STUDIA SOCJOLOGICZNE 2017, 1 (224)
ISSN 0039−3371

Marcin Zaród
Uniwersytet Warszawski

HAKERZY I KOLEKTYWY HAKERSKIE W POLSCE. OD OPERACJONALIZACJI DO LABORATORIÓW I STREF WYMIANY

Artykuł zawiera wyniki badań w środowiskach hakerskich w Polsce, realizowanych z zastosowaniem teorii aktora-sieci w latach 2013–2015. W pierwszej części prezentowane są operacjonalizacje pojęć hakera, odchodzące od stereotypu medialnego na rzecz uwzględnienia wiedzy z zakresu nauk społecznych, autodeskrypcji badanych oraz rezultatów fazy eksploracyjnej badania. Proponowana operacjonalizacja pozwala na lepszy opis zjawisk zachodzących w polskich grupach nazywających się hackerspace, makerspace czy fab-lab. W drugiej części przedstawione są analizy materiału zebranego w ramach operacjonalizacji, koncentrujące się na tworzeniu i wymianie wiedzy, w których uczestniczą hakerzy i kolektywy hakerskie. Analiza kolektywu hakerskiego jako laboratorium wskazuje na rolę czasu, humoru oraz stabilności. Kombinacja humoru i niestabilności sprzyja powstaniu „karnawału poznawczego", w trakcie którego koszt porażki jest obniżony. Analiza kolektywu hakerskiego jako strefy wymiany kieruje uwagę na mediacje kultur epistemicznych oraz rolę niestabilności w ułatwianiu wymiany. Rezultatem operacjonalizacji, etnografii i analizy jest nie tylko lepsze zrozumienie nowej grupy, ale również propozycja syntezy dotychczasowych badań kultury hakerskiej z konstruktywistyczną socjologią nauki i techniki.

Główne pojęcia: studia nad nauką i techniką; haker; kolektyw hakerski; teoria aktora-sieci; etnografia.

Media często przedstawiają hakera jako złodzieja danych, niszczyciela porządku lub jako wyrafinowanego cyberprzestępcę. Obraz ten nie jest podzielany przez wszystkie środowiska związane z bezpieczeństwem komputerowym. Według manifestów hakerskich (Raymond 2001a; The Mentor 1986; Wark 2004) istnieje granica etyczna między testowaniem zabezpieczeń z powodu ciekawości lub chęci doskonalenia techniki (tzw. *white hat*) a działalnością cyberprzestępczą i niszczeniem danych (tzw. *black hat*). Majsterkowanie z zabezpieczeniami w obu kontekstach nawiązuje do hasła „zrób to sam" (*do it yourself* – DIY), bo

Instytut Socjologii, e-mail: m.zarod@is.uw.edu.pl

* Artykuł powstał w ramach grantu „Aktorzy-Sieci w zbiorowościach hakerskich. Studium etnograficzne z zakresu badań nad nauką i techniką.", sfinansowanym ze środków Narodowego Centrum Nauki w konkursie Preludium (nr grantu 2014/13/N/HS6/04113).

zakłada kontrolę autora nad możliwie dużą częścią programu lub systemu. Nawet specjaliści bardziej krytyczni wobec hakerów podkreślają trudności związane z jednoznaczną klasyfikacją moralną (Schneier 2015).

W niniejszym artykule przedstawię wyniki badań zrealizowanych wśród grup hakerów niełamiących prawa, choć mocno krytycznych wobec ustalonych obiegów wiedzy technicznej i komputerowej. Takie grupy powstają w Polsce od 2012 roku, najczęściej w formie prawnej stowarzyszeń i grup nieformalnych. Nazwy kolektywów hakerskich akcentują jednocześnie związki z kulturą hakerską, jak i z konkretnym miastem, np. Hackerspace Kraków, Hackerspace Warszawa, Hackerspace Silesia.

Wykorzystując obserwacje prowadzone w tego rodzaju środowiskach przedstawię operacjonalizację pojęcia „hakera", w której połączyłem autodeskrypcje środowiskowe, istniejącą wiedzę z zakresu nauk społecznych oraz koncepcje studiów nad nauką i techniką. Operacjonalizacji tej użyję, aby pokazać, że wiedza hakerów pochodzi z serii krótkich operacji na systemie lub programie. Często ma charakter lokalny, brakuje jej stabilizacji, przez co nie zawsze jest w stanie funkcjonować poza kontekstem kolektywu hakerskiego. Ta niestabilność pozwala kolektywom hakerskim na działania, które byłyby trudne do realizacji w bardziej formalnych laboratoriach. Pokażę, że kolektywy hakerskie jednocześnie funkcjonują jako osobne laboratoria, jak i jako miejsca wymiany między różnymi porządkami wiedzy technicznej.

Zanim przejdę do tych analiz, proponuję – przynajmniej tymczasowo – hakera rozumieć jako zdolnego, choć niekiedy złośliwego miłośnika techniki komputerowej, niezwiązanego z instytucjami formalnymi, niekiedy działającego na granicy prawa.

Grupy hakerów będę określał mianem kolektywów hakerskich, co zachowuje autodeskrypcję środowiskową (patrz np. Farr 2009). Pracę swoją umieszczam w kontekście konstruktywistycznej socjologii nauki i techniki, zachowując dwa dodatkowe znaczenia. Po pierwsze: skojarzenie z kolektywem myślowym według Ludwika Flecka (2014). Po drugie: praca korzysta z teorii aktora-sieci Bruno Latoura (2010), w której kolektyw oznacza specyficzny zbiór ludzi i aktorów nieludzkich. Wszystkie trzy źródła pojęcia kolektywu hakerskiego (środowiskowy, fleckowski i latourowski) są dla niniejszej pracy równie istotne.

Badania hakerów w naukach społecznych. Problemy i triangulacja

Najstarszą, choć nadal często przywoływaną interpretację etosu hakerskiego znajdziemy u Stevena Levy'ego, który opisał przekształcanie się klubu miłośników komputerów w pionierów biznesu i techniki programistycznej. Wyróżnił on wartości mające być wyznacznikami kultury hakerskiej: wolność informacji

i dostępu do komputerów, niechęć do hierarchii, artystyczny i estetyczny wymiar praktyk informatycznych, merytokrację i samodoskonalenie (Levy 2010, rozdz. 2). Podobne elementy były wymieniane w manifestach kolejnych pokoleń hakerów (The Mentor 1986; Raymond 2001a), były też elementem badań socjologicznych (Juza 2008, 2011). Przykładowo: Pekka Himanen opisał etos hakerski jako kontrastujący z klasycznym, weberowskim etosem pracy; zatracanie się w zabawie-pracy, dążenie do otwartości i uznania społeczności miały być postawami charakterystycznymi dla epoki Internetu (Himanen 2002).

W niniejszej pracy odchodzę od poszukiwania esencjalizacji etosu hakerskiego na rzecz zrozumienia mechanizmów tworzenia wiedzy w kolektywach hakerskich. Poszczególne wykładnie norm i etosów hakerskich są istotne wyłącznie jako elementy autodeskrypcji badanych niż jako rezultaty analizy.

Takie usytuowanie łączy niniejszą pracę z badaniami Gabrieli Coleman, dotyczącymi hakerów związanych z wolnym / otwartym oprogramowaniem (2013) oraz hakerami-aktywistami politycznymi / haktywistami (2015). W tego rodzaju badaniach mniej uwagi poświęca się normom i „prawdziwej postaci" etosu hakerskiego, bardziej skupiając się na tym, jak dane elementy są interpretowane przez różne środowiska albo na tym, jak różne grupy zaangażowane w hakowanie radzą sobie ze sprzecznościami i kontrowersjami.

Prace Coleman zyskały rozgłos również poza obiegiem akademickim, bywały rekomendowane przez uczestników badania. Badaczka skupiła się na działaniach hakerskich, mających bezpośrednie znacznie polityczne, np. w kontekście wolności słowa lub prywatności (haktywizm). Takie działania, choć czasami nielegalne, stanowią akty obywatelskie mieszczące się w ramach amerykańskiej tradycji liberalizmu i obywatelskiego nieposłuszeństwa. Ta perspektywa odnosi się nie tylko do zabronionego haktywizmu, ale również do „zwykłych" hakerów, deklarujących brak zainteresowania problemami politycznymi i opisanych w poprzedniej pracy autorki (Coleman 2013). Tropem tym poszedł Johan Söderberg, którego interpretacje czerpały z teorii aktora-sieci (Actor-Network Theory – ANT) i teorii krytycznej (Söderberg 2011b).

Według Coleman sednem kultury hakerskiej nie jest ani preferowanie konkretnych rozwiązań technicznych, ani przywiązanie do konkretnej wykładni etosu, ani nawet konkretny stosunek do państwa i prawa własności intelektualnej. Sednem jest umiejętność ciągłych negocjacji pozornie sprzecznych wartości (np. prywatność danych *versus* publiczny dostęp do wiedzy, wiedza informatyczna dostępna dla wszystkich *versus* elitarność grup hakerskich). Wolność tworzenia kodu i narzędzi jest – według tej interpretacji – tożsama z wolnością słowa (Coleman i Golub 2008).

Rozróżnienie środowiskowe pomiędzy legalnymi hakerami-majsterkowiczami a cyberprzestępcami, przywołane we wstępnie, zostało przyjęte również w pracach dotyczących antropologii kultury hakerskiej i kryminologii

przestępstw komputerowych (Taylor 1999; Chiesa i wsp. 2009). Paul Taylor przeprowadził serię wywiadów z hakerami oraz przeanalizował fragmenty dyskursu prasowego, korzystając między innymi z beckerowskiej teorii dewiacji (Becker 2009).

Pokazał też, że status hakera często bywa elementem kariery specjalisty od zabezpieczeń komputerowych, krytycznie odniósł się też do obietnic egalitaryzmu i merytokracji proponowanych w manifestach środowiskowych.

Do podobnych wniosków, choć opartych na innych materiałach doszedł też włoski badacz bezpieczeństwa komputerowego Raoul Chiesa z zespołem badawczym UNICRI (jedna z agend ONZ ds. badań kryminologicznych). Przeprowadzili oni duże badanie ilościowe uzupełniane wywiadami i elementami obserwacji, próbując stworzyć profil kryminologiczny hakerów poruszających się na granicy prawa. Zespół zebrał 576 kwestionariuszy (w tym 276 specjalnie rozbudowanych o elementy badania jakościowego) wypełnionych przez osoby, które złamały zabezpieczenia serwera testowego lub uczestniczyły w konferencjach środowiskowych pokazując np. nieznane wcześniej luki w zabezpieczeniach (tzw. *zero day*). Sami autorzy wyraźnie precyzują, że badanie dotyczy raczej szarej strefy (np. osób atakujących systemy z powodów politycznych lub z ciekawości), nie zaś zawodowych przestępców pracujących w grupach zorganizowanych.

Publicznie dostępne są wyłącznie wstępne wyniki badania (siatka ogólnych profili kryminalistycznych hakerów, elementy analiz biograficznych w Chiesa i wsp. 2009) i fragmenty późniejszych referatów. Co najmniej jeden z uprzywilejowanych informatorów, znający specyfikę włoskiej sceny hakerskiej, z którymi miałem kontakt, był zdania, że wyniki badania ilościowego Chiesy zostały przekazane agendom rządowym lub siłom policyjnym. Nawet jeśli ta informacja jest niepewna, to brak publikacji pełnych wyników badania ilościowego sugeruje na problemy etyczne związane z badaniem środowiska.

W takich wypadkach trudno ustalić warunki reprezentatywności próby. Na rzecz trafności wyników wstępnych zespołu Chiesy przemawia analiza socjologiczno-kryminologiczna zawartości dysków twardych hakerów, którzy zostali aresztowani (Dupont 2012) oraz wywiady z aresztowanymi hakerami-aktywistami (Coleman 2015). We wszystkich wypadkach istotne było tworzenie własnych narzędzi, niezależność i różnicowanie zaufania wobec instytucji, innych hakerów i własnych umiejętności. Trudno jednak ustalić zakres stosowania tego rodzaju triangulacji, z uwagi na wspomniany wcześniej brak publikacji głównych wyników badania w ogólnym obiegu naukowym.

Wspomniane powyżej prace dotyczyły głównie hakerów pochodzących z krajów anglojęzycznych. Europejskie środowisko hakerskie znane jest zdecydowanie słabiej, choć najstarszy i najliczniejszy kolektyw europejski, czyli niemiecki Chaos Computer Club powstał w 1981 roku. Największa i najstarsza

europejska konferencja hakerska (Chaos Communication Congress) odbywa się regularnie od 1984 roku. Sebastian Kubitschko pokazał, że poprzez umożliwienie publicznej dyskusji nad lukami w infrastrukturze, prace w ramach tej konferencji stały się elementem niemieckiego społeczeństwa obywatelskiego (Kubitschko 2015).

Odmienność prawa autorskiego i różnice w genezach hakerów między Stanami Zjednoczonymi a Europą dodatkowo komplikują sytuację (Alberts i Oldenziel 2014). To, co w Polsce jest legalnym majsterkowaniem (np. próba naprawy domowego routera, zmiana systemu operacyjnego telefonu), w Stanach Zjednoczonych może być karane właśnie jako cyberprzestępczość, ponieważ ochrona prawna całych systemów komputerowych wykracza poza ataki na infrastrukturę sieciową. Zasadnym wydaje się więc założenie, że korporacje komputerowe mogą czasami korzystać z tej dychotomii, by używać etykiety hakera-cyberprzestępcy do odstraszania nadmiernie ciekawskich użytkowników lub do kreowania niebezpieczeństwa jako narzędzia sprzedaży produktu. Przykładem tego drugiego zjawiska może być kampania jednej z firm komputerowych pod nazwą „Marzenie hakera", konstruująca zachętę do zakupu oprogramowania na strachu przed hakerami. Obserwowałem dyskusje środowiskowe i poszukiwanie form protestu przeciw tej kampanii, ponieważ był to moment, w którym rozproszone grupy próbowały skonstruować spójną kontrdefinicję. Analiza tej dyskusji stanowiła okazję do walidacji proponowanych poniżej operacjonalizacji, związanej z czarnymi skrzynkami techniki komputerowej.

Drugim problemem jest różnorodność zainteresowań hakerów i majsterkowiczów, w szczególności renesans zainteresowania kulturą materialną (tzw. *maker movement*, ruch wytwórców), skutkujący rozwojem grup przyjmujących nazwy *makerspace* lub *fab-lab* (laboratoria fabrykacji). Wedle manifestów i badań socjologicznych zjawiska, wyznacznikami ruchu ma być koncentracja na tworzeniu konkretnych rzeczy, kreatywność i samodzielność (Fleischmann i wsp. 2016; Gershenfeld 2007; LoWalter-Herrmann i Büching 2013). Nurt ten jest obecny również w Polsce, gdzie „spejsy" (określenie środowiskowe na makerspace, fab-lab lub hackerspace) współpracują ze sobą (Zaród 2013). Makerzy uczestniczący w niniejszym badaniu, choć nie wypierali się podobieństw z hakerami, akcentowali raczej tradycje majsterkowania i radzenia sobie, mniej uwagi kładąc na kwestie cyberbezpieczeństwa.

Polskie piśmiennictwo na temat kultury hakerskiej skupia się raczej na okresie lat dziewięćdziesiątych XX wieku traktując ją jako zjawisko międzynarodowe. Mniej uwagi poświęca się różnorodności lokalnych kultur hakerskich oraz współczesnym, wewnętrznym przeobrażeniom zjawiska. Marta Juza analizowała wpływ kultury hakerskiej na Internet i pionierów jego wdrożenia w Polsce (Juza 2008, 2011). Patryk Wasiak pisał o giełdach komputerowych i innych nieformalnych obiegach wiedzy w technice komputerowej (Wasiak 2016). Prace te

były użyteczne dla walidacji niektórych informacji pozyskanych we fragmentach biograficznych niniejszego badania (np. rola giełdy komputerowej jako często występującego wspomnienia). W podobnej roli użyłem też propozycji Bartłomieja Knosali z zakresu filozofii techniki dotyczącej relacji między kulturą hakerów a manifestami ekologicznymi kontrkultury (Knosala 2015).

W większości dyskutowanych powyżej prac wywiady indywidualne i manifesty były podstawą do konstrukcji ogólnej kultury hakerskiej. Jedynie wyjątkowo analizy dotyczyły poziomu grup, w szczególności mechanizmach grupowego tworzenia wiedzy technicznej (Alberts i Oldenziel 2014). Chcąc wyjść poza dobrze opisane kwestie kultury i tożsamości hakerów, zdecydowałem się na użycie koncepcji związanych ze studiami nad nauką i techniką (Science and Technology Studies – STS), które dopiero niedawno zostały zastosowane do badania zjawiska hakowania (przegląd aktualnych prac w: Söderberg i Delfanti 2015). Niniejszą pracę sytuuję w tym nurcie, z tym, że silniej czerpię z korzeni epistemologicznych, a mniej uwagi poświęcam relacjom hakerzy–użytkownicy–instytucje. Ten drugi problem rozważałem w innej pracy (Zaród 2015b).

Pracując nad obszarem szybko zmiennym i słabo opisanym, zdecydowałem się na użycie dyskutowanych powyżej prac jako elementów triangulacji teoretycznej.

Poprzednikom opisującym etosy hakerskie zawdzięczam kryteria kodowania użyte w jednym z kryteriów operacjonalizacji oraz wiedzę, która ułatwiła mi wejście w dość hermetyczne środowisko.

Podobnie jak Gabriela Coleman odszedłem od poszukiwania typów idealnych hakerów, skupiając się na analizie skutków konkretnych praktyk. Część sprzeczności zidentyfikowanych przez nią wraz z Aleksem Golubem użyłem jako inspiracji do analiz w perspektywie ANT. Innymi słowy: myśląc kategoriami studiów nad nauką i techniką, sprawdzałem, jak moje rozumowanie wyglądałoby w ujęciu Coleman. Doprowadziło to do uogólnienia koncepcji hakowania jako praktyki liberalnej również na wymiar epistemologii. Inaczej niż Coleman traktuję humor hakerów: nie jako indywidualny sposób radzenia sobie ze złożonością, ale jako grupowy mechanizm redukcji kosztów porażki (patrz część dotyczącą laboratoriów) i kłopotów z kontaktami (patrz część dotyczącą strefy wymiany).

Paul Taylor zainspirował mnie do myślenia o tym, jak zróżnicowanie definicji hakerów może mieć wymiar polityczny. Od zespołu Chiesy zaczerpnąłem krytycyzm wobec akceptowania „pokojowej" definicji hakera oraz elementy walidacji kryterium operacyjnego związanego z bezpieczeństwem komputerowym. Żaden z nich jednak nie analizował grup spotykających się w przestrzeni fizycznej, ani testujących systemy inne niż sieci komputerowe (np. smartfony, karty miejskie, liczniki energetyczne).

Zastosowane koncepcje z zakresu studiów nad nauką i techniką

Klasyczne dla STS prace powstały w wyniku badań etnograficznych w laboratoriach jako element polemiki z mertonowskim ideałem nauki (przykład Latour i Woolgar 1986, omówienie znaczenia i metody prac w Hess 2014). Teoria aktora-sieci stanowiła jednocześnie rozwinięcie wniosków metodologicznych płynących z badań (Latour 1988a i 1988b) oraz mocno nawiązywała do Mocnego Programu Socjologii Wiedzy (Barnes i Bloor 1993), w szczególności 4 postulatów:

1. Przyczynowość. Socjologia nauki winna być zainteresowana warunkami powstawania wiedzy naukowej.
2. Bezstronność wobec prawdy i fałszu, racjonalności i irracjonalności, sukcesu i porażki. Socjologia nauki winna analizować obie strony każdej z tych dychotomii.
3. Symetria w stylach wyjaśniania prawdy i fałszu naukowego. Socjologia nauki winna stosować te same wyjaśnienia względem stwierdzeń naukowych uznanych za prawdziwe, jak i sfalsyfikowanych.
4. Refleksyjność. Zastosowania mocnego programu dotyczą również samej socjologii wiedzy.

Postulaty te ukształtowały studia nad nauką i techniką, choć ich stosowalność wzbudziła wiele dyskusji. W jednej z tych dyskusji Michel Callon zaproponował rozszerzenie założeń o postulat symetrycznego badania ludzi i czynników pozaludzkich (Callon 2014), dając tym samym impuls do powstania teorii aktora-sieci jako osobnego podejścia do badania złożoności przyrodniczo-społecznej.

Z perspektywy niniejszego tekstu, tenże postulat symetrii wydaje się szczególnie istotnym elementem metodyki, ponieważ hakerzy są ściśle powiązani ze swoim sprzętem. Nie sposób zrozumieć hakerów bez rozumienia ich narzędzi, zatem do lepszego rozumienia zbiorowości hakerskiej użyłem koncepcji inskrypcji, laboratorium, próby sił i czarnej skrzynki (Latour 1988a, 2009, 2010, 2013). Ponieważ koncepcje te były różnie definiowane w ramach ANT, pokażę, jakie rozstrzygnięcia teoretyczne przyjąłem na potrzeby artykułu.

Definicję i kryteria inskrypcji przyjmuję za Latourem (2012). Inskrypcje to szczególny rodzaj zapisów naukowych lub inżynieryjnych, które zapośredniczają przejścia między różnymi poziomami złożoności lub liczebności. Inskrypcje to element, który wiąże mikrometrowe tranzystory, kilometrowe światłowody i miliardowe korporacje. Przykładem inskrypcji najczęściej spotykanym w trakcie niniejszego badania jest schemat elektroniczny układu, tabela z logami serwera lub projekt do wykonania w maszynie sterowanej numerycznie.

Laboratorium analizuję według tekstu Latoura „Dajcie mi laboratorium a poruszę świat" (polski przekład z 2009) oraz późniejszej książki *Science in*

Action (1988a), jako miejsce, gdzie przetwarzani są ludzie i czynniki pozaludzkie (np. miejsce testów szczepionki na wściekliznę). Różne skale łączone są za pośrednictwem inskrypcji. Według przykładu Bruno Latoura: główne etapy przekształceń w laboratorium to przejmowanie cudzych interesów, zmiana relacji siły, poruszenie światem zewnętrznym. W pierwszym etapie potencjalni sojusznicy gromadzą się w laboratorium (od grantodawców aż po odczynniki i bakterie). W drugim, powiązania między ludźmi i czynnikami pozaludzkimi są definiowane na nowo (np. gdy do układu ludzie–mikroby wścieklizny dodamy szczepionkę). W trzecim poprzednie rozwiązania są stabilizowane i replikowane w większej skali (np. przez organizację krajowej siatki szczepień i standaryzację klasyfikacji wirusów wścieklizny). Pytanie: „Czy kolektyw hakerski jest laboratorium?" było punktem wyjścia niniejszego badania.

Próba sił, zgodnie *Science in Action* (Latour 1988a), to działanie wykonywane najczęściej w laboratorium, w efekcie którego zerwane zostaje połączenie między zbiorowością a jej rzecznikiem. Rzecznik to osoba lub przedmiot, który w danej sytuacji ma prawo mówić w imieniu danej zbiorowości. Przykładowo: jeśli jakiś haker twierdzi, że jego układ elektroniczny powinien zachowywać się w pewien konkretny sposób, to próba siły przyjmuje najczęściej formę pomiaru parametrów na oscyloskopie lub test praktyczny układu w stosownej roli. Jeśli układ zawiedzie, haker nie będzie zaakceptowany jako osoba, która zna działanie układu. Jeśli dany haker spróbuje mówić w imieniu układu, by wyjaśnić jego działanie lub aby połączyć go z innymi częściami, wtedy układ lub koledzy zakwestionują legitymację danego hakera jako rzecznika.

Czarna skrzynka to szczególny typ zbiorowości (układu ludzi i przedmiotów), który na skutek wielu prób sił identyfikowany jest wyłącznie na podstawie sygnału wejścia i wyjścia. Sukces projektanta układu sprawia, że staje się on niewidzialny dla kolejnych użytkowników (Latour 2013: 379). W trakcie badania okazało się, że umiejętność dekonstrukcji czarnych skrzynek związanych z elektroniką i techniką komputerową jest wysoko ceniona przez hakerów. Jest też elementem odróżniającymi laboratoria akademickie od hakerskich: w tych drugich czarne skrzynki nie są zamykane i stabilizowane po modyfikacjach.

W uproszczeniu, na użytek niniejszego tekstu można przyjąć, że czarna skrzynka to element techniki, który został usystematyzowany, opisany i łatwo go powielać, montować i używać jako narzędzia, bez potrzeby dodatkowej refleksji lub pracy poznawczej. Przykładem czarnej skrzynki dla Czytelników niniejszego tekstu może być sprawny laptop w rękach doświadczonej specjalistki od bezpieczeństwa, na którym z powodzeniem pracuje bez rozważania poziomów Curie w tranzystorach, charakterystyk bramek logicznych i potencjałów elektrochemicznych baterii.

Szczegółowa trajektoria powstawania czarnych skrzynek jest istotnym elementem ANT (Latour 2013: 379). Szersza dyskusja tego problemu wykracza

poza łamy tego tekstu, zatem pozwolę sobie jedynie zasygnalizować główne wnioski. Z tych samych powodów nie stosuję też w tekście rozróżnienia na mediację i translację (Abriszewski 2008).

Koncepcja kultury epistemicznej nie wywodzi się z ANT, a z prac STS silniej inspirowanych interakcjonizmem symbolicznym i klasyczną socjologią organizacji: „Kultura odnosi się do połączenia wzorów i dynamik, które są okazywane w praktyce fachowej i różnią się w zależności od poziomu biegłości" (Knorr Cetina 1999: 8). W takiej interpretacji istotne dla niniejszej pracy jest przywiązanie do konkretnych działań i sfery symbolicznej związanych z wytwarzaniem i walidowaniem wiedzy. Tak rozumiana kultura epistemiczna jest jednym z elementów spajających konkretne kolektywy, którego hakerzy mogą być świadomi.

Stosowanie pojęć związanych z kulturą w kontekście ANT wymaga uwagi, ponieważ, jak ostrzega Latour, zbyt łatwo można powołać do życia niewidoczny i wszechpotężny „eter społeczny", który służy jako uniwersalne wyjaśnienie (patrz Latour 2010, rozdz. 1 i 2). Mając świadomość tych zagrożeń, podejmuję to ryzyko, aby opisać splot norm epistemologicznych, warstwę symboliczną właściwą dla inskrypcji komputerowych oraz praktyki wytwarzania i walidacji wiedzy.

Kolektywy hakerskie w Polsce. Lokalizacja, finansowanie i formy działalności

W trakcie badania odnotowałem aktywność wokół co najmniej 10 kolektywów hakerskich. Grupy, których aktywność została potwierdzona w trakcie badania przez trzy różne źródła (obserwacja, wywiad, aktywność na stronach internetowych, uczestnictwo w ogólnopolskich wydarzeniach, uczestnictwo w liście dyskusyjnej) na przestrzeni co najmniej roku, uznaję za ustabilizowane. Do takich grup należą kolektywy w Warszawie, Łodzi, Poznaniu, Trójmieście, Katowicach i Krakowie. Stabilizacja kolektywu jest o tyle istotna, że wiele z grup było jedynie efemerydami (pojedyncze spotkania lub też jedynie strona internetowa). Dla porównania: wszystkie kolektywy ustabilizowane mają stałe miejsce spotkań, które jest otwarte dla członków co najmniej 5 dni w tygodniu. Te kryteria i terminologia oparte są na wypowiedziach i kodach in vivo. Informacje o stanie środowiska w momencie rozpoczęcia badania oraz ówczesny stan operacjonalizacji zostały omówione w innym artykule (Zaród 2013).

Część grup ustabilizowała się jako tzw. hackerspace (np. Kraków, Warszawa), część jako Fab-Laby (np. Trójmiasto, Łódź). Zgodnie z deklaracjami na stronach internetowych, w ramach pierwszej formy większy nacisk położony jest na programowanie, technikę komputerową i przywiązanie do różnych form

etosu hakerskiego. Fab-Laby, wpisują się w ruch makerów i odnoszą się raczej do obróbki materiałów fizycznych (wycinarki, obrabiarki) i druku 3D. Jak przyznaje część badanych, różnica między fab-labem a hackerspacem jest płynna i często jest wyborem taktycznym między bardziej „podziemną estetyką hakerską" a „legalniejszym" majsterkowaniem. Drugie podejście, które dominuje w komunikatach fab-labów, sprawia wrażenie „legalności" i ułatwia angażowanie członków, którzy nie czują się kompetentni w technice komputerowej, ale są np. zdolnymi mechanikami, artystkami pracującymi z materiałami itp.

Najliczniejsze z ustabilizowanych kolektywów liczą ponad 60 osób, najmniejsze: około 10. Wedle wszystkich posiadanych danych: wśród regularnych gości „spejsów" przeważają mężczyźni w wieku 16–30 lat. Kobiety stanowią mniejszość, zarówno hakerki, jak i sojuszniczki.

Jednym z etapów stabilizacji jest przyjęcie pewnych rozwiązań prawnych, które umożliwiają np. wynajem przestrzeni i zapewnienie dostępu do Internetu. Przeważają formy organizacji pozarządowych (stowarzyszenia i fundacje). Pierwszy model finansowania to składki comiesięczne, których wysokość jest dobrowolna (najczęściej około 50–100 zł miesięcznie, choć lepiej zarabiający hakerzy nierzadko łożą nawet 400 zł miesięcznie lub dokonują jednorazowych darowizn w podobnej kwocie). Inny model to abonament za korzystanie z urządzeń (w modelu „warsztat do wynajęcia"). Kolejny to sponsoring od firm komputerowych lub instytucji samorządowych.

Głównym wydatkiem jest wynajem pomieszczenia oraz opłaty za media. Dodatkowe koszty to zakupy i utrzymanie sprzętu. Niektóre fab-laby zatrudniają personel (od 1 do 3 osób/kolektyw), którego zadaniem jest dbanie o urządzenia i BHP nowych użytkowników lub pozyskiwanie środków.

W badanych kolektywach zaobserwowałem zwrot w stronę produkcji materialnej, zgodnie z obserwacjami środowiskowymi z zagranicy (Maxigas 2012; Farr 2009). W tekstach tych uznaje się, że nowa fala powstających kolektywów hakerskich powiązana jest z upowszechnieniem łatwo programowalnej elektroniki (układy Arduino i Raspberry Pi), popularnością druku 3D oraz kwestiami ochrony prywatności. Wyznacznikiem poprzedniej fali jest popularyzacja wolnego i otwartego oprogramowania oraz technik internetowych. Jeden z kolektywów w Polsce ma genezę charakterystyczną dla poprzedniej fali „spejsów" (warsztaty systemu operacyjnego Linux przerodziły się w klub komputerowy, który z kolei dał początek hackerspace), ale nawet w tym kolektywie Arduino, druk 3D i warsztaty związane z szyfrowaniem (tzw. cryptoparty) były obowiązkowymi próbami sił dla nowych członków kolektywu (Latour 2013).

Metodyka zbierania i analizy danych

Niniejszy tekst jest rezultatem analiz opartych na danych zbieranych w kolektywach hakerskich w Polsce od 2013 roku. Ponieważ badania hakerów spotykających się w przestrzeni fizycznej stanowią rzadkość, również w obiegu międzynarodowym (wyjątek Söderberg 2011a), pierwszy okres pracy (do czerwca 2014) miał charakter eksploracyjny.

Od samego początku praca koncentrowała się na kwestiach związanych z produkcją, wymianą i walidacją wiedzy technicznej i naukowej, od samego początku przyjęto też ramy ANT i etnografii laboratorium (Latour 1988a, 2010). Pytaniem wyjściowym było: „Czy kolektyw hakerski jest laboratorium". Z uwagi na przyjętą orientację teoretyczną, metodykę i brak uprzedniej wiedzy o zjawisku, nie formułowano hipotez przed rozpoczęciem badania.

Do wejścia w środowisko stosowałem najczęściej kontakt z gate-keeperami (mail zapowiadający wizytę) w połączeniu z uczestnictwem w wydarzeniach otwartych (np. zapisałem się na publiczne warsztaty dotyczące prywatności oraz drugie, dotyczące elektroniki). Pierwsze reakcje obejmowały zarówno drwiny, jak i zaciekawienie lub chęć pomocy. Ogółem do grudnia 2015 roku w dzienniku badania znalazło się około 170 rekordów opartych na obserwacji bezpośredniej (120 not z obserwacji) i internetowej (50 wpisów, głównie zarchiwizowanych dyskusji mailowych i czatowych).

Wszystkie obserwacje przeprowadzono jawnie i za zgodą osób badanych. W trakcie obserwacji wykonywałem notatki skrócone, które były przepisywane do postaci pełnych wpisów w dzienniku nie później niż 24 godziny po obserwacji. Jedynie w wyjątkowych wypadkach (np. awarie, dodatkowe wywiady), dziennik był aktualizowany na podstawie mniej aktualnych wspomnień.

Większość obserwacji przeprowadzono w dwóch najstarszych kolektywach w Polsce. Kluczem wyboru był ich rozmiar i stabilizacja w 2013 roku. Oprócz tych dwóch miejsc, stabilny był jeszcze jeden ośrodek, w którym miałem doświadczenia osobiste, które mogły utrudnić świeże spojrzenie badawcze. Z tego powodu wybrałem ośrodki inne niż ten, który początkowo współtworzyłem – a jednocześnie w miarę stabilne. W toku badania zrealizowałem też krótkie obserwacje i wywiady w 3 kolektywach w Polsce (dobór celowy) i 3 trzech poza granicami (dobór dogodnościowy, jako walidacja, nie zaś jako źródło materiału pierwotnego). Obserwacje uzupełniające miały formę weekendowych wyjazdów do innych kolektywów, najczęściej połączonych z wydarzeniem specjalnym (np. lokalny festiwal majsterkowiczów, uruchomienie nowego miejsca itp.).

Wszyscy członkowie kolektywów wydali indywidualną zgodę na bycie obserwowanym. Dodatkowo co roku wnioskuję o zgodę na kontynuację badania na forum kolektywu (coroczne zebranie, związane z wyborem władz i kwestiami

finansowymi). Na wszystkich dotychczasowych głosowaniach kolektyw taką zgodę wyrażał w powszechnym głosowaniu członków. Miarą zaufania środowiskowego mogą być zaproszenia kolejnych grup do wizyty oraz prośby o włączenie do badania konkretnych sytuacji nieobserwowanych przeze mnie osobiście. W takich wypadkach archiwizowałem dyskusje z listy mailowej i realizowałem uzupełniające wywiady improwizowane, ukierunkowane na dany temat.

Podstawą do analizy były jednak strukturyzowane wywiady indywidualne (scenariusz modyfikowany przed każdym wywiadem oparty na dodatkowym kodowaniu materiału z obserwacji i e-maili, aby rozwinąć części zbieżne z zainteresowaniami/doświadczeniami uczestników badania), wywiady improwizowane (np. w momencie kontrowersji lub wizyty gościa) i nagrywałem rozmowy swobodne wokół konkretnych projektów. Analizą objąłem około 40 transkrypcji.

Dane analizowałem w programie MaxQDA w cyklach naprzemiennego kodowania otwartego i teoretycznego (zbieranie danych – kodowanie otwarte – praca konceptualna i literatura – kodowanie teoretyczne – kolejny etap zbierania danych jako walidacja). Kod główny „haker" obejmuje pracę nad operacjonalizacjami omówioną powyżej. Kody główne „laboratorium" i „strefa wymiany" to propozycje mające rodowód w STS. Kod „aktanci" to jednocześnie indeks ludzi i nieludzi (przydatny przy analizie ukierunkowanej np. przed wywiadem z daną osobą lub do śledzenia losów konkretnego projektu).

Jako element walidacji, w kwietniu 2015 roku przeprowadziłem też warsztat badawczy dla studentów[1]. Interesowało mnie spojrzenie osoby patrzącej na kolektywy ze świeżej perspektywy, ponieważ po dwóch latach uczestnictwa w środowisku mogłem przeoczyć pewne elementy, oczywiste dla osób spoza środowiska. Uczestnicy nie znali wcześniejszych analiz ani literatury przedmiotu, jednak potwierdzili główne tezy związane z modelami pracy i proksemiką miejsc (patrz część dotyczącą strefy wymiany).

Zebrany materiał opisuje większość działań w jednym z najbardziej ustabilizowanych kolektywów hakerskich w Polsce. Dzięki obserwacjom uzupełniającym mogłem przekonać się, że charakterystyka pracy poznawczej hakerów, jak i różnorodność zaangażowanych specjalności technicznych przedstawione w niniejszym tekście dotyczą w różnym stopniu wszystkich kolektywów w Polsce. Zarówno w obserwacjach uzupełniających, jak i w wywiadach, i dyskusjach mailowych powszechne było zainteresowanie drukiem 3D, nowymi odmianami elektroniki popularnej w rodzaju systemów Arduino oraz nastawienie na osobiste testowanie techniki.

[1] Osoby, które sporządziły noty i wzięły udział w dyskusji podsumowującej: Weronika Gawarska, Krzysztof Gubański i Justyna Kościńska. Noty z przeprowadzonych przez nich obserwacji zostały włączone do korpusu analizowanych danych.

Kto to jest haker? Kryteria operacjonalizacji

Wykorzystując wiedzę nauk społecznych dotyczącą hakerów, koncepcje teoretyczne zapożyczone z ANT oraz wnioski z fazy eksploracyjnej badania (wrzesień 2013–czerwiec 2014), proponuję następującą operacjonalizację: haker to człowiek, który spełnia co najmniej dwa z poniższych kryteriów:

Kryterium deskrypcji osobistej lub środowiskowej. *Jeśli w wywiadzie indywidualnym badany odpowiedział twierdząco na bezpośrednie pytanie. Ew. jeśli w trakcie obserwacji byłem świadkiem, gdy ktoś określił tym mianem danego badanego lub jeśli grupa badanych określiła się jako hakerzy*. Kryterium to ma uzasadnienie środowiskowe, ponieważ co najmniej 15 razy badani wskazywali, że „*Haker to osoba, którą ktoś inny nazwie hakerem*". Kryterium to spełniały też autodeskrypcje „maker, dłubacz, majsterkowicz" w odniesieniu do osób zaangażowanych w fab-laby i makerspace'y.

Kryterium etyki hakerskiej. *Jeśli w wywiadzie indywidualnym badany wskazał konkretne manifesty hakerskie jako istotne dla niego osobiście albo jeśli w wywiadzie indywidualnym lub w rozmowach swobodnych odwoływał się do wartości opisanych w ww. manifestach lub w klasycznej rekonstrukcji historii kultury hakerskiej według* Stevena Levy'ego (2010). Była ona wskazywana jako istotna w praktycznie wszystkich pracach omówionych wcześniej. Przykładowa wykładnia etosu hakerskiego wskazywana przez Levy'ego i parafrazowana przez badanych: wolność informacji, swobodny i bezpośredni dostęp do techniki komputerowej, komputer jako źródło piękna i rozwoju. Lista ta nie jest ani jedyną, ani ostateczną wykładnią etyki hakerskiej, więc korzystano też z innych koncepcji środowiskowych i akademickich (Coleman 2013; The Mentor 1986; Juza 2008), jeśli wersja proponowana przez badanego była im bliższa. Kryterium to uznawałem za spełnione, jeśli na analogicznej zasadzie pojawiały się odnośniki do manifestów fab-labowych (Gershenfeld 2007).

Kryterium bezpieczeństwa komputerowego. *Jeśli w trakcie obserwacji badany kilkukrotnie angażował się w czynności związane z bezpieczeństwem komputerowym lub haktywizmem.* Przykłady takich działań to: dyskusje o zabezpieczeniach danego typu sprzętu i udział w testowaniu odporności danego typu serwera na dany typ ataku, uczestnictwo w atakach pozorowanych (tzw. testy penetracji, przeprowadzane za zgodą właściciela sprzętu), udział w zawodach bezpieczeństwa komputerowego (tzw. *capture the flag*). Działania takie były wskazywane jako hakerskie przez ankietowanych jako wspólne punkty w trajektoriach edukacyjnych hakerów i cyberprzestępców (Chiesa i wsp. 2009).

Kryterium czarnej skrzynki. *Jeśli w trakcie obserwacji badany kilkukrotnie demontował i modyfikował sprzęt, realizował próby siły związane z elektroniką i techniką komputerową przy użyciu niestandardowych narzędzi lub dla niestandardowych celów.* W środowisku inżynierskim i hakerskim, proces

dekonstrukcji czarnych skrzynek często jest określany jako inżynieria odwrotna (*reverse engineering*), jako opis sytuacji, gdy mając dany przedmiot próbuje się ustalić zasadę działania. Przykładem obserwowanym w badaniu może być łamanie i rekonstrukcja zabezpieczeń automatu z napojami zakupionego ze składek kolektywu, aby przeprogramować go do sprzedaży innych produktów. Inny przykład to demontaż starych komputerów, pomiary oscyloskopowe wybranych części i konstruowanie nowego sprzętu na potrzeby lokalnego muzeum techniki. Standardowość oceniałem wedle wskazań środowiska (jeśli inni hakerzy określili dany projekt jako nietypowy), posiłkując się przy tym własnym wykształceniem inżynierskim oraz literaturą (Vinck 2009; van der Hoek i Petre 2014; Bucciarelli 1996). Określenie „czarna skrzynka" pojawiło się też in-vivo w wywiadach i nagranych rozmowach, co pozwoliło na walidację środowiskową niektórych działań (np. na ile wymagają tworzenia narzędzi ad-hoc, na ile są standaryzowane).

Konieczność spełnienia dwóch kryteriów jest celowa i służy do zawężenia stosowalności definicji. Nie wszyscy członkowie kolektywu hakerskiego muszą być hakerami, podobnie jak nie każdy specjalista od bezpieczeństwa komputerowego (kryterium 3) lub elektronik-majsterkowicz (kryterium 4). Jeśli jednak któryś z nich odwołuje się do etosu hakerskiego lub bywa określany przez innych jako haker, wtedy traktuję go jako hakera na potrzeby niniejszej analizy.

Ta sama operacjonalizacja posłuży do zdefiniowania kolektywu hakerskiego: Kolektyw hakerski to zbiorowość ludzi i czynników pozaludzkich, który wytwarza i jest wytwarzany przez hakerów, definiowanych jak powyżej. Kolektyw wytwarza hakerów, bo daje okazję do bycia ocenionym przez hakerów (kryterium 1), okazję do kontaktu z manifestami hakerskimi (kryterium 2), sposobność do nauki bezpieczeństwa komputerowego (kryterium 3) lub nietypowego stosowania techniki komputerowej (kryterium 4). Kolektyw jest wytwarzany przez hakerów, ponieważ ich działania są niezbędne do utrzymania czynników pozaludzkich tworzących zbiorowość (serwery, zamki, drukarki 3D, automaty z napojami). Relacyjność i wzajemność takiej konstrukcji mają uzasadnienie w założeniach ontologicznych ANT (Abriszewski 2008).

Hakerzy nie muszą być jedynymi osobami związanymi z kolektywem. W trakcie obserwacji odnotowałem liczne przypadki chwilowych sojuszników. Przykładem mogą być przedsiębiorcy zlecający hakerom prace związane z drukiem 3D lub bezpieczeństwem komputerowym, korzystający przy tym z kanałów komunikacyjnych wytworzonych przez kolektyw. Obserwacja ta stała się punktem wyjścia analizy kolektywu hakerskiego jako strefy wymiany, przedstawionej w dalszej części tekstu.

Hakowanie zyskuje dodatkowy wymiar społeczny, pojawia się nowy poziom pomiędzy pojedynczym hakerem i jego komputerami a całością kultury hakerskiej. Dotychczasowe prace (oprócz: Söderberg 2011a). korzystały z danych

opartych na wywiadach indywidualnych, a nie na obserwacji grup, stąd też przesunięcie analizy w stronę indywidualnych narracji.

Zarówno kolektyw hakerski, jak i haker są definiowani relacyjnie i performatywnie, co zgodne jest z założeniem ANT o unikaniu esencjonalizacji (Latour 2010). Powyższa operacjonalizacja nie powinna być traktowana jako „typ idealny" „prawdziwego hakera", jest raczej narzędziem istniejącym w kontekście konkretnego badania.

Perspektywa ta obejmuje też majsterkowiczów (kryterium czarnej skrzynki), pod warunkiem, że identyfikują się jako członkowie ruchu hakerskiego (kryterium 1) lub nawiązują w autodeskrypcjach do etosu tego ruchu (kryterium 2).

Ponieważ źródłem wiedzy dla badania były grupy zajmujące się bardziej różnorodną techniką niż w pracach Coleman lub Taylora, kryterium 4 odnosi się nie tylko do programowania, ale również do pracy ze sprzętem, drukiem 3D, czynnościami administratora oraz testera zabezpieczeń. Istotniejszy wydaje mi się tu sam fakt testowania granic (programów i systemów), samodzielne tworzenie narzędzi niż opisywanie konkretnych narzędzi hakerskich.

Przyjęcie perspektywy konstruktywistycznej pozwala na nowo spojrzeć na genezę luki bezpieczeństwa. Może być ona albo odkrywana, albo wytwarzana. Pierwszy porządek uzasadniania kieruje nas w stronę perspektywy realistycznej i zbliża hakerów do stereotypu naukowców, odkrywających prawdę o świecie. Drugi – zakłada, że użycie narzędzi i niestandardowych metod testowania raczej wytwarza zagrożenie, niż je odkrywa. W tym porządku wiedza jest traktowana jako konstrukcja w sensie ANT, a hakerom łatwiej przypiąć etykietę przestępców. Fakt przyjęcia jednego z tych dwóch porządków (realistycznego lub konstruktywistycznego) przekłada się na nieco inne rozpisanie sporu politycznego i etycznego.

Nie wszyscy hakerzy muszą wchodzić w skład kolektywu hakerskiego, co pozwala na uwzględnienie osób podróżujących między kolektywami, gości okazjonalnych oraz samotników. Większość analizowanych danych dotyczy procesów grupowych, ale zrealizowałem też kilka wywiadów z osobami, które sytuują się poza pojedynczym kolektywem.

Kolektyw hakerski jako laboratorium. Karnawał poznawczy

Praca serwerów zgromadzonych w hackerspace obejmuje procesy, gdy inskrypcje (np. logi internetowe, schematy programów, projekty techniczne związane z drukiem 3D) są gromadzone, zestawiane i przygotowywane do kolejnych mobilizacji. Część kolektywów używa tych danych do rekonstruowania samych siebie: np. zbiera dane z wykorzystania lokalnej sieci, anonimizuje je i zlicza, by na bieżąco informować o tym, ile urządzeń pracuje w danym momencie. W ten

sposób hakerzy mogą rozpoznać, czy spejs jest zapełniony lub pusty. Na podstawie tego mogą zdecydować się na wizytę towarzyską lub zaplanowanie „pracy cichej" (np. lutowanie wymaga koncentracji i względnego spokoju).

To, czy kolektyw w danym momencie okaże się warsztatem precyzyjnym czy przestrzenią towarzyską, zależy właśnie od szeregu działań, które przetwarzają inskrypcje dotyczące ruchu sieciowego (logger obciążenia sieci, program zliczający aktywność w danej jednostce czasu) i wizualizują je na zewnątrz laboratorium. Oczywiście w laboratoriach akademickich istnieją systemy zarządzania obłożeniem sprzętu (Latour i Woolgar 1986; Vinck 2009), ale najczęściej odnoszą się one do pojedynczych urządzeń, a nie do całego laboratorium. Rzadziej zdarza się też, że „zajętość" danego urządzenia jest traktowana jako pretekst do wizyty towarzyskiej.

Załóżmy jednak, że trafiliśmy na moment koncentracji, a nie na imprezę, choć w trakcie jednego wieczoru obie sytuacje mogą się przeplatać. Na pierwszy rzut oka zobaczymy od 4 do 10 osób pracujących w osobnych punktach (przy laptopach, przy urządzeniach). Część – jak sama przyzna – właśnie zdalnie reaguje na sytuację krytyczną w pracy zawodowej. Część testuje nową konfigurację sprzętu, korzystając z lokalnych serwerów. Część konsultuje coś na kanałach komunikacji internetowej, przegląda podręczniki programowania lub strony humorystyczne.

Niemal wszyscy obserwowani hakerzy pracowali głównie w interfejsach tekstowych z pominięciem dodatkowych manipulatorów (np. myszy). Polecenia wprowadzane były z klawiatury, najczęściej za pomocą skrótów uruchamiających dodatkowe skrypty. Część uczestników badania przyznała, że przejście z interfejsu graficznego na tekstowy było ważnym momentem w procesie stawania się hakerem. Samo korzystanie z interfejsu tekstowego nie jest oczywiście specyficzne dla hakerów, bo w podobnym trybie pracują też np. programiści lub specjalistki od symulacji ekonomicznych (Knorr Cetina 2009).

Specyficzny jest za to rytm pracy. Konstruowane są pojedyncze polecenia lub krótkie programy, bardziej złożona praca jest rozbijana na małe części, nawet jeśli pracuje nad nią tylko jedna osoba. Obserwowani hakerzy testują dany pomysł prawie natychmiast po jego opracowaniu. Dopiero, gdy kilka kolejnych prób zawiedzie (lub jeśli nastąpi poważniejsza awaria), haker rozpisuje schemat programu lub obwodu, wykonuje szacunkowe obliczenia lub sprawdza źródła. Mediacje hakerów z czynnikami nieludzkimi są ciągłe, oparte na krótkich komunikatach, a reakcja następuje zaraz po działaniu. Krótki cykl akcji i reakcji prowadzi do osiągnięcia tzw. stanu przepływu, w którym zaburzona jest percepcja czasu, zachodzi wyostrzenie koncentracji uwagi i wrażenie jedności z obsługiwanym sprzętem (Voiskounsky i Smyslova 2003), cenionego zresztą przez innych pasjonatów techniki komputerowej (Turkle 2005).

Z uwagi na tempo i złożoność zmian, różnice te trudno obserwować etnograficznie, pomóc mogłaby tu okulografia i narzędzia badań interakcji człowiek-komputer. W zasięgu etnografa było jednak zauważenie, że część hakerów próbuje stosować ten rodzaj podejścia do innych technologii (np. do druku 3D). Najczęściej nie dawało to rezultatów, bo plastik odpowiada wolniej niż oprogramowanie, trudniej też wycofać się z błędnej decyzji. Dopiero w trakcie kolejnych interakcji, haker uczył się modyfikować strategię działania, by np. dokonać szacunkowych obliczeń przed uruchomieniem drukarki.

Wracając do klasycznych elementów laboratorium, według tekstu „Dajcie mi laboratorium, a poruszę świat" (Latour 2009), zauważymy, że:

W kolektywie hakerskim łączą się różne interesy. Hakerzy dyskutują na temat czarnych skrzynek, czasami pojawi się zleceniodawca, aktywista lub osoba zainteresowana drukiem 3D. Przykładowe interesy to: zlecenie zaprojektowania nietypowego urządzenia pomiarowego składane hakerowi przez pracownika lokalnego instytutu badawczego, test nowej drukarki 3D, biznesmen szukający podwykonawcy.

Zdarza się, że kolektyw hakerski rekonstruuje czynniki pozaludzkie „na swoich warunkach". Lokalny serwer może być np. używany do testowania rozwiązania, które w firmie zatrudniającej danego hakera było zbyt ryzykowne. Inny przykład to tworzenie nowych połączeń w zaprojektowanym *ad-hoc* układzie elektronicznym. Dostęp do lutownicy, układów sterujących i pomocy jest często podawany jako podstawowy powód, dla którego warto przystąpić do kolektywu.

O ile otwieranie czarnych skrzynek jest częste, o tyle do rzadkości należy ich powtórne zamykanie (tworzenie dokumentacji, produkcja kolejnych urządzeń według standardu, dokumentacja charakterystyki pracy danego układu). Projektom hakerskim brakuje często dokumentacji, szkolenia użytkowników i kolejnych etapów stabilizowania techniki. W wywiadach i rozmowach hakerzy przyznają, że ich zainteresowanie często kończy się na poznaniu zasady działania lub przydatności wyłącznie dla nich samych. Dużo rzadziej dany przedmiot jest standaryzowany i badany na tyle długo, aby móc przekazać go „zwykłemu użytkownikowi". Obserwację tę potwierdzają też badania prowadzone w kolektywach hakerskich w Czechach (Söderberg 2011b).

Jako kwestię otwartą pozostawiam pytanie, czy te różne porządki rozumowania w kolektywie hakerskim odpowiadają podziałowi na oportunistyczne i symboliczne (Knorr Cetina 1981) lub też czy rozumowanie w trakcie szybkich iteracji jest podobne do refleksyjności rzemieślnika (Ferguson 1992). Porównanie twardych i miękkich faktów (Latour 1988) z twardymi i miękkimi odmianami interakcji z komputerem (Turkle 2005) również wymagałoby osobnej analizy.

Niezależnie od rozstrzygnięć tych problemów szczegółowych, widać, że perspektywa laboratorium współgra z proponowaną operacjonalizacją kolektywu

hakerskiego i pozwala spojrzeć na hakowanie jako działanie zbiorowości. Proponuję następujące podsumowanie tej ścieżki analizy:

Kolektyw hakerski ma cechy laboratorium (Latour 2009), w zakresie tworzenia nowych aktantów, prób siły i otwierania czarnych skrzynek. Perspektywa laboratorium kieruje uwagę w stronę różnych konfiguracji czasu, siły i przestrzeni – kwestii rzadziej obecnych w dotychczasowych badaniach hakerów.

Działania hakerów i czynników pozaludzkich bywają podobne do pracy naukowej, szczególnie dotyczy to pracy z inskrypcjami, prób siły i zbiorowego wytwarzaniu wiedzy. Koncentracja na inskrypcjach oraz różnych trybach rozumowania hakerskiego pozwala na spojrzenie na kulturę hakerską jako na osobną kulturę epistemiczną (Knorr Cetina 1999).

Cechą różniącą kolektyw hakerski od innych laboratoriów jest rzadsze konstruowanie czarnych skrzynek. Hakerom wystarczy samo dokonanie prób siły w systemach, nie mają potrzeby ich ponownej stabilizacji, zmiany w inskrypcje. Ograniczenie to nie wynika z braku zasobów, ale z braku zainteresowania hakerów stabilizacją przedmiotów i faktów.

Cechą szczególną dla kolektywów hackerskich, a mniej akcentowaną w uprzednich badaniach laboratoriów, jest humor i gwara środowiskowa. Zaobserwowałem, że haker często śmieje się lub obraża dany przedmiot w konsekwencji nieudanej próby siły. Często żartem i wyzwiskami opisuje też własne działania. Humor w kolektywie hakerskim służy nie tylko inkluzji/ekskluzji nowych członków. Moim zdaniem redukuje on koszty nieudanych prób siły – problemu dotąd niepodejmowanego przez ANT. Propozycja ta została pozytywnie walidowana w dyskusji z badanymi. Gabriela Coleman również obserwowała specyficzny humor hakerski, z tym że łączyła go z indywidualnym radzeniem sobie ze złożonością systemów, mniej akcentując rolę kosztów społecznych porażki (Coleman 2013, rozdz. 3).

Kwestionowanie gotowych rozwiązań oraz przechodzenie od żartów do intensywnej pracy sprzyjają wytworzeniu stanu, który nazywam „karnawałem poznawczym". Dowolna operacja może być zaproponowana i dyskutowana, hakerzy szybko przechodzą od koncepcji do pierwszych prób praktycznych. Propozycja, która w laboratorium formalnym mogła by się wydawać idiotyczna, tutaj zostaje szybko wyartykułowana i sprawdzona. Jeśli jest błędna, to dzięki humorowi koszty porażki są niższe, bo haker zawsze może stwierdzić: „To gówno to nie było na serio, tak sobie kucuję" (cytat z obserwacji). Porażka nie obciąża kariery zawodowej hakera, a ponieważ testy odbywają się na sprzęcie „z drugiej ręki", to nawet zniszczenie urządzenia nie ma istotnych skutków finansowych.

Kolektyw hakerski jako strefa wymiany

Problematyka wymiany była podnoszona zarówno w manifestach (Raymond 2001b), jak i w badaniach hakerów (Taylor 1999). W odróżnieniu od nich, zebrany materiał analizowałem nie tylko pod kątem wymian i darów pomiędzy hakerami, ale również wymian między różnymi kulturami epistemicznymi, w których hakerzy są pośrednikami, a kolektyw hakerski strefą wymiany.

Genezą dla podjęcia takiej analizy był fakt, że wiele z działań hakerów i sojuszników nie prowadziło do powstania nowych przedmiotów ani programów. Jak mówili uczestnicy badania, celem wielu działań w spejsie jest poznanie konkretnej technologii, przedmiotu lub programu – bez ambicji konkretnego i bezpośredniego zastosowania. Wychodziło to poza koncepcję latourowskiego laboratorium, choć niewątpliwie łączyło się z walidacją i stabilizacją wiedzy technicznej. Ponieważ zaobserwowałem wiele przypadków wymiany i dzielenia się wiedzą między specjalistami z różnych nurtów (np. między administratorem a uczniem liceum, albo między projektantem wydruków 3D a specjalistą od bezpieczeństwa komputerowego), konieczne było uzupełnienie perspektywy laboratorium o mechanizmy wymiany wiedzy.

Pojęcie strefy wymiany (*trading zone*) zostało zapożyczone z antropologii międzykulturowej, aby opisać rozwój fizyki cząstek elementarnych po 1945 roku (Galison 1997). Cechą charakterystyczną strefy wymiany według Galisona jest mieszanie teorii i metod wywodzących się z różnych dyscyplin. Jednocześnie poszczególne dyscypliny zachowują swoją odrębność poza strefą wymiany. Tymczasowości wymiany towarzyszy powstanie gwary lokalnej, przez Galisona określanej jako pidżin naukowy. Podobne sytuacje wymiany oraz pidżiny obserwowałem w kolektywach hakerskich.

Uczestnikami wymiany nie są pojedyncze jednostki, ale grupy połączone wspólnymi praktykami poznawczymi. Korzystając ze słownika STS, proponuję użycie koncepcji kultur epistemicznych (Knorr Cetina 1999), w której kultura jest opisywana w wymiarze performatywnym (np. analiza określeń stosowanych na zebraniach) i symbolicznym (analiza elementów składowych inskrypcji). Galison nie mógł przyjąć tego określenia, ponieważ zostało wprowadzone w dwa lata po publikacji jego książki.

Pierwszym uzasadnieniem przyjęcia takiej perspektywy jest rozmaitość obserwowanych sojuszników kolektywu hakerskiego. W trakcie obserwacji odnotowałem obecność: programistów, administratorów sieci, aktywistów prywatności, naukowców, osób z organizacji pozarządowych, anarchistów, elektroników, artystów, wojskowych i polityków. Część z tych grup konstruuje tożsamość opartą na innych dokumentach niż hakerzy. Część z tych grup miałaby zapewne problemy z wzajemnym porozumieniem się poza ramami kolektywu.

Jak wskazałem wcześniej, humor może służyć redukcji kosztów porażki, usprawniając nietypowe próby siły i propozycje w ramach laboratorium (w momencie, gdy w kolektywie są sami hakerzy). Może być też uzasadnieniem dla przyjęcia perspektywy strefy wymiany, bo humor i przekleństwa mogą łagodzić tarcia między różnymi grupami zaangażowanymi w wymianę wiedzy (np. różne standardy w różnych środowiskach programowania, kontakt między hakerami a akademią).

Trzecie uzasadnienie to kwestia ciągłości hakowania, pomimo zmian w technologii komputerowej, etyce hakerskiej i metodach łączności. Poszczególne kolektywy hakerskie mogą zostać unicestwione w każdej z tych kontrowersji (np. trudno spotkać dziś hakerów/cyberprzestępców atakujących centrale telefoniczne tzw. phreakerów), ale kultura epistemiczna zachowuje ciągłość. Współgra to też z opisami hakowania jako praktyki liberalnej (Coleman i Golub 2008), z tym, że przedmiotem negocjacji są nie tylko kwestie polityczne, ale też elementy epistemologii (kryteria prawdziwości, próby siły, kryteria stabilności dla danej czarnej skrzynki).

Osobną kwestią pozostaje ograniczenie stosowalności tej koncepcji w ramach późniejszych komentarzy autora (Galison 2010). Analiza tej problematyki wykracza poza ramy tego artykułu, stąd też sygnalizuję momenty, w których kolektyw hakerski nie jest strefą wymiany: Kiedy brakuje regularności w kontaktach między przedstawicielami danych grup. Wtedy wracałem do analizy jednostkowych przypadków, zgodnie z modelem kontrowersji proponowanym przez ANT (Latour 2010).

W momencie, gdy istniały przedmioty wspólne dla kilku grup, ale nie dochodziło do rekombinacji praktyk. W takich wypadkach stosowałem koncepcję obiektów granicznych (Star i Griesemer 1989), którą można uznać za pośrednią między ANT a strefą wymiany. Koncepcję tę wskazują jako zbliżoną do ich teorii zarówno Galison, jak i Latour.

Jeśli dochodziło do dyskusji o praktykach, ale bez wspólnych aktantów nieludzkich. Galison sugeruje użycie wtedy koncepcji doświadczenia interakcyjnego (*interactional expertise*) według Harry'ego Collinsa i Roberta Evansa (Collins i Evans 2007). Jak zostało to pokazane w innym miejscu, istnieją pewne problemy teoretyczne z pogodzeniem tego wariantu z ANT (Zaród 2015a).

W odróżnieniu od koncepcji proponowanej w książce *The Cathedral and the Bazaar* (Raymond 2001b), wymiana nie jest domeną racjonalnych ekonomicznie aktorów. Nie jest też ograniczona do kwestii otwartego / zamkniętego oprogramowania, ale również do wiedzy o bezpieczeństwie, elektronice, systemach społecznych itp. Mniejszą rolę odgrywa tu ekonomia daru lub aspekty współdzielenia, większą – wytwarzanie obszarów, w których różne kultury epistemiczne mogą ze sobą negocjować, zachowując jednocześnie odrębność. Szczegółową dyskusję między podejściem ekonomicznym a antropologicznym

do wymiany przeprowadził Peter Galison w późniejszym komentarzu metodologicznym (Galison 2010).

Podsumowanie. Perspektywy badawcze i zastosowania

W niniejszej pracy nie rozpatrywałem wszystkich możliwych problemów związanych z hakerami. Prace związane z etosem hakerskim, ekonomią współdzielenia, kontrkulturą czy sztuką były dla mnie elementami triangulacji rozważań dotyczących wiedzy, a nie były samodzielnymi problemami badawczymi. Niniejszy tekst stanowi próbę podsumowania głównego wątku badania, związanego z teorią aktora-sieci, etnografią laboratorium, inskrypcjami i wiedzą hakerską.

W świetle zebranych danych potwierdzam intuicję Gabrieli Coleman i Aleksa Goluba o hakowaniu jako praktyce liberalnej. Po zastosowaniu koncepcji zaczerpniętych z STS, stwierdzam, że praktyka liberalna hakerów dotyczy nie tylko kwestii politycznych, ale również stosunku do różnych porządków wiedzy. Klasyczny problem miejsca wiedzy w demokracji hakerzy rozwiązują poprzez rozproszenie i delegację autorstwa systemu, co trudne jest do pogodzenia z czarnymi skrzynkami produkowanymi przez formalne obiegi nauki i techniki.

Rozproszenie autorstwa i słabość mechanizmów stabilizacji wiedzy, które były analizowane pod kątem laboratorium, każą też krytycznie spoglądać na propozycje rozszerzenia kultury epistemicznej hakerów na inne obszary społeczeństwa, proponowane np. przez Himanena (2002). Sprzeczności wynikają nie tylko z charakterystyk kultur epistemicznych wytwarzanych przez hakerów, ale również z ustaleń teoretycznych STS. Stawia to pod znakiem zapytania nadzieje wiązane z hakerami artykułowane przez badaczy związanych z tradycją marksistowską i operaistyczną (szczegółowa polemika: Zaród 2015c).

Traktowanie kolektywu hakerskiego jako strefy wymiany nie wyklucza stosowania perspektywy laboratorium, a raczej uzupełnia ją. Laboratorium to momenty, w których hakerzy konstruują lub dekonstruują czarne skrzynki i wypracowują własne próby sił, z minimalnym udziałem zewnętrza. Kolektyw hakerski staje się wtedy kolektywem myślowym w sensie proponowanym przez Ludwika Flecka – hermetycznym środowiskiem specjalistów, mających własny, specyficzny styl myślowy i wytwarzającym wiedzę (Fleck 2014). Strefa wymiany to sytuacje, w których kolektyw hakerski staje się miejscem wymiany wiedzy między różnymi kulturami epistemicznymi. Być może to pozory „tymczasowości", „nieformalności" i „podziemności" kolektywu hakerskiego ułatwiają negocjacje między rzecznikami (w sensie latourowskim) różnych instytucji.

Elementy perspektywy laboratorium warte bardziej szczegółowej analizy dotyczą głównie inskrypcji, szczegółów specyfiki stabilizacji czarnych skrzynek

i proporcji mediacji/translacji. W obrębie strefy wymiany interesującym przypadkiem może być przejście od hermetycznej gwary hakerskiej do pidżinu zrozumiałego przez inne grupy.

Można się spierać, czy nie lepiej byłoby zastosować węższą, bardziej powszechną w dyskursie popularnym, perspektywę hakera jako cyberprzestępcy (Turgeman-Goldschmidt 2008; Taylor 1999; Chiesa i wsp. 2009) i ściślej skupić się na najbliższym kryminologii i technice zabezpieczeń komputerowych kryterium 3. Wiele z obserwowanych sytuacji, choć leżało w granicach prawa, dotyczyło bezpieczeństwa systemów publicznych. Przykładami mogą być: biały wywiad na temat różnych systemów szyfrowania, dyskusja i modele dotyczące zabezpieczeń kart płatniczych i systemów monitorowania zużycia energii, otwarte warsztaty dotyczące szyfrowania komunikacji elektronicznej. Odnotowano też przypadki komunikacji między służbami mundurowymi a kolektywami hakerskimi.

Choć wszystkie te działania mają kontekst kryminologiczny, z perspektywy kolektywu hakerskiego były równie rutynowe co np. projektowanie nietypowych drukarek 3D, warsztaty dotyczące krótkofalarstwa lub testy nietypowych urządzeń pomiarowych. Perspektywy laboratorium i strefy wymiany opisują szeroki zakres działań kolektywów hakerskich, w tym specyfikę konstrukcji i wymiany wiedzy. Dzięki temu nieco lepiej możemy zrozumieć rytm pracy, specyfikę wymiany wiedzy, podejście do standaryzacji i interakcje hakerów z instytucjami. Walidacja proponowanych koncepcji (np. elementów biografii, podejścia do czarnych skrzynek i rytmu pracy) w odniesieniu do indywidualnych pasjonatów bezpieczeństwa komputerowego może stanowić rozwinięcie niniejszego badania.

Wątkiem jedynie marginalnie rozważanym w niniejszym badaniu jest dysproporcja w liczebności między hakerami a hakerkami w obserwowanych kolektywach. Dysproporcja ta ma zapewne genezę w historii zawodów informatycznych i kulturowym stereotypie majsterkowania jako zajęcia męskiego (Margolis i Fisher 2002). Wydaje się jednak, że elementy stereotypu hakera mogą dodatkowo wzmacniać te wzorce. Hakerki i aktywiści równościowi dostrzegli tę asymetrię, inicjując rozwój feministycznych odmian kolektywów hakerskich (Toupin 2014), jednak nie zaobserwowałem takich działań w Polsce. Wydaje się jednak, że fab-laby i makerspace'y są przyjaźniejsze dla kobiet niż hackerspace'y. Potwierdzenie tych intuicji wymagałoby jednak dodatkowej triangulacji z użyciem perspektywy bardziej wrażliwej na nierówności płciowe niż ANT.

Innym wątkiem wartym rozwinięcia byłby stosunek hakerów do instytucji wytwarzających wiedzę z zakresu informatyki i techniki komputerowej. Odciąganie od studiów przez kolektywy ma odbicie w często powtarzanej w środowisku hakerskim maksymie „Jeśli trafiłeś do spejsu, to studiów nie skończysz".

Podobne doświadczenia powtarzały się w odniesieniu do kilku uczelni w Polsce i dotyczyły osób, które zostały specjalistami w swoich dziedzinach. Jednocześnie znane są przypadki, gdy kolektywy myślowe hakerów były wpisywane w edukację formalną (Cho 2008).

Rozwój nowych obszarów działalności kolektywów hakerskich obejmuje aktywizm polityczny (haktywizm, policy-hacking), biologię syntetyczną (biohacking) oraz obszar praktyk codziennych (lifehacking). Uczestnicy niniejszego badania deklarowali zainteresowanie każdym z tych obszarów, ale do sfery praktyki przeszły tylko pierwsze dwa. Na ile praktyki związane z modyfikacją sprzętu komputerowego mogą być przenoszone na inne obszary życia? Na ile kultura epistemiczna hakerów jest powiązana z inskrypcjami technicznymi? Na ile pośredniczenie w wymianie zmienia same kolektywy hakerskie? Tego rodzaju pytania warte są osobnych analiz. Należy jednak pamiętać, że przyjęcie koncepcji aktora-sieci jako metodyki zbierania danych, pociąga za sobą konsekwencje dla analiz teoretycznych, ponieważ nie wszystkie wyjaśnienia da się pogodzić z założeniami ontologicznymi ANT. Przykładowo: o problemach z godzeniem ANT z tradycją marksowską pisał Johan Söderberg (2011a).

Wiemy też z prac Taylora (1999), że kolektywy hakerskie są czasami przedstawiane właśnie jako zagrożenie dla cywilizacji, w procesach wytwarzania dewiacji znanych od czasów Howarda Beckera. Rozróżnienie środowiskowe na „podziemne" hackerspace i „neutralne" fab-laby zdaje się wspierać tę intuicję. Tym istotniejsze wydaje mi się podanie kryteriów operacjonalizacji i opieranie triangulacji na badaniach, a nie na stereotypach. Operacjonalizacja nie ma na celu obiektywności etnografii – ma jedynie na celu jawne pokazanie elementów wspólnych z innymi podejściami. Przesunięcie uwagi na kwestie produkcji wiedzy pozwala też na wytworzenie dystansu analitycznego wobec niektórych stereotypów i faktów związanych z hakerami.

Podsumowując: praca stanowi rezultat badania etnograficznego zrealizowanego w środowisku hakerów i miłośników techniki komputerowej w Polsce w latach 2013–2015. Wyniki zbierałem i analizowałem w ramach koncepcji aktora-sieci oraz innych ustaleń związanych ze studiami nad nauką i techniką. W świetle danych i analiz stwierdzam, że:

Narzędzia metodologiczne wypracowane w toku badania laboratoriów naukowych mogą być użyteczne do analizy tworzenia procesów przekształcania wiedzy, przedmiotów i ludzi w grupach spoza formalnych obiegów akademickich.

W kontekście badania kolektywu hakerskiego szczególnie istotna jest koncepcja czarnej skrzynki oraz łączące się z tym kryteria stabilizacji i destabilizacji wiedzy. Pozwalają one lepiej zrozumieć specyfikę łączącą procesy badania nieznanych systemów komputerowych oraz ich stabilizacji / destablizacji. Humor pozwala redukować koszty nieudanych eksperymentów hakerskich.

W obserwowanych grupach hakerzy pracowali głównie za pomocą szybkich iteracji kolejnych prób i błędów, rzadziej stabilizując ją i uogólniając za pomocą inskrypcji i teorii. Taka specyfika pracy sprzyja rozpoznawaniu nieznanych systemów, utrudnia jednak rozpowszechnianie zebranej wiedzy.

Kolektyw hakerski tworzy strefy wymiany między grupami mającymi różną specyfikę wytwarzania i walidacji wiedzy. Specyficzne dla hakerów jest to, że zarówno ułatwiają oni wymianę, jak i uczestniczą w niej jako osobna kultura epistemiczna. Destabilizacja przedmiotów może w praktyce oznaczać wyłączenie ich z pierwotnych systemów, co ułatwia wymianę wiedzy. Innymi słowy: redukcja zaplecza teoretycznego i nastawienie na wiedzę stosowną hakerów ułatwia pracę z przedmiotami i wiedzą z innych porządków.

Prymat osobistego doświadczenia i ciekawość to cechy zarówno dobrego badacza-socjologa, jak i hakera. Symetria ta sięga głębiej, bo hakerzy zajmujący się bezpieczeństwem komputerowym mają też mikroteorie socjologiczne dotyczące zdobywania dostępów do systemów dzięki ludzkim słabościom (tzw. inżynieria społeczna / social engineering). Skoro nie można zrozumieć techniki bez zrozumienia człowieka, to być może łatwiej będzie zrozumieć społeczeństwa, jeśli dokładniej spojrzymy na technikę? Być może socjolog lub socjolożka nauki mogą nauczyć się od hakerów właśnie tego, jak radzić sobie z czarnymi skrzynkami?

Literatura

Abriszewski, Krzysztof. 2008. *Poznanie, zbiorowość, polityka: Analiza teorii aktora-sieci Bruno Latoura.* Kraków: Towarzystwo Autorów i Wydawców Prac Naukowych „Universitas".

Alberts, Gerard i Ruth Oldenziel (red.). 2014. *Hacking Europe: From Computer Cultures to Demoscenes*. London: Springer.

Barnes, Barry i David Bloor. 1993. *Mocny program socjologii wiedzy*. Tłum. Z. Jankiewicz i in. Warszawa: IFiS PAN.

Becker, Howard. 2009. *Outisiderzy: Studia z socjologii dewiacji*. Tłum. O. Siara. Warszawa: WN PWN.

Bucciarelli, Louis L. 1996. *Designing Engineers.* Cambridge, MA: MIT Press.

Callon, Michel. 2014. *Społeczeństwo w procesie tworzenia: badania technologii jako narzędzie analizy socjologicznej*. Tłum. R. Sojak. W: E. Bińczyk i A. Derra (red.). *Studia nad nauką i technologią*: Wybór tekstów. Toruń: Wydawnictwo Naukowe UMK, s. 263–289.

Chełmiński, Michał i Edwin Bendyk. 2014. *Fraktale: Przypadki/Warszawski Hackerspace.* W projekcie: *Laboratorium żywej kultury/Metakultura, infrastruktura, akupunktura*. Warszawa: Bęc Zmiana. Https://spisekkultury.wordpress.com/fraktale-przypadki/przypadki-warszawski-hackerspace/ [dostęp 9.02.2017].

Chiesa, Raoul, Stefania Ducci i Silvio Ciappi. 2009. *Profiling Hackers: The science of criminal profiling as applied to the world of hacking.* Boca Raton, FL: Auerbach Publications.

Cho, Adrian. 2008. *Cryptography. University Hackers Test the Right to Expose Security Concerns.* „Science" 322: 1322–1323.

Coleman, E. Gabriela i Alex Golub. 2008. *Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism.* „Anthropological Theory" 8 (3): 255–77.

Coleman, E. Gabriela 2009. *Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers.* „Cultural Anthropology" 24 (3): 420–54.

Coleman, E. Gabriela. 2013. *Coding Freedom: The Ethics and Aesthetics of Hacking.* Princeton, NJ: Princeton University Press.

Coleman, E. Gabriela. 2015. *Hacker, Hoaxer, Whistleblower, Spy: The many faces of Anonymous.* London, Brooklyn, NY: Verso.

Collins, Harry i Robert Evans. 2007. *Rethinking Expertise.* Chicago, IL: University of Chicago Press.

Dupont, Benoit. 2013. *Skills and Trust: A Tour Inside the Hard Drives of Computer Hackers.* W: Morselli Claudio (red.). *Illicit Networks*. London, UK: Routledge, s. 195–217.

Farr, Nicholas. 2009. *Respect the Past, Examine the Present, Build the Future* (http://blog.hackerspaces.org/2009/08/25/respect-the-past-examine-the-present-build-the-future/, dostęp 8 sierpnia 2016).

Ferguson, Eugene S. 1992. *Engineering and the mind's eye.* Cambridge, MA: MIT Press.

Fleck, Ludwik. 2014. *Teoriopoznawcze rozważania nad historią odczytu Wassermana.* Tłum. M. Tuszkiewicz. W: E. Bińczyk i A. Derra (red.). *Studia nad nauką i technologią: Wybór tekstów*. Toruń: Wydawnictwo Naukowe UMK, s. 25–47.

Fleischmann, Katja, Sabine Hielscher, i Timothy Merritt. 2016. *Making things in Fab Labs: A case study on sustainability and co-creation.* „Digital Creativity" 1–19.

Galison, Peter. 1997. *Image and Logic: A Material Culture of Microphysics.* Chicago, IL: University of Chicago Press.

Galison, Peter. 2010. *Trading with the Enemy.* W: M. E. Gorman (red.). *Trading Zones and Interactional Expertise.* Cambridge, MA: MIT Press.

Gershenfeld, Neil A. 2007. *Fab: The coming revolution on your desktop—from personal computers to personal fabrication.* New York, NY: Basic Books.

Hess, David. 2014. *Ethnography and the Development of Science and Technology Studies*. W: P. Atkinson, A. Coffey, S. Delamont, J. Lofland i L. Lofland (red.). *Handbook of Ethnography.* Los Angeles, CA, London, New Delhi, Singapore, Washington DC: Sage, s. 234–246.

Himanen, Pekka. 2002. *The Hacker Ethic. A Radical Approach to the Philosophy of Business*. New York, NY: Random House.

Juza, Marta. 2008. *Kształtowanie się społeczności i kultury hakerskiej oraz ich znaczenie dla rozwoju Internetu.* „Studia Socjologiczne" 4(191): 67–89.

Juza, Marta. 2011. *Społeczność polskich pionierów Internetu i jej dokonania. 20 lat Internetu w Polsce*. „Studia Socjologiczne" 3(202): 8–28.

Knorr Cetina, Karin. 1981. *Manufacture of Knowledge: An Essay on the Constructivist and Contextual Nature of Science.* Oxford, New York, NY, Toronto, Sydney: Pergamon.

Knorr Cetina, Karin. 1999. *Epistemic Cultures: How the Sciences Make Knowledge.* Cambridge, MA: Harvard University Press.

Knorr Cetina, Karin. 2009. *The Synthetic Situation: Interactionism for a Global World*. „Symbolic Interaction" 32(1): 61–87.

Knosala, Bartłomiej. 2015. *Fablaby jako realizacja humanizmu technologicznego.* „Zeszyty Naukowe Politechniki Śląskiej" z. 85: 179–92.

Krapiński, Bartosz, Stanisław Szultka, Martyna Grabowska, Tomasz Szlendak, Władysław Zawistowski, Olga A. Marcinkiewicz, Jarosław Bujny i in. 2014. *Kreatywny łańcuch – powiązania sektora kultury i kreatywnego w Polsce.* Gdańsk: Instytut Badań nad Gospodarką Rynkową.

Kubitschko, Sebastian. 2015. *Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements.* „Convergence: The International Journal of Research into New Media Technologies" 21 (3): 388–402.

Latour, Bruno i Steve Woolgar. 1986. *Laboratory Life: The Construction of Scientific Facts.* Princeton, NJ: Princeton University Press.

Latour, Bruno. 1988a. *Science in Action: How to Follow Scientists and Engineers Through Society.* Cambridge, MA: Harvard University Press.

Latour, Bruno. 1988b. *The Pasteurization of France.* Cambridge, MA: Harvard University Press.

Latour, Bruno. 2009a. *Dajcie mi laboratorium a poruszę świat*. Tłum. K. Abriszewski i Ł. Aftelowicz. „Teksty Drugie" 1–2: 163–192.

Latour, Bruno. 2009b. *Polityka natury.* Tłum. A. Czarnacka. Warszawa: Wydawnictwo Krytyki Politycznej.

Latour, Bruno. 2010. *Splatając na nowo to, co społeczne: Wprowadzenie do teorii aktora-sieci*. Tłum. A. Derra i K. Abriszewski. HN Horyzonty Nowoczesności 72. Kraków: Universitas.

Latour, Bruno. 2012. *Wizualizacja i poznanie: Zrysowywanie rzeczy razem*. Tłum. A. Derra i M. Frąckowiak. „Avant" T: 207–257.

Latour, Bruno. 2013. *Nadzieja Pandory: Eseje o rzeczywistości w studiach nad nauką.* Tłum. K. Abriszewski i in. *Polityka w kulturze*. Toruń: Wydawnictwo Naukowe UMK.

Levy, Steven. 2010. *Hackers: Heroes of the Computer Revolution.* 1st (25th anniversary edition). Beijing, Cambridge, UK, Farnham, Koeln, Sebastopol, Tokyo: O'Reilly.

LoWalter-Herrmann, Julia i Corinne Büching (red.). 2013. *FabLab: Of machines, makers and inventors*. Bielefeld: Transcript-Verlag.

Margolis, Jane i Allan Fisher. 2002. *Unlocking the Clubhouse: Women in computing*. Cambridge, MA: MIT Press.

Maxigas. 2012. *Hacklabs and Hackerspaces: Tracing Two Genealogies*. „Journal of Peer Production" 2.

Raymond, Eric S. 2001a. *How to become a hacker* (http://www.catb.org/esr/faqs/hacker-howto.html, dostęp sierpień 2016).

Raymond, Eric S. 2001b. *The Cathedral and the Bazaar. Musings on Linux and Open Source by an accidental revolutionary*. Beijing, Cambridge, MA: O'Reilly. [Wyd. Popr.]

Schneier, Bruce. 2015. *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W.W. Norton & Company.

Sismondo, Sergio. 2010. *An Introduction to Science and Technology Studies.* Drugie wydanie. Chichester, U.K., Malden, MA: Wiley-Blackwell.

Söderberg, Johan i Alessandro Delfanti. 2015. *Hacking Hacked! The Life Cycles of Digital Innovation*. „Science, Technology & Human Values" 40: 793–798.

Söderberg, Johan. 2011a. *Free Software to Open Hardware: Critical theory on the frontiers of hacking*. Gothenburg: University of Gothenburg.

Söderberg, Johan. 2011b. *Free Space Optics in the Czech Wireless Community: Shedding Some Light on the Role of Normativity for User-Initiated Innovations.* „Science, Technology & Human Values" 36 (4): 423–50.

Star, Susan Leigh i James R. Griesemer. 1989. *Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39.* „Social Studies of Science" 19 (3): 387–420.

Taylor, Paul A. 1999. *Hackers: Crime and the Digital Sublime.* New York: Routledge.

The Mentor. 1986. „The Conscience of a Hacker." (Hacker's Manifesto). *Phrack Inc.* 3 (7). http://www.phrack.org/archives/issues/7/3.txt. [Dostęp: 13 czerwca 2016]

Toupin, Sophie. 2014. *Feminist Hackerspaces: The Synthesis of Feminist and Hacker Cultures*. „Journal of Peer Production" 4.

Turgeman-Goldschmidt, Orly. 2008. *Meanings that Hackers Assign to their Being a Hacker*. „International Journal of Cyber Criminology" 2 (2): 382–96.

Turkle, Sherry. 2005. *The Second Self: Computers and the Human Spirit.* 20th anniversary ed., MIT Press ed. Cambridge, MA: MIT Press.

van der Hoek, André i Marian Petre (red.). 2014. *Software Designers in Action: A Human-Centric Look at Design Work*. Boca Raton, FL: Taylor & Francis.

Vinck, Dominique. 2009. *Everyday Engineering: An ethnography of Design and Innovation. Inside Technology*. Cambridge, MA, London: MIT.

Voiskounsky, Alexander i Olga Smyslova. 2003. *Flow-based Model of Computer Hackers' Motivation*. „Cyber-psychology & Behaviour" 6 (2): 171–180.

Wark, McKenzie. 2004. *A Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Wasiak, Patryk. 2016. *Formalne i nieformalne obiegi wiedzy z zakresu nauki samodzielnego programowania komputerów domowych w Polsce*. W: *Historia informatyki polskiej [w druku]*.

Zaród, Marcin. 2013. *Fabryki edukacji: Laboratoria wytwórcze jako nowe narzędzie edukacji technicznej*. „Edukacja Biologiczna i Środowiskowa" 48 (4): 38–44.

Zaród, Marcin. 2015a. *Hacking Collective as a Trading Zone. Notes from the ethnography of hackerspaces in Poland.* „Kultura i Edukacja" *(w druku)* (4).

Zaród, Marcin. 2015b. *Polityka, organizacja i praktyki tworzenia wiedzy w kolektywach otwartego kodu*. „Praktyka Teoretyczna" 15 (1): 266–286

Hackers and Hacking Collectives in Poland. From Operationalization to Laboratories and Trading zones

Summary

The paper is a summary of ethnographical research on hacking groups in Poland, conducted within Actor-Network Theory approach between 2013 and 2015. In the first part of the paper, operationalization of a hacker is proposed. New proposal moves away from popular stereotypes, instead including concepts from social sciences, autodescriptions and results from exploratory phase. Proposed operationalization enables better description of Polish groups using names such as hackerspace, makerspace and fab-lab.

Second part includes analysis of material gathered within such operationalization, concentrating on processes of knowledge creation, conducted by hackers and hacking collective. By analysing hacking collective as a laboratory, analysis focuses on role of time, humour and stability. Mixture of instability and humour enables cognitive carnival, when costs of failure are lowered. Analysing hacking collective as a trading zone, focuses attention of mediations between different epistemic cultures and role of instability as a trade facilitator.

As a result of proposed operationalization, ethnography and analysis is not only a description of new group, but also a proposal of synthesis between studies of hacking cultures and constructivist studies of science and technology.

Key words: science and technology studies; hacker; hacking collective; actor-network theory; ethnography.