομίας και των υπηρεσιών πληροφοριών τόσο εύκολη, παραδίδοντάς τους τα κοινωνικά μας δίκτυα και το ιστορικό γεωγραφικού εντοπισμού σε ασημένιο πιάτο.

Εάν δεν φύγετε από το σπίτι με τηλέφωνο, η αστυνομία θα πρέπει να καταφύγει σε φυσική παρακολούθηση για να προσδιορίσει πού βρίσκεστε, η οποία απαιτεί πόρους και είναι ανιχνεύσιμη. Εάν ποτέ βρεθείτε υπό φυσική παρακολούθηση, το πρώτο βήμα του ερευνητή είναι να κατανοήσει το «προφίλ κίνησης» σας και το ιστορικό γεωγραφικής θέσης του τηλεφώνου σας παρέχει μια λεπτομερή εικόνα των καθημερινών σας μοτίβων.

Μερικοί αναρχικοί ανταποκρίνονται στα προβλήματα με τα smartphones χρησιμοποιώντας flip phones ή σταθερά τηλέφωνα για να επικοινωνούν μεταξύ τους, αλλά αυτό δεν είναι μια καλή λύση. Τα κινητά και σταθερά τηλέφωνα δεν υποστηρίζουν κρυπτογραφημένη επικοινωνία†, οπότε το κράτος μαθαίνει ποιος μιλάει σε ποιον και για τι μιλάει. Ένας πρωταρχικός στόχος της στοχευμένης επιτήρησης είναι η χαρτογράφηση του κοινωνικού δικτύου του στόχου προκειμένου να εντοπιστούν άλλοι στόχοι. Ο μόνος τρόπος για να αποφύγουμε να δώσουμε αυτές τις πληροφορίες στους εχθρούς μας είναι να χρησιμοποιήσουμε μόνο κρυπτο-

[7] notrace.how/resources/el/#ivan

γραφημένα μέσα[8] για να επικοινωνήσουμε με άλλους αναρχικούς μέσω της τεχνολογίας.

# Μοτίβα μεταδεδομένων

Η κανονικοποίηση της συνεχούς συνδεσιμότητας εντός της κυρίαρχης κοινωνίας έχει οδηγήσει ορισμένους αναρχικούς να σημειώσουν σωστά ότι τα μεταδεδομένα† του τηλεφώνου είναι χρήσιμα για τους ερευνητές. Ωστόσο, το συμπέρασμα που βγάζουν κάποιοι από αυτή τη διαπίστωση, ότι δηλαδή "δεν πρέπει ποτέ να κλείνουμε το τηλέφωνο"[9], μας οδηγεί σε λάθος κατεύθυνση. Η λογική τους είναι ότι οι αλληλεπιδράσεις σας με την τεχνολογία σχηματίζουν ένα βασικό μοτίβο μεταδεδομένων και οι στιγμές που αποκλίνουν από αυτή τη βασική γραμμή γίνονται ύποπτες εάν συμπίπτουν με το πότε συμβαίνει μια δράση, η οποία μπορεί να χρησιμοποιηθεί από τους ερευνητές για να περιορίσουν τους υπόπτους. Ενώ αυτό είναι αλήθεια, το αντίθετο συμπέρασμα είναι πολύ πιο λογικό: οι αναρχικοί θα πρέπει να ελαχιστοποιήσουν τη δημιουργία μοτίβων μεταδεδομένων στα οποία οι ερευνητές θα έχουν πρόσβαση.

Οι συνδέσεις μας με τις υποδομές της κυριαρχίας πρέπει να παραμείνουν αδιαφανείς και απρόβλεπτες, αν θέλουμε να διατηρήσουμε την ικανότητά μας να χτυπήσουμε τον εχθρό. Τι γίνεται αν η αναγνώριση που απαιτείται για μια δράση περιλαμβάνει ένα ολόκληρο Σαββατοκύριακο μακριά από ηλεκτρονικές συσκευές;Ή ας ξεκινήσουμε με το απλό γεγονός ότι τα τηλέφωνα πρέπει να αφήνονται στο σπίτι κατά τη διάρκεια μιας δράσης - αυτό γίνεται η εξαίρεση σε ένα μοτίβο μόνο αν τα τηλέφωνα μας συνοδεύουν κατά τα άλλα όπου κι αν πάμε.Σε μια κανονιστικά "πάντα συνδεδεμένη" ζωή, οποιαδήποτε από αυτές τις αλλαγές μεταδεδομένων θα κολλήσει σαν πονεμένος αντίχειρας, αλλά αυτό δεν συμβαίνει εάν αρνηθείτε να είστε συνεχώς συνδεδεμένοι. **Για να ελαχιστο-**

[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



## 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".

## 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].

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

[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/

## 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!

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].

[41] anarsec.guide/glossary/#encryption

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

[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/



**ποιήσετε το αποτύπωμα μεταδεδομένων, πρέπει να αφήσετε το τηλέφωνό σας στο σπίτι από προεπιλογή.**

# Χρειάζεστε πραγματικά ένα τηλέφωνο;

Τα τηλέφωνα έχουν αποικίσει την καθημερινή ζωή επειδή οι άνθρωποι έχουν ενσταλαχθεί με την πεποίθηση ότι χρειάζονται *σύγχρονη* επικοινωνία κάθε στιγμή. *Σύγχρονη*† σημαίνει ότι δύο ή περισσότερα μέρη επικοινωνούν σε πραγματικό χρόνο, σε αντίθεση με κάτι *ασύγχρονο*† όπως το ηλεκτρονικό ταχυδρομείο, όπου τα μηνύματα αποστέλλονται σε διαφορετικές χρονικές στιγμές. Αυτή η «ανάγκη» έχει κανονικοποιηθεί, αλλά αξίζει να αντισταθούμε μέσα στον αναρχικό χώρο. Η αναρχία μπορεί να είναι μόνο αντιβιομηχανική[10]. Πρέπει να μάθουμε να ζούμε χωρίς τις ανέσεις που μας πωλούν οι εταιρείες τηλεπικοινωνιών, πρέπει να υπερασπιστούμε (ή να αναζωπυρώσουμε) την ικανότητά μας να ζούμε χωρίς να είμαστε συνδεδεμένοι στο Διαδίκτυο ανά πάσα στιγμή, χωρίς αλγοριθμικές οδηγίες σε πραγματικό χρόνο και χωρίς την άπειρη ευελιξία να αλλάζουμε σχέδια την τελευταία στιγμή.

Εάν αποφασίσετε να χρησιμοποιήσετε ένα τηλέφωνο, προκειμένου να δυσκολέψετε όσο το δυνατόν περισσότερο έναν αντίπαλο να το γεωπαρακολουθήσει, να υποκλέψει τα μηνύματά του ή να το χακάρει, χρησιμοποιήστε το GrapheneOS[11]. Αν μπορούμε να συμφωνήσουμε να **χρησιμοποιούμε μόνο κρυπτογραφημένες επικοινωνίες[12] για να επικοινωνούμε με άλλους αναρχικούς**, αυτό αποκλείει τα flip phones και τα σταθερά τηλέφωνα. Το GrapheneOS είναι το μόνο λειτουργικό σύστημα smartphone που παρέχει εύλογο απόρρητο και ασφάλεια.

**Για να αποτρέψετε την παρακολούθηση των κινήσεών σας, αντιμετωπίστε το smartphone σαν σταθερό τηλέφωνο και**

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

[11] anarsec.guide/posts/grapheneos/

[12] anarsec.guide/posts/e2ee/

**αφήστε το στο σπίτι όταν είστε έξω από το σπίτι**. Ακόμα κι αν χρησιμοποιείτε μια κάρτα SIM που αγοράσατε ανώνυμα, εάν συνδεθεί με την ταυτότητά σας στο μέλλον, μπορεί να υποβληθεί αναδρομικά ερώτημα στον πάροχο υπηρεσιών για δεδομένα γεωγραφικής θέσης. Εάν χρησιμοποιείτε το τηλέφωνο όπως συνιστούμε (ως συσκευή μόνο Wi-Fi[13] που διατηρείται σε λειτουργία πτήσης ανά πάσα στιγμή), δεν θα συνδεθεί σε κεραίες κινητής τηλεφωνίας. Δεν αρκεί να αφήνετε το τηλέφωνο στο σπίτι μόνο όταν πηγαίνετε σε μια συνάντηση, πορεία ή δράση, επειδή αυτό θα είναι μια εξαίρεση από το κανονικό μοτίβο συμπεριφοράς σας και θα χρησιμεύσει ως ένδειξη ότι η εγκληματική δραστηριότητα λαμβάνει χώρα σε αυτό το χρονικό παράθυρο.

Μπορείτε να επιλέξετε να ζήσετε χωρίς τηλέφωνα εξ ολοκλήρου, εάν δεν αισθάνεστε ότι χρειάζεστε ένα "κρυπτογραφημένο σταθερό τηλέφωνο". Οι ακόλουθες στρατηγικές για την ελαχιστοποίηση της ανάγκης για τηλέφωνα βασίζονται σε υπολογιστές, όπου η σύγχρονη επικοινωνία είναι επίσης δυνατή αλλά πιο περιορισμένη.

## Γραφειοκρατία

Πολλοί γραφειοκρατικοί θεσμοί με τους οποίους είμαστε αναγκασμένοι να ασχοληθούμε καθιστούν δύσκολη τη ζωή χωρίς τηλέφωνο: υγειονομική περίθαλψη, τραπεζικές συναλλαγές κ.λπ. Η επικοινωνία με τις γραφειοκρατίες δεν χρειάζεται να είναι κρυπτογραφημένη, επομένως μπορείτε να χρησιμοποιήσετε μια εφαρμογή Voice over Internet Protocol (VoIP)[†]. Αυτό σας επιτρέπει να πραγματοποιείτε τηλεφωνικές κλήσεις μέσω του Διαδικτύου και όχι μέσω πύργων κινητής τηλεφωνίας. Οποιαδήποτε εφαρμογή VoIP που είναι διαθέσιμη σε έναν υπολογιστή είναι ασύγχρονη επειδή δεν κουδουνίζει όταν ο υπολογιστής είναι απενεργοποιημένος — βασίζεστε στη λειτουργία αυτόματου τηλεφωνητή για να επιστρέψετε αναπάντητες κλήσεις. Για παράδειγμα, μια υπηρεσία όπου

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



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].

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].

# Παράρτημα: Γλωσσάρι

## 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.).

[35] anarsec.guide/posts/linux
[36] anarsec.guide/posts/qubes/
[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

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 "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

[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/
[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



πως το jmp.chat[14] σας δίνει έναν αριθμό VoIP, τον οποίο μπορείτε να πληρώσετε σε Bitcoin και πραγματοποιείτε κλήσεις χρησιμοποιώντας μια εφαρμογή XMPP — το Cheogram[15] λειτουργεί καλά.

Το VoIP συνήθως λειτουργεί για οποιονδήποτε έλεγχο ταυτότητας δύο παραγόντων† (2FA) χρειάζεστε (όταν μια υπηρεσία απαιτεί να λάβετε έναν τυχαίο αριθμό για να συνδεθείτε). Οι διαδικτυακοί αριθμοί τηλεφώνου[16] είναι μια άλλη επιλογή. Αν και συνήθως πιο ακριβό από το VoIP, ένα αποκλειστικό flip phone ή σταθερό τηλέφωνο λειτουργεί επίσης καλά για την πραγματοποίηση και λήψη «γραφειοκρατικών» κλήσεων από το σπίτι, όπως αυτές που αναφέρονται παραπάνω.

## Επικοινωνία

Το να μην κουβαλάτε το τηλέφωνο παντού απαιτεί μια αλλαγή στον τρόπο που κοινωνικοποιείστε, αν έχετε ήδη πιαστεί στο δίχτυ[17]. Το να προσπαθούμε σκόπιμα να ελαχιστοποιήσουμε τη διαμεσολάβηση των οθονών στις σχέσεις μας είναι ένας πολύτιμος στόχος από μόνος του.

Η χρήση ενός "κρυπτογραφημένου σταθερού τηλεφώνου" για την πραγματοποίηση τηλεφωνικών κλήσεων και ενός υπολογιστή για κρυπτογραφημένα μηνύματα μας επιτρέπει να αποφύγουμε την ατελείωτη ροή ειδοποιήσεων σε μια συσκευή που είναι πάντα προσβάσιμη.

Θα έκανε σε όλους μας καλό να ρίξουμε μια σκληρή ματιά στη μονοκαλλιέργεια των ομαδικών συνομιλιών Signal που έχουν αντικαταστήσει τις πρόσωπο με πρόσωπο συναντήσεις σε ορισμένα μέρη του αναρχικού χώρου. Αυτή η σύλληψη της οργάνωσης των σχέσεων από την κουλτούρα των smartphones μας αναγκάζει

[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

σε μια ατελείωτη συνάντηση που είναι σχετικά εύκολο να επιτηρηθεί.

Τούτου λεχθέντος, η κρυπτογραφημένη επικοινωνία μπορεί να είναι χρήσιμη για τον ορισμό ημερομηνίας και ώρας συνάντησης ή για έργα που μοιράζονται σε μεγάλες αποστάσεις. Δείτε το Encrypted Messaging for Anarchists[18] για διάφορες επιλογές κατάλληλες για ένα αναρχικό μοντέλο απειλής†.

## Κλήσεις έκτακτης ανάγκης

Ένας περαστικός στο δρόμο θα σας δανείσει συχνά το τηλέφωνό του για να κάνετε μια επείγουσα κλήση εάν του πείτε ότι το δικό σας έχει ξεμείνει από μπαταρία. Για να λαμβάνετε κλήσεις έκτακτης ανάγκης, εάν δεν μπορούν να επικοινωνήσουν μαζί σας όπως περιγράφεται παραπάνω, μπορούμε να σταματήσουμε ο ένας από το σπίτι του άλλου ή να κανονίσουμε εκ των προτέρων check-in μέσω κρυπτογραφημένων μηνυμάτων. Ποια σενάρια απαιτούν πραγματικά να είστε διαθέσιμοι για να λάβετε μια κλήση ανά πάσα στιγμή; Αν αυτά υπάρχουν πραγματικά στη ζωή σας, μπορείτε να οργανωθείτε γύρω τους χωρίς να προβάλλετε αυτή την επείγουσα ανάγκη σε όλους τους άλλους τομείς και στιγμές.

## Οδηγίες

Αγοράστε έναν χάρτινο χάρτη της περιοχής σας και φέρτε τον μαζί σας. Για μεγαλύτερες διαδρομές ή διαδρομές όπου χρειάζεστε οδηγίες, χρησιμοποιήστε το OpenStreetMap[19] για να τις σημειώσετε εκ των προτέρων.

## Μουσική και podcast

Εξακολουθούν να κάνουν MP3 players! Για πολύ χαμηλότερη τιμή, μπορείτε να παίξετε μουσική και podcast, αλλά η συσκευή δεν διαθέτει GPS ή ραδιοφωνικό υλικό. Ωστόσο, αυτό δεν σημαίνει ότι

[18] anarsec.guide/posts/e2ee/

[19] openstreetmap.org/



μιλάμε για έναν εντελώς διαφορετικό κόσμο; Και αν δεν μπορούμε καν να μιλήσουμε για έναν άλλο κόσμο, πώς μπορούμε να τον φτάσουμε;

Η άμεση επικοινωνία μεταξύ αυτόνομων ατόμων είναι η βάση κάθε κοινής εξέγερσης, είναι το σημείο εκκίνησης κοινών ονείρων και κοινών αγώνων. Χωρίς αδιαμεσολάβητη επικοινωνία, ένας αγώνας ενάντια σε αυτόν τον κόσμο και για την ελευθερία είναι αδύνατος. Ας ξεφορτωθούμε λοιπόν τα smartphones και ας συναντηθούμε πρόσωπο με πρόσωπο σε μια εξέγερση εναντίον αυτού του κόσμου! Ας γίνουμε ανεξέλεγκτοι!

*από athens.indymedia.org*[21]

# Παράρτημα: Προτάσεις

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…"

[21] athens.indymedia.org/post/1631201

[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/

σότερα γνωρίζουν οι κυβερνήτες για τα ποίμνιά τους, τόσο καλύτερα μπορούν να τα κυριαρχήσουν – με αυτή την έννοια, η τεχνολογία στο σύνολό της είναι ένα ισχυρό εργαλείο ελέγχου για να προβλέψει και έτσι να αποτρέψει τους ανθρώπους από το να ενωθούν για να επιτεθούν σε αυτό που τους καταπιέζει.

Αυτά τα smartphone φαίνεται να χρειάζονται λίγο περισσότερο από λίγη ηλεκτρική ενέργεια... Στη γενιά μας, η οποία τουλάχιστον γνώριζε έναν κόσμο χωρίς smartphones, μπορεί να υπάρχουν ακόμα μερικοί άνθρωποι που καταλαβαίνουν για τι πράγμα μιλάω, που εξακολουθούν να ξέρουν πώς είναι να έχεις μια συζήτηση χωρίς να κοιτάς το τηλέφωνό τους κάθε τριάντα δευτερόλεπτα, να χάνεσαι και να ανακαλύπτεις νέα μέρη με αυτόν τον τρόπο ή να συζητάς κάτι χωρίς να ρωτάς αμέσως την Google για την απάντηση. Αλλά δεν θέλω να επιστρέψω στο παρελθόν, παρόλο που δεν θα ήταν δυνατό ούτως ή άλλως, αλλά όσο περισσότερο η τεχνολογία διεισδύει στη ζωή μας, τόσο πιο δύσκολο γίνεται να την καταστρέψουμε. Τι γίνεται αν είμαστε μία από τις τελευταίες γενιές που μπορούν να σταματήσουν αυτή την εξέλιξη των ανθρώπων σε πλήρως ελεγχόμενα ρομπότ;

Και τι γίνεται αν κάποια στιγμή δεν μπορέσουμε να αντιστρέψουμε αυτή την εξέλιξη; Η ανθρωπότητα έχει φτάσει σε ένα ιστορικά νέο στάδιο με την τεχνολογία. Ένα στάδιο όπου είναι σε θέση να εκμηδενίσει όλη την ανθρώπινη ζωή (πυρηνική ενέργεια) ή να την τροποποιήσει (γενετική τροποποίηση). Το γεγονός αυτό υπογραμμίζει για άλλη μια φορά την ανάγκη να δράσουμε σήμερα για να καταστρέψουμε αυτήν την κοινωνία. Για να γίνει αυτό, πρέπει να συναντήσουμε άλλους ανθρώπους και να επικοινωνήσουμε τις ιδέες μας.

Δεν είναι προφανές ότι αν αντί να μιλάμε μεταξύ μας, επικοινωνούμε μόνο σε μηνύματα των πέντε προτάσεων ή λιγότερο, θα υπάρξουν μακροπρόθεσμες επιπτώσεις; Προφανώς όχι. Πρώτα απ ’όλα, ο τρόπος που σκεφτόμαστε επηρεάζει τον τρόπο που μιλάμε και αντίστροφα - ο τρόπος που μιλάμε και επικοινωνούμε επηρεάζει τον τρόπο που σκεφτόμαστε. Αν μπορούμε να ανταλλάσσουμε μόνο τα πιο σύντομα και συνοπτικά μηνύματα, πώς μπορούμε να



δεν μπορείτε να εντοπίσετε γεωγραφικά από ένα MP3 player. Εάν συνδέεται σε Wi-Fi, η κατά προσέγγιση τοποθεσία της συσκευής αναπαραγωγής MP3 μπορεί να προσδιοριστεί από τη διεύθυνση IP της.

# Παράρτημα: Ενάντια στο smartphone

*από Fernweh (#24)*[20]

Είναι πάντα μαζί μας, πάντα ενεργό, ανεξάρτητα από το πού βρισκόμαστε ή τι κάνουμε. Μας κρατά ενήμερους για τα πάντα και για όλους: τι κάνουν οι φίλοι μας, πότε φεύγει το επόμενο μετρό και πώς θα είναι ο καιρός αύριο. Μας φροντίζει, μας ξυπνάει το πρωί, μας υπενθυμίζει σημαντικά ραντεβού και πάντα μας ακούει. Ξέρει τα πάντα για εμάς, πότε πηγαίνουμε για ύπνο, πού είμαστε και πότε, με ποιους επικοινωνούμε, ποιοι είναι οι καλύτεροι φίλοι μας, τι μουσική ακούμε και ποια είναι τα χόμπι μας. Και το μόνο που ζητάει είναι λίγο ηλεκτρικό ρεύμα πού και πού;

Όταν περπατάω σε μια περιοχή ή παίρνω το μετρό, το βλέπω σχεδόν σε όλους, και κανείς δεν μπορεί να αντέξει περισσότερο από μερικά δευτερόλεπτα χωρίς να πιάσει μανιωδώς την τσέπη του: το κινητό βγαίνει, ένα μήνυμα στέλνεται, ένα email ελέγχεται, μια φωτογραφία αρέσει. Το βάζουμε πάλι στην άκρη, ένα σύντομο διάλειμμα, και να ’μαστε πάλι, ξεφυλλίζοντας τις σημερινές ειδήσεις και τσεκάροντας τι κάνουν όλοι οι φίλοι...

Είναι ο σύντροφός μας όταν είμαστε στην τουαλέτα, στη δουλειά ή στο σχολείο και προφανώς βοηθά στην καταπολέμηση της πλήξης ενώ περιμένουμε ή εργαζόμαστε κ.λπ. Είναι ίσως αυτός ένας από τους λόγους για την επιτυχία όλων αυτών των τεχνολογικών συσκευών, ότι η πραγματική ζωή είναι τόσο βαρετή και μονότονη που μερικά τετραγωνικά εκατοστά οθόνης είναι σχεδόν πάντα πιο συναρπαστικά από τον κόσμο και τους ανθρώπους γύρω μας; Εί-

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

ναι σαν εθισμός (οι άνθρωποι έχουν σίγουρα συμπτώματα στέρησης...) ή έχει γίνει ακόμη και μέρος του σώματός μας; Χωρίς αυτό, δεν ξέρουμε πλέον πώς να προσανατολιστούμε και νιώθουμε ότι κάτι λείπει; Επομένως, δεν είναι πλέον μόνο ένα εργαλείο ή ένα παιχνίδι, αλλά ένα μέρος μας που ασκεί επίσης έναν ορισμένο έλεγχο πάνω μας, στον οποίο προσαρμόζουμε, για παράδειγμα, να μην φύγετε από το σπίτι μέχρι να φορτιστεί πλήρως η μπαταρία; Είναι το smartphone το πρώτο βήμα για να θολώσει τη γραμμή μεταξύ ανθρώπου και ρομπότ;

Όταν βλέπουμε τι προφητεύουν τεχνοκράτες όλων των ειδών (γυαλιά Google, εμφυτευμένα τσιπ κ.λπ.), φαίνεται σχεδόν σαν να οδεύουμε προς το να γίνουμε cyborgs, άνθρωποι με εμφυτευμένα smartphones που ελέγχουμε μέσω των σκέψεών μας (μέχρι να ελεγχθούν τελικά οι ίδιες οι σκέψεις μας). Δεν προκαλεί έκπληξη το γεγονός ότι τα μέσα μαζικής ενημέρωσης, οι εκπρόσωποι της κυριαρχίας, μας δείχνουν μόνο τις θετικές πτυχές αυτής της εξέλιξης, αλλά είναι συγκλονιστικό το γεγονός ότι σχεδόν κανείς δεν αμφισβητεί αυτή την άποψη. Είναι ίσως το πιο τρελό όνειρο κάθε κυβερνήτη: να μπορεί να παρακολουθεί τις σκέψεις και τις πράξεις του καθενός ανά πάσα στιγμή και να παρεμβαίνει αμέσως σε περίπτωση οποιασδήποτε διαταραχής. Απόλυτα ελεγχόμενες και επιτηρούμενες εργατικές μέλισσες που τους επιτρέπεται να διασκεδάζουν (εικονικά) ως ανταμοιβή, ενώ κάποιοι λίγοι κερδίζουν.

Με τις τεράστιες ποσότητες δεδομένων που είναι πλέον τόσο άμεσα διαθέσιμες από οποιονδήποτε και από όλους οποιαδήποτε στιγμή της ημέρας, ο κοινωνικός έλεγχος και η επιτήρηση έχουν επίσης φτάσει σε ένα εντελώς νέο επίπεδο. Αυτό τώρα πηγαίνει πολύ πέρα από την παρακολούθηση κινητών τηλεφώνων ή το κοσκίνισμα μηνυμάτων (όπως κατά τη διάρκεια των ταραχών του 2011 στο Ηνωμένο Βασίλειο). Με πρόσβαση σε έναν απίστευτο όγκο πληροφοριών, οι υπηρεσίες πληροφοριών είναι σε θέση να ορίσουν τι είναι «φυσιολογικό». Μπορούν να καθορίσουν ποιες τοποθεσίες είναι «φυσιολογικές» για εμάς, ποιες επαφές είναι «φυσιολογικές» κ.λπ. Εν ολίγοις, μπορούν γρήγορα να διαπιστώσουν και σχεδόν σε πραγματικό χρόνο εάν οι άνθρωποι αποκλίνουν α-



πό την «κανονική» συμπεριφορά τους. Αυτό δίνει σε μερικούς ανθρώπους τεράστια δύναμη, η οποία χρησιμοποιείται όποτε υπάρχει η ευκαιρία να επωφεληθούν από αυτή τη δύναμη (δηλαδή να παρακολουθούν τους ανθρώπους).

Η τεχνολογία είναι μέρος της εξουσίας, προέρχεται από την εξουσία και χρειάζεται εξουσία. Χρειάζεται ένας κόσμος στον οποίο οι άνθρωποι έχουν ακραία εξουσία για να καταστεί δυνατή η παραγωγή κάτι σαν το smartphone. Όλη η τεχνολογία είναι προϊόν του σημερινού καταπιεστικού κόσμου, είναι μέρος του και θα τον ενισχύσει. Στον σημερινό κόσμο, τίποτα δεν είναι ουδέτερο. Μέχρι σήμερα, όλα όσα έχουν αναπτυχθεί ή αναπτύσσονται έχουν σχεδιαστεί για να επεκτείνουν τον έλεγχο και να κερδίσουν χρήματα. Πολλές από τις καινοτομίες των τελευταίων δεκαετιών (όπως το GPS, η πυρηνική ενέργεια ή το διαδίκτυο) προέρχονται ακόμη και απευθείας από τον στρατό. Τις περισσότερες φορές αυτές οι δύο πτυχές πάνε χέρι-χέρι, αλλά η «ευημερία της ανθρωπότητας» σίγουρα δεν αποτελεί κίνητρο, ειδικά όταν αναπτύσσεται από τον στρατό.

Ίσως παίρνοντας το παράδειγμα της αρχιτεκτονικής μπορεί να απεικονίσει καλύτερα κάτι τόσο περίπλοκο όσο η τεχνολογία: ας πάρουμε μια άδεια και εγκαταλελειμμένη φυλακή, τι πρέπει να γίνει με αυτή τη δομή εκτός από το να την γκρεμίσουμε; Η ίδια η αρχιτεκτονική του, οι τοίχοι του, τα παρατηρητήρια του, τα κελιά του, περιέχουν ήδη τον σκοπό αυτού του κτιρίου: να φυλακίσει τους ανθρώπους και να τους καταστρέψει ψυχολογικά. Θα ήταν αδύνατο για μένα να ζήσω εκεί, απλά επειδή το κτίριο είναι καταπιεστικό. Είναι το ίδιο με όλες τις τεχνολογίες του σήμερα που μας παρουσιάζονται ως πρόοδος και ως κάτι που κάνει τη ζωή ευκολότερη. Σχεδιάστηκαν με την πρόθεση να βγάλουν χρήματα και να μας ελέγξουν, και πάντα θα το φέρουν αυτό. Ανεξάρτητα από το πόσα υποτιθέμενα οφέλη σας προσφέρει το smartphone σας, όσοι πλουτίζουν συλλέγοντας τα δεδομένα σας και παρακολουθώντας σας θα επωφελούνται πάντα περισσότερο από εσάς.

Αν στο παρελθόν λεγόταν ότι «η γνώση είναι δύναμη», σήμερα πρέπει να ειπωθεί ότι «η πληροφορία είναι δύναμη». Όσο περισ-