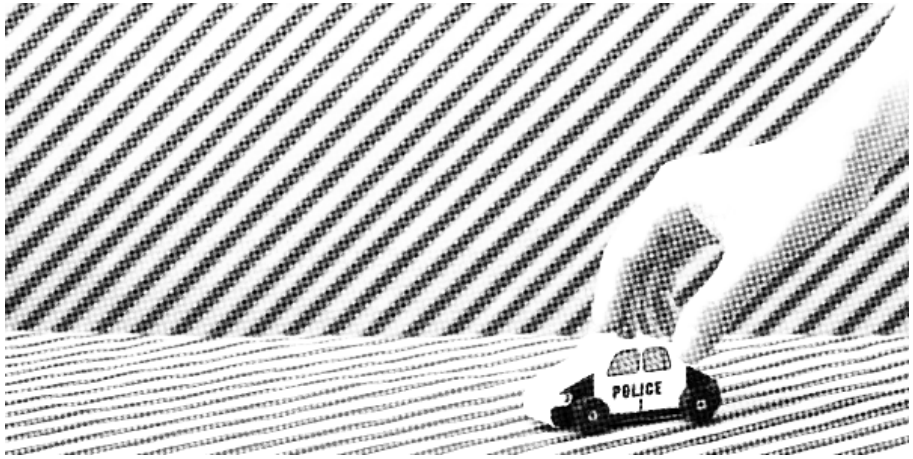
Det finns många guider därute som beskriver alltifrån hur du bäst bygger tidsin-ställda brandbomber till hur du hanterar DNA, anti-forensiska metoder och hur du bäst säkrar digital information mot husrannsakan eller statlig övervakning. Vissa av dem är över fyrtio år gamla, andra är nyare, vissa av dem håller än medan andra behöver uppdateras. Vi tänkte att det inte skulle skada med ett litet förslag, en liten att-tänka-på-artikel, som ligger någorlunda i fas med fiendens metoder.

Att (försöka) hålla snuten på avstånd



No Trace Project / No trace, no case. En samling verktyg för att hjälpa anarkister och andra aktivister **förstå** sina motståndares kapacitet, **motarbeta** försök till övervakning, och **agera** utan att åka dit.

I vissa sammanhang kan innehav av vissa dokument vara kriminaliserat eller dra till sig oönskad uppmärksamhet. Var försiktig med vilka zine du skriver ut och var du förvarar dem.

Att (försöka) hålla snuten på avstånd

Originaltext på svenska

2020

web.archive.org/web/20201117135555/
https://325.nostate.net/2020/09/16/svart-mane-black-moon-pdf

Layout

No Trace Project

notrace.how/resources/#att-forsoka-halla-snuten-pa-avstand

att minska risken för detta: Använd Linux, öppna aldrig okända mejl och var medveten om vad du laddar ner på datorn

- Vid en husrannsakan, dra ut strömmen/stäng av alla elektroniska apparater med hårddisk, minneskort eller nätverkskort

Det finns gott om fördjupande texter inom ämnet, så detta är bara att betrakta som en liten post it-lapp.

Till slut vill vi bara lyfta fram att målet för oss inte är att göra det så svårt, avancerat, tråkigt eller krävande som möjligt att agera, att fysiskt angripa den värld som vägrar oss vår frihet. Varje situation kräver sin analys, sina metoder och experiment, där våra förslag kan vara helt irrelevanta. Samtidigt har vi av flera generationers kamper lärt oss vad fienden har i sin arsenal och försökt att se bortom den. Vi försöker lära oss av våra egna och andra kamraters misstag men lika mycket av våra egna och andra kamraters framgångar.

Å ena sidan: vad är möjligt trots den intensiva övervakningen och forensiska kapaciteten. Å andra sidan: vilka luckor uppstår där de ännu inte lyckats utveckla eller pröva sina repressiva metoder? Vi kämpar av lust och längtan, vi måste vilja utmana oss själva och deras repression, annars är det ingen mening att vi kämpar. Fienden kan inte vara överallt hela tiden, skuggorna tillhör oss.

Det finns många guider därute som beskriver allt-ifrån hur du bäst bygger tidsinställda brandbomber till hur du hanterar DNA, anti-forensiska metoder och hur du bäst säkrar digital information mot husrannsakan eller statlig övervakning. Vissa av dem är över fyrtio år gamla, andra är nyare, vissa av dem håller än medan andra behöver uppdateras. Vi tänkte att det inte skulle skada med ett litet förslag, en liten att-tänka-på-artikel, som ligger någorlunda i fas med fiendens metoder. Lite lärdomar och erfarenheter blandat med ren teknisk info men i ett format som förhoppningsvis inte känns alltför stelt och auktoritärt.

Ibland känns det som att det råder ett extra repressivt klimat i världen eller den region en lever i men historiskt sett så råder det sällan mer repression i en tid än det gör i en annan. Den enkla förklaringen är att staten ständigt för ett krig mot sina fiender, det är bara mer påtagligt om en drabbas av det direkt eller indirekt, som individ, grupp eller helt samhälle. Undantagen må vara situationer som världskrig men även där så handlar det om andra mekanismer och i vår mening går det oftast att säga att repressionen är konstant, det vill säga, det går inte att tänka: det kommer inte att drabba mig. För förr eller senare kommer strålkastaren att vändas från gårdagens fiende till dig.

Att vi nämner detta är för att det i skrivande stund är många från ”vår generation” anarkister i ”vår region” i vid mening, som drabbats av en likartad repression. En generation som förhållandevis smärtfritt kunnat agera djärvt i sina attacker

mot staten och samtidigt komma undan med det, oftast utan att ens ha behövt tänka på nationalstaternas gränser eller, i vissa fall, den teknologiska och digitala utvecklingen. Det vi menar är alltså inte att folk har skitit i säkerheten, utan tvärtom att det har funnits en bra säkerhetskultur bland kamrater som grundar sig på icke-digitala metoder men som samtidigt tillåtit en utveckling av elektronisk infrastruktur för till exempel publikationer och för att dölja vem som umgås med vem bakom krypterad kommunikation (även om kommunikationen såklart aldrig innehållit något som avslöjat kriminella aktiviteter).

Det vi är ute efter är att denna generation har delat metoder med varandra och varit framgångsrika i respektive sammanhang men att det under de sista par åren vid flera tillfällen gripits kamrater eller att kamrater tvingats gå under jorden, där dessa metoder har avslöjats och säkerhetsrutinerna genomskådats, vilket påkallar allas vår uppmärksamhet. Vi behöver alltså diskutera, dela erfarenheter med varandra och överväga hur vi ska kunna springa om snuten, när de för ögonblicket tycks ha sprungit om oss. I vissa fall handlar det om att kamrater har varit slarviga med säkerheten och tillåtit sig att bli övervakade, kanske bara för att det har varit så enkelt under alla år och säkerhetsrutinerna till slut kändes överflödiga. I andra, mycket få fall, så handlar det om snutar som kan tänka utanför boxen. Oavsett vad så har deras repressiva framgångar gett dem en inblick i hur vi jobbar. Deras utredningar ger oss i sin

kommunicerar aldrig digitalt om något som vi inte lika gärna kan säga direkt till en snut eller åklagare; inte krypterat, inte med PGP, inte genom Signal, Telegram eller OTR eller ens i utkast på hemliga mejladresser. Vi använder inte Smartphones, inte privat, inte när vi skrider till handling. Det går t.ex. att använda Signal på dator men gör vi det, så är det för att dölja våra sociala kontakter, inte för att konspirera.

Själva grunden för att bespara sig själv och sina kamrater en massa problem, i vardagen såväl som vid en husrannsakan, är enligt oss att organisera sitt digitala liv så här (eller liknande uppställning):

- En dator för privata angelägenheter: surf, mejl, titta på film osv. Helst på ett krypterat Linuxsystem
- En dator med persistent TAILS för kontakt med kamrater, för projekt, för eventuell informationsinsamling och bearbetning eller författande av texter, bilder etc.
- Om aktionskommunikéer ska skrivas: ha ytterligare en dator utan nätverkskort med TAILS och använd den för att skriva men publicera aldrig från en dator eller ett nätverk som kan kopplas till dig
- Om du har externa hårddiskar: kryptera med t.ex. Veracrypt eller med Linux olika krypteringsmöjligheter
- Om staten lyckas komma in i ditt system, med en trojan e.dy. så spelar kryptering och andra säkerhetsåtgärder ingen eller liten roll, då har du troligen redan en Keylogger installerad. För

mot kamraten och dens närmaste omgivning, utan att avslöja om det är via installerad kamera utnför bostaden, genom ett övervakningsteam eller annat. Då det är det landets säkerhetspolis som drivit utredningen saknas mycket information på detaljnivå.

Låt oss dröja oss kvar vid cykeln. Denna övervakningsform, att i hemlighet placera och installera en GPS-spårsändare i cykelns håligheter, sker alltså i ett sammanhang där det ingår i säkerhetsrutinerna att söka igenom privata cyklar för att undvika just detta scenario, framförallt för att inte locka snutar till möten eller rekognoseringsrundor. Om det inte var så kamraten var slarvig, använde sin egen cykel utan att genomsöka den—vi kan inte veta, då kamraten fortfarande sitter inspärrad i fiendens betongbuk—så kan det vara fallet att snuten har tillgång till svårupptäckt teknologi. Det troligaste är ändå att kamraten inte snodde eller lånade en cykel och att den inte lossade styre och sadel för att med lampa, fingrar och lämpliga tillhyggen söka av håligheterna. Lärdomen? Använd aldrig din egen cykel i en attack eller något som har med en attack mot fienden att göra. Sök med jämna mellanrum men framförallt inför en aktion igenom cykeln, för att se om extra säkerhetsåtgärder är nödvändiga.

Vi som skriver detta tillhör dem som längtar efter internets död, tillsammans med civilisationen och all den infrastruktur som möjliggör dess överlevnad och expansion. Samtidigt är vi som folk är mest och använder skiten i tid och otid. Ibland slarvar vi men något som vi aldrig slarvar med är följande: vi

tur en viss inblick i hur de nu jobbar, och det är där vi tänker att vi kan bygga vidare för att laga de tidigare skyddande rutiner vi byggt upp över generationer och eror.

Det handlar heller inte bara om tekniska rutiner, det handlar också om förhållningssätt: till varandra, till världen, till fienden och till sig själv. Vi låter ett citat från en sentida manual bli vår utgångspunkt:

- Var inte effektiva enligt samhällets normer. Att utföra en uppgift så effektivt som möjligt men sedan må skit, behandla andra illa eller inte orka med resten av livet, skiljer sig inte nämnvärt från lönearbete annat än att du själv är den slavdrivande arbetsgivaren.
- Vägen och målet är sällan samma sak och liknar mer förhållandet mellan dröm och vaket tillstånd. Om målet är ”ingen är fri förrän alla är fria,” så kan vi bara försöka att agera så frihetligt, hänsynstagande, omsorgsfullt och ansvarstagande som möjligt. Konflikter kommer alltid att finnas, motsägelsefulla känslor och svårbegripliga impulser också. Men drömmer du om en värld utan sociala hierarkier och institutioner, så är det en god idé att inte reproducera dem i dina relationer. Försök att bygga relationer så att ni kan prata om alla upplevelser ni delar, för att minska behovet att prata med utomstående om det. Ju mer begränsade samtalen mellan er är, desto större är risken att någon av er känner ett behov av att prata med andra vänner eller i värsta fall med psykolog eller snuten. Det är

inte lätt men om vi är mjuka mot varandra, är det lättare att vara hårda mot fienden.

- INGA MOBILER ELLER ELEKTRONISKA APPARATER!!! Det är inte en överdrift: du bär på en liten snut i fickan. Lämna den hemma: vid möten, när platser spanas på, när du handlar material och när ni genomför aktionen. Moderna bilar bör undvikas och definitivt hyrbilar, som alla är utrustade med GPS. Om ni planerar att stjäla verktyg, redskap eller fordon från företag eller privatpersoner, tänk på att många har GPS-sändare på dem. Försök att memorera så mycket du kan i huvudet och det som du känner dig tvingad till att anteckna mår bäst av att brännas så snart det går.

Så långt det är möjligt, använd inte internet för att samla information. Det finns gott om bibliotek och myndigheter du kan besöka för att samla information anonymt. Om du ändå känner dig tvungen att använda internet, läs på om och använd anonymiseringsprojekt som TAILS, TOR, MAC-changer m.m. Och använd isåfall bara internet för informationssamlande, aldrig för kommunikation om planerna. Internet kontrolleras av företag och stater, inte frihetliga hackers, även om det kan kännas så i vissa digitala rum.

- Lämna så få spår som möjligt. Skyddsdräkter, munskydd, handskar, skoskydd, glasögon, kläder som kan kastas bort (i second hand-containrar eller eldas upp), allt för att du inte ska lämna DNA på brandsatsen, byggplatsen,

brottsplatsen eller på vägen dit och tillbaka. Flaskor och annat material som lämnas på platsen bör så långt det går, rengöras med till exempel Mr Muscle-gel, som löser upp fett och hår. Andra kamrater använder steriliseringsmedel som används inom vården eller livsmedelshantering men vi har själva ingen erfarenhet av det.

- Lär känna var det finns kameror och undvik dem. De finns på många offentliga platser, kollektivtrafik, affärer, företag, bankomater, vägtullar osv. Sök efter kameralösa vägar. Om det inte går, klä ut dig så att det från kameravinklarna inte går att känna igen dig. Stjäl eller låna cyklar av avlägsna vänner och bekanta, använd aldrig din egen till en aktion. (Sök igenom cyklarna efter GPS-utrustning). Handla alltid kontant inför en aktion. Allt från biljetter till nödproviant, kläder och material till brandsats. Sök efter säkra ”byggplatser”, där ni utan att lämna eller samla spår kan bygga brandsatserna. Om det inte finns, skaffa billiga tält och slå upp dem där ni känner er säkra. Kasta sedan bort eller elda upp dem. Gå igenom alla steg före, under själva aktionen och efter, om och om igen, och se om ni lämnar spår någonstans eller riskerar att senare bli avslöjade.

I ett i skrivande stund pågående fall mot flera kamrater kan det i utredningen konstateras att snuten använt GPS-spårsändare i en av kamraternas cyklar, därtill antyds flera övervakningsoffensiver