Pewne rzeczy

Wprowadzenie do bezpieczeństwa operacyjnego dla osób anarchistycznych zainteresowanych akcją bezpośrednią

współudział

2023

Spis treści

1. Wstęp

1.1. Dlaczego akcja bezpośrednia?

Akcja bezpośrednia (AB) jest jedną z kluczowych anarchistycznych koncepcji. AB zakłada działanie bez pośrednictwa przedstawicieli i instytucji społecznych celem jak najszybszego rozwiązania problemu z którym się borykasz. Jeśli potrzebujesz drzewa – sadzisz je, jeśli przeszkadza ci płot – niszczysz go, jeśli trzeba zatrzymać wycinkę – zatrzymujesz ją za pomocą skutecznych metod. AB to anarchia tu i teraz. AB to nie jest jakaś abstrakcyjna, niezrozumiała idea (jak wolność), albo coś na co trzeba bezczynnie czekać (jak „moment rewolucyjny"). AB przypomina ci, że są rzeczy, na które możesz mieć wpływ, często nawet ogromny wpływ, i że twoje działanie może się skupić właśnie na nich.

AB wbrew obiegowej opinii nie musi być wcale konfrontacyjna, nie musi łamać ustanowionych praw, ani nie musi uciekać się do przemocy. Różne taktyki partyzantki ogrodowej, takie jak sianie roślin na ogólnodostępnych miejskich skwerach, także są przykładami akcji bezpośredniej. AB oczywiście jednak może uciekać się do przemocy, łamać ustanowione prawa i być konfrontacyjna. Takie akcje są zresztą najbardziej archetypiczne, najbardziej zapadają w zbiorową pamięć i często napędzają do działania kolejne generacje osób anarchistycznych, choć akurat nie wiem, czy to jest najważniejsze. Ta broszura ma ci pomóc w robieniu takich akcji jakie chcesz i jakie czujesz, że w danym momencie są potrzebne. Ocenę potencjalnych korzyści i strat pozostawiam tobie.

Zabawne jest to, że to jak brutalnie potraktuje cię państwo, nie zależy od tego jak bardzo ograniczysz swoje działania. Wiele osób anarchistycznych które znam, porzuciło ideologie non-violence wskutek doświadczenia ciężkich represji za zupełnie błahe, niegroźne i pokojowe działania.

Ta publikacja nie zachęca do popadania w paranoje i zamykania się w domach. Mnie na przykad mało co tak motywuje do działania jak świadomość tego, że unikając przez całe życie ryzyka mogę zostać zamordowanx przez p*icję, która mnie z kimś pomyli. Ten zin ma w założeniu dostarczyć narzędzi, które mogą sprawić, że w pewnych sprawach poczujesz się pewniej, a nie żerować na twoim strachu. Zachęca do tego, żeby poważnie podejść do prowadzonych działań, uważnie je zaplanować i zawczasu przeanalizować możliwe konsekwencje.

Żyjemy w czasach sterowanych protestów, których wystąpieniem i przebiegiem najbardziej zaskoczone są osoby w nich uczestniczące. Ten zin nie poprzestaje więc na opisaniu garści narzędzi technicznych, ale zawiera kilka bardzo ogólnych refleksji o wyborze taktyk, a nawet strategii działania. Przekonanie o tym, że jeśli państwo może powiązać twoje

działania z twoimi oficjalnymi danymi, to w imię demokracji pozwoli ci stanowić realne zagrożenie, jest całkowicie błędne. Popularność zawdzięcza ono tylko temu jak bardzo na rękę jest ono agentom państwowego wpływu (np. mediom i finansowanym przez państwa NGOsom).

Ten zin proponuje zupełnie odwrotne podejście do działania, niż to do którego przyzwyczaił nas medialny spektakl. Zamiast reakcji na działania przeciwnika – inicjatywa. Zamiast biegania za wciąż poruszającym się światłem kamery – plan.

Nie jest jednak tak, że jeśli nie zgadzamy się strategicznie to ten zin ci się nie przyda. Nawet jeśli akurat przygotowujesz „kampanie" w swojej zbiurokratyzowanej anarchistycznej organizacji, która od NGOsa różni się tym, że ma mniej pieniędzy, to prawdopodobnie zauważysz, że narzędzia, które omawiam są uniwersalne. Być może ich konsekwentne używanie skłoni cię do zmiany założeń. Jeśli jednak tego nie zrobisz, nadal pozostaną one przydatnymi narzędziami, choć skutki ich użycia będą ograniczone ograniczeniami twojej strategii.

1.2. Co to jest bezpieczeństwo operacyjne i dlaczego warto używać wojskowej terminologii

Niniejsza broszura traktuje w największym skrócie o tym jak być wrogiem państwa i nie dać się złapać. Pod słowo "państwo" możesz podstawić sobie zresztą coś innego, na przykład cywilizację, kapitalizm, cistem czy p*icję. Jeśli jesteś wrogiem jednej z tych rzeczy, to jesteś wrogiem państwa i, uwierz mi, jeśli kiedykolwiek zrobisz coś, co według ciebie będzie ciekawe, twórcze, satysfakcjonujące czy niszczycielskie, to państwo się tobą zainteresuje.

Tematyka poruszana w tym zinie bywa czasem, w naszym kontekście językowym, określana mianem "kultury bezpieczeństwa". To pojęcie zostało spopularyzowane przez tłumaczenie fragmentu pracy CrimethIncu, wydane po p*lsku pod nazwą "O co chodzi z kulturą bezpieczeństwa". Równolegle, zwłaszcza w innych kontekstach językowych, funkcjonuje pojęcie "opsec". Ja konsekwentnie będę używać tego drugiego. Słowo opsec jest skrótem od „Operations Security" czyli angielskiego „Bezpieczeństwo Operacyjne" i ma pochodzenie wojskowe, choć już całkiem mocno przeniknęło do słownika dziennikarzy, dysydentów, kryminalistów i wielu innych „wysoko profilowanych celów" państwowych służb na całym świecie.

Używanie terminów o pochodzeniu wojskowym nie jest specjalnie rozpowszechnione wśród osób anarchistycznych, co w gruncie rzeczy powinno dziwić, gdyż jesteśmy ludźmi wojny. Zaangażowanie w konflikt z państwem jest istotnym składnikiem naszej tożsamości i praktyki. Dla państwa jest to konflikt o „niskiej intensywności" i bardzo długim czasie trwania, ale niewątpliwie - przynajmniej momentami - jest to konflikt zbrojny (nawet jeśli my nie strzelamy, to oni to robią). Jeśli kiedyś spotkałby mnie ten zaszczyt, żeby poproszono mnie o udzielenie jednej, ważnej rady osobie anarchistycznej to powiedziałxbym jej,

żeby zainteresowała się teorią wojskowości. Działania osób anarchistycznych często przypominają pewne rzeczy, które wojskowi robią zawodowo i które zazwyczaj robią po prostu lepiej. Na pewno mają też więcej czasu i środków na poważne analizy różnych ciekawych zagadnień (np. kamuflażu). Zachowując zatem zdrową wrogość do zbrodniczej machiny państwa i wojen miliarderów (której swoją drogą moim zdaniem anarchistkom ostatnio brakuje) warto studiować teksty naszych nieprzyjaciół i uczyć się od nich[1].

Zaletą używania ugruntowanych pojęć jest to, że odnoszą się one do całych stojących za nimi teorematów i przychodzą wraz z gotowymi narzędziami i instrukcjami stosowania. Pojęcia wojskowe mają ten dodatkowy czar, że stojące za nimi koncepcje są proste i nastawione na szybkie wdrażanie w praktykę bez popadania w zbyteczne dywagacje. Tak samo jest z pojęciem opsec, które przychodzi w pakiecie z całym zestawem wskazówek.

Definicja opsec widnieje w kilku miejscach na stronach amerykkkańskich ministerstw i agencji rządowych, nie musiałxm jej więc długo szukać.

Opsec (Operations Security) to systematyczny i ustalony proces, za pomocą którego można odmówić rozpoznanemu przeciwnikowi dostępu do informacji na temat możliwości i zamiarów, poprzez identyfikację, kontrolę i ochronę niejawnych danych na temat planowania i wykonania wrażliwych aktywności. Proces ten składa się z pięciu kroków: ustalenia krytycznych informacji, analizy zagrożeń, analizy podatności, oszacowania ryzyka i wprowadzenia odpowiednich środków przeciwdziałania[2].

Definicja zawiera kilka rzeczy, które wydają mi się obce anarchistycznej praktyce. Po pierwsze opsec to ma być proces systematyczny, który wymaga refleksji i analizy. Dotyczy on określonych „wrażliwych aktywności" i zamiarów, a zatem trzeba mieć jakiś plan. Wreszcie należy rozpoznać przeciwnika, czyli trzeba mieć świadomość siebie, linii podziałów i ogólnie konfliktu.

Co więcej, nie ma tutaj żadnych dogmatów, o które można się bezrefleksyjnie oprzeć, w stylu „Signal jest bezpieczny". Jest zachęta do przemyślenia swojej strategii i dobrania środków, które będą dla niej odpowiednie, na podstawie wiedzy o możliwych problemach. To wszystko sprawia, że taka definicja stanowi konkretnie określone, ale bardzo elastyczne narzędzie, przydatne do pracy przy różnych okazjach. Z pewnością jednak aby go użyć musisz polubić planowanie.

---

[1] Jeśliby ktoś chciał zacząć dziś interesować się wojskowością, to całkiem dobrym początkiem jest moim zdaniem [„The art of rebelion - martial tradition for the anarchists"](https://theanarchistlibrary.org/library/seaweed-the-art-of-rebellion-martial-traditions-for-anarchists). Były pracownik National Security Agency, czyli głównej amerykkkańskiej agencji szpiegowskiej, pracujący obecnie niezależny konsultant i znany jako Grugq, jako najlepszą lekturę opsec dla osób hakerskich polecił [„Spec Ops" Williama H. Macravena](https://medium.com/@thegrugq/on-pre-op-hackers-7e7f25eeccdc). „Spec Ops" to książka stanowiąca dość sztampowy przykład akademickiej rozprawy o wojskowości, analizująca 5 najbardziej udanych specjalnych operacji przeprowadzonych przez siły zbrojne różnych państw. Jako całość to niezbyt pasjonująca lektura, ale znajduje się w niej kilka ciekawych obserwacji.

[2] Strona amerykkkańskiego Office of Security: https://www.commerce.gov/osy/ programs/operationssecurityopsec

2. Część najważniejsza

2.1. Co to są „działania wrażliwe”?

To państwo, czyli nasz przeciwnik, decyduje o tym na jakie działania reaguje, a jakie ignoruje. Ostatnie lata przyniosły wysyp zdecydowanych reakcji służb na działania, które przez lata przechodziły niezauważone i które zasługują bardziej na miano happeningów niż akcji. Jedna z osób „oskarżonych” o wieszanie tęczowych flag na pomnikach została zatrzymana przez nieumundurowanych p*icjantów kilkaset kilometrów od miejsca swojego zamieszkania i położenia „znieważonych” pomników i przewieziona nieoznakowanym samochodem do stołecznej izby zatrzymań. Inna osoba trafiła do aresztu śledczego za rzekome popisanie fasady kościoła, choć z pewnością tysiące innych przypadków popisania kościołów przeszło niezauważonych przez media i p*icje. Radiowozy bywały w p*lsce niszczone i podpalane, ale tylko raz próba podpalenia, nieudana zresztą, została nazwana przez Ziobrę „terroryzmem”. Zdarzały się nawet w p*lsce udane zamachy bombowe na komisariaty, które przechodziły bez większego echa. Wiele aktywistek „non-violence” spotkało się z ciężkimi pobiciami przez p*icje, z trwałym uszkodzeniem ciała włącznie. Nie jest to jednak, jak chcą liberałowie, wynik rządów takiej albo innej ekipy, ale raczej tego, kogo ta ekipa wybrała na rekwizyt w swoim spektaklu. Państwo zawsze wobec kogoś jest faszystowskie, a wobec kogoś innego liberalne w tym samym momencie. Zmieniają się po prostu ofiary faszyzmu. Decydując się na jakieś działanie przeciwko państwu, p*icji, kapitałowi, cywilizacji czy cistemowi nigdy nie możesz być pewnx skali reakcji, a już zwłaszcza tego jakie siły p*icji i innych służb zostaną skierowane do badania twojej sprawy. Kwestia zarzutów jest bardziej przewidywalna, choć ogólnie prokuratury i sądy bywają kreatywne, a w prawie karnym dla wyroku „postawa sprawcy” ma większe znaczenie niż popełniony czyn. Wiele wskazuje na to, że p*icja i inne służby, a także prokuratura i sądy nadania na pewne sprawy dostają „z góry”, czyli od polityków, a ostatecznym produktem ich działań jest zawsze medialny spektakl.

Służby specjalne posiadają także w swym słowniku słowo „figurant”, oznaczające osobę, która jest wrabiana w przestępstwo i często sądzona, a potem skazywana za czyny, których nie popełniła. Czasem można zostać skazanx za czyny, które wcale nie miały miejsca. Znane są przypadki osób anarchistycznych pełniących role figurantów i figurantek. Samo bycie anarchistką generalnie oznacza znalezienie się w kręgu zainteresowania służb specjalnych. Oczywiście nie ma sprawiedliwości w tym systemie, więc nawet robiąc całkiem „legalne” rzeczy należy spodziewać się represji i uwięzienia.

Sprawić żeby państwo wiedziało o twoich poglądach to bardzo ważny wybór, którego część z nas dokonuje bezrefleksyjnie. Bartolomeo Vanzetti został oskarżony o morderstwo i skazany na śmierć na krześle elektrycznym dlatego, że śledczy wiedzieli, że jest anarchistą[1]. Resztę dowodów i zeznań potrzebnych do tego aby go zabić spreparowali. Przypadek Vanzettiego jest skrajny, ale wcale nie odosobniony, figurantami była także Belgradzka Szóstka[2], wiele osób anarchistycznych na b*orusi i przede wszystkim ofiary r*syjskiej sprawy „Sieci"[3].

Dla mnie takie rozważania mają dwie konsekwencje. Po pierwsze, zawsze planując działania warto spodziewać się większego zaangażowania służb w sprawę niż miało to miejsce we wcześniejszych przypadkach podobnych działań. Lepiej zawsze założyć, że możliwe konsekwencje mogą być poważniejsze niż wynika z samej analizy prawniczej. Warto mieć świadomość tego, że najważniejszy element ryzyka, czyli skala państwowej reakcji, jest nieznany. To na jakie działania ostatecznie się zdecydujesz i jak postanowisz się zabezpieczyć, jest już konsekwencją twoich wyborów. Możesz - ale nie musisz - kierować się przede wszystkim ostrożnością. Po drugie, świadomość pewnej nieprzewidywalności naszego przeciwnika może dać ci poczucie paradoksalnej wolności. Jeśli osoby siedzące na chodniku państwo traktuje jak kryminalistki, to może nie warto ograniczać się do takich akcji i śmiało można sięgać po bardziej destrukcyjne i skuteczne metody oporu. Rób co chcesz. Tobie zostawiam odpowiedź na pytanie co warto robić.

2.2. Tworzenie planów

Jest sporo dobrej literatury o tworzeniu planów, w tym o tworzeniu planów akcji. Nie będę więc rozwodzić się nad tym specjalnie i odeślę do kilku fajnych pozycji, takich jak wspomniane już w przypisie „The art of rebelion - martial tradition for the anarchists", a także „Arson Around With Auntie Alf", „ALF Primer, a guide to direct action and Animal Liberation Front", i „Earth First Direct Action Manual". Niemniej, tak często będę się odnosić do planowania w tej broszurze, że niepraktycznie by było nie zawrzeć tu jakiegoś podsumowania. Plany mogą być długofalowe i krótkofalowe i co ważne, w obydwu wypadkach możesz i powinnxś stosować procedury opsec w podobny sposób.

Plan powinien mieć jasno zdefiniowany cel. Najlepiej w taki sposób, by nie było żadnych wątpliwości co do tego kiedy cel jest osiągnięty, a kiedy nie. Pomoże to w podejmowaniu decyzji w trakcie działań i w ewaluacji.

Wyobraź sobie, że chcesz zrealizować taki przykładowy plan krótkofalowy:

[1] przyp. red.: Ferdinando „Nicola" Sacco (18911927) i Bartolomeo Vanzetti (1888 1927) anarchiści i robotnicy amerykańscy pochodzenia włoskiego; w 1920 w trakcie organizowania wiecu zostali zatrzymani pod zarzutem działalności go dzącej w dobro publiczne, a dodatkowo oskarżono ich o napad rabunkowy i dwa morderstwa. Pomimo posiadanego alibi i wątpliwych dowdów, skazano ich na śmierć na krześle elektrycznym w atmosferze powszechnej nagonki (prowadzą cy proces sędzia ich „anarchistycznymi kanaliami").

[2] Odsyłam tu do artykułu Belgrade: anarchists arrested; state attorney seeks in ternational terrorism charge, który można znaleźć na libcom.org

[3] Sprawa "Sieci" – nowe informacje, rupression.com

Chcesz udać się do lasu, rozebrać upatrzoną wcześniej ambonę, przetransportować drewno do swojego legowiska i wykorzystać je jako opał. Celem jest uprzykrzenie życia myśliwym i pozyskanie opału.

Dobry plan jest prosty - to znaczy, że powinno dać się go streścić w kilku zdaniach. Ten plan trudno będzie zrealizować samotnie, z uwagi na ciężar drewna do transportu, dlatego na jakimś etapie będzie trzeba z kimś omówić jego założenia. Im prostszy plan, tym mniejsze ryzyko niezrozumienia kluczowych założeń. Oczywiście plan wymaga doprecyzowania miliona szczegółów, zwłaszcza jeśli jest długofalowy, ale w sytuacji wystąpienia problemów decyzje ad hoc podejmuje się w odniesieniu do kluczowych założeń. Dla przykładu: jeśli celem jest rozebranie ambony, to należy rozbierać ambonę, a nie gonić przypadkowo napotkanych myśliwych. Ważne zatem aby główne założenia planu były jasne dla ciebie i innych zaangażowanych osób.

Ciekawa obserwacja dot. robienia planów operacji specjalnych znajduje się we wspomnianym „Spec Ops" Macravena. Macrven zwraca mianowicie uwagę, że wszystkie udane operacje specjalne składały się dla wykonując je żołnierzy z czynności rutynowych. AB często przypominają operacje specjalne, w tym sensie, że warunki akcyjne jeśli chodzi o poziom stresu i ryzyka często niewiele albo wcale ustępują warunkom bojowych operacji na tyłach wroga. Akcja nie jest dobrym momentem na uczenie się rzeczy od podstaw, na improwizowanie (ach, ten dreszczyk emocji!), ani na przypominanie sobie skomplikowanych procedur. Najwięcej szans na powodzenie mają akcje, na których prowadzi cię twoja pamięć mięśniowa. Dlatego, jeśli masz rozebrać ambonę to w zależności od przyjętej metody i okoliczności: odbijanie desek młotkiem, praca łomem, czy poruszanie się po drabinie i ogólnie na wysokości powinny być twoją powszedniością. Warto też zastanowić się, co może pójść nie tak i przećwiczyć sobie także czynności wykonywane w sytuacjach awaryjnych (w wypadku ambony może być to poruszanie się na wysokości po niestabilnej konstrukcji, a jeśli ambona jest bardzo wysoka, albo umieszczona na drzewie, to być może zjazd na linie czy coś takiego.) Jeśli zapragniesz zrealizować pomysł z amboną zanim nauczysz się obsługiwać młotek, to daj sobie jakiś czas na praktykę stolarską.

Plan, oprócz jasnego i prostego zdefiniowania celu, powinien zawierać także równie jasno zdefiniowany cel zapasowy (czyli np. jeśli okaże się, z jakiegoś powodu nie możesz dotrzeć do wybranej ambony to udasz się do innej, położonej nieco dalej ale w łatwiejszym terenie), a także jasno określone warunki brzegowe, w których zrezygnujesz z realizacji celu głównego i zmienisz go na zapasowy. Powinno być też jasno określone w jakich warunkach całkiem zrezygnujesz z działań. Określenie warunków brzegowych pozwoli szybkie podjęcie decyzji, uniknięcie zbędnego zastanawiania się lub dyskusji w strefie w której mogą operować przeciwnicy i generalnie pozwoli zaoszczędzić czas. Dobry plan także nie kończy się na osiągnięciu celu, a opisuje wszystkie czynności związane z bezpiecznym powrotem, likwidacją śladów, dowodów itp. Oczywiście warto mieć także ustalone z góry scenariusze postępowania w sytuacjach awaryjnych, drogi bezpiecznej ewakuacji, miejsca spotkania po ewentualnym wycofaniu itp. W wypadku planu długoterminowego warto zaplanować przerwy na odpoczynek i zgubienie ogona - plan może na przykład zakładać, że

po wykonaniu jakiejś aktywności zrobisz sobie pół roku przerwy i w międzyczasie pozbędziesz się całego sprzętu, albo dobrze go ukryjesz w z góry znany sposób.

Po więcej informacji na temat planowania odsyłam do literatury.

2.3. Opsec w pięciu krokach

Mając już podstawową wiedzę dotyczącą planowania, możemy wrócić do 5 kroków opsec. Dla przypomnienia były to:

1. Ustalenie krytycznych informacji
2. Analiza zagrożeń
3. Analiza podatności
4. Oszacowanie ryzyka
5. Wprowadzenie odpowiednich środków przeciwdziałania

W nieco bardziej przystępnej formie ten sam proces rozpisany jest w postaci pięciu pytań na ciekawej i godnej polecenia stronie Surveillance Self-Defense[4]. Oto one:

1. Co chcę ochronić?
2. Przed kim chcę tego bronić?
3. Jakie będą konsekwencję przechwycenia danej informacji kluczowej?
4. Na ile prawdopodobne są zagrożenia?
5. Ile trudności sprawi mi zabezpieczenie przed konsekwencjami i na ile chcę to robić?

Powyższe pytania całkiem dobrze oddają istotę procesu opsec, którą jest osiągnięcie założonego celu. Twoim najważniejszym zadaniem w tym procesie jest taki wybór środków, które bardziej utrudnią pracę przeciwnikom niż tobie i przez to uprawdopodobnią osiągnięcie twojego celu. Jeśli twoja ostrożność uniemożliwia ci osiąganie celów, to nie jest ona elementem opsec, a paraliżującym strachem. Strach rzecz jasna ma znaczenie ewolucyjne, natomiast zakładam, że skoro czytasz tego zina, to propagacja genów nie jest twoim głównym zmartwieniem. Pominę więc tutaj ględzenie o biologicznym znaczeniu strachu i wbudowanego w nas mechanizmu utrzymywania się przy życiu. Ja mam swój własny sposób na życie ze strachem, ale podejście, które chcę tutaj opisać jest dużo bardziej zestandaryzowane niż moje emocje.

[4] https://www.eff.org/pages/surveillanceselfdefense

1. Co chcę ochronić?

Kluczowe informacje, to takie, których przejęcie przez przeciwnika uniemożliwi realizację planu. W wypadku planu z amboną będą to:

a. Wybrana przez nas ambona

b. Czas operacji

c. Nasza tożsamość

d. Droga dojścia do ambony

e. Sposób powrotu i lokalizacja naszego leża

Przechwycenie nawet jednej z powyższych informacji pozwoli zdeterminowanemu przeciwnikowi o pewnych zasobach (głównie czasu) uniemożliwić realizację planu, a zapewne także cię schwytać. Natomiast nawet jeśli przeciwnik już będzie wiedzieć, że ktoś gdzieś realizuje taki plan (bo zauważy, że tu i tam czasem znikają ambony), to dopóki nie przechwyci którejś z powyższych informacji, możesz działać w miarę spokojnie.

Oczywiście do wielu z tych informacji przeciwnik może dojść drogą dedukcji, zwłaszcza jeśli będziesz działać w sposób schematyczny, np. wybierając cele w pobliżu swojego miejsca zamieszkania, w kolejności od najłatwiejszych itp.

2. Przed kim chcę tego bronić?

Ten punkt może wydawać się żmudnym ćwiczeniem, ale warto je przejść. Zatem w scenariuszu z amboną twoimi przeciwnikami są oczywiście:

- p*icja
- straż leśna
- koła myśliwskie
- część wiejskiej społeczności sympatyzująca z myśliwymi
- straż graniczna (w niektórych terenach)

Warto też przemyśleć jakimi zasobami w twoim terenie dysponuje przeciwnik, jakie ma zwykle metody działania. Jak często strażnicy leśni, myśliwi czy nieżyczliwi lokalsi pojawiają się w okolicy, jak są wtedy wyposażeni, na ile łatwo możesz się przed nimi ukryć. Należy też wiedzieć jak łatwo możesz ujść pościgowi, czy w okolicy mogą być foto-pułapki, czy ktoś może cię wytypować na potencjalnego sprawcę na podstawie znajomości twoich działań i czy możesz znaleźć się wtedy pod stałą obserwacją itp.

3. Jakie będą konsekwencję przechwycenia danej informacji kluczowej?

Celem odpowiedzi na to pytanie jest nadanie wagi poszczególnym informacjom, tak aby w kolejnych krokach łatwo można było wybrać środki zaradcze. Jeśli przeciwnik pozna twoją tożsamość to najprawdopodobniej doprowadzi do twojego uwięzienia, co pewnie jest scenariuszem, którego najmniej sobie życzysz. Natomiast jeśli przechwyci w jakiś sposób informacje o twoim kolejnym celu, drodze podejścia itp. to z pewnością udaremni ci tę i pewnie każdą kolejną akcję póki nie wprowadzisz znacznych zmian w metodzie. Być może jednak w takim scenariuszu uda się tobie ujść cało, przy założeniu, że będziesz odpowiednio zamaskowanx i nie zostawisz identyfikujących śladów (np. śladów logowania twojego telefonu w sieci telefonii komórkowej). Odpowiadając sobie na to pytanie powinnxś już widzieć, w którym miejscu jesteś podatnx, jakie dane musisz najlepiej chronić i jakie metody przeciwdziałania akcjom przeciwnika będą najlepsze.

Na tym etapie powinnxś już także odpowiedzieć na pytanie ile ryzykujesz, co wydarzy się w najgorszym możliwym scenariuszu. Powinnxś poważnie przemyśleć, czy jesteś gotowx na takie konsekwencje.

4. Na ile prawdopodobne są zagrożenia?

Gdy będziesz robić taką akcję z amboną po raz pierwszy, to szansa na to, że przeciwnik będzie z góry wiedział o twoich działaniach i przechwyci informację o celu itp. zanim dojdzie do akcji jest bardzo mała. Jest to właściwie możliwe tylko wtedy, gdy samx powiesz o swoich zamiarach komuś nieodpowiedniemu. Natomiast to, że słowa rzucane ot tak, w wiejskiej knajpie albo obserwacje wścibskiego sąsiada zostaną przekazane przeciwnikowi, wydaje się bardzo prawdopodobne. Bardzo prawdopodobne jest też to, że przeciwnik będzie post factum próbował wyobrazić sobie profil „przestępcy" skłonnego do takiej akcji i poszukiwał osób pasujących do tego profilu w najbliższej okolicy zdarzenia. Całkiem możliwe jest też, że spotkasz kogoś idąc na akcję lub wracając z niej - pytanie, jakich informacji o swoich działaniach dostarczysz takiej osobie swoim wyglądem i zachowaniem. Z pewnością też zostawisz jakieś ślady na podłożu w terenie działania, istotne więc co będzie dało się z tych śladów wyczytać.

5. Ile trudności sprawi mi zabezpieczenie przed konsekwencjami i na ile chcę to robić?

Masz już gotowy model zagrożeń, wiesz jakich działań przeciwnika spodziewać się z jakim prawdopodobieństwem i gdzie są twoje czułe miejsca. Teraz możesz zastanowić się nad tym jakie środki zaradcze powziąć i ile będzie cię kosztować pracy, czasu i pieniędzy zabezpieczenie się przed różnymi scenariuszami. Twoje działania wiele mogą zyskać na skuteczności dzięki niewyróżniającemu się strojowi, czapce i okularom utrudniającym identyfikację, a także na atakach bez jasnego schematu, w terenie, w którym nie jesteś znanx jako gwiazda pro-zwierzęcego aktywizmu. Bardziej kosztowne i problematyczne

może być zatarcie śladów podczas śnieżnej zimy lub błotnistej jesieni - dobry wybór czasu akcji powinien rozwiązać ten problem. Niezabieranie na takie wyjście telefonu komórkowego to już pewien koszt - bo wiadomo: bez telefonu jak bez ręki - ale wydaje mi się on do przyjęcia przy założeniu, że w miarę znasz teren; jeśli nie, to warto byś spędziłx czas na poznawaniu go. Najbardziej problematyczną częścią tego planu z punktu widzenia opsec będzie powiedzenie komuś o nim. Jeśli jeszcze nie masz sprawdzonej osoby partnerskiej do takiego zadania, to podejmujesz bardzo duże ryzyko szukając jej. Z drugiej strony trudno będzie ten plan zrealizować w pojedynkę.

2.4. Różne modele działań i ich konsekwencje

Twoja tożsamość w wypadku działań wrażliwych (czyli w wypadku, wszystkich działań groźnych dla państwa/p*icji/cistemu etc.) zawsze powinna stanowić informację krytyczną i powinnxś ją chronić przed przeciwnikiem. Jednak wielu wspaniałych planów po prostu nie da się zrealizować w pojedynkę, dlatego często będziesz chcieć okazać zaufanie tej czy innej osobie. W odniesieniu do zaufania możemy wydzielić kilka modeli organizacji i „nie-organizacji".

1. **Model darknetowy** – jest on trudny do realizacji offline i generalnie ryzykowny przy zastosowaniach innych niż stricte internetowe, choć zdarzają się takie próby. Używają go sieci „cyberprzestępcze", czyli na przykład handlarze on-line, hakerzy czy szajki pedofilskie. Istotą modelu jest to, że żadnych informacji o sobie nie przekazuje się nie tylko przeciwnikom, ale również najbliższym współpracownicom i generalnie okazuje się wszystkim tak samo zerowe zaufanie. Jedna z zasad tego modelu mówi „jeśli działasz on-line, zostań on-line", czyli nigdy nie spotykaj się osobiście z nikim, z kim współpracujesz. Wbrew pozorom, tak długo jak twoje działania nie wymagają wspólnego robienia fizycznych rzeczy, model ten jest całkiem efektywny. Ułatwia on poszukiwania współpracownic, nie musisz bowiem im ufać, pozostajesz wobec nich całkowicie anonimowx. Mogą nawet być z p*icji jeśli pomogą ci zrealizować twoje cele.

   Użycie tego modelu wymaga znajomości Tora i innych narzędzi technicznych. Jest on skuteczny tylko, jeśli nasza „oficjalna" tożsamość nie zwróci na siebie niczym uwagi służb i pozostanie ściśle odseparowana od tożsamości „darknetowej". O narzędziach technicznych potrzebnych do realizacji tego modelu i o separacji tożsamości traktuje druga część zina - Pewne Rzeczy II, do której niniejszym zapraszam. Tutaj wspominam ten bardziej jako ciekawostkę, z uwagi na ograniczoną przydatność dla większości działań anarchistycznych. Dobrze został on opisany w broszurze „Jolly Roger's Security Thread for Beginners", natomiast dużo technicznych informacji jest w niej już nieaktualnych lub błędnych. Tak czy inaczej, warto się z ową broszurą zapoznać, a techniczne informacje weryfikować w nowszych źródłach.

Oczywisty problem z zastosowaniem tego modelu poza darknetem to twoja fizyczność, która nosi wiele cech identyfikujących. Nigdy nie wiadomo kiedy ktoś ci zrobi zdjęcie, które umożliwi p*icji identyfikacje. W praktyce spotykanie się fizyczne z ludźmi, którym nie ufasz, celem dokonywania wrażliwych aktywności jest ekstremalnie ryzykowne. Natomiast jeśli jesteś w stanie „pracować wyłącznie zdalnie" to jest to ciekawa opcja. Nawet jeśli pracujesz ze szpiclem to pozna on twoje plany, ale prawdopodobnie uda ci się ujść przed konsekwencjami.

2. **Model afinitek** – najmocniej promowany przez organizacje typu Animal Liberation Front i Earth Liberation Front, a także np. Federazione Anarchica Informale. Afinitka to grupa ufających sobie znajomych. Praktyka działania w takich grupach jest używana przez anarchistki w różnych modelach „organizacyjnych". Natomiast omawiany model zakłada ograniczenie wszelkiego planowania i podejmowania działań do grupy osób, która dobrze się zna i sobie ufa, natomiast nie okazuje żadnego zaufania nikomu spoza grupy. Broszury ALFu zalecają zakładanie nowych grup z osobami, które się zna „od lat" i nieinformowanie innych grup ALFu o swoim istnieniu. Jedna z zasad mówi, że jeśli wiesz o istnieniu grupy ALFu, której nie zakładałxś, to znaczy, że ta grupa ma zły opsec. Model ten jest niezwykle użyteczny, wygodny i całkiem skuteczny jeśli uda ci się właściwie wybrać osoby do działania w grupie. Model ten nie zakłada powiększenia początkowej afinitki, ale w pewnym sensie klonowanie jej przez nowopowstające grupy, nie mające z innymi grupami afinicji nic wspólnego. Grupy nawzajem inspirują się swoimi działaniami, nie znając tożsamości nikogo spoza swojej afinitki. ALF i ELF były w stanie skutecznie działać przez dekady, ELF zaś stał się przedmiotem największej operacji w historii istnienia FBI (tak, ELF, a nie Al-Kaida). Nie ukrywam, że model ten budzi wiele mojej sympatii.

3. **Organizacja z filtrem** – Ten model jest dość popularny wśród anarchistek i zakłada działanie w grupach, do których może dołączyć każda osoba, pod warunkiem przejścia jakiejś ograniczonej weryfikacji. Organizacja jest więc nastawiona na powolny wzrost liczby osób członkowskich, a żeby dodać do niej nową osobę wymagane jest polecenie, okres kandydacki itp. Takie organizacje zwykle urządzają raz na jakiś czas otwarte spotkania, na których przynajmniej część obecnych członkiń i członków ujawnia na przykład swój wygląd. W odróżnieniu od modeli 1 i 2 poziom wewnętrznego zaufania do innych osób w grupie jest niejasny, co prowadzi do wątpliwości chociażby na tle tego, jakie informacje można sobie przekazywać. W rzeczywistości także niezwykle trudno jest utrzymać listę członkiń i członków w tajemnicy, a informacje o tym, kto co robi w takiej grupie, krążą w postaci plotek. Jeśli grupa zostanie objęta stałą obserwacją, to prawdopodobnie służby nie będą miały problemu z ustaleniem kompletnej lub prawie kompletnej listy osób członkowskich. Od kilku lat popularne w takich grupach w p*lsce jest używanie zmienionych imion/ksywek, co podnosi bezpieczeństwo, ale tylko tak długo, jak grupa nie jest przedmiotem jakiegoś poważnego śledztwa. Próby ukrycia swojej tożsamości w takiej „organizacji"

często przypominają stosowanie modelu 1 offline. „Pod spodem" takiej grupy działają niekiedy grupy afinicji zajmujące się bardziej wrażliwą pracą, o której nie informują wcale lub informują resztę tylko w ograniczonym zakresie. To nosi znamiona łączenia modeli, o którym opowiem za chwilę.

4. **Organizacja otwarta** – każda osoba może dołączyć do oganizacji i brać udział w podejmowaniu decyzji, organizacja jest nastawiona na szybki wzrost. Przykładem takiej organizacji może być Ende Gelande lub Reclaim the Streets. Działając w takiej grupie, należy się liczyć z tym, że p*icyjni prowokatorzy i różni inni agenci wpływu mają mniejszy lub większy wpływ na jej działania. Anarchistyczna praktyka zakłada, że jeśli organizacja jest niehierarchiczna, to najgorsze przejawy tego wpływu uda się zniwelować, gdyż szpicle nie będą miały jak kompletnie przejąć sterów. W kontekście ochrony tożsamości sprawa wygląda podobnie jak w modelu 3. Takaże w takich organizacjach część pracy jest zwykle wykonywana przez grupy afinicji, które mogą nie ujawniać nawet swojego istnienia innym. To również stanowi przykład łączenia modeli.

Zarówno w modelu 3 jak i 4 właściwie każde wystąpienie na forum takiej organizacji należy traktować tak jak wystąpienie publiczne. Nie wiadomo, dokąd w postaci plotek trafiają informacje ze spotkań, a poziom zaufania do poszczególnych członkiń jest zróżnicowany i często całkiem zasadnie można założyć, że powinien być zerowy. Tymczasem, jeśli grupa jest na poważnie rozpracowywana przez p*icję, to ukrycie swojej tożsamości jest ekstremalnie trudne (zdjęcia i nagrania wykonane z ukrycia, ewentualnie wspomagane śledzeniem lub spisaniem, pomogą p*icji ustalić personalia wszystkich osób członkowskich), zwłaszcza jeśli grupa działa przez dłuższy czas.

Tutaj jednak chciałxm zaznaczyć, że fakt, że jakieś działania nie stanowią „kuloodpornego" zabezpieczenia w danym kontekście nie oznacza, że całkiem powinnxś z nich zrezygnować. Nie chcę sprawiać wrażenia, że próby ukrywania swojej tożsamości w modelach 3 i 4 są niecelowe i należy z nich zrezygnować.

Niemniej, działając w modelach 3 i 4, z dużym prawdopodobieństwem zostaniesz rozpoznanx jako osoba anarchistyczna i może to ściągnąć na ciebie uwagę służb. Duże jest także ryzyko, że działania organizacji zostaną powiązane z twoją oficjalną tożsamością. Takiego ryzyka nigdy nie powinnxś podejmować bezwiednie, bez przemyślanej strategii i nie zyskując nic w zamian. Więcej o separacji tożsamości piszę w drugiej części zina.

2.5. Łączenie modeli

Stara anarchistyczna mądrość mówi, żeby pracy oficjalnej i rzeczniczej w jakimś temacie nie łączyć z wrażliwymi działaniami na tym samym polu. W praktyce znane są przypadki osób, które łamały tę zasadę i wpadały dopiero po latach, ale prawidło to wydaje się jak najbardziej rozsądne. Jeśli zostanie wykonana jakaś skuteczna i radykalna akcja pro-

zwierzęca, to p*icja w pierwszej kolejności obejmie obserwacją aktywistki pro-zwierzęce mieszkające w pobliżu miejsca tej akcji.

Organizacje działające wedle typów 3 i 4 stanowią dla p*icji łatwe cele do zauważenia i objęcia obserwacją. Dzięki takiej obserwacji mundurowi mogą uzyskać dużo informacji o osobach, ich zainteresowaniach, umiejętnościach i przekonaniach, a także wybrać cele do bardziej uważnego rozpoznania. Nawet jeśli grupy afinicji złożone z członkiń takich organizacji działają bardzo ostrożnie i w pełnym utajeniu przed innymi osobami w tych grupach, p*icja może być w stanie wyłowić osoby odpowiedzialne za bardziej wrażliwe działania na podstawie nasłuchiwania plotek, obserwowania kontaktów społecznych pomiędzy członkiniami (kto z kim się trzyma), typowania osób o dużym autorytecie i określonych umiejętnościach.

P*icja i wszystkie inne służby to ogromne struktury, które rutynowo zbierają i przetwarzają duże ilości danych, które często wydają się zupełnie niepotrzebne, ale przeanalizowane zaczynają ujawniać pewne wzorce. Duża część operacji Backfire, wspomnianej największej w dziejach FBI operacji, której celem był ELF, polegała na monitorowaniu imprez i zbieraniu zeznań osób zatrzymanych do rutynowych kontroli przy okazji punkowych wydarzeń. Na 30 000 stron, które śledczy zebrali szukając śladów działalności ELF znajduje się podobno ogrmna ilość plotek i pozornie nieistotnych informacji[5]. Gdy ktoś zebrał i przeczytał wszystkie notatki z takich przesłuchań, mógł dowiedzieć się co nieco o anarchistycznym „środowisku" z tamtego okresu. Informacje tego typu rzadko z miejsca wskazują sprawców poważnych „przestępstw" (chyba że są bardzo nieostrożni), ale mogą pomóc p*icji choćby dostarczyć haki do łamania potencjalnych współpracowników i wytypować miejsca, w których należy ich szukać. Dlatego łączenie działań w modelach 3 i 4 z jakimikolwiek innymi należy uznać za potęgowanie ryzyka. Więcej o metodach pracy p*icji piszę w rozdziale 4.

2.6. Ruch, środowisko i miejscówki – różne nazwy na ten sam problem

Powyższe rozważania nieuchronnie doprowadzają nas do problemu istnienia tak zwanego ruchu anarchistycznego. Ów „ruch" przyjmuje i porzuca nowy przymiotnik w zależności od panującej mody, np. przez dekadę 2005-2015 w tak zwanej p*lsce „ruch" radził sobie zupełnie bez przymiotników, a jego uczestniczki zapytane o tożsamość mamrotały coś o „aktywizmie". Wcześniej miał tożsamość „alterglobalistyczną", co z całą pewnością było określeniem skopiowanym z bełkotu kapitalistycznych mediów. Mnie doprowadza to do przekonania, że nie chodzi w „ruchu" o anarchizm - nie mówiąc już o anarchii. Z litości nie będę tutaj roztrząsać „programów" całkiem bolszewickich organizacji funkcjonujących w tym „ruchu", które - jeśli już muszą się jakoś podpisać - nazywają się „anarchosyndyka-

[5] CrimethInc., Green Scared? Lessons from the FBI Crackdown on EcoActivists; dostępne na Anarchist Libraries

listycznymi", choć właściwie nikt nigdy nie powiedział co to znaczy. Krytyka „ruchu" z perspektywy anarchistycznej jest przedmiotem dziesiątek lub setek dobrych artykułów, a debata pomiędzy lewicowcami działającymi w „ruchu", a anarchistami przecieka już nawet do p*lskojęzycznej literatury, nie będę cię nią zanudzał.

Ważniejsza dla mnie teraz jest perspektywa praktyczna, dotycząca tego, co właściwie zyskujemy, a co tracimy jako osoby anarchistyczne działając w „ruchu".

„Ruch" posiada pewną bazę materialną, nazywaną miejscówkami, czyli bary, skłoty, houseprojekty, biblioteki, a także leśne okupacje i dziesiątki innych miejsc, które, nie oszukujmy się, często są naprawdę fajne. Wokół tej bazy materialnej tworzy się siatka relacji społecznych, nazywana środowiskiem (także zwykle bez żadnego przymiotnika, najbardziej adekwatne przymiotniki zresztą mogłyby być uznane za obraźliwe). Te trzy powiązane zjawiska – „ruch", „środowisko" i „miejscówki" – choć rzadko kiedy ktokolwiek nazywa je na serio anarchistycznymi, stanowią dla służb specjalnych i p*icji użyteczny filtr pozwalający wyławiać osoby, które należy obserwować i które mogą potencjalnie uczestniczyć w akcjach bezpośrednich.

Fakt, dla nas, osób anarchistycznych, pełnią one również istotne funkcje, zwłaszcza związane z pracą opiekuńczą. Większość z nas nie potrafi funkcjonować w społecznej izolacji lub wyłącznie w otoczeniu ludzi, którzy akceptują obecny porządek społeczny. Potrzeba bliskości z innymi osobami, które naprawdę nienawidzą p*icji, kieruje nas w te rejony, gdzie, jak nam się wydaje, łatwo będzie je spotkać. Ponadto wiele „miejscówek" tworzy pewne ograniczone, pozarynkowe mechanizmy, które mogą ułatwiać przetrwanie, oferując nieco łatwiejszy dostęp do pożywienia i mieszkania.

Będąc świadomym tych ewidentnych plusów warto pamiętać o kosztach. „Miejscówki", „środowisko" i „ruch" tworzą iluzję bezpiecznej przestrzeni, i to pod każdym względem. Miejsca te pozostają w obszarze dominacji państwa, kapitału, hetero-matriksu i patriarchatu, co oznacza także pozostawanie w przestrzeni monitorowanej przez służby. Nasi nowi „przyjaciele" poznani w zeszłym tygodniu na skłocie mogą być dosłownie każdym z wymienionych: p*icjantami, gwałcicielami, donosicielami, komunistami, faszystami, wolontariuszami pro-p*icyjnego NGOsa, członkiniami partii politycznej (naprawdę!) czy – co chyba najbardziej szokujące – katolikami. Dodatkowo „środowisko" zawsze otacza się aurą wyjątkowości (sprowadzającą się w praktyce do kilku modnych gadżetów w stylu koca w panterkę), która służy przede wszystkim samoizolacji, czyli sekciarstwu. W praktyce znalezienie bezpiecznej przestrzeni wewnątrz „środowiska" jest tak prawdopodobne, jak zbudowanie jej poza nim, natomiast główną funckją „środowiska" jest przekonanie swoich uczestniczek, że jest inaczej. Nie chcę tutaj napisać, że korzystanie z dobrodziejstw bycia w „środowisku" powinno być dla nas zakazane. Po prostu nie ma nic gorszego niż fałszywe poczucie bezpieczeństwa. Myślę, że można mieć udane, anarchistyczne życie zarówno trzymając się z daleka od „środowiska" jak i korzystając z niego z pełną świadomością jego wad. W obydwu wypadkach należy jednak zachować taką samą ostrożność.

Pisząc o funkcjach opiekuńczych „środowiska", warto wspomnieć o tym, że tak zwany „romans wywiadowczy" jest praktyką używaną od zawsze przez służby na całym świecie. Mark Kennedy, to najbardziej znany szpicel pracujący w „ruchu". Był on etatowym pracow-

nikiem londyńskiej policji, pracującym pod przykryciem w 22 krajach przez 7 lat. Uwodził wiele aktywistek (w tym osoby mieszkające w p*lsce). Inny p*icjant pracujący w tej samej jednostce co Kennedy miał dziecko z jedną z osób aktywistycznych, którą rozpracowywał. Gdy wszczęto śledztwo w sprawie nadużyć w tej jednostce p*icji, zgłosiło się łącznie 8 rozpracowywanych kobiet, które uprawiały seks z 5 różnymi szpiclami pracującymi w tej tylko jednej jednostce[6].

Informacje zdobyte w łóżku mają nawet specjalną nazwę w języku służb, określane są mianem „pillow talk", czyli „gadkami przy poduszce", co stanowi dla nas wyraźny sygnał, że chwile rozluźnienia spowodowane orgazmem i/lub używkami nie powinny zwalniać nas z przestrzegania opsec. Nawiasem mówiąc, picie alkoholu jest ogólnie ryzykowne, ze względu na jego silne „odhamowujące" działanie i sposób, w jaki wpływa on na nasze kontakty społeczne.

Osobom zainteresowanym tym, jak daleko potrafią posunąć się służby, polecam bardzo ciekawą biografię Marity Lorenz, która, będąc informatorką prowadzoną przez CIA, wzięła ślub z Fidelem Castro i zaszła z nim w ciążę.

2.7. Case study: imprezka na skłocie

Zacznę od pewnej historii, która może początkowo wydać ci się niezwiązana z tematem. Nie wiem dokładnie, jak jest teraz z melinami, czyli z miejscami, gdzie sprzedaje się „nielegalnie" wytworzony alkohol, ale miejsca takie funkcjonowały bez przeszkód w p*lsce przez całe lata 80., 90. i początek 00. Wiem przynajmniej o jednej melinie, która istniała przez ponad 20 lat i doczekała się początku internetowych portali informacyjnych, tak że zrozpaczeni sąsiedzi mieli wreszcie okazje pytać publicznie (w komentarzach) jak to możliwe, że wszyscy znają adres tej meliny a „p*icja nic nie robi". Rzeczywistość tymczasem była taka, że p*icja bardzo wspierała i szanowała osoby prowadzące meliny, gdyż były one niezwykle cennymi informatorkami. Wiem o podobnych układach dotyczących klubów techno, w których bez problemu można było kupić narkotyki (i czasem „nielegalny" alkohol też), a które długo działały pod p*icyjnym parasolem. Można nawet z przekąsem powiedzieć, że p*icjanci lubią dobrą zabawę. Oprócz wspomnianego już wpływu alkoholu na rozmowność istotne jest to, że osoby, które p*icja nazywa „zawodowymi przestępcami" (jeśli to określenie ma jakikolwiek sens, to mi pasuje najbardziej do samej p*icji), miewają nagłe przypływy gotówki, które często wydają właśnie na melinach, w klubach, w kasynach i na usługi osób pracujących seksualnie. Monitorowanie miejsc rozrywki i osób pracujących seksualnie pozwala namierzyć tych, którym zaczęło się w życiu powodzić. Warto zapamiętać, że wszelkie miejsca, gdzie pojawiają się spore ilości gotówki, są interesujące dla p*icji, zwłaszcza jeśli gotówka ta choćby potencjalnie pochodzi z „nielegalnych" źródeł. p*icja może zatem celowo tolerować, a nawet ochraniać pewne miejsca, jeśli dostarczają jej one użytecznych informacji – a już zwłaszcza jeśli służby mają tam szpicli.

[6] Polecam tutaj wikipedyjny artykuł UK *undercover policing relationships scandal*

My, osoby anarchistyczne, często nie śmierdzimy groszem i nagłe powodzenie finansowe nam nie grozi. Natomiast schematy odreagowywania stresu mamy podobne co złodzieje samochodów. Niesamowicie niebezpieczny jest zwyczaj afterparty po akcji, który towarzyszy niektórym działaniom masowym, w stylu blokad antyfaszystowskich. Takie afterparty gromadzi osoby zaangażowane w określone działania, które przychodzą na nie niezamaskowane, są razem w jakiejś określonej, zwykle publicznej przestrzeni, piją alkohol i rozmawiają o stresach. W związku z nakładem pracy i napięciem przed akcją, to często pierwsza okazja to napicia się i spędzania czasu w towarzystwie – piją więc łapczywie i rozmawiają chętnie. Nieraz dopiero w momencie afterparty kluczowe dla jakiejś akcji osoby znajdują się wszystkie razem, w przestrzeni, która łatwo poddaje się obserwacji i paradoksalnie są wtedy mniej powściągliwe niż na zamkniętych spotkaniach organizatorskich. Im więcej jest problemów i stresu, tym bardziej opsec się sypie. Na afterparty wszystkie problemy mamy na świeżo, emocje są silne, a dostępność alkoholu jest nie bez znaczenia. Dla p*icji często najłatwiejszą metodą na dowiedzenie się wszystkiego o danej akcji byłoby zainstalowanie podsłuchu w nieprzytomnym punku leżącym w strategicznym punkcie na afterparty. Na afterach nikt nie zwraca uwagi na nieprzytomnych punków, to sprawdzone info.

Organizowanie afterów to zły pomysł. Jeśli już są, to lepiej na nie nie przychodzić. A jeśli już musisz przyjść z jakiegoś powodu to zastanów się czy to dobry moment na picie alkoholu, czy przyjmowanie innych używek. Ty możesz ocenić jak one na ciebie działają i czy pod ich wpływem będziesz stanowić zagrożenie dla siebie i innych.

Często prosta obserwacja kto z kim pije wystarczy, żeby dowiedzieć się dużo o grupie. Wystarczy, że p*icja zna wygląd jednej osoby z grona organizatorskiego (co jest częste) i może łatwo zaobserwować z kim ta osoba spędza czas. To, kto cieszy się specjalną estymą i na widok kogo wszystkie osoby milczą, także widać. Kto odbiera gratulacje, a kto przeprosiny również.

„Zwykła" imprezka na skłocie rządzi się podobnymi prawami. Zawsze należy założyć, że jest na niej przynajmniej jeden szpicel. Analogicznie, jeśli podpalisz komisariat, to nie idź opić tego na pobliskim skłocie. Najbliższe załoganckie karaoke to także nie jest dobre miejsce na ewaluacyjne spotkanie twojej afinitki i odreagowanie stresu. Lepiej zorganizuj to w górach lub na innym odludziu, nie bezpośrednio po akcji i/lub rozważ zostawienie telefonów w domach (oczywiście jeśli weźmiesz telefon ze sobą, to nie bierz go na ewaluacyjne spacery). Jeśli już musisz bywać w „miejscówkach" (tak, jesteśmy społecznymi zwierzętami, wiem o tym), to nigdy nie rozmawiaj w nich o wrażliwych działaniach (tzn. nigdy nie rozmawiaj o wrażliwych działaniach, ale już na pewno nie tam). I najlepiej nie imprezuj tam ze swoją grupą afinicji. Ludzie nie muszą wiedzieć, że działacie razem. I po raz kolejny, przemyśl to jak działają na ciebie używki, a zwłaszcza alkohol, bo „rozwiązywanie języka" to jego główna funkcja.

2.8. Samotne działania

Działania prowadzone jednoosobowo mają naprawdę wiele zalet. Jeśli plan istnieje tylko w jednej głowie i nigdy nie został nigdzie spisany, to nie da się go przechwycić, a więc i udaremnić. Właściwie to działania pojedynczych osób, które nie wahają się stosować skutecznych metod, są tym, czego służby specjalne boją się najbardziej i co jest dla nich najtrudniejsze do kontrolowania. W literaturze dotyczącej pacyfikacji ruchu oporu jednostki skłonne do samotnego działania określane są mianem „samotnych wilków" (mózgi trepów są uwikłane w patriarchalne schematy i samotne wilczyce znajdują się poza granicami ich percepcji). Wśród ekspertów panuje konsensus, że zagrożenia ze strony samotnych osób wilczych wyeliminować się nie da. Samotność rozbraja państwo z jego najpotężniejszych broni: masowej inwigilacji, donosicielstwa i szpicli.

Ostatecznie to ty jesteś jedyną osobą, której intencji możesz być absolutnie pewnx. Właściwie, to wiele wskazuje na to, że służby wolą same zakładać ultraradykalne organizacje lub maleńkie „komórki" (poszukaj informacji o sprawa Brunona Kwietnia) niż pozwalać, aby osoby o radykalnych poglądach pozostawały całkiem niezorganizowane. Tak ja odczytuję zdanie, którym Mike Davis kończy Planetę Slumsów: „Bogowie chaosu zawsze stoją po stronie wyrzutków". Jeśli zostaje ci tylko samotność i desperacja, wtedy naprawdę stajesz się groźnx. Na nieszczęście służb taki jest los miliardów ludzi, a ich liczba wciąż rośnie.

Samotne działania rodzą też kilka problemów. Ryzyko jest większe, bo nie możesz liczyć na tak zwaną obczajkę, czyli osobę, która ostrzeże cię przed nadchodzącym zagrożeniem. Prawda jest jednak taka, że często obczajka daje iluzję bezpieczeństwa, bo w wielu wypadkach gdy cię ostrzega, to i tak jest za późno na ucieczkę. Od miejsca akcji i ukształtowania terenu zależy to, czy obczajka ma w ogóle sens. Tam gdzie nie ma, lepiej prowadzić samotne akcje. Samotnie trudniej się obronić, trudniej forsować niektóre przeszkody, trudniej transportować niektóre przedmioty, aczkolwiek to wszystko jest bardzo względne i zależne od kontekstu. Często walka i tak byłaby nieskuteczna, a niektóre przeszkody wygodniej pokonać w jedną osobę. Samotnie łatwiej też się ukryć, jedna osoba często mniej zwróci uwagę patrolu niż dwie lub więcej. To, co jest zupełnie inne przy akcji samotnej, to nie tyle samo ryzyko, co jego percepcja. Większość czynników, które różnią akcję samotną od małej akcji grupowej, jest natury psychicznej i w gruncie rzeczy nie poznasz ich dopóki nie spróbujesz.

2.9. Case study: idziemy na terapię

Niezależnie od tego jakie jest twoje zdanie o terapiach i psychiatrii (moje jest dość krytyczne, tak samo zresztą jak o innych „naukach") to i ja i ty musimy zaakceptować fakt, że nasi bliscy często korzystają z takich usług. Nie zamierzam pisać rzeczy w stylu: nie chodź na terapię, bo wiem, że i tak tego nie posłuchasz. Nadmienię tylko, że psychologia i psychiatria doczekały się całkiem wielu krytycznych artykułów pisanych z różnych anarchistycznych perspektyw. Tu polecę tylko jeden tekst, a mianowicie „Descending into

madness" napisany przez Flower Bomb. Tymczasem postaram się przyjrzeć terapii i leczeniu psychiatrycznemu z perspektywy opsec.

Terapia jest problematyczna, gdyż podobno podstawą relacji terapeutycznej jest zaufanie do osoby terapię prowadzącej i to właśnie to zaufanie rzekomo decyduje o skuteczności terapii. Sprawia to, że osobom terapeutycznym możesz chcieć powiedzieć wiele rzeczy o sobie, w tym coś o swoich działaniach i poglądach. Jednocześnie terapia jest słabo umocowana w prawie, terapeuci nie są lekarzami, więc nie obowiązują ich przepisy dotyczące ochrony zdrowia. Istnieją natomiast prawne regulacje dotyczące tajemnicy zawodowej psychologów i są one, delikatnie mówiąc, niezbyt zachęcające. Po pierwsze osoba terapeutyczna ma OBOWIĄZEK (tak samo zresztą, jak każda inna osoba w świetle prawa, po prostu nie ma dla osób prowadzących terapie wyjątku) powiadomić odpowiednie służby, jeśli tylko nabierze przekonania, że stanowisz zagrożenie dla życia lub „zdrowia" swojego lub innych osób. Oznacza to np. że jeśli twoja osoba terapeutyczna uzna, że chcesz się samookaleczyć lub popełnić samobójstwo, to może doprowadzić do umieszczenia cię w zamknięciu. Co więcej, nie musi cię wówczas informować, że podejmuje działania w tym kierunku (nie ma takiego obowiązku wobec ciebie, ma natomiast wobec państwa i p*icji).

Nie wiem jak ty, ale ja znam kilka wspaniałych osób anarchistycznych, które stanowią dumne zagrożenie dla „zdrowia" innych osób. Mam nadzieję, że żadna nie zostanie nigdy wsypana przez osobę terapeutyczną. Co więcej, chociaż w pozostałych przypadkach (tzn. gdy nie ma zagrożenia „zdrowia" lub życia) osoba wykonująca zawód psychologa jest związana tajemnicą zawodową, to ta tajemnica może zostać uchylona przez sąd. Oznacza to, że jeśli sąd każe zeznawać twojej osobie terapeutycznej, to nie może ona odmówić, inaczej narazi się na odpowiedzialność karną.

Terapeutę obowiązuje zatem tajemnica zawodowa – nie może on więc plotkować na twój temat – może jednak zeznawać w sądzie i warto założyć, że jeśli posiada jakąś wiedzę, to podzieli się nią w trakcie procesu. Nie sądzę bowiem, by ta osoba chciała iść za ciebie do więzienia lub choćby narażać się na problemy z wykonywaniem zawodu, mając na koncie wyrok za składanie fałszywych zeznań. Osobie prowadzącej terapię można zatem zaufać trochę bardziej niż przypadkowemu punkowi napotkanemu na skłocie, ale niewiele bardziej. Musisz bardzo poważnie odpowiedzieć sobie na pytanie, jakie zagrożenie sprowadzasz na inne osoby w twoim otoczeniu przez to, że chodzisz na terapię. Samx możesz ocenić jakie ryzyko chcesz podjąć osobiście, jeśli chodzi o działania, których dokonujesz samotnie. Ale jeśli zaangażowane są w nie inne osoby, to najlepiej by było, jakby osoba prowadząca twoją terapię w ogóle nie dowiedziała, się, że takie działania mają miejsce. Jeśli już zdecydujesz się mówić na terapii o działaniach, w które zaangażowane są inne osoby, to poinformuj je o tym zanim zaczniesz. Pozwól osobom z którym współpracujesz sprzeciwić się twojej decyzji lub wycofać z działań jeśli uznają, że łamie to ich zasady opsec.

Jeśli już zdecydujesz się rozmawiać z osobą terapeutyczną o wrażliwych działaniach – niezależnie od tego, czy samotnych, czy grupowych – to koniecznie wróć do pięciu kroków opsec, przeanalizuj swój plan i ustal, jakie powinny być twoje środki ostrożności w tym wypadku. Przynajmniej wymyśl dla wszystkich rzeczy, miejsc, grup i osób, które są jakkolwiek związane z wrażliwą aktywnością nazwy kodowe (np. fałszywe pseudonimy dla osób,

fałszywe nazwy dla grup, fałszywe nazwy dla miejsc), pamiętając przy tym, że jeśli dokonasz akcji, która stanie się głośna (np. będzie można o niej przeczytać w mediach), fakty mogą stać się łatwiejsze do powiązania. Warto zawczasu ustalić listę informacji, których nie przekażesz osobie terapeutycznej i listę pytań na które odmówisz odpowiedzi.

Jeszcze poważniej sprawy wyglądają w wypadku leczenia psychiatrycznego. Nie ma znaczenia, czy leczysz się w szpitalu, czy w gabinecie i czy prywatnie, czy na NFZ. Leczenie psychiatryczne jest objęte bardzo ścisłymi regulacjami dotyczącymi wykonywania czynności medycznych. Zwłaszcza chodzi tu o obowiązek prowadzenia indywidualnej dokumentacji medycznej, która musi być przechowywana przez okres 20 lat. Co więcej, placówki medyczne muszą udostępniać dokumentację medyczną wszystkim służbom, sądom i prokuratorom, a dostęp ten jest dla służb łatwy. Ustawa przewiduje nawet, że pojedynczy p*icjant może uzyskać dostęp do twojej dokumentacji medycznej, nie przedstawiając żadnych dokumentów poza odznaką. Prawo nie przewiduje natomiast żadnych przypadków, w których placówka medyczna może odmówić udostępnienia dokumentacji medycznej. Oznacza to, że właściwie należy traktować informacje udostępnione lekarzowi lub lekarce tak samo, jak informacje udostępnione p*icji. Jeśli zatem zdecydujesz leczyć się psychiatrycznie musisz wziąć na siebie odpowiedzialność za filtrowanie informacji, które przekazujesz psychiatrom, a które mogą sprowadzić na ciebie lub twoich bliskich kłopoty prawne.

3. Podstawy podstaw – Zanim choćby pomyślisz o Signalu

3.1. Podstawy opsec w terenie – maskowanie się, minimalizacja śladów

Opsec w terenie to także temat licznych opracowań, które są dobre i nie tracą specjalnie na aktualności. Odeślę cię zatem do 3 pozycji, które wspominałxm już w wypadku planowania: „Arson Around With Auntie Alf", „ALF Primer, a guide to direct action and Animal Liberation Front", i „Earth First Direct Action Manual". Tutaj zaledwie podsumuję pewne obserwacje, które w większości są zawarte w tych pozycjach.

Przygotowując się do akcji należy rozważyć kilka możliwych zagrożeń, przed którymi warto się zabezpieczyć, a mianowicie:

- Kamery monitoringu i fotopułapki.
- Możliwość bycia zauważonym przez przypadkowych przechodniów oraz przez ochronę i p*icję, zarówno w „strefie zero", czyli w terenie bezpośrednio chronionym przez przeciwnika, jak i poza nim.
- Analizę śladów przeprowadzoną przez techników p*icyjnych.

Mając na uwadze powyższe zagrożenia przyjąć należy, że akcja zaczyna się w momencie wyjścia z domu, a kończy bezpiecznym powrotem i trzeba mieć zaplanowane stosowanie dopasowanych środków zabezpieczających na każdym jej etapie.

3.1.1. Kamery i fotopułapki

Warto wcześniej wiedzieć gdzie są kamery, a zwłaszcza, czy – jeśli mieszkasz w bloku – masz kamerę na klatce schodowej i w windzie. Jeśli mieszkasz w wolnostojącym domu, to czy twój sąsiad ma kamerę filmującą kawałek drogi przed swoim domem? Na ilu kamerach monitoringu będziesz widocznx przemieszczając się na miejsce akcji, działając na nim i wracając? Wypatrywanie kamer jest ogólnie ciekawym hobby, można je traktować jako coś podobnego do birdwatchingu. Będzie to angażujące zajęcie, zwłaszcza jeśli mieszkasz w mieście. Kamery różnią się na przykład typem, polem widzenia; wreszcie całkiem

popularne są także atrapy kamer. Problem polega na tym, że bardzo trudno odgadnąć z daleka, czy kamera jest prawdziwa i jakie ma parametry. Należy zatem założyć, że wszystko co wygląda na kamerę może nagrywać obraz tego, co znajduje się przed obiektywem i to zarówno w dzień, jak i w nocy. Po niektórych kamerach trudno odgadnąć w którą stronę są skierowane, należy zatem przyjąć pole widzenia 360 stopni. W p*sce jednak, nawet na nowych, miejskich osiedlach, na których monitoring jest największą plagą, często się zdarza, że np. monitorowana jest tylko jedna strona chodnika, tylko niektóre skrzyżowania. Pozwala to wytyczyć trasy, które może nie są najkrótsze, ale pozwalają przemieszczać się poza polem widzenia kamer, co generalnie jest cenną umiejętnością i powinno być naszym podstawowym wyborem w dniu akcji. Jeśli już musimy przejść przez monitorowany obszar należy być świadomym ryzyka z tym związanego i podjąć jakieś środki zaradcze.

Jeśli masz kamery w pobliżu miejsca zamieszkania i musisz być przez nie zarejestrowanx w dniu akcji (np. masz nie dające się ominąć kamery na klatce lub na twojej ulicy), to pojaw się w ich polu widzenia w innym ubraniu niż będziesz mieć na sobie na miejscu działań akcyjnych. W mieście generalnie unikaj podróżowania samochodem (samochody mają tablice rejestracyjne i są łatwe do rozpoznania na kamerach, również z uwagi na kolor i cechy charakterystyczne modelu) i pamiętaj, że właściwie już każdy pojazd komunikacji miejskiej ma monitoring. Domyślnym wyborem środka transportu w mieście powinien być zatem spacer lub rower. W wypadku wyboru roweru warto przemyśleć to, na ile nasz pojazd jest charakterystyczny i w razie czego wymienić go na mniej rozpoznawalny. Działając w terenie niezurbanizowanym często jesteśmy skazanx na samochód. Warto wówczas wybrać uczęszczane i niemonitorowane miejsca do parkowania (parkingi małomiasteczkowych centrów handlowych, miejsc rekreacji, popularne leśne parkingi itp. – często są monitorowane, ale niezwykle rzadko w całości).

Plan powinien zakładać miejsce, gdzie zmienisz ubrania na „akcyjne". Przebranie się często jest dobrym pomysłem, nawet jeśli nie masz kamer w miejscu zamieszkania. Nigdy nie można wykluczyć spotkania kogoś w sąsiedztwie twojego domu, gdy idziesz na akcję lub z niej wracasz. Musisz też pamiętać, że w pobliżu twojego celu mogą być fotopułapki, czyli ukryte kamery aktywowane ruchem. Dlatego przy samym celu musisz być już dobrze zamaskowanx.

3.1.2. Strój na akcję

Ubrania akcyjne powinny być ciemne. Zapomnij o moro, chyba że działasz w bardzo specyficznym terenie, głównie w dzień i wiesz co robisz. Wojskowy kamuflaż ma sens jeśli jest bardzo dobrze dobrany do warunków. Oddziały specjalne działające w nocy nie noszą moro, tylko czarne ubrania. Noc jest także porą działania pierwszego wyboru przy akcjach bezpośrednich, stąd twoje ubrania powinny być ciemne. Jednolicie czarny strój jest optymalny, ale w zależności od kontekstu może być trochę podejrzany, np. w wypadku przypadkowej kontroli p*icyjnej, czy napotkania kogoś. Ostatnio moda na czarny przenikła trochę do szerszej publiki, więc być może w okolicy twoich działań można chodzić całkiem na czarno i nie zwracać na siebie niechcianej uwagi. Jeśli jednak czujesz, że się wy-

różniasz, warto przełamać czerń ciemnym granatem, ciemną szarością itp. Przypadkowo zestawione ciemne kolory lepiej kamuflują w nocy niż źle dobrany kamuflaż wyskokowy.

Jeśli chodzi o osłonę twarzy, to problem jest podobny co w wypadku kolorów. Idealna jest kominiarka i to taka z dwoma osobnymi otworami na oczy, ewentualnie z trzema – na oczy i usta (nie bez przyczyny zwana „zadymiarą"). Inne kominiarki często odsłaniają bardzo dużo charakterystycznych cech twarzy. Natomiast posiadanie takiej kominiarki, a już zwłaszcza noszenie jej na głowie, może zwrócić na ciebie uwagę przy przypadkowej kontroli lub gdy spotkasz przechodniów. Jazda rowerem w zimie generalnie czyni taki strój mniej podejrzanym, choć nigdy nie przechodzi on całkiem niezauważony. Tymczasem czapka z daszkiem lepiej ukrywa charakterystyczne cechy twarzy, zwłaszcza przed kamerami filmującymi z góry, niż kiepska kominiarka. Połączenie czapki z daszkiem, tzw. komina (w wojsku nazywanego szalokominiarką) i okularów (w dzień ciemnych) stanowi bardzo dobrą ochronę naszej tożsamości, która ułatwia także szybkie przybranie „normalnego" wyglądu w wypadku rutynowej kontroli. Wystarczy zsunąć komin pod szyję i oto jesteś zwyczajnie wyglądającą osobą na spacerze. Idealne są szalokominiarki ze ściągaczem, który uniemożliwia przypadkowe zsunięcie się z twarzy. Ostatnia pandemia sprawiła, że noszenie osłony twarzy już tak nie rzuca się w oczy jak dawniej. Zimą dobrą alternatywą dla okularów są gogle (np. narciarskie), które dodatkowo stanowią bardzo dobrą osłonę oczu przed urazami i podrażnieniami.

Strój powinien ukrywać twoje charakterystyczne cechy sylwetki, a zatem idealne są ubrania za luźne i za duże (ale nie krępujące ruchów). Dobrym pomysłem są także za duże buty, które można w środku wyłożyć gazetą i kilkoma warstwami skarpet. Nie tylko spowodują one, że zostawisz inne ślady niż normalnie, ale także zmienią sposób w jaki się poruszasz i uniemożliwią zidentyfikowanie cię na podstawie chodu. Na wierzch butów możesz ubrać skarpetki, co sprawi, że nie zostawisz śladów bieżnika. Strój powinien być dobrany do warunków atmosferycznych i pogody oraz umożliwiać szybkie bieganie. Każdy ma swoje własne preferencje co do ubioru, ale moda na sportowe obuwie (adidasy) nie wzięła się znikąd.

Ostatni punkt to rękawiczki. Dobrym pomysłem jest użycie tanich rękawiczek jednorazowych i założenie na wierzch odpowiednich do pogody rękawic (bawełnianych, polarowych, czy innych), lub w ostateczności dwóch par rękawic jednorazowych. Sprawi to, że nie zostawisz DNA ani odcisków palców. Wewnętrzne rękawice powinienxś wyrzucić w miejscu niezwiązanym z akcją, do śmietnika, do którego nie wyrzucisz niczego innego. Badanie DNA wciąż jest drogie i trudne. Wiem z pierwszej ręki, że nadal p*icja w p*sce nie stosuje go rutynowo, a jedynie przy sprawach „dużej wagi", ale możesz także związać włosy i ubrać na głowę takie nakrycie, które uniemożliwi zgubienie ich na miejscu akcji. Ubrania i sprzęt użyty na akcji powinny być jak najmniej charakterystyczne, bez logotypów, odblasków itp. W miarę możliwości zdobywając ubrania i sprzęt należy wybierać tanie i popularne modele. Zdobywanie wszystkiego (sprzętu i ciuchów) w tanich, masowych sieciówkach jest dobrą praktyką.

3.1.3. Działania poza „strefą zero”

Jadąc na akcję i wracając z niej nigdy nie używaj przejazdów na aplikację, taksówek, miejskich rowerów, wypożyczanych hulajnóg itp. To wszystko są urządzenia szpiegowskie. Zwykła taksówka (nie na aplikację) jest najbezpieczniejsza do szybkiej ewakuacji, natomiast taksówkarze to zwykle szpicle i często byli p*icjanci, więc jeśli nikt się nie wykrwawia, to lepiej się przejść. Jeśli z akcji wracasz zranionx to staraj się poruszać tak, żeby nie było tego widać ani na kamerach, ani jeśli ktoś przypadkowo cię obserwuje, na przykład z okna.

Osobną sprawą jest tak zwane „cover story”, czyli uzasadnienie naszego przebywania w pobliżu rejonów kontrolowanych przez przeciwnika. Przeprowadzenie każdej akcji będzie wymagało rozpoznania terenu, a więc musisz się trochę pokręcić po okolicy. Warto nie dać się spisać w czasie takich wyjść na rozpoznanie, a także nie zwrócić na siebie uwagi i nie zostać zapamiętanxm.

Na misje rozpoznawcze dobrym kamuflażem jest spacer z psem, o ile nie jest to obszar mocno monitorowany (psy są łatwo rozpoznawalne na podstawie obrazu z kamer) lub niebezpieczny dla czworonoga. Nigdy nie słyszłxm o osobie zatrzymanej przez p*icję podczas spaceru w dwuosobowym składzie: człowiek i pies. Większe grupy to osobna historia, bo często zwracają uwagę p*icji, ale mało kto mniej się rzuca w oczy niż pojedynczy człowiek wyprowadzający psa. Psa nie zabierzesz na akcję z uwagi na oczywiste zagrożenia dla niego i dla ciebie, ale do pewnego stopnia to przydatny patent przy rozpoznaniu terenu. Specjalną zdolność pozostawania niewidzialnymi mają też osoby uprawiające sport, a zwłaszcza biegacze ubrani w strój do joggingu. Widywałxm takie osoby przemierzające bez przeszkód zamknięte tereny wojskowe. Podobnie amatorzy motocrossu są zaskakująco często ignorowani przez ochronę obszarów, do których nie powinni mieć wjazdu. Natomiast wjechanie na chroniony obszar motorem udając osobę, która się zgubiła szukając „fajnej górki” stanowi rozpoznanie metodą „na bezczelnego”, a więc jest ryzykowne i lepiej stosować je w ograniczonym zakresie. Tego typu misje zwiadowcze bywają udane, ale nie należy takich patentów nadużywać.

Pancernym cover story jest randka, o ile rzecz jasna idziesz w parze z kimś, z kim masz heteropassing. Nawet wracając z akcji możesz zaproponować osobie idącej z tobą, która wygląda na mającą ”przeciwną” płeć, że weźmiecie się za ręce. Jeśli na wierzchu plecaka masz koc i butelkę wina może to zmylić czujność niektórych p*icjantów.

Jeśli masz taką możliwość to stroju i sprzętu akcyjnego nie trzymaj w domu, tylko w kryjówce, którą odwiedzaj tylko w okolicach akcji. Zdarzały się już osoby anarchistyczne sądzone za posiadanie drabiny (naprawdę!).

3.1.4. Działania w „strefie zero”

Gdy już przemieszczasz się w obserwowanym terenie, w którym napotkanie przeciwnika może być równoznaczne z uwięzieniem, pamiętaj o zasadzie, którą w treningu wojskowym nazywa się „5 razy S”. Są to:

1. **Cisza (*silence*)** – szept jest ok, o ile nikt nie stoi bezpośrednio koło ciebie. Podobnie łamanie pojedynczych gałęzi w lesie przechodzi niezauważone. Ale już zamykanie drzwi od samochodu słychać na ogromnym dystansie, jeśli wokół jest cicho. Podobnie przedzieranie się przez las (żadne zwierze nie robi tego tak głośno jak człowiek) i normalna rozmowa są przy odpowiednich warunkach słyszalne z dużej odległości.

2. **Cień (*shadow*)** – należy samemu pozostawać w cieniu i cienia nie rzucać. Przy sztucznym oświetleniu, lub w księżycową noc, zwłaszcza jeśli jesteś na wzniesieniu, twój cień może być widoczny setki metrów od ciebie (np. poniżej ciebie, u podstawy wzgórza) i może zdradzić cię w zupełnie niespodziewany sposób. Generalnie dobrym pomysłem jest sprawdzenie pogody w dniu akcji i wiedza o tym jak jest faza księżyca, o której księżyc i słońce wschodzą, zachodzą i jakiego oświetlenia możemy na miejscu się spodziewać. Takie rzeczy należy sprawdzić w praktyce na miejscu akcji przed właściwym działaniem. Jeśli widzisz źródło światła, to zastanów się, gdzie rzucasz cień.

3. **Prędkość (*speed*)** – ludzkie oko jest szczególnie wrażliwe na ruch, więc jeśli nie chcesz zwrócić niczyjej uwagi, to ogólnie masz przemieszczać się powoli. Żołnierze pozostający w kamuflażu przemieszczają się często niewyobrażalnie powoli, wolniej niż muchy w smole. Wyjątkiem są sytuacje, w których chcesz szybko przemierzyć otwartą przestrzeń, na której spotkanie przeciwnika jest bardzo prawdopodobne. Wówczas „speed" może oznaczać dla ciebie bieg. Ale biegnąc zwracasz na siebie uwagę, więc sytuacje gdy bieg bardziej się opłaca są okazjonalne – np. przebieganie w poprzek dróg samochodowych w strefie zero bywa zasadne.

4. **Blask (*shine*)** – używanie białego światła jest głupie. Latarki są widoczne z setek metrów, trudne do pomylenia z czymkolwiek innym i niezwykle przykuwają uwagę. Należy pozbyć się wszelkich odblasków, a elementy, które mogą mieć połysk, wysmarować czymś matowym (ziemią, błotem, węglem). Tak samo można potraktować jasne logotypy na ciemniej odzieży, choć najlepiej je w ogóle na trwałe zaszyć łatami. Brud jest dobrym kamuflażem. W kryzysowych sytuacjach można użyć czerwonego światła (jest mniej widoczne z daleka). Używając czerwonego światła należy upewnić się, że jest się za dobrą osłoną (np. leży się w rowie).

5. **Kształt (*shape*)** – ostre, kanciaste kształty bardziej rzucają się w oczy. Dobry kamuflaż może polegać na zaokrągleniu kanciastych krawędzi wyposażenia przez doczepienie czegoś do nich.

3.2. Podstawy dobrych praktyk – nigdy nie rozmawiaj o akcjach

Nigdy nie rozmawiaj o akcjach bezpośrednich i innych działaniach wrażliwych. Wynika to wprost z zasady minimalizacji śladów. Każda rozmowa to okazja do przechwycenia informacji przez przeciwnika. Uzasadnieniem do rozmawiania o akcji jest jej wspólne planowanie, uzgodnienia w jej trakcie i ewaluacja po jej zakończeniu. W żadnych innych okolicznościach nie należy rozmawiać o akcji z nikim. Nie rozmawiaj o akcjach nawet z osobami, które w niej uczestniczyły i wszystko o niej wiedzą. Zaplanowane rozmowy związane z planowaniem, wykonaniem i ewaluacją powinny mieć z góry ustalone środki bezpieczeństwa w ramach pięciu kroków opsec. Zwłaszcza ewaluacja to ważny i wrażliwy etap, na którym często ponoszą emocje. Dlatego warto zawczasu zaplanować ją samą i środki ostrożności jakie będą dla niej stosowne.

Nierozmawianie o akcji dotyczy także nie zadawania żadnych pytań o akcje, w których nie brałxś udziału. Nie pytaj i nie zaczynaj tematu. Jeśli ktoś powierza ci jakieś informacje w związku z akcją, którą wykonuje, nie zadawaj zbędnych pytań i uszanuj milczenie. To najlepszy rodzaj wsparcia, jaki możesz okazać. Im mniej wiesz o cudzych działaniach, tym jesteś bezpieczniejszx. Pamiętaj też, że mówienie innym o swoich akcjach to narażanie ich na ryzyko i nakładanie na nich psychicznej presji. Jeszcze raz: nie rozmawiaj o akcjach bezpośrednich!

3.3. Nigdy nie ufaj elektronice - Podstawowe informacje o elektronicznych nośnikach danych

Całkowita nieufność wobec elektroniki jest generalnie całkiem zdrowa. Wystarczy wyobrazić sobie taki przykład. Siedzisz samx w miejscu, które uważasz za bezpieczne (np. na łące, nie spodziewasz się tu kamery). Przychodzi ci do głowy jakaś myśli i spisujesz ją na kartce. Szkicujesz proste drzewko decyzyjne, albo robisz listę plusów i minusów. Takie techniki wizualne czasami pomagają podjąć decyzję, dopracować plan, czy lepiej coś zapamiętać. Po chwili podpalasz kartkę, np. wrzucając ją do ogniska. Kartka płonie doszczętnie, po informacji nie zostają żadne ślady, znów znajduje się jedynie w twojej głowie. Taka sytuacja nigdy nie ma miejsca w wypadku danych wprowadzonych do telefonu lub komputera.

W powyższym przykładzie z kartką, jeśli zwrócisz uwagę na ślady jakie długopis mógł zostawić na ewentualnym miękkim podłożu pod kartką (np. na kolejnej kartce w bloku), to kontrolujesz wszystkie czynniki ryzyka. Przede wszystkim dlatego, że kartkę dość trudno w takiej sytuacji skopiować bez twojej wiedzy. Istnieje ona w jednym egzemplarzu i w momencie, w którym ją niszczysz, jedyna kopia znika. Dane zapisane na elektronicznym nośniku – pendrive, telefonie, dysku, komputerze – można natomiast skopiować bardzo tanio, można szybko wytworzyć niewyobrażalną liczbę kopii i co więcej, operacja taka nie zostawia żadnych śladów na oryginalnym „egzemplarzu”. Nie wiesz nawet, ile razy stwo-

rzone przez ciebie dane zostały skopiowane, gdzie zostały przesłane i co się z nimi dzieje. Oznacza to, że jeśli wprowadzisz jakieś dane do urządzenia elektronicznego, to powinnxś założyć, że wszystkie ślady jakie przy tym zostawiłxś, zostaną tam na zawsze. Zniszczenie wszystkich kopii jest z założenia niemożliwe, bo nie wiesz i nigdy się nie dowiesz, ile kopii istnieje.

Inna sprawa, że to co zwykle uważamy za „kasowanie" plików z telefonu czy komputera w rzeczywistości nim nie jest. Nawet jeśli nie tylko „przeniesiesz coś do kosza" (co jest przecież domyślną opcją na wielu urządzeniach i to często nawet wtedy, gdy wydaje się, że coś usunęłxś), ale rzeczywiście użyjesz opcji „kasuj", dane są do odzyskania z dysku jeszcze przez długi czas. Dopiero wtedy, gdy dana przestrzeń na dysku zostanie ponownie zapisana nowymi danymi, to co jest „pod spodem" staje się nieczytelne. To, co uważamy za „skasowanie" danych, zwykle jest tylko ich ukryciem przed nami samymi. Istnieją specjalne aplikacje i programy do skutecznego niszczenia danych (po angielsku nazywane zbiorczym słowem „shredder"), ale przecież niszczą one tylko te kopie, o których wiemy.

Kolejną rzeczą, o której musimy pamiętać, gdy rozważamy wprowadzanie danych do telefonu lub komputera, jest kwestia szyfrowania. Generalnie istnieje coś takiego jak „mocna kryptografia", czyli kryptografia, która opiera się na algorytmach szyfrujących, które przy współczesnych możliwościach technologicznych są niełamalne. Dokładnie chodzi o to, że wykonanie obliczeń potrzebnych do złamania szyfru jest niemożliwe w sensownym czasie, przy użyciu współczesnej techniki obliczeniowej.

Właściwie wszystkie znane „bezpieczne technologie" internetowe, w tym aplikacje bankowe, Signal czy Tor, oparte są na tej samej matematyce, która spełnia powyższą definicję mocnej kryptografii. I tu dochodzimy do szkopuliku. Czyli do wzrostu mocy obliczeniowej komputerów. Według dostępnych źródeł postęp w dziedzinie komputerów kwantowych doprowadzi do złamania algorytmów szyfrujących w ciągu 10 – 15 lat[1]. Wiedząc o tym, amerykkkańskie służby przechwytują i zapisują cały szyfrowany ruch, jaki uda im się znaleźć w sieci (w tym prawdopodobnie całego Tora) i spokojnie czekają, aż będą mogły go odszyfrować. Oznacza to, że nim popełniane teraz „przestępstwa" się przedawnią, to służby specjalne będą mogły odszyfrować nasze „bezpieczne" wiadomości w poszukiwaniu dowodów.

Ostatnią kwestią są liczne dziury w zabezpieczeniach, które z punktu widzenia nawet średnio-zaawansowanego użytkownika komputerów czy telefonów są zupełnie nie do załatania. Dobrym przykładem jest dziura o ładnej nazwie Silent Bob is Silent, która sprawia, że nad sporą częścią laptopów i komputerów różnych producentów wprowadzonych na rynek w w latach 2008-2017 można zdalnie przejąć całkowitą kontrolę. Silent Bob działa niezależnie od tego czy na maszynie zainstalowany jest Windows, Linux czy MacOS i nie „łatają" go żadne aktualizacje systemu operacyjnego ani antywirusy. Bob jest bowiem dziurą w tak zwanym firmwarze, czyli w oprogramowaniu fabrycznym, które startuje zanim uru-

[1] PostQuantum Cryptography (PQCrypto), kicksecure.com; polecam też wątek na ten temat na tor.stackexchange.com pod hasłem Does Tor team have plans to implement postquantum asymmetrical encryption schemes?

chomi się system. Aby pozbyć się Silent Boba należy zainstalować aktualizację firmware'u, która jest trudna i rzadko wykonywana. Jeśli masz laptopa wyprodukowanego w tych latach, to Silent Bob is Silent prawdopodobnie nadal jest twoim problemem. A jest on tylko jedną z setek trudnych do załatania dziur.

Służby na całym świecie skupują tak zwane błędy dnia zerowego, czyli dziury wykryte, ale nieupublicznione. Niektóre osoby biorą od służb łapówki po to, żeby nie ogłaszać publicznie wykrytych dziur, żeby jedynie służby mogły z nich korzystać – czasami zapewne przez lata, nim ktoś mniej potrzebujący pieniędzy je zauważy i ujawni. Życie ze sprzedaży błędów dnia zerowego jest zapewne miłe i dostatnie. Nie wiem, czy służby specjalne wiedziały o istnieniu Silent Bob is Silent przed jego upublicznieniem, a jest to całkiem możliwe i nie wiem, czy nie posiadają teraz wiedzy o podobnych dziurach, o których ja i ty dowiemy się za kilka lat.

4. Jak działają nasi przeciwnicy

Statystyka należy do tej samej dziedziny fikcji co prawo i za nim podąża, ale tym razem się nią posłużmy. Poczta to oficjalnie największy „pracodawca" w p*lsce. „Pracownik" to według statystyki ktoś zatrudniony na umowę o pracę. Poczta ma takich „pracowników" około 80 tysięcy. Na drugim miejscu jest koncern posiadający markę Biedronka, z około 70 tysiącami „pracowników". Na ósmym miejscu jest grupa PKP z 34 tysiącami. Tymczasem w p*lsce mamy prawie 100 tysięcy p*icjantów. Jak słyszę od kogoś „dlaczego p*icja miałaby się mną interesować?", to od razu myślę o poczcie. Popatrzcie, że poczta interesuje się nami wszystkimi. Osoby w okienkach, sortowniach i na ulicach przyjmują, sortują, przewożą i wydają przesyłki dla każdej z nas. Listy docierają do każdej z nas, choć często wcale tego nie chcemy. Poczta ma dość zasobów by zaopiekować się nami wszystkimi. A p*icjantów jest o dwadzieścia procent więcej. Jest ich prawie tylu, co pocztowców i kolejarzy razem wziętych. Dla państwa wciąż jest ich za mało (wciąż otwarte są tysiące rekrutacji) i wciąż są trochę za biedni, chociaż ich budżet to prawie 10 miliardów złotych. W gruncie rzeczy to p*cjanci muszą się tobą interesować, bo gdyby się tobą nie interesowali to nie mieli by nic do roboty. Albo inaczej, oni muszą się interesować każdym kto choć trochę odbiega od ich wizji normy. Po to państwo utrzymuje i szkoli armię uzbrojonych zwyrodnialców.

4.1. Masowe legitymowanie

Takie zasoby ludzkie p*icji sprawiają, że jej działania mają trochę inną logikę niż ta, do której my przyzwyczajamy się pracując w małych grupach lub samotnie. Czynności rutynowe, powtarzane w kółko, z minimalną ilością rozpoznania, mogą przynosić zaskakujące dobre rezultaty, gdy ma się takie zasoby. Jeśli przeszukasz piętnastu chłopców w bluzie z kapturem to szanse, że trafisz na kuriera wiozącego trawę są małe. Ale jak przeszukasz ich piętnaście tysięcy, to taki wysiłek zaczyna mieć sens. Jak tysiąc razy przejedziesz pod skłotem, to w końcu spotkasz kogoś, kogo będzie można pobić tak, by wywołać reakcję i znaleźć pretekst do eksmisji.

Na przykład gdy p*icja zabrała się za tak zwanych cyberprzestępców, czyli ludzi żyjących z przekrętów on-line, zrobiła to w drastycznie niewyszukany sposób. Zwykłe, umundurowane patrole stały po prostu cały czas pod wpłatomatami, o których wiadomo było, że są w nich regularnie wpłacane duże kwoty pieniędzy i spisywały wszystkich. Jak ktoś się pytał o pretekst, to jakiś pretekst był wymyślany. Krawężniki na 100% nie znali celu operacji, a być może nie wiedzieli nawet o jej istnieniu. Mieli rozkaz „spisywać" i spisywali. Tym

oto sposobem, za pomocą korelacji miejsca i czasu, p*icjantom udało się powiązać tożsamość wielu osób z wpłatami na konta. Niektóre czasy i kwoty korelowały ze zgłoszeniami dokonanymi na p*cji przez ofiary internetowych „wyjebek". Na niektórych kontach były bardzo wysokie obroty, pochodzące właśnie z wpłat gotówki. Resztę obrazu zniszczenia dopełniło to, że kilka osób, które zostały zidentyfikowane jako wpłacające na podejrzane konta, zostało zatrzymanych i chętnie rozmawiało z p*icjantami. Jak zatem widzisz, nie była to operacja jak z serialu. Morał z tej historii nie ogranicza się jednak tylko do tego, że p*icja nie ma zbyt wyrafinowanych metod (bo i po co by miała mieć). Dla mnie ważne jest to, że niektórzy ludzie poszli do więzienia tylko dlatego, że dali się spisać w określonym miejscu i czasie. Tylko dlatego. Mądrzejsi ode mnie już pisali: jeden błąd wystarczy.

Masowe legitymowanie jest dobrą strategią monitorowania wszystkiego co dzieje się na jakimś obszarze. Tymczasem w p*sce, w odróżnieniu od wielu innych krajów ani społeczny opór, ani prawo nie ogranicza specjalnie tej praktyki. p*icjia stosuje ją więc właściwie tak rutynowo, że „uliczne protesty" często wyglądają po prostu jakby osoby protestujące przyszły tam wymienić się danymi z p*icjantami. p*icja nie ma też żadnych ograniczeń dotyczących czasu przechowywania takich danych i sposobu ich analizowania. Są one zatem zapewne wykorzystywane przez lata do wielu spraw i wraca się do nich przy każdej możliwej okazji, gdy tylko mogą wydać się przydatne. Obecnie masowe legitymowanie pozwala p*icji tworzyć i aktualizować bazy osób o określonych poglądach, a także być może ich wzajemnych powiązań.

4.2. Tajniacy

Drugą ważną strategią, która nasiliła się w ostatnich latach, jest użycie nieumundurowanych p*icjantów (tajniaków) celem prowadzenia rozpoznania. Wokół miejsc demonstracji i akcji kręcą się ich dziesiątki, w różnym stopniu wtapiając się w tłum. Oczywiście część z nich ma za zadanie wyłapywanie bardziej aktywnych osób w czasie dem i akcji, ale często są obecni też przed i po wydarzeniu, a także poza jego miejscem. Sądzę, że pierwszą reakcją komendantów na nieco mniejszą ilość informacji podawanych przez organizatorki w mediach i w postaci zgłoszeń urzędowych, jest mocniejsze rozpoznanie w terenie prowadzone właśnie przez nieumundurowanych p*icjantów.

Zdarzają się także nieumundurowani p*icjanci śledzący osoby anarchistyczne przed i po akcjach, obserwujący „miejscówki" i podążający ze mediami znanymi ze współpracy z „aktywisktami". Wreszcie tajniacy odwiedzają „miejscówki" i to także takie bardzo luźno powiązane z „ruchem". Czasem maskują się przy tym lepiej, a czasem gorzej. Jeden z tajniaków pracujących w ramach operacji Feniks, wymierzonej w cz*skie osoby anarchistyczne, przez miesiące był stałym bywalcem maleńkiej knajpy, w której rzadko przebywało więcej niż kilka osób naraz. Knajpa ta wcale nie była miejscem jakichś specjalnych wydarzeń anarchistycznych. Była po prostu położona niedaleko jednego z praskich skłotów i miała sympatyczny klimat. Część jej bywalców mieszkała na owym skłocie, na którym zresztą także mieszkali tajniacy. Nie znam tak drastycznych przykładów głębokiej infiltracji z p*skiego

podwórka, ale w p*sce prawo jest niekorzystne i właściwie nie ma prawnych mechanizmów pomagających w ujawnianiu pracy tajniaków nawet po latach. W n*mczech, na przykład, osoby oskarżone na podstawie dowodów zebranych przez tajniaków dowiadują się o tym w trakcie procesu. W p*sce zwykle nie. Natomiast ci słabiej zamaskowani, ale jednak nieumundurowani, p*icjanci bywają widywani na licznych p*skich miejscówkach.

4.4. Dostęp fizyczny do telefonów i laptopów

P*icjanci bardzo chętnie uzyskują dostęp fizyczny do telefonów, laptopów i tabletów, aby wydobyć z nich określone informacje. Dość powszechnie p*icjanci wykorzystują rutynowe kontrole, a także zatrzymania do przeglądania esemesów i wiadomości oraz innych danych zapisanych w telefonie. Zdążyli oni także już się zorientować, że osoby anarchistyczne chętnie korzystają z zaszyfrowanych komunikatorów. Stąd p*icjanci mogą wykorzystać dowolny pretekst aby cię skontrolować i zmusić do oddania im telefonu. Jest wiele powodów dla których nie warto mieć żadnych informacji powiązanych z twoją wrażliwą działalnością na telefonie, a to, że masz go zwykle przy sobie i to, jak łatwo ci go odebrać to tylko dwa z nich. P*icjanci z pewnością stwierdzą, że mają podejrzenie, że telefon jest kradziony i poproszą cię o odblokowanie klawiatury, aby mogli sprawdzić numer IMEI. Jeśli się zgodzisz, to po prostu wykorzystają to, że mają odblokowany telefon w rękach i zaczną przeglądać twoje wiadomości. Możesz przyjąć taką taktykę, że na twoim telefonie nie będzie żadnych istotnych danych i po prostu chętnie oddasz go przy kontroli. Jeśli jednak odmówisz odblokowania telefonu, co jest całkiem rozsądną i zrozumiałą reakcją, musisz się liczyć, z jego bezterminowym odebraniem.

P*icjanci wiedzą także, że laptopa należy przechwycić gdy jest włączony, a dysk jest odszyfrowany i potrafią stosować różne sztuczki dla zmylenia twojej czujności. Dwójka agentów FBI zatrzymała Rossa Ulbrichta, twórcę internetowego sklepu z bronią i narkotykami, celowo odwracając jego uwagę tak, by przechwycić jego komputer, kiedy był włączony. Więcej o zabezpieczaniu laptopów i telefonów piszę w Pewnych Rzeczach II.

4.5. Rozpytania i przesłuchania

Zaskakujące jest to, jak dużo informacji p*icjanci mają z tak zwanych „osobowych źródeł informacji". Możecie między bajki włożyć wszystkie historie o CSI i inne takie bzdury. Laboratoryjne metody kryminalistyczne są drogie, pracochłonne i czasochłonne. P*icja zatrzymuje ludzi, prokuratury ich oskarżają a sądy skazują na podstawie informacji udzielonych przez innych ludzi. Na podstawie nieuważnie wypowiedzianych zdań na imprezce na skłocie, na demonstracji, w czasie zatrzymania, w czasie transportu na komisariat. Dla p*icji rozmawianie z ludźmi i wyciąganie od nich informacji, zwykle za pomocą kłamstw i manipulacji, a czasem zastraszania, szantażu, przekupstwa lub tortur, to podstawowe techniki pracy,

Podstawowa zasada brzmi po prostu „nie rozmawiaj z p*icjantami". Właściwie to należałoby ją rozszerzyć, „nie rozmawiaj z żadnymi przedstawicielami służb". Nie musisz tego robić, nie powinnxś tego robić, rozmawianie z nimi jest głupie i zawsze przynosi więcej strat niż pożytku.

Rozumiem, że możesz nie wiedzieć, że ktoś jest p*icjantem. Dlatego inna zasada mówi "nigdy nie rozmawiaj o akcjach bezpośrednich". Może się zdarzyć, że dasz się wciągnąć w nieistotną konwersację z kimś kto nagle przedstawi się jako p*icjant. OK, to się zdarza. Jak już zobaczysz blachę to stanowczo utnij rozmowę.

P*icja oprócz standardowego przesłuchania, które jest opisane w prawie, stosuje dodatkową technikę, nazywaną w ich żargonie rozpytaniem. Rozpytanie, w odróżnieniu od przesłuchania, nie ma żadnej formalnej struktury i nie regulują go żadne przepisy. P*icjanici są szkoleni aby w przypadkowych sytuacjach, na przykład w czasie jazdy radiowozem, w czasie przeszukania lub spisywania innej osoby, zadawać z pozoru niewinne pytania, które mogą dostarczyć im cennych informacji. Czasem informacje uzyskane z rozpytania są wykorzystywane przy formalnych przesłuchaniach innych osób, czasem od razu trafiają do akt sprawy. Często p*icjanci w cywilu rozmawiają z zatrzymanymi na komisariacie, zupełnie „poza protokołem", gdy ci oczekują na korytarzu na kolejne czynności. Gdy masz do czynienia z p*icją, po prostu pamiętaj o tym, by z nimi nie rozmawiać. Nie ma czegoś takiego jak „niezobowiązujące" rozmowy z p*icją. Dodatkowo pamiętaj, że oni właściwie zawsze kłamią; niezależnie od tego, czy mówią o swoich uprawnieniach, o twoim dalszym losie, o tym co na ciebie mają - zawsze najbezpieczniej założyć że kłamią. Pała to pała. Jej jedyną funkcją jest cię krzywdzić i dręczyć. Nie rozmawiaj z p*icjantami. Kropka.

Musisz założyć, że p*icja będzie cię przesłuchiwać i że będzie robić to dobrze. Że będą cię okłamywać i manipulować tobą w taki sposób, byś się przyznałx i abyś złożyłx wyjaśnienia obciążające i ciebie, i innych. Mogą wmawiać ci, że i tak już wszystko wiedzą, że wszystkie informacje mają już od innych osób. Mogą ci mówić, że jeśli od razu się przyznasz dostaniesz dużo niższy wyrok. Pamiętaj, że oni kłamią. Przysięgam ci, że nigdy nie usłyszałxm prawdy od p*icjanta i nigdy nie widziałxm, żeby spełnili daną obietnicę.

Swoją drogą, okropna praktyka rozmawiania z p*icją w czasie akcji i protestów pod pretekstem „deeskalowania" czy negocjacji powinna być jak najszybciej porzucona. Jej popularyzacja przyszła wraz z upowszechnieniem akcji okupacyjnych, a zwłaszcza takich prowadzonych zgodnie z ideologią non-violence. Obrona zajętej pozycji często prowadzi do oblężenia, a oblężenie do negocjacji. To podstawowe obserwacje dotyczące doktryny wojennej. Broniąc się można małymi siłami, długo utrzymać pozycje, a dla strony atakującej zwykle „oblężenie" jest mniej kosztowne niż szturm. Prowadzi to do długich godzin spędzanych w p*icyjnych kotłach, które często są właściwie skonstruowanymi na dworze aresztami, dokładnie obstawionymi przez kamery.

Nie jest szczególnie dziwne, że ta praktyka została wstrzyknięta do „ruchu" przez te same NGOsy, które wstrzyknęły do niego wiele innych szkodliwych zwyczajów. Dla wielu z nich taka sytuacja jest atrakcyjna ponieważ jest dostępna dla mediów, a zatem stanowi część spektaklu, którego uczestnikami starają się być te organizacje. Problem polega jednak na tym, że bardzo często strona „oblężona" stoi na z góry przegranej pozycji, a najlep-

szym wynikiem negocjacji może być powiedzenie kilku słów za dużo p*icyjnym negocjatorom. A oblężenia warto unikać. Miłość lewicowych NGOsów do aranżowania pułapek na „aktywistki", w których te mogą biernie dawać się bić p*icji na oczach kamer jest totalnie niezrozumiała. NGOsy żerują na błędnym wyobrażeniu o liberalnej publice, którą poruszą sceny przemocy. Zawsze może się zdarzyć, że znajdziesz się w oblężeniu, nawet jeśli zrobiłxś wszystko, żeby tego uniknąć. Wówczas możesz się poddać od razu lub stawiać opór. To twoja decyzja. Ani w jednym, ani w drugim przypadku nie widzę uzasadnienia dla bratania się z p*icjantami.

4.6. Dźwignie i propozycje współpracy - czyli co mi zrobią, jak mnie złapią

Dźwignia to szantaż, którego p*icja może użyć, by nakłonić cię do wyjawienia im informacji, których byś normalnie nie chciałx wyjawić. Za pomocą dźwigni p*icja może nakłonić cię, abyś nie tylko jednorazowo przekazałx ważne dane, ale także aby wykorzystać cię do długotrwałej inwigilacji twojej grupy. Jeśli raz się złamiesz, p*icja może odwiedzić cię po raz kolejny i kolejny, aby zdobywać informacje, których potrzebuje w innych sprawach. Z czasem sam fakt, że przekazujesz p*icji informacje, może stać się dodatkową dźwignią. Funkcjonariusze będą cię bowiem straszyć, że wyjawią ten fakt twoim bliskim. Tak naprawdę jednak p*icja nie ujawnia swoich źródeł, jeśli nie musi. Woli korzystać z nich przez lata.

Typowym przykładem dźwigni jest status oskarżonego w sprawie karnej. P*icja rutynowo poluje na osoby palące marihuanę, licząc, że wsypią swoich dilerów w zamian za łagodne potraktowanie. P*icjanci celowo wybierają na ofiary takich szantaży osoby, którym nawet drobna sprawa karna może bardzo zaszkodzić. Osoby wykonujące tak zwane „zawody zaufania publicznego" (cokolwiek to znaczy – to pojęcie nie ma jasnej definicji) mogą stracić pracę, nawet jeśli nie zostaną skazane, ponieważ p*icja ma prawo poinformować ich pracodawców o samym fakcie wszczęcia postępowania. Jeśli taka osoba dodatkowo jest w trudnej sytuacji materialnej, np. ma osoby zależne na utrzymaniu, staje się ciekawym celem do szantażu. Znane są przypadki służb specjalnych wykorzystujących chorobę dziecka. Taka dźwignia składała się zarówno z propozycji wsparcia leczenia, jak i z groźby utrudnienia go. Donoszono także o służbach składających oferty spłaty kredytu. Wreszcie prokuratorzy, chcąc kogoś zniszczyć lub zastraszyć, mogą zainteresować się sprawami cywilnymi toczącymi się przeciwko takiej osobie i poszukać w nich materiałów na ewentualną sprawę karną (Rafał Gaweł, założyciel Ludzi Przeciwko Myśliwym, został skazany na 5 lat więzienia na podstawie zarzutów „wyciągniętych" z toczącej się przeciwko niemu sprawy cywilnej). P*icjanci mogą także wykorzystywać sprawy „obyczajowe" takie jak bycie osobą nie-hetero, nie-cis, albo wykonywanie pracy seksualnej do zastraszania osób, które nie są wyoutowane przed swoimi bliskimi.

Zastanów się jakie dźwignie mogą być użyte przeciwko tobie. Jak zareagujesz gdy zostaną wykorzystane? Wyobraź sobie ten dzień, gdy spotykasz się z p*icją w twoim domu lub na komisariacie i stajesz przed groźbą uwięzienia, utraty pracy lub gdy grożą twoim bliskim. Porozmawiaj o tym z osobami, z którymi dzielisz sekrety dotyczące waszych wrażliwych działań. Omów z nimi swój stosunek do użycia poszczególnych dźwigni. Nie rozmawiaj jednak o tym z ludźmi, którym nie ufasz. Nie ma sensu podsuwać pomysłów p*icji.

Pamiętaj, że w repertuarze p*icjantów są także tortury. Zastosowanie przemocy fizycznej i poniżającego traktowania jest powszechne i akceptowane wśród funkcjonariuszy służb. Spodziewaj się tego i spodziewaj się, że spotka to twoich bliskich, a także osoby, z którymi działasz. Pamiętaj też, że możesz zostać skonfrontowanx z zarzutami, których się nie spodziewasz. Na przykład - nawet jeśli nie myślałxś nigdy o tak ryzykownych działaniach, p*icja może dość łatwo zarzucić ci „terroryzm" i „usiłowanie" poważnego przestępstwa jak morderstwo. Takie zarzuty trudniej nieco podtrzymać w sądzie, ale w pierwszym etapie postępowania p*icja może próbować cię zastraszyć również w taki sposób. To w połączeniu z torturami i dźwignią może sprawić, że zupełnie inaczej spojrzysz na świat, niż gdy spokojnie siedzisz w domowym zaciszu.

Dlatego warto stawiać się choć w myślach w takiej sytuacji i być na nią przygotowanx . Jeśli czujesz, że możesz nie wytrzymać presji, powiedz o tym szczerze osobom, z którymi działasz.

4.7. Szpicle

Marius Mason to anarchista odsiadujący obecnie wyrok 22 lat więzienia za swój rzekomy udział w 13 podpaleniach dokonanych przez Earth Liberation Front. Marius został skazany na podstawie zeznań Franka Ambrose'go, czyli osoby, która w momencie składania zeznań była jego mężem. Ambrose wpadł po tym, jak wyrzucił do tego samego komunalnego śmietnika w Detroit maskę przeciwgazową, petardę o mocy na tyle dużej, że w USA na jej posiadanie wymagane jest pozwolenie i swoje odręczne notatki, a także inne przedmioty, które umożliwiły zidentyfikowanie go. Ambrose podjął aktywną współpracę z FBI i jako kapuś działał w ukryciu przed swoimi niedawnymi bliskimi. W tej roli 7 razy podróżował do innych stanów USA w celu zbierania dowodów, które umożliwiły potem skazanie na długoletnie więzienia nie tylko jego męża, ale także innych osób z Earth Liberation Front. Sam Ambrose przyznał się do dwóch podpaleń i został za nie skazany na wyrok 9 lat więzienia, 3,7 miliona USD odszkodowania i dożywotni nadzór p*icji. Jego aktywna współpraca z FBI pozwoliła mu, według orzeczenia sądu, zredukować czas odsiadki o ponad połowę[1].

Kilka lat wcześniej inny członek ELF, Jacob Ferguson został kapusiem. Ferguson również podróżował po Stanach owinięty podsłuchami, w które wyposażyło go FBI i wkręcał znajomych z ELF w rozmowy o wspólnie dokonanych akcjach. To właśnie materiały do-

[1] Activist turned informant sentenced to 9 years in prison in ecoterrorism case, mlive.com

starczone przez Fergusona miały największe znaczenie dla Operacji Backfire[2]. Jeden z zatrzymanych w ramach tej operacji, William Rodgers (aka Avalon), popełnił samobójstwo w areszcie. Większość pozostałych zatrzymanych natomiast poszła na współpracę. Dobre wiadomości są dwie: Ferguson nie żyje, a wszystkie jego ofiary oprócz tragicznie zmarłego Avalona - także te, które nie dały się złamać - już są na wolności. Co jeszcze warto wiedzieć o Fergusonie, to fakt, że przez lata zmagał się z uzależnieniem od heroiny. Osoby uzależnione często miewają niekończące się problemy finansowe. Jeśli uzależnienie zdąży już całkowicie zdemolować układ nagrody w mózgu, to mogą one robić równie podłe rzeczy jak Ferguson, nawet jeśli wcześniej nie były do tego zdolne.

Ferguson i Ambrose należą do grupy ludzi, którzy zdradzili tych, z którymi przez moment byli autentycznie blisko. Takich jak oni można nazwać kapusiami.

Osobną kategorią szpicli są infiltratorzy, czyli ludzie, którzy nie mają nic wspólnego z daną grupą, zanim nie podejmą się misji rozpracowywania jej. Nie wszyscy infiltratorzy to etatowi pracownicy p*icji czy służb (nie wszyscy infiltratorzy to tajniacy). Mogą to być także dziennikarze, prywatni detektywi, a także hobbyści (np. faszyści rozpracowujący grupy antyfaszystów i odwrotnie). Służby mogą także prowadzić infiltratorów, nie będących etatowymi pracownikami, a tak zwanymi „tajnymi współpracownikami". TW to ludzie, którzy zwykle z pobudek zarówno finansowych jak i ideologicznych, a czasem z połączenia ich ze strachem, zaczynają współpracować ze służbami, ale nie są to osoby formalnie zatrudnione w tych instytucjach.

Niewiele wiemy o tym, jak często p*icja w p*sce wykorzystuje infiltratorów. Wiemy, że zdarzali się tutaj prawicowy dziennikarze i aktywiści infiltrujący grupy pro-zwierzęce i feministyczne, a także antygraniczne. Oznacza to, że działając w p*lsce należy brać pod uwagę możliwość spotkania się zarówno z kapusiami, jak i z infiltratorami zupełnie różnych rodzajów. To sprawia, że dość trudno określić jakie cechy powinny sprawić, że nabierzemy podejrzeń. Przecież kapuś może mieć zupełnie spójną biografię i nienaganne aktywistyczne CV, a infiltrator może być niezwykle miłą i przekonującą osobą, która mogła zostać zwerbowana z bliskiego nam środowiska. Tym, co powinno budzić bardzo poważne wątpliwości, jest oskarżanie innych o współprace z służbami. Ta taktyka nazywa się „snitch jacketting" i jest uprawiana przez szpicli na całym świecie. Po pierwsze pozwala ona odwrócić uwagę od siebie, a po drugie niszczy grupę przez burzenie zaufania, sianie paranoi i krzywdzenie niewinnych osób.

Jest natomiast jedna wspólna cecha wszystkich szpicli. Jest nią kłamstwo. Szpicle zawsze w pewnym momencie muszą zacząć kłamać. Często kłamią w drobnych sprawach, po to, żeby zamaskować swoje intencje, działania i aby zyskać wiarygodność, na którą nie zasługują. Jeśli zauważysz, że ktoś kłamie wobec swoich bliskich, nawet w pozornie drobnych kwestiach, to natychmiast przestań prowadzić jakiekolwiek wrażliwe działania z tą osobą i odizoluj ją od wszelkich wrażliwych informacji. To państwo posługuje się kłamstwem i manipulacją. Nasze działania muszą być oparte na szczerości. To jasne, że mamy sekrety.

[2] Operacja Backfire to wspomniana już wcześniej największa operacja w dziejach FBI, której celem było uwięzienie jak największej ilości osób z Earth Liberation Front.

To jasne, że jeśli mieszkasz z najbliższą ci osobą na świecie, ale zdecydujesz się prowadzić akcję bezpośrednią bez niej, to jej o tym nie powiesz. Nie oznacza to jednak, że powinnxś kłamać. Szczera i uczciwa komunikacja jest konieczna, aby pozbyć się hierarchii władzy z naszego życia. Dlatego ważne jest budowanie z naszymi bliskimi komunikacji, która jest wolna od natrętnych pytań, która akceptuje milczenie i która tworzy możliwość odmowy odpowiedzi i zachowania swoich spraw w tajemnicy. Nie powinno być w niej natomiast miejsca na kłamstwo. Kłamstwo niech pozostanie domeną państwowych szpicli.

Aby uchronić się przed szpiclami warto prowadzić działania z ludźmi, których zna się dobrze. Jeśli działasz z ludźmi, których znasz lata, to trudno nagle „wstrzyknąć" ci infiltratora. Jeśli zaś chodzi o kapusi, to każdy może się nim okazać, ale jeśli znasz jakąś osobę, to pewnie potrafisz ocenić jakie są szanse, że zachowa się w porządku. Zazwyczaj potrzeba lat żeby poznać kogoś na tyle żeby zrozumieć jaki ma stosunek do życia, jakie wartości wyznaje i jak się zachowa, gdy stanie przed naprawdę trudnym wyborem, choć pewnie 100% pewności nie będziesz mieć nigdy. Jako osoba, która miała okazję współpracować blisko z kapusiami, mogę ci powiedzieć, że pół roku to dla mnie za mało, by poznać się na człowieku. Jeśli znasz kogoś naprawdę dobrze, to umiesz także odczytywać nastrój tej osoby. Warto zwracać uwagę na to, jak czują się osoby, z którymi działasz, również po to, by umieć wychwycić zmiany w zachowaniu, które mogą być spowodowane ciężkimi przesłuchaniami, niezależnie od ich wyniku. Dbanie o siebie nawzajem i praca emocjonalna wzmacniają grupę, chroniąc ją przed infiltracją.

Moim zdaniem lepiej poznać kogoś dobrze w jego naturalnym środowisku, mieć przez lata okazję patrzeć jak ta osoba radzi sobie ze zwykłymi wyzwaniami dnia codziennego, niż obserwować kogoś krótko w ekstremalnej sytuacji. To więcej mówi o człowieku.

Swoją drogą, moje osobiste doświadczenie współpracy z pewnym kapusiem sprawiło, że bardzo zwracam uwagę na reakcję na stres – tchórz to dobry materiał na kapusia, zwłaszcza jeśli nie zdaje sobie sprawy z własnych słabości.

Możesz także przeprowadzić prostą kalkulacje, przed jaką stanie potencjalny kapuś z twojej grupy. Jeśli wasze działania są dodatkiem do „prawdziwego życia", to potencjalny kapuś odmawiając współpracy kładzie na szali takie rzeczy jak „prawdziwa praca", „rodzina", „kariera" i inne mieszczańskie gówna. Czy zaprzepaści to, jeśli działania są dla niego czymś w rodzaju „hobby"? Jeśli czujesz, że dla osób z twojej grupy może to prezentować się w ten sposób, to spodziewaj się donosów. Jeśli natomiast czujesz, że działasz z ludźmi, dla których relacja z innymi sprawcami czynów, za które możecie być sądzone jest bardzo ważna, a świat poza nią jest mało istotny, to ten sam wybór wygląda zupełnie inaczej. Najmniej kapusi jest w społecznościach rdzennych, wiejskich, dyskryminowanych, tam gdzie zachowały się resztki więzi między ludźmi[3]. Z drugiej strony, ja nigdy nie byłxm częścią społeczności tego typu, a późny kapitalizm nie sprzyja ich budowaniu. Dlatego tak wiele osób decyduje się na samotne ataki, które często są tylko aktami desperacji, choć pewnie jest tu pole do poprawy skuteczności.

[3] CrimethInc., Green Scared? Lessons from the FBI Crackdown on EcoActivists

Szpicle mają jeszcze jedną cechę. Lubią kwasy i gównoburze. Wiele wspaniałych osób anarchistycznych ma konfliktowe charaktery. Stara anarchistyczna zasada mówi też, że największe skurwysyny, popełniając najgorsze skurwysyństwa, nawołują do „jedności ruchu". Sprawdza się to tak dobrze, że właściwie od razu jak słyszę o „jedności ruchu" to mam wyrobione zdanie i o osobie do niej nawołującej, i o sytuacji, w której to wezwanie pada. Nie chodzi więc o to, żeby oskarżać o bycie szpiclem kogokolwiek, a już zwłaszcza te osoby, które pod presją zachowują własne zdanie. Ale nasilające się konflikty wewnętrzne mogą być jednym z objawów pracy szpicla. Jeśli w twojej grupie rosną napięcia, jest to powód do analizy. Tak samo jeśli przeciwnik wydaje się być lepiej niż wcześniej przygotowany na twoje działania.

Nie słyszałxm w p*lsce o udanej identyfikacji szpicla. Może kiedyś dowiesz się, że ktoś okazał się kapusiem czytając jego wyjaśnienia w aktach sprawy. Ale wtedy pewnie i ty, i ta osoba będziecie już mieć przerwę w działaniu. Nie należy zatem spodziewać się, że ze stu procentową pewnością rozpoznasz szpicla w czasie, gdy reakcja będzie możliwa. Rzucanie niepotwierdzonych oskarżeń jest tymczasem krzywdzące i głupie. Nie zmienia to faktu, że prowadzić wrażliwe działania powinienxś tylko z osobami, którym ufasz. Nie daj sobie wmówić, że powinno być inaczej. Jeśli komuś nie ufasz, zachowaj zdrowy dystans.

Nie rób nic z ludźmi, którzy kłamią. Nie powierzaj żadnych sekretów pijakom i plotkarzom. Unikaj ryzykowania z ludźmi, którzy nie są w stanie pokonać strachu. Polegaj na swojej intuicji. To powinno wystarczyć.

Właściwym celem działań służb i organów represji jest zwiększenie izolacji społecznej i wykluczenia. To po to służby wkręcają do grup szpicli, to po to łamią ludzi propozycjami współpracy, wreszcie po to izoluje się nas w celach rotując ich obsady. Społeczeństwo rozbite na atomy i pogrążone w paranoi jest generalnie mniej zdolne do oporu, choć także bardziej skłonne do aktów desperacji, które bywają groźne.

5. Najczęściej popełniane błędy

5.1. Nadmierna technicyzacja problemu

Mówiąc najkrócej: opsec to nie jest zestaw narzędzi technicznych. Żadne narzędzie techniczne, komunikator, aplikacja itp. nie zapewni „bezpieczeństwa" (cokolwiek zresztą to słowo ma znaczyć). Nie zapewni go też wymiana jednego narzędzia na inne, ani nawet skasowanie konta w Google i przejście na jakiś egzotyczny system operacyjny.

Myślenie o opsec w kategoriach technicznych nosi zresztą znamiona myślenia magicznego. Często odnoszę wrażenie, że osoby anarchistyczne oczekują, iż zainstalowanie tego, albo innego narzędzia zwolni je z obowiązku pozostawania czujnymi i myślenia. Obserwacja znajomej mi osoby doświadczonej w pracy antyrepresyjnej jest także taka, że osoby anarchistyczne domagają się wiedzy na temat najnowszych narzędzi technologicznych i często chcą być szkolone z obsługi komputerów, ale później „wykładają się na podstawach", na przykład rozmawiając o swoich planach na skłotach.

Oparcie się na technice nosi też znamiona oparcia się na autorytecie. Mało kto bowiem zadaje sobie trud zbadania, jak działa taki czy inny kanał komunikacji. Chcemy po prostu wiedzieć, że ktoś „za nas" zrobi robotę i zadba o to, żeby p*icjanci trzymali się z dala. Dobrym przykładem jest popularność poczty i VPNa Riseup. Samx od lat korzystam z usług kolektywu Riseup. W rzeczywistości jednak Riseup jest bardzo łakomym celem dla służb. Jeśli od 20 lat korzysta z niego zdecydowana większość wszystkich osób anarchistycznych na świecie, to zadajcie sobie takie pytanie: ile pieniędzy FBI byłoby wstanie wydać, żeby złamać kogoś z kolektywu Riseup? Myślę, że to ogromna kwota, a Riseup istnieje od dawna, więc i czas żeby się za to zabrać był całkiem długi. Tymczasem zarówno mail, jak i VPN to usługi, które opierają się wyłącznie na zaufaniu.

Riseup jest przykładem czegoś, co gdyby nie istniało, to pewnie służby chciałyby to założyć. Jest taka taktyka, która nazywa się „honey pot" – czyli „garnek z miodem". Chodzi o to, by pokazać przeciwnikowi jakieś bardzo atrakcyjne dla niego miejsce i tam urządzić na niego zasadzkę. Czasami wystawia się jakiś atrakcyjny dla przeciwnika cel i czeka na atak po to, żeby zebrać dane na jego podstawie. Można dzięki temu ustalić chociażby liczebność grupy, sposób ataku czy tożsamość atakujących. I cóż, Riseup nie musi, ale może być garnkiem z miodem wystawionym przez naszych przeciwników, po to aby sprawdzić, kto do niego przyjdzie. To, co sprawia, że hipoteza ta staje się niebezpiecznie prawdopodobna, to istnienie riseupowego VPNa. Nie widzę powodu, dla którego łącząc się przez VPNa Riseupa z jakąś stroną, miałxbym się czuć bezpieczniej niż łącząc się z mojego zwykłego łącza po

Neostradzie od Orange. Nie ufam ani Orange ani Riseupowi. Ale pewnie niektórzy ufają Riseupowi bardziej. I myślę, że to jest właśnie niebezpieczne.

Popularne wśród anarchistek podejście do „bezpiecznych technologii" bardzo często opiera się na ślepej wierze w autorytety. W gruncie rzeczy, jeśli ktoś oczekuje od was ślepego zaufania to może sugerować, że ma złe intencje.

Innym dobrym przykładem wiary w technologiczne cuda jest tworzenie baz wrażliwych danych, a potem zastanawianie się jak te dane zabezpieczyć. Generalnie zapamiętaj sobie raz na zawsze: bazy danych tworzy p*icja, a nie anarchistki. Jeśli już stworzysz taką bazę numerów telefonów powiązanych z rolami na akcji, czy coś podobnie absurdalnego, to znaczy, że podchodzisz źle do problemu i to, jakich narzędzi użyjesz do zabezpieczenia takiej bazy, jest w takiej sytuacji drugorzędne. Istnienie takiej bazy danych bardzo rzadko jest konieczne, a minimalizacja śladów to podstawowa zasada jaką powinniśmy się kierować. Jeśli tworzymy coś, co potencjalnie może być dowodem, to tylko jeśli jest to absolutnie konieczne. Jeśli akurat tak się zdarzy, że z analizy wszystkich okoliczności wynika, że jakaś baza danych musi powstać, to powinna ona zawierać jak najmniej informacji. Najlepiej, jakby nie zawierała żadnych informacji identyfikujących oraz żeby była tak efemeryczna, jak to możliwe - czyli w razie czego powinna być ona bardzo łatwa do nieodwracalnego zniszczenia. Oczywiście idealnie efemeryczna baza danych istnieje tylko w ludzkiej pamięci, a jeszcze lepiej jak jedna osoba nie posiada wszystkich kluczowych informacji. Im mniej wiesz tym lepiej śpisz. A ktoś, kto bez wyraźnej konieczności zbiera informacje, nie zasługuje na twoje zaufanie.

5.2. Granie na warunkach przeciwnika

Analogicznie jak do tworzenia baz danych, można podejść do pisania oświadczeń i wysuwania osób rzeczniczych. Bardzo często ustępstwa w dziedzinie opsec wynikają z chęci uczestnictwa w spektaklu. Niektóre osoby mają potrzebę „zabrania głosu", w sposób, w jaki według ich wyobrażenia dotrze do wyobrażonej publiczności. Przypadkiem albo nie przypadkiem, tak się składa, że nasłuchujące takich głosów media działają dokładnie tak samo jak p*icja. Media - tak samo jak p*icja - chcą znać twarze, motywy, chcą móc przypisać indywidualną odpowiedzialność za jakieś czyny jednostce, o której chcą móc opowiedzieć jakąś historię. Wszystko to sprawia, że zaczynając myśleć w kategoriach spektaklu, zaczynasz czuć pokusę, by się trochę odsłonić. To jest oczywiście dokładnie to, o co chodzi w tej gierce. Trzeba brać odpowiedzialność za swoje czyny – tak głosi chrześcijaństwo, w to wierzą i p*icjanci i liberałowie.

Moim zdaniem nie trzeba. Za nic nie musisz brać odpowiedzialności (cokolwiek to znaczy). Niczego nie musisz oświadczać, nie musisz niczego żądać.

To twój wybór, czy po udanej akcji zechcesz napisać oświadczenie i wysłać je do mediów lub opublikować w internecie. Zrobienie tego z pewnością spotęguje ryzyko i stworzy dodatkową przestrzeń na błąd. Zrób jak zechcesz, to twoja akcja, twój plan, twój opsec i twoje wybory. Moim zdaniem dobre akcje mówią za siebie. I nie potrzebują osób rzeczniczych.

Zresztą to, czy w jakimś miejscu coś płonie, czy nie, to jest rzecz, którą być może naprawdę możesz zmienić. Spektaklu raczej zmienić ci się nie uda.

5.3. Działanie bez planu

Tego chyba nie muszę rozwijać. Jesteś tutaj bo przeczytałxś zina, czy zaczęłxś od końca? Opsec jest elementem planu. Tylko i aż.

5.4. Niedostosowanie środków do celów

Opsec ma ci ułatwić realizację zadania, a nie ją utrudnić. Opsec to proces, który zaczyna się od uświadomienia sobie ryzyka, zaakceptowania go i wykonywania planu, tak aby się udał, przy akceptacji skutków możliwych niepowodzeń. Jeśli nie akceptujesz ryzyka, to zmień plan. Ale jeśli narzucasz sobie zabezpieczenia, które uniemożliwiają ci działanie, to tracisz czas i zużywasz swoją wolę.

C. D. N.

Anarcho-Biblioteka
Dobry pieróg to wywrotowy pieróg

współudział
Pewne rzeczy
Wprowadzenie do bezpieczeństwa operacyjnego dla osób anarchistycznych zainteresowanych akcją bezpośrednią
2023