Security Culture: Richtlijnen voor veilige subversie

Door CrimethInc.

- Verschenen: 2004
- Oorspronkelijke titel: What is Security Culture?
- Bron: https://cerclenoir.wordpress.com/2013/04/01/security-culture-richtlijnen-voor-veilige-subversie/; https://crimethinc.com/2004/11/01/what-is-security-culture
- Vertaling: Circle Noir, https://cerclenoir.wordpress.com

Deze publicatie is een vertaling van een tekst van het CrimethInc. collectief uit de VS en gaat over *security culture*. Dat wilt zeggen, het ontwikkelen van een verzameling gewoontes en handelingen die een groep of gemeenschap weerbaarder maken tegen (staats)repressie. In tijden zoals deze, waar de surveillance- en controlestaat zich almaar uitbreidt, waar de publieke ruimte bedekt is met camera's, iedereen van alles op social media gooit, het aantal telefoontaps de pan uit rijst, geluidsopnames en foto's van alles en iedereen worden gemaakt met smartphones en politie en leger gretig gebruik maken van onbemande vliegende drones, is het des te meer van belang voor activisten, revolutionairen en iedereen die zich verzet tegen deze wereld om verstandig en bewust om te gaan met veiligheid.

De tekst is tevens als PDF te downloaden: https://cerclenoir.files.wordpress.com/2013/04/security.pdf

---

Security Culture: Richtlijnen voor veilige subversie

Inleiding

Er is vaak een enorm gebrek aan een verstandige middenweg tussen met aluminiumhoedjes bedekte, verlammende ultra paranoia enerzijds en compleet roekeloze laksheid ("ach, ze weten alles toch al", "wat kan dat nu voor kwaad?", "ik ben niet interessant genoeg", "ik heb toch (nog) niets te verbergen?") anderzijds. Om niet in een van deze twee valkuilen te trappen, is het van belang om duidelijk te maken wat de collectieve manier van omgaan met deze zaken is, waar wel en niet over gesproken wordt, wat wel en niet verstandig is, en bovenal: hoe we dit alles balanceren. Het is daarom belangrijk om niet te krampachtig over dit soort zaken te doen, niet de ene kant op (waarbij alles, tot op wie er wel of geen frietje mee gaat eten na een vergadering, verzwegen wordt terwijl men koortsachtig om zich heen kijkt) en niet de andere kant op (waarbij iedereen die een soms wat moeizamer en strikter veiligheidsprotocol hanteert meteen af wordt geschilderd als een gestoorde X-files fanaat).

Deze tekst is uiteraard geen bijbel of blauwdruk en gezond verstand en instinct moeten nooit uit het oog verloren worden. Zie deze publicatie eerder als een stel richtlijnen, een uitgangsbasis. Het is dan

ook belangrijk dat de tekst niet slechts kort doorgelezen wordt, maar dat ze besproken wordt onder vrienden, bondgenoten en kameraden. Dat ze niet alleen praktisch toegepast wordt op de momenten dat het er 'toe lijkt te doen', dat de 'vlam in de plan slaat', maar juist ook op al die schijnbaar onbelangrijke en saaie momenten vooraf en achteraf. Veiligheid is iets wat alleen werkt als het serieus en proactief in acht wordt genomen en niet als mosterd na de maaltijd.

Wat is security culture?

Een security culture is een verzameling gewoontes die gedeeld worden door een gemeenschap waarvan de leden het doelwit van staatsrepressie kunnen zijn, om zodoende risico's te minimaliseren

Door gebruik te maken van een security culture voorkomt men het keer op keer opnieuw uitwerken van veiligheidsmaatregelen en helpt het om paranoia en paniek in stressvolle situaties tegen te gaan. Bovendien kan het je misschien uit de gevangenis houden. Het verschil tussen protocol en cultuur is dat cultuur iets onbewusts wordt, instinctief en daarmee moeiteloos; wanneer het veiligste gedrag een gewoonte is geworden voor iedereen in de kringen waarin je verkeerd, hoef je minder tijd te spenderen aan het benadrukken van de noodzaak hiertoe, of de consequenties van het gebrek hieraan te ondergaan, of je druk te maken om het gevaar dat je misschien loopt, omdat je weet dat je enigszins veilig bezig bent. Als het je gewoonte is om niks gevoeligs over jezelf te vertellen, dan kan je samenwerken met vreemden zonder constant bang te hoeven zijn of ze wel of geen informanten zijn; als iedereen weet waar ze hun mond over moeten houden aan de telefoon, dan kunnen je vijanden afluisteren wat ze willen en brengt het hen nergens.[1]

Het basisprincipe van alle security culture, het punt wat niet genoeg benadrukt kan worden, is dat mensen nooit meer gevoelige informatie moeten weten dan ze hoeven te weten

Hoe meer mensen op de hoogte zijn van iets dat individuen of projecten in gevaar kan brengen – of dat nu de naam is van iemand die iets illegaals heeft gedaan, de locatie van een privébijeenkomst of een plan voor toekomstige activiteit – hoe groter de kans is dat die informatie in de verkeerde handen terecht komt. Dit soort informatie delen met mensen die het niet nodig hebben benadeelt hen samen met degenen die het in gevaar brengt: het plaatst hen in de oncomfortabele positie waarin ze in staat zijn om de levens van anderen te verknallen door een simpele misstap. Als ze verhoord worden, bijvoorbeeld, hebben ze iets te verbergen in plaats van de mogelijkheid om in alle eerlijkheid onwetendheid te kunnen claimen.

Don't ask, don't tell

Vraag anderen niet om gevoelige informatie te delen die je niet nodig hebt. Loop niet op te scheppen over illegale dingen die jij of anderen hebben gedaan, noem geen dingen waarvan je weet dat ze gaan gebeuren of kunnen gaan gebeuren en praat niet over zelfs maar de interesse van anderen om aan zulke dingen deel te nemen. Let op wanneer je praat, laat niet zomaar gevoelige informatie vallen in een onbewaakt moment.

Je kan nee zeggen op alles, op elk moment dat je dat wilt

Beantwoord geen vragen die je niet wilt beantwoorden – en dat geldt niet alleen bij de politie, maar ook bij andere activisten en zelfs bij trouwe vrienden: als er iets is wat je niet wilt delen, doe dat dan

ook niet. Dit betekend ook dat je je op je gemak moet voelen bij anderen als je geen antwoord op vragen geeft: als er een gesprek plaatsvindt dat ze voor zichzelf willen houden, of als ze je vragen geen deel uit te maken van een bijeenkomst of project, dan moet je dit niet persoonlijk opvatten – het is voor iedereens bestwil dat dit mogelijk is. Neem ook geen deel aan projecten waar je je niet goed over voelt en werk niet samen met mensen waar je geen goed gevoel bij hebt of je niet prettig bij voelt. Negeer je intuïtie nooit in dat soort gevallen; als iets verkeerd gaat en je in de problemen komt, dan wil je geen spijt hebben. Jij bent verantwoordelijk voor het je niet laten aanpraten van risico's waar je niet klaar voor bent.

Lever je vrienden nooit uit aan je vijanden

Als je gevangen wordt genomen, geef dan nooit en te nimmer enige informatie af die anderen in gevaar kan brengen. Sommigen zijn voorstanders van een expliciete eed gezworen door alle deelnemers aan een directe actie groep: op die manier weet iedereen, wanneer de druk in het worst-case scenario het moeilijk maakt om het verschil te zien tussen een paar 'nutteloze' details en een volledige verklaring afleggen, wat men elkaar beloofd had.

Maak het je vijanden niet te makkelijk om uit te vogelen wat je van plan bent

Wees niet te voorspelbaar in de methoden die je hanteert, of de doelwitten die je uitkiest, of de tijden en plaatsen waar je bijeenkomt om zaken te bediscussiëren. Wees niet te zichtbaar in de publieke aspecten van de strijd waarin je je meest serieuze directe actie wilt hanteren: hou je naam van de mailinglijsten en uit de media, vermijd misschien zelfs de associatie met de publieke organisaties en campagnes compleet. Als je betrokken bent bij heel serieuze clandestiene activiteiten met een paar kameraden dan wil je je publieke interactie misschien beperken of elkaar misschien zelfs ontlopen. Agenten van inlichtingendiensten kunnen makkelijk de telefoonnummers opvragen die vanaf jouw telefoon gebeld zijn en zullen zulke lijsten gebruiken om connecties tussen individuen bloot te leggen; hetzelfde geldt voor je e-mail en de boeken die je leent in de bibliotheek en uiteraard vooral social networking sites zoals Facebook of Myspace. Laat geen spoor achter: het gebruik van creditcards, benzinekaarten, telefoontjes, etc. laten allemaal een logboek van je bewegingen, aankopen en contacten achter. Zorg dat je een alibi klaar hebt wat te verifiëren is met feiten, mocht dat nodig zijn. Wees erg voorzichtig met wat je afval over je kan vertellen – dropouts zijn niet de enigen die gaan dumpsterdiven! Houd ieder geschreven document en belastende kopie bij – bewaar ze allemaal op een plek zodat je er niet een vergeet – en vernietig ze meteen wanneer ze niet meer nodig zijn. Hoe minder er überhaupt van zijn, hoe beter; wen aan het gebruik van je geheugen. Zorg ook dat er geen afdrukken van zulke documenten achterblijven in de ondergrond waar je op schrijft, of dat nu houten tafels of stapels papieren zijn. Ga er ook van uit dat alle gebruik van computers haar sporen achterlaat.

Werp geen directe actie ideeën op in het publiek die je later nog een keer wilt proberen

Wacht met het voorstellen van een idee tot je een groep individuen bij elkaar hebt waarvan je verwacht dat ze allemaal geïnteresseerd in het idee zijn; de uitzondering hierop zijn erg goede kameraden waarmee je brainstormt en van te voren details uitwerkt – veilig buiten je huis en weg van gemengd gezelschap, uiteraard. Stel je idee niet voor totdat je denkt dat de tijd rijp is om het te proberen. Nodig alleen diegenen uit waarvan je vrij zeker bent dat ze mee willen doen – iedereen die je uitnodigt en die besluit niet mee te doen is een onnodig potentieel veiligheidsrisico en dit kan dubbel zo problematisch zijn als ze uiteindelijk van mening zijn dat de activiteit die voorgesteld werd contraproductief of moreel verkeerd is. Nodig alleen mensen uit die met een geheim om kunnen gaan – dit is cruciaal of ze nu mee willen doen of niet.

Ontwikkel een shorthand voor publieke communicatie met kameraden

Het is belangrijk om een heimelijke manier van communicatie in publieke situaties over veiligheidszaken en comfortniveaus te ontwikkelen met betrouwbare vrienden, zoals tijdens een bijeenkomst over mogelijke directe actie. Weten hoe je elkaars gevoelens over een situatie kan peilen zonder dat anderen dit door hebben kan je de koppijn besparen van het proberen te gissen naar elkaars gedachtes over een situatie of individu, en kan helpen voorkomen dat je je raar gedraagt wanneer je je vriend niet apart kan spreken om van gedachten te wisselen. Tegen de tijd dat een grotere groep bij elkaar is gekomen om een actieplan voor te stellen, zouden jij en je vrienden van elkaar moeten weten wat ieder's intenties, risicobereidheid, toegewijdheid en meningen over anderen zijn, om tijd te besparen en nodeloze ambiguïteit te voorkomen. Als je nog nooit deel hebt uitgemaakt van het plannen van een directe actie, dan zal je je verbazen over hoe gecompliceerd en moeilijk dingen kunnen worden zelfs als iedereen voorbereid op komt dagen.

Ontwikkel methodes om het veiligheidsniveau van een groep of situatie vast te stellen

Een snelle procedure die je uit kan voeren aan het begin van een grotere bijeenkomst waar je niet met iedereen bekend bent is het 'koosjer' spelletje: als iedereen zich introduceert, steekt iedereen die weet dat deze persoon 'koosjer' is zijn of haar hand op. Beschouw alleen diegenen als koosjer waarvan je zeker bent dat ze te vertrouwen zijn. Hopelijk is iedereen wel verbonden met iemand anders in de ketting; hoe dank ook: iedereen weet nu hoe de zaken ervoor staan. Een activist die het belang van een goede security culture kent zal zich niet beledigd voelen als er niemand is die voor hem of haar garant kan staan en anderen hem of haar vragen te vertrekken.

Bijeenkomstlocaties zijn een belangrijke factor in de veiligheid

Je wilt geen plek waar je makkelijk geobserveerd kan worden (privé woningen), je wilt geen plek waar je allemaal samen gezien kan worden (het park tegenover de plek van de actie de volgende dag), je wilt geen plek waar je gezien kan worden bij het naar binnen en buiten gaan of waar iemand onverwachts naar binnen zou kunnen, stel uitkijkposten aan en doe de deur op slot wanneer de bijeenkomst begint en hou je ogen open voor verdachte zaken.[2] Kleine groepjes kunnen een blokje om lopen en wat kletsen; grotere groepen kunnen bijeenkomen in stille plattelandslocaties – ga wandelen of kamperen bijvoorbeeld als er tijd is – of in privéruimtes in publieke gebouwen, zoals studeerkamers in de bibliotheek of lege klaslokalen. Best-case scenario: hoewel hij geen idee heeft dat je betrokken bent bij directe actie ben je close met de oude kerel die het café aan de rand van het dorp runt en het maakt hem niet uit of je de achterkamer gebruikt voor een 'privéfeestje' op een namiddag – no questions asked.

Wees op de hoogte van de betrouwbaarheid van de mensen om je heen, vooral van diegenen met wie je misschien samenwerkt in ondergrondse activiteiten

Wees je bewust van hoe lang je mensen kent, hoe ver terug hun betrokkenheid in jouw gemeenschap en hun levens daarbuiten getraceerd kan worden, en wat de ervaringen van andere mensen met hen zin. De vrienden waar je mee op bent gegroeid, als die nog een rol in je leven spelen, zijn misschien wel de beste medestanders voor directe actie, omdat je hun sterke en zwakke punten kent en de manieren waarop ze omgaan met druk – en je weet dat ze zijn wie ze zeggen te zijn. Verzeker jezelf ervan dat je je veiligheid en de veiligheid van je projecten alleen toevertrouwd aan mensen die hun hoofd koel houden en dezelfde prioriteiten en toewijding hebben als jij en die niks te bewijzen hebben. Streef er op de lange termijn naar om een gemeenschap van mensen met langdurige vriendschappen en ervaring in samenwerking op te bouwen, met banden met andere zulke gemeenschappen.

Wees niet te afgeleid door kopzorgen over of mensen al dan geen infiltranten zijn; als je

veiligheidsmaatregelen effectief zijn, zou dat niet al te veel moeten uitmaken

Verspil je energie niet door jezelf paranoïde en asociaal te maken door iedereen die je tegenkomt te verdenken. Als je alle gevoelige informatie binnen de kring van mensen die het aangaat houdt, en alleen samenwerkt met betrouwbare en ervaren vrienden wiens geschiedenis je kan verifiëren, en nooit iets los laat over je privéactiviteiten, dan staan agenten en informanten machteloos in hun pogingen om bewijs tegen je te verzamelen. Een goede security culture zou het vrijwel irrelevant moeten maken of dit ongedierte actief is in jouw gemeenschap of niet. Het belangrijkste is niet of een persoon actief is voor de politie, maar of hij of zij wel of geen veiligheidsrisico vormt; als hij of zij onveilig wordt geacht, zou hij of zij nooit in een situatie mogen eindigen waar iemands veiligheid van hem of haar afhangt.

Leer en houd je aan de veiligheidsverwachtingen van iedere persoon waar je mee omgaat, en respecteer verschillen in stijl

Samenwerken met anderen betekend dat ze zich thuis moeten voelen bij jou; zelfs als je niet met ze samenwerkt, wil je niet dat mensen zich oncomfortabel rondom je voelen of een gevaar negeren dat ze beter begrijpen dan jij. Als het aankomt op het plannen van directe actie, kan het aan je laars lappen van de security culture in een gegeven gemeenschap niet alleen je kansen op samenwerking in andere projecten verpesten, maar ook de mogelijkheid dat het project überhaupt doorgaat – als je bijvoorbeeld een idee opwerpt wat anderen aan het plannen waren in een omgeving die zij onveilig achten, moeten ze dat plan misschien opgeven omdat het nu met hen geassocieerd kan worden. Vraag mensen of ze hun security culture voor jou kunnen schetsen voordat je überhaupt ingaat op het onderwerp van directe actie.

Laat anderen weten wat precies jouw eisen zijn als het op veiligheid aankomt

Het gevolg van je houden aan de verwachtingen van anderen is dat je het makkelijk moet maken voor anderen om zich aan die van jou te houden. Aan het begin van iedere relatie waarin je private politieke leven een issue kan worden, benadruk dan dat er details van je activiteiten zijn die je voor jezelf moet houden. Dit kan je een hoop drama besparen in situaties die al stressvol genoeg zin; het laatste wat je nodig hebt als je terugkomt van een geheime actie die misging is ruzie met je lover: “Maar als je me vertrouwde, zou je me dit vertellen! Hoe weet ik dat je niet ergens vreemd aan het gaan bent met …!”. Het is geen kwestie van vertrouwen – gevoelige informatie is geen beloning die je kunt verdienen.

Zorg voor andere mensen

Maak het expliciet duidelijk aan anderen om je heen wat de risico’s zijn die jouw aanwezigheid met zich mee kan brengen[3] of met acties die je geplanned hebt, ten minste, zoveel als mogelijk zonder andere aspecten van security culture te schenden. Laat ze weten voor zover mogelijk, wat voor risico’s je zelf loopt: of je het bijvoorbeeld kan veroorloven gearresteerd te worden (of er nog uitstaande boetes zijn of je een illegale immigrant bent, etc.), wat voor verantwoordelijkheden je hebt, of je allergieën hebt. Breng anderen niet in gevaar met je besluiten, vooral als je niet in staat bent concrete ondersteuning te leveren als iemand gearresteerd of veroordeeld wordt vanwege jouw acties. Als iemand anders een spandoek ophangt in een omgeving onmiddellijk naast de plek die jij in de fik hebt gezet, kan de politie ze oppakken voor brandstichting; zelfs als de beschuldiging geen stand houdt wil je dat niet veroorzaken, of per ongeluk hun ontsnappingsplan blokkeren. Als je helpt om een afsplitsingsdemonstratie te organiseren die zich buiten de toegestane zone begeeft, zorg dan dat je je lichaam tussen de politie en anderen houdt die misschien mee zijn gegaan maar zich niet helemaal van de risico’s bewust zijn; als je een spontane parade laat escaleren door middel van materiële schade, zorg dan dat anderen die hier niet op voorbereid waren niet verward rond lopen te

hangen als de politie op komt draven. Wat voor risicovolle projecten je ook onderneemt, zorg dat je voorbereid bent en hier intelligent mee omgaat, zodat niemand anders onverwachte risico's loopt als ze jou proberen te helpen.

Security culture is een vorm van etiquette, een manier om onnodige misverstanden en potentieel desastreuze conflicten te vermijden

Veiligheidsmaatregelen zouden nooit een excuus mogen zijn om anderen zich minderwaardig of buitengesloten te laten voelen – hoewel het wat subtiliteit vereist om dat te vermijden! – net zoals niemand zich zou mogen kunnen beroepen op het 'recht' om zich bij iets te voegen wat anderen liever voor zichzelf houden. Diegenen die de security culture van hun gemeenschappen overtreden zouden hier niet te hard mee geconfronteerd moeten worden als het de eerste keer is – het is geen kwestie van hip genoeg te zijn om bij de in-crowd te horen, maar van het vaststellen van groepsverwachtingen en mensen beleefd te helpen om hun belang te begrijpen; bovendien zijn mensen het slechtst in staat om constructieve kritiek te absorberen als ze in het defensief gedreven worden. Desondanks moet zulke mensen altijd onmiddellijk verteld worden hoe ze een risico voor anderen vormen en wat de consequenties zijn als ze zo door gaan. Diegenen die dit weigeren te begrijpen moeten tactvol maar effectief buiten gevoelige situaties gezet worden.

Security culture is geen geïnstitutionaliseerde paranoia, maar een manier om ongezonde paranoia te vermijden door risico's op tijd te minimaliseren

Het is contraproductief om meer energie te verspillen aan je afvragen onder hoeveel surveillance je staat dan nodig is om het gevaar dat dit vormt te verminderen, net zoals het verlammend werkt om constant je voorzorgsmaatregelen in twijfel te trekken en de oprechtheid van potentiële kameraden te betwijfelen. Een goede security culture zou iedereen zich meer ontspannen moeten laten voelen en zelfverzekerder, niet minder. Tegelijkertijd is het even onproductief om diegenen die striktere veiligheidsmaatregelen nemen dan jij te beschuldigen van paranoia – onthoud dat onze vijanden er uiteindelijk wel op uit zijn om ons te pakken.

Laat verdenking niet tegen je gebruikt worden

Als je vijanden je geheimen niet kunnen achterhalen, dan zullen ze proberen om mensen tegen elkaar op te zetten. Undercover agenten kunnen geruchten verspreiden of beschuldigingen rondstrooien om conflict, wantrouwen en nijd in of tussen groepen te creëren. Ze kunnen brieven vervalsen of vergelijkbare stappen ondernemen om activisten te framen. De mainstream media kan hieraan meedoen door te vermelden dat er een informant in een groep zit terwijl dit niet het geval is, of door de politiek of geschiedenis van een individu of een groep te vertekenen om potentiële bondgenoten te vervreemden, of door keer op keer te benadrukken dat er een conflict is tussen twee takken van een beweging tot dat ook echt het geval is. Wederom zou een goede security culture die een adequaat hoog niveau van vertrouwen en verzekerdheid stimuleert zulke provocaties bijna onmogelijk moeten maken op het persoonlijke niveau; en waar het aankomt op de relaties tussen voorstanders van verschillende tactieken en organisaties van verschillend pluimage, onthoud dan het belang van solidariteit en diversiteit van tactieken en vertrouw er op dat ook anderen dat doen, ook al zegt de media iets anders. Accepteer geen geruchten als feiten: ga iedere keer naar de bron voor bevestiging en wees hierin diplomatiek.

Wees niet geïntimideerd door gebluf

Politieaandacht en surveillance zijn niet noodzakelijkerwijs een indicatie dat ze iets specifieks weten over je plannen of activiteiten: vaak is het een teken dat ze dat niet weten en je proberen bang te

komen zodat je hiermee ophoudt. Ontwikkel een instinct waarmee je aan kan voelen of je echt ontmaskerd bent of dat je vijanden proberen te manipuleren om hun werk voor hen te doen.

Wees altijd voorbereid op de mogelijkheid dat je onder observatie staat, maar verwar surveillance aandacht niet met effectief bezig zijn

Zelfs als alles wat je doet volkomen legaal is, kan je nog steeds aandacht en intimidatie van inlichtingendiensten krijgen, als ze het gevoel hebben dat je lastig bent voor hun opdrachtgevers. Soms kan dit goed uitpakken; hoe meer ze in de gaten moeten houden, hoe meer ze hun energie moeten verdelen en hoe moeilijker het is om subversievelingen te identificeren en neutraliseren. Tegelijkertijd moet je je niet laten meeslepen in de ‘spanning’ van het onder observatie staan en er van uit gaan dat hoe meer aandacht de autoriteiten aan je schenken, hoe gevaarlijker je waarschijnlijk voor ze bent – zo slim zijn ze nu ook weer niet. Ze neigen ernaar om zich bezig te houden met organisaties wiens aanpak het meest op die van hen lijkt; maak hier misbruik van. De beste tactieken zijn diegenen die mensen bereiken, punten maken en druk uitoefenen zonder op de radar van de autoriteiten te verschijnen, ten minste, pas als het te laat is. Ideaal zou zijn als de activiteiten bij iedereen bekend zijn, behalve bij de autoriteiten.

Security culture bevat een zwijgcode, maar het is geen van zwijgplicht

De verhalen van onze waaghalzerij in de strijd tegen kapitalisme moeten op de een of andere manier verteld worden, zodat iedereen weet dat verzet een reële optie is die ondernomen kan worden door echte mensen; open uitnodigingen voor de opstand dienen verstuurd te worden, zodat would-be revolutionairen elkaar kunnen vinden en de revolutionaire sentimenten die begraven liggen in de harten van de massa hun weg naar de oppervlakte kunnen vinden. Een goede security culture bewaart zoveel geheimhouding als nodig voor individuen om veilig ondergronds te opereren, terwijl ze nog steeds zichtbaarheid voor radicale perspectieven bieden. Het overgrote deel van de veiligheidstraditie in het activistische milieu vandaag de dag is afkomstig uit de afgelopen dertig jaar aan dierenbevrijding en ecologische acties; daarmee is ze perfect gericht op de behoeftes van kleine groepen de geïsoleerde illegale handelingen uitvoeren, maar niet altijd voor de meer bovengrondse campagnes die zich richten op veralgemeende opstandigheid. In sommige gevallen is het logisch om de wet openlijk te breken, om de deelname van een grote massa uit te lokken, die op haar beurt weer veiligheid in pure aantallen kan bieden.

Balanceer de behoefte om detectie door je vijanden te vermijden met de behoefte om toegankelijk te zijn voor potentiële vrienden

Op de lange termijn kan geheimzinnigheid alleen ons niet beschermen – vroeger of later vinden ze ons allemaal, en als niemand begrijpt wat we doen en wat we willen, vermorzelen ze ons met gemak. Alleen de kracht van een geïnformeerd en sympathiek (en hopelijk vergelijkbaar uitgerust) publiek kan ons dan nog helpen. Er zouden altijd ingangen moeten zijn in gemeenschappen waar directe actie uitgevoerd wordt, zodat meer mensen zich hier bij kunnen voegen. Diegenen die zich met echt serieuze zaken bezig houden moeten dat voor zichzelf houden, uiteraard, maar iedere gemeenschap zou ook een aantal personen moeten hebben die openlijk stelling nemen voor directe actie en die discreet betrouwbare nieuwelingen wegwijs kunnen maken.

Wanneer je een actie plant, begin dan met het adequate veiligheidsniveau vast te stellen, en handel daar vervolgens naar

Leren de risico’s van een activiteit of situatie in te schatten en hoe hiermee om te gaan is niet alleen een cruciaal onderdeel van uit de gevangenis blijven; het helpt ook om te weten waar je je geen zorgen over maakt, zodat je geen energie verspilt aan onnodige, vermoeiende

veiligheidsmaatregelen. Onthoud dat een gegeven actie verschillende aspecten kan hebben die verschillende veiligheidsniveaus vereisen; verzeker jezelf ervan om deze gescheiden te houden. Hier is een voorbeeld voor een mogelijke indeling van veiligheidsniveaus:

1. Alleen degenen direct betrokken bij de actie mogen van haar bestaan weten.
2. Betrouwbare ondersteuningspersonen mogen van de actie weten, maar iedereen in de groep bepaalt wie dit zijn.
3. Het is acceptabel voor de groep om mensen uit te nodigen die er voor kunnen kiezen om niet deel te nemen – dat wil zeggen, sommigen buiten de groep mogen van de actie afweten maar er wordt nog steeds verwacht dat het geheim blijft.
4. De groep hanteert geen strikte lijst van wie wel of niet uitgenodigd is; deelnemers zijn vrij om anderen uit te nodigen en worden aangemoedigd om hetzelfde te doen, ondertussen benadrukken dat kennis van de actie binnen betrouwbare kringen gehouden dient te worden.
5. “Geruchten” van de actie mogen wijd verspreid worden door de gemeenschap, maar de identiteiten van de betrokkenen bij de organisatie dienen geheim te blijven.
6. De actie wordt openlijk aangekondigd, maar met zekere discretie, zodat de slaperigere autoriteiten niet op de hoogte zijn.
7. De actie wordt open en bloot aangekondigd en is bovengronds op alle manieren.

Om een voorbeeld te geven, veiligheidsniveau #1 is voldoende voor een groep die een SUV-dealership met molotovs wilt bestoken, terwijl niveau #2 acceptabel is voor de kleinere vormen van materiële schade, zoals graffiti. Niveau #3 of #4 zou voldoende zijn voor het houden van een vergadering voorafgaande aan een black bloc op een grote demonstratie, afhankelijk van de risico-noodzaak voor aantallen verhouding. Niveau #5 zou perfect zijn voor projecten zoals het organiseren van een spontane demonstratie zonder toestemming: als iedereen bijvoorbeeld vooraf hoort dat de Ani DiFranco voorstelling gaat eindigen in een ‘spontane’ anti-oorlogs mars, kunnen mensen zich voorbereiden maar weet niemand wiens idee het is zodat niemand verantwoordelijk gesteld kan worden. Niveau #6 zou voldoende zijn voor het aankondigen van een Critical Mass fietstocht: flyers onder de snelbinders van alle fietsen, maar geen aankondigingen in de kranten zodat de politie niet meteen klaarstaat als de groep nog kwetsbaar is. Niveau #7 is adequaat voor een toegestane antioorlogsdemonstratie of onafhankelijke filmavond, tenzij je disfunctioneel en paranoïde bent en zelfs openlijke projecten geheim wilt houden.

Het is ook handig om de communicatiemiddelen die je gebruikt aan te geven met het veiligheidsniveau dat ze vereisen. Hier is een voorbeeld van verschillende communicatieveiligheidsniveaus, corresponderend met het bovenstaande schema:

1. Geen communicatie over de actie behalve persoonlijk, buiten de huizen van de betrokkenen, in surveillance-vrije gebieden (ie. De groep gaat kamperen om de plannen te bediscussiëren); geen discussie omtrent de actie behalve wanneer absoluut noodzakelijk.
2. Buiten bijeenkomsten van de groep staat het betrokken individuen vrij om de actie te bespreken in surveillance-vrije omgevingen.
3. Discussies zijn toegestaan in huizen die zeker niet onder surveillance staan.
4. Communicatie via versleutelde e-mail of beveiligde telefoonlijnen is toegestaan.
5. Mensen kunnen praten over de actie via telefoon, e-mail, etc. er vanuit gaand dat ze voorzichtig zijn om bepaalde details niet te bespreken – wie, wat, wanneer, waar.
6. Telefoon, e-mail, etc. is allemaal prima; mailinglijsten, flyeren in het openbaar, aankondigingen in de krant, etc. kan wel of niet acceptabel zijn, afhankelijk van de situatie.
7. Communicatie en aankondiging op alle mogelijke media wordt aangemoedigd.

Als je schadelijke informatie uit de roulatie houdt en adequate veiligheidsmaatregelen in acht neemt

in ieder project waar je aan deelneemt, dan ben je goed op weg naar wat CrimethInc.'er avant-la-lettre Abbie Hoffman beschreef als de eerste taak van iedere revolutionair: niet gepakt worden. We wensen je het beste in al je avonturen en onthoud – dit alles heb je niet van ons!

Verder lezen

- Security Culture: The Puppet Show
- Anonymity: Dressing for Success

Voetnoten

- [1] "Maar hoe zit het dan met infiltranten en informanten?" vroeg een CrimethInc.'er lang geleden bij zijn eerste grote mobilisatie. "Die laten we de aardappels schillen" was het terloopse antwoord van een ervaren activist.
- [2] Een CrimethInc. cel zal nooit de ultra-high security bijeenkomst in de kelder van een universiteit vergeten, waar ze er achter kwamen dat ze ingesloten waren omdat een groep liberale studentendemonstranten de aangelegen kamer in gebruik had genomen om daar een powerpoint presentatie te bekijken – en alle organisatoren van het militante black bloc van de volgende dag hier nogal beschaamd doorheen moesten.
- [3] Een hilarisch voorbeeld van waarom dit van belang is is de keer toen CrimethInc. betrokkenen Paul F. Maul en Nick F. Adams probeerden om terug naar de continentale VS te keren na een maand ondergedoken te zitten in Alaska. Ze maakten zich zorgen over hoe de Canadese douane zou reageren op de vrij grote hoeveelheid kogels die ze bij hadden, en daarom hadden ze de deurpanelen van de auto verwijderd en de boel hier achter verstopt. Op weg naar de grens pikten ze een lifter op, een algemeen uitziende, goed geschoren kerel die vrij normaaltjes leek. Bij de grens hielden allebei de CrimethInc.'ers hun adem in toen hun ID's gecontroleerd werden maar haalden opgelucht adem toen ze deze zonder problemen terug kregen. Ze dachten dat alles prima zou verlopen totdat de douane het ID van de lifter controleerde; plotseling verschenen overal gewapende agenten rondom de auto en dwongen ze hen met getrokken wapens uit te stappen. De lifter, zo bleek, was een veteraan van Greenpeace die in meer dan dertig landen gearresteerd was! De politieagenten doorzochten de auto en verwijderden uiteindelijk de deurpanelen zodat de kogels op het plaveisel klaterden. Onze helden spendeerden de volgende vier uur opgesloten in verhoorkamers. Canadese agenten schreeuwden "Waar zijn de pistolen? We weten dat jullie die bij hebben – zeg ons waar ze zijn!" en wilden niet echt luisteren naar de uitleg: "Dit is een groot misverstand – we hebben helemaal geen wapens bij. We zijn grafisch ontwerpers – deze kogels zijn voor een ontwerpproject. Eerlijk waar agent!".

repressie, security culture

From:
https://anarchisme.nl/ - **Anarchisme.nl**

Permanent link:
https://anarchisme.nl/namespace/security_culture_-_richtlijnen_voor_veilige_subversie?rev=1494410019

Last update: **16/10/19 09:40**