Stabilire una Base di Sicurezza per Anarchicx e Radicali

Testo originale in Inglese:
Tinderbox: An Offline Journal of Combative Anarchy, #8
2025

Il collettivo Tinderbox ha dato il permesso di pubblicare questo articolo online. Noi ci siamo sentitx libere di tradurlo in italiano.

Indice

- Stabilire una base di sicurezza per anarchicx e radicali
- Comunicazione digitale
  - -Messaggi e telefonate
  - -Uso dei social media
- Comunicazione faccia a faccia
  - -Dove parliamo
  - -Di cosa parliamo
- Uso di telefoni e dispositivi
- Lettura e ricerca
- Scrittura
- Azione
- Parlare con la polizia
- Discutere della repressione
- Casi studio per approfondire

Stabilire una base di Sicurezza per anarchicx e radicali

Questo testo è stato scritto in risposta a un bisogno continuo, a Philly e altrove, di pratiche di sicurezza più rigorose. Risponde anche in parte a "To the International Anarchist Movement: Three Security Proposals" del No Trace Project,[1] che include una proposta per stabilire localmente delle basi comuni di sicurezza. Loro stessx scrivono:

> "Le anarchiche che portano avanti azioni dirette dovrebbero analizzare i rischi associati alle loro azioni e prendere precauzioni adeguate: vestirsi in modo anonimo, fare attenzione alla videosorveglianza e alle tracce di DNA, e così via. Tuttavia, questo non basta. Se soltanto coloro che compiono azioni prendono precauzioni, diventa più facile per i nostri nemici individuare queste persone. Questo, innanzitutto, perché si distinguono: se solo poche compagne lasciano sempre il telefono a casa, per esempio, questo potrebbe diventare un punto di partenza evidente per un'indagine senza altre piste specifiche. E in secondo luogo perché i nostri nemici possono ottenere informazioni su di loro tramite amicizie che non partecipano alle azioni: se qualcuna non usa i social media ma viene menzionata nei social delle proprie amicizie, per esempio, un'indagine potrebbe analizzare i social di queste per ottenere informazioni su quella persona. Dovremmo quindi stabilire una base di sicurezza che tutte nelle reti anarchiche accettino di seguire, incluse coloro che non hanno mai partecipato ad azioni dirette e non intendono farlo."

> "Può essere difficile convincere le persone a seguire una simile base di sicurezza, soprattutto se pensano di non avere un interesse personale nel farlo. Se qualcuna è riluttante, dovremmo ricordargli che non è in gioco soltanto la sua sicurezza, ma anche quella di altre anarchiche intorno a lei che potrebbero stare compiendo o pianificando azioni dirette. Chiunque voglia che certe azioni avvengano ha interesse a rendere le reti anarchiche il più difficili possibile da reprimere per le autorità."

In questo testo cerchiamo di identificare bisogni specifici — per esempio diversi tipi di comunicazione reciproca — e di stabilire alcune pratiche di base condivise che possano renderci bersagli più difficili per la repressione statale. Sentiamo che ciò sia particolarmente urgente in quest'epoca di crescente repressione contro molte popolazioni oppresse negli Stati Uniti e contro le forme di resistenza più in generale. Questa repressione è stata imprevedibile, caotica e terrificante. Possiamo rafforzarci per continuare a lottare per l'anarchia e la liberazione stabilendo pratiche condivise nello spazio anarchico/radicale di Philadelphia che rendano tutti noi più sicuri.

Detto questo, la risposta dello Stato a forti lotte radicali non sarà mai né gradevole né prevedibile, e proporremmo raccomandazioni simili sulle pratiche di sicurezza indipendentemente da chi governa il paese. Queste raccomandazioni si basano in parte sull'attuale livello di attività radicale presente a Philly, ma sono anche calibrate sul livello di attività verso cui stiamo lavorando, sul potenziale che vediamo. Questo potrebbe includere il ritorno di diffuse e prolungate insurrezioni nelle strade. Oppure, in assenza di sollevazioni di massa, potrebbe significare una cultura più ampia ed escalation di azioni dirette e attacchi, una diffusione più vasta delle idee anarchiche e liberatorie, e l'adozione di pratiche autonome da parte di più persone. Questi sono solo alcuni esempi, e ognuna avrà la propria visione, ma il punto è che se vogliamo diventare una minaccia più seria, ha senso prepararci a essere trattate come tale.

Possiamo imparare da altri paesi e contesti, così come dal nostro, in che modo lo Stato potrebbe indagare e reagire a qualcosa come una campagna prolungata di azioni dirette e attacchi intensificati. In quei contesti, quando non ci sono sospetti immediati ed evidenti, lo Stato è costretto a investigare in modi che ci insegnano molto sulle sue risorse e su come possiamo mitigare quelle risposte statali. Qui a Philly, non molto tempo fa, c'è stata una perquisizione domiciliare — che possiamo presumere fosse collegata a un'indagine di polizia più ampia — contro attiviste studentesche in risposta agli accampamenti di solidarietà nei campus e ad alcuni lievi atti vandalici. Quindi questo

tipo di situazione non è ipotetico.

Immaginiamo che ci sia un'indagine attiva contro una scena anarchica a Philly (o contro qualsiasi parte dello spazio radicale che senti rilevante). Immaginiamo anche che gli individui prendano solide precauzioni riguardo alle attività criminalizzate e che non ci siano sospetti evidenti per episodi specifici. Basandoci su informazioni provenienti da altri contesti, questa indagine di polizia potrebbe apparire così:

- Un primo passo sarebbe geolocalizzare i telefoni per tenere traccia delle posizioni di certi anarchici, di chi incontrano, ecc.
- I telefoni di alcune persone verrebbero intercettati (non necessariamente di chi ti aspetteresti).
- Un passo successivo sarebbe installare microspie e/o telecamere negli spazi anarchici, fuori (o dentro) le case di anarchiche e/o nei luoghi di incontro abituali conosciuti. I localizzatori GPS possono anche essere facilmente collocati sulle auto delle persone.
- Un ulteriore passo sarebbe la sorveglianza fisica. Potrebbe essere evidente, come pattuglie occasionali davanti a casa, e/o del tipo che richiede una certa esperienza per essere individuata con affidabilità.[²]

Basandoti, per esempio, sull'uso che fai del telefono: cosa scoprirebbe la polizia se fossi una dei bersagli di questo tipo di sorveglianza? Cosa verrebbero a sapere di te se venisse preso di mira una tua amicizia? Tieni presente che non possiamo mai essere completamente "sicure" e che il fatto di non esserlo totalmente non dovrebbe mai portarci all'inazione. Ma dovremmo anche considerare quali piccoli passi possiamo fare fin da ora verso una maggiore sicurezza, per noi stesse e per le nostri amicizie.

La nostra proposta è iniziare lavorando sulle proprie pratiche. Cercate di stabilire pratiche condivise con le persone più vicine e/o con individui con cui già portate avanti progetti specifici. Tenete presente che il livello di sicurezza che scegliete per un progetto specifico dovrebbe dipendere dal progetto stesso. Per

esempio, organizzare un free store mensile al parco sarà diverso dal pianificare un'azione di sabotaggio tra tre persone. Non ci concentriamo su questo qui perché stiamo cercando di mantenere il testo breve e diretto. Ma per maggiori informazioni su come valutare i bisogni di sicurezza specifici di un progetto particolare, vedi la "Threat Library" del No Trace Project.[4]

Le seguenti sono proposte basate su errori che noi abbiamo fatto o visto fare in spazi anarchici e radicali. Sono pensate per essere discusse. Se hai commenti o critiche su queste proposte, scrivi a: phillysecuritybaseline@riseup.net.

Comunicazione digitale

-Messaggi e telefonate

Una regola generale è questa: quando scrivi messaggi o parli al telefono (incluso Signal), chiediti: vorrei che ciò che sto dicendo venisse letto in aula durante un processo?

- Non usare Signal per organizzare nulla di anche solo lontanamente illegale, inclusi progetti editoriali anarchici o altri scritti che rivendichino o incoraggino attività criminalizzate.
- Se necessario, usa Signal per fissare incontri o conversazioni di persona, durante i quali organizzerete poi ciò che volete organizzare.
- Non alludere su Signal al fatto che stai organizzando qualcosa di "piccante", o che la conversazione che stai cercando di fissare lo sarà, ecc. Per favore, comportati normalmente. Omettere certi dettagli o evitare certi argomenti via messaggio può sembrare scomodo all'inizio, ma col tempo diventa più naturale.
- Evita di entrare in grandi chat di gruppo. Se la polizia arresta qualcuna che ha con sé il proprio dispositivo, oppure fa una perquisizione e sequestra dispositivi ancora accesi, spesso può esaminarli e questo compromette ogni altra persona presente nella chat di gruppo con il proprietario del dispositivo sequestrato. Ne vale davvero la pena? Considera se esistono altri modi per ricevere le informazioni di quella chat.

-Uso dei Social Media

I profili social sono completamente pubblici o, nel peggiore dei casi, estremamente facili da consultare per forze dell'ordine, fascisti e altri avversari. I social media sono la prima cosa che la polizia consulta per saperne di più sulle reti radicali o anarchiche locali, proprio perché sono così accessibili. Se consideri che tutto ciò che dici sui social può essere letto dalle forze dell'ordine e che quantomeno viene conservato passivamente in qualche archivio dati per usi futuri, continuare a regalare informazioni (di qualsiasi tipo) su un piatto d'argento comincia a sembrare piuttosto assurdo. Rendiamoglielo più difficile! :)

- Raccomandiamo di non usare i social media per la maggior parte dei progetti. Per progetti con una dimensione sociale — come un centro sociale anarchico o una cassa di solidarietà per le cauzioni — i social possono talvolta aiutare a diffondere consapevolezza sul progetto. Ma i social non dovrebbero essere usati per organizzare, valutare l'efficacia della nostra organizzazione o comunicare sul radicalismo in modi diversi dalla pubblicazione di informazioni su eventi o progetti.
- Valuta la possibilità di non avere profili social personali, dato che rappresentano una risorsa incredibilmente facile per le indagini di polizia. Offrono un'enorme quantità di informazioni sulla personalità e la vita privata delle persone, aiutano a tracciare reti sociali e politiche, mappano le attività delle persone, e così via.

Eliminare i propri account social può sembrare impossibile perché può dare l'impressione di rinunciare a qualcosa di importante per la nostra felicità e il nostro benessere, e in effetti in parte è così: queste piattaforme sono progettate per renderci dipendenti dai picchi di dopamina che ci procurano. Ma non si tratta solo di rinunciare a qualcosa; si tratta anche delle possibilità che ci offre il non usare i social. Immagina i mondi che possiamo aprire una volta ridotto l'uso di queste forme digitali alienate di relazione reciproca, e avendo più tempo e spazio per quella felicità e quel benessere personale che derivano da relazioni fondate su connessioni reali. Qualcosa su cui

riflettere...

La conclusione: non parlare di altre anarchiche o di azioni sui social media. Non diffondere informazioni non pubbliche che possano essere utili a un'indagine di polizia.

Comunicazione Faccia a Faccia

- Dove Parliamo

- Non discutere di azioni illegali avvenute, di azioni che stai pianificando o di altre informazioni sensibili vicino ai telefoni, al chiuso, sul portico, nel giardino di casa, ecc.

- Fate una passeggiata, incontratevi in un parco, ecc.

- Quando pianificate azioni più intense, provate a incontrarvi in un punto concordato e poi camminare verso un altro luogo, idealmente uno in cui non siete mai state o che non frequentate abitualmente.

- Non rendete evidente con chi parlate di argomenti sensibili (per esempio chiedendo a qualcuna di "fare una passeggiata" nel mezzo di un gruppo di persone).

-Di Cosa Parliamo

- Non vantarti di azioni avvenute né lasciar intendere un tuo coinvolgimento.

- Se pensi abbia senso condividere informazioni sensibili con qualcuna, prova prima a chiedergli se vuole ascoltarle. È scorretto dire a qualcuna più di quanto abbia bisogno di sapere senza il suo consenso. Nell'eventualità che quella persona venga poi convocata davanti a un gran giurì o interrogata dalle

forze dell'ordine, sarà molto più facile per lei non dire nulla se realmente non sa niente.

- Non discutere del coinvolgimento in azioni dopo che sono avvenute, nemmeno con le persone con cui le hai compiute. A seconda dell'azione, un debriefing programmato poco dopo può costituire un'eccezione. Il punto è evitare di rievocare casualmente certe cose, soprattutto mesi o anni dopo.

- Se sei coinvolto in una pubblicazione o in un sito che discute e/o promuove azioni illegali, mantieni segreto il tuo coinvolgimento.[5]

Uso di Telefoni/Dispositivi

- Non portare assolutamente il telefono (o qualunque altro dispositivo connesso alla rete, inclusi laptop, smartwatch, baby monitor, GPS dell'auto) a qualunque attività illegale. Non portare telefoni o altri dispositivi connessi a conversazioni in cui vengono condivise informazioni private o confidenziali. Comprendi che, se lo fai, stai portando una potenziale spia all'azione o alla conversazione. È una cosa molto seria

.

- Evita di portare il telefono anche ad altri incontri o eventi in cui la mappatura delle reti sociali (che il tuo telefono potrebbe fornire alla polizia) sarebbe utile alle autorità. Per esempio workshop radicali, presentazioni, training, supporto ai detenuti, ecc.

- Valuta di non portare il telefono neppure quando incontri amicizie, dato che questo ostacola la capacità delle forze dell'ordine di mappare le reti sociali ed è sempre piacevole sapere che nessuno dei tuoi nemici[7] sta ascoltando e imparando dalle conversazioni tra te e le tue amicizie riguardo alla vostra vita privata, alle opinioni politiche, ai drammi della scena, ecc.

- Molte anarchiche a Philly hanno iniziato a lasciare il telefono a casa sempre o quasi sempre, e incoraggiamo questa pratica a

diffondersi ulteriormente. È importante che esista una cultura più ampia del non portare il telefono ovunque, così che le poche persone che già lo fanno non si distinguano troppo.

- Non attivare l'autenticazione biometrica (riconoscimento facciale, impronte digitali) sui tuoi dispositivi. La polizia può costringerti a usarla per sbloccare i dispositivi; non può obbligarti a digitare la password.

- Crittografa il telefono e il laptop, se li possiedi. Ricorda che se il dispositivo è acceso, la crittografia sarà facile da aggirare per la polizia. Se sei coinvolta in lotte o attività che comportano il rischio di una perquisizione in casa, dovrebbe diventare pratica standard spegnere telefoni e computer prima di andare a dormire. Questo garantisce che siano effettivamente crittografati e riduce i rischi durante perquisizioni all'alba.

- Non usare dispositivi non crittografati per attività legate all'anarchia o all'organizzazione radicale; idealmente, non usare affatto dispositivi non crittografati.

Lettura e Ricerca

- Usa Tor Browser per leggere articoli riguardanti attività criminalizzate o articoli rilevanti per future azioni che potresti compiere.

- Valuta di usare sempre una VPN quando sei su internet. Raccomandiamo Mullvad VPN; funziona in background e quasi non te ne accorgi. L'uso di una VPN riduce drasticamente la capacità degli avversari di accedere ai tuoi dati, anche senza usare Tor Browser.

- Usa Tails OS per fare ricerche su azioni illegali. Tails non lascia tracce di attività sul computer e forza tutte le connessioni internet attraverso la rete Tor.

- Usa Tails OS per moderare siti potenzialmente rischiosi.

- Se sei interessata o già coinvolta in azioni più intense e userai internet per documentarti o scrivere/inviare comunicati, puoi aggiungere ulteriori precauzioni all'uso di Tails. Non sono necessarie per tutte, ma rappresentano una buona pratica, soprattutto se sei già conosciuta dalla polizia come radicale o anarchica e quindi più probabilmente soggetta a sorveglianza.

- Procurati di persona un computer che userai esclusivamente per Tails.

- Assicurati di usare una chiavetta USB per Tails che non sia mai stata usata prima né manomessa.

- Non collegare mai questo laptop alla rete wifi di casa — usa internet altrove.[8]

- Tieni presente che non tutte le persone in un gruppo di affinità devono svolgere questi compiti; quindi, se le risorse condivise sono limitate, assicuratevi almeno che il gruppo abbia accesso ad almeno uno di questi computer se siete interessate a questo tipo di attività.

Scrittura

- Usa Tails per inviare comunicati.

- Soprattutto per azioni più pesanti, considera la possibilità di non scrivere un comunicato se l'azione parla da sé. Oppure scrivi un comunicato breve, prevalentemente descrittivo, evitando scelte lessicali riconoscibili, slang, stile di scrittura e altri potenziali identificatori. La polizia usa la linguistica forense per attribuire i testi ai loro autori.[10]

Azione

- Per favore, non usare un'auto per raggiungere un'azione illegale (a meno che non sia stata rubata in modo molto sicuro). Usa una bici o vai a piedi. Se si tratta di un'azione meno rischiosa e sei in città, puoi usare i mezzi pubblici con mascherina e contanti (o provare a non pagare il biglietto!). Talvolta è utile avere abbastanza contanti con sé per prendere un taxi in caso di emergenza e dover sparire rapidamente.[12]

- Esistono molte risorse su come vestirsi e altre precauzioni da adottare per partecipare a una manifestazione conflittuale o compiere atti vandalici; per esempio "Baby's First Black Bloc", "A Recipe for Nocturnal Direct Actions",[13] "PRISMA: Primer on Radical Information for Secure Militant Actions",[14] oppure "A Practical Security Handbook: No Trace Project Edition".[15]

- Leggi la zine "DNA You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces"[16] per le migliori pratiche su come evitare di lasciare DNA sulla scena di un'azione o nei dintorni.

Parlare con la Polizia

- Non parlare con la polizia. Questo non è negoziabile. Include essere fermate durante una manifestazione, ricevere la visita dell'FBI, essere interrogate in carcere, poliziotti che bussano alla porta o ti fermano per strada chiedendo qualcosa apparentemente casuale o scollegato dall'attività anarchica (in realtà potrebbe non esserlo affatto), essere contattate dall'accusa in un procedimento, ricevere una convocazione davanti a un gran giurì, ecc.

- In tutti i casi, dite che non potete parlare senza il vostro avvocato (va bene anche se non ne avete realmente uno). Probabilmente sarete obbligate a fornire nome e data di nascita (e forse

indirizzo) in caso di arresto, e questo va bene. Se ricevete una visita dell'FBI, chiedete il biglietto da visita.

- Dopo, contattate Up Against the Law o un altro gruppo locale contro la repressione e discutete con le vostre compagne se abbia senso diffondere informazioni sull'episodio nelle vostre reti. Non ogni interazione con la polizia richiede una dichiarazione pubblica (per esempio controlli stradali, arresti apolitici, arresti di massa durante manifestazioni, ecc.), ma in caso di visita dell'FBI, convocazione davanti a un gran giurì o altri tentativi di interrogatorio, di solito è utile diffondere ampiamente la notizia, poiché probabilmente collegata a un'indagine più ampia sulle vostre reti. Discutete di cosa ha chiesto la polizia e come l'ha chiesto; di cosa potrebbe essere utile sapere per altre persone coinvolte nelle lotte; e, se necessario, di come far circolare queste informazioni tra altre compagne. Questo riduce anche il senso di isolamento derivante dall'essere prese di mira dalla legge, che può sembrare molto peggiore se ci si sente sole. E questo ci porta all'ultimo argomento...

Discutere della Repressione

- Lo Stato sa chi è stato arrestate e quali sono le accuse; sa che l'FBI è venuta a casa tua, che qualcuno ha ricevuto una convocazione da un gran giurì, e così via. Le informazioni di base sulla repressione e sulle indagini di polizia dovrebbero essere condivise ampiamente affinché altre persone siano consapevoli del livello di attenzione che le anarchiche stanno attirando dalle forze dell'ordine e possano regolarsi di conseguenza.

- Praticamente tutte le informazioni già nelle mani della polizia e dell'accusa (per esempio quanto scritto in un affidavit of probable cause per un arresto) possono essere condivise con altre. Quando descrivete il motivo dell'arresto di qualcuna, assicuratevi di riferirvi alle informazioni dello Stato o a ciò che avete letto nei media ("La polizia sostiene che...", "L'imputata avrebbe...", "Ho

letto che…", ecc.). Non parlate dalla vostra esperienza personale e non dite che l'accusata ha fatto qualcosa di illegale; dite soltanto che è accusata di averlo fatto.

- Non speculate sul perché qualcuna possa aver ricevuto una certa accusa, ecc. Accontentatevi del fatto di non sapere nulla e di poter dire onestamente alla polizia che non potete riferire niente qualora veniste interrogati.

- Se per qualche motivo le forze dell'ordine vi interrogano o vi fanno domande su una scena anarchica di Philadelphia, su individui specifici, ecc., è vostra responsabilità informare le altre anarchiche dell'interrogatorio. Non c'è motivo di non farlo, a meno che non abbiate fornito informazioni durante quella conversazione e stiate cercando di nasconderlo. Se non avete risposto alle loro domande, non c'è ragione per non informare le compagne dell'accaduto.

Casi Studio per Approfondire

- "No Bars: Bringing Down the Techno-Prison"[17]
- "Cops and Robbers? A History of Investigative Techniques"[18]
- "Green Scared?"[19] di Rolling Thunder

Note

[1] https://notrace.how/blog/three-proposals/three-proposals.html
[2] Per maggiori informazioni sulla sorveglianza fisica e su come individuarla, vedi "Measures Against Surveillance"[3], che contiene esempi dalla Germania.
[3] https://notrace.how/resources/#measures-surveillance
[4] https://notrace.how/threat-library
[5] Negli Stati Uniti e altrove ci sono stati casi in cui persone che

moderavano siti web che ripubblicavano azioni criminalizzate sono state incriminate e hanno scontato pene detentive (si veda per esempio il caso degli SHAC 7). Esiste inoltre un precedente, in altri paesi, in cui individui presumibilmente coinvolti in pubblicazioni di giornali anarchici (che "premiano e giustificano l'azione criminale") sono stati accusati di appartenere a un'organizzazione criminale; inoltre la pubblicazione stessa è stata usata come punto di partenza per un'indagine (su attacchi diffusi) che non aveva altre piste investigative (si vedano gli scritti sul caso §129 a Monaco, come "Petrol, Printer Ink, and Paranormal Activity"[6]).
[6] https://actforfree.noblogs.org/2025/08/03/about-munich-2019-2025-petrol-printer-ink-and-paranormal-activity
[7] Nota del No Trace Project: termine che significa oppositori/nemici.
[8] Secondo la guida "Tails Best Practices" di AnarSec,[9] un avversario come la NSA potrebbe essere potenzialmente in grado di compromettere Tor tramite un attacco di correlazione. Quindi, se usi il wifi in uno spazio pubblico e viene effettuato un attacco di correlazione non mirato, l'indirizzo internet in quella situazione non ricondurrà direttamente a te come individuo. Nel caso di Jeremy Hammond, egli era già sotto sorveglianza e lo Stato effettuò attacchi di correlazione mirati presso la sua abitazione, poi usati come prove corroboranti nel suo processo: "Nello specifico, hanno correlato il traffico della rete Tor proveniente dalla casa del sospettato con gli orari in cui il suo alias anonimo risultava online nelle chatroom."
[9] https://anarsec.guide/posts/tails-best
[10] Vedi "Chi ha scritto questo?"[11] da Zündlumpen #76. su revs.noblogs.org per la traduzione in italiano
[11] https://notrace.how/resources/#who-wrote
[12] Negli ultimi due anni ci sono stati molti casi negli Stati Uniti in cui compagni sono stati identificati dalla polizia come sospetti e successivamente condannati anche perché avevano guidato un'auto o una motocicletta fino al luogo dell'azione.
[13] https://notrace.how/resources/#a-recipe
[14] https://notrace.how/resources/#prisma
[15] https://notrace.how/resources/#security-handbook-2
[16] https://notrace.how/resources/#dna-you-say
[17] https://rupture.noblogs.org/post/2002/10/04/no-bars
[18] https://notrace.how/resources/#cops-and-robbers
[19] https://notrace.how/resources/#green-scared