Helge Godø

Hacking som fenomen

NIFU skriftserie nr. 13/99

NIFU – Norsk institutt for studier
av forskning og utdanning
Hegdehaugsveien 31
0352 Oslo

ISSN 0808-4572

Forord

Denne rapporten er utarbeidet som ledd i et prosjekt om "Formgiving av virtuelle nøkler og rom i IKT: Konfigurering av teknologi, brukere og samfunn". Hovedtema i dette prosjektet er hvordan de nye, IKT-baserte nøklene og låsene (elektroniske passord, PIN-koder, smartkort, krypteringsalgoritmer, etc.) skapes – og hva som skiller disse produktutviklingsformene fra tidligere tiders mer konvensjonell produktutvikling. De IKT-baserte nøklene og låsene er av spesiell interesse fordi de i økende grad har fått innpass i, og regulerer våre moderne liv. Man kan dermed ane konturene av en nye type samfunnsorden som styres av de nye nøklene og måten disse er formgitt på. I denne utviklingstendensen representerer hacking – som er hovedtema i foreliggende rapport – en viktig faktor. Hacking forklares svært ulikt og utfordrer vår kunnskap om hvordan og hvorfor teknologi skapes. Dette forklaringsmangfoldet er fokus i rapporten, som er første i flere planlagte rapporter fra prosjektet om formgiving av IKT-baserte nøkler. Prosjektet er finansiert av Norges forskningsråd gjennom programmet SKIKT – Samfunnsmessige og kulturelle forutsetninger for IKT. Prosjektarbeidet utføres av Helge Godø.

Petter Aasen
Direktør

Egil Kallerud
Seksjonsleder

Innhold

1 Innledning - hacking som fenomen

Er hacking *bare* et "normalt", pubertertsrelatert ungdomsfenomen? Eller er det noe mer alvorlig: Er det et sosialt avvik, eller er det en mer grunnleggende politisk konflikt og motsetningsforhold i en teknologipreget samfunnsutvikling som utspiller seg? Representerer hacking en trussel i kampen om hvordan fremtiden skal se ut? Fordi hacking og IKT er nært knyttet sammen, og fordi det i økende grad synes som samfunnsutviklingen er påvirket av IKT-utviklingen, er analyse og forklaring av fenomenet hacking av interesse. Av denne grunn er det viktig å få bedre kjennskap til hva hacking er, fordi dette kan gi en type innsikt som utvider vår forståelse av IKT-utviklingen.

Forskningsstrategisk kan analyse av avvik og konflikter gi verdifull innsikt – ved å analysere *hvorfor* et avvik oppstår eller en konflikt skapes er det lettere å forstå *hva* det avvikes fra, eller *hva* som er konfliktgrunnlaget. Et avvik forutsetter noe bestandig – noe som er konstituert og legitimert som gyldig og riktig, vanligvis en norm, institusjon eller standard. Noen normer opprettholdes av makt og sterke interesser, andre fordi de har status av institusjoner og har dermed en selvfølgelig egentyngde som foreskriver kulturell mening, roller, adferd, verdikoder, etc. Kontrasten som et avvik blottlegger kan være et fokuspunkt hvor man kan søke å finne en forklaring på hvorfor et avvik oppsto. I analyse av konflikter gir stridstema et lignende inntak til forståelse av hva slags verdier som står på spill – hva man sloss om, og hvorfor. Hvordan striden utspilles kan også kaste lys over dyptliggende verdier, normer og idealer. Derfor er en analyse av hacking av interesse – uansett om man velger å kalle dette for et avvik eller mer grunnleggende sosial eller politisk konflikt, så vil en analyse kunne gi oss innsikt. Dette kan i sin tur bidra til å belyse *hvordan* fenomenet hacking analyseres og forklares.

Fenomenet "hacking" som egenbenevnelse i IKT-sammenheng oppsto i det spede for ca 40 år siden og har en utvikling som løper parallelt med IKTs moderne utvikling. Dette skal utdypes i neste kapittel, men selv om hacking har en historie som strekker seg over 40 år, er det også et flyktig og mangslungent fenomen – noe som bidrar ytterligere til dens flertydighet. Hvor mange personer som kan kalles for hackere, hvem som oppfyller kriteriene for denne betegnelsen – og hva som er kriteriene for å være en hacker, er flyktige og diffuse. På det ytre kan hacking analyseres som en typisk ungdomsbevegelse, i all hovedsak er det unggutter i senpuberteten som utgjør det store gross av hackere. Et annet kjennetegn er nær tilknytning til IKT-utviklingsmiljøer, både offisielle og uformelle, noe som forklarer at hovedtyngdepunktet er – og har alltid vært – i USA. Men ettersom både IKT og cyberspace har utviklet seg, har hacking blitt en internasjonal bevegelse. Enkelt sagt kan man si at overalt der det er datamaskiner, dukker det opp unge menn, magnetisk tiltrukket av datamaskiner og dens muligheter. I løpet av 1990-årene har et økende antall unge kvinner i samme alderstrinn blitt tiltrukket og i gavnet blitt hackere, selv om mange ikke liker denne benevnelsen. Etterhvert som mange datamaskiner og –systemer har fått tilknytning til hverandre gjennom forskjellige former for datanett, så har

hackerne slått følge – noen vil si at de sågar har vært pionerer og avantgardister i utviklingen av cyberspace, som i IKT-utviklingen ellers. Internetts raske utbredelse i 1990-årene har hatt stor betydning for hvordan hacking har utviklet seg de senere årene.

I analyser av forholdet mellom teknologi og samfunn inntar analyser av avvik og konflikter en forskningsstrategisk viktig rolle, enten det gjelder spørsmål om innføring av ståløkser i såkalt primitive (lavteknologiske) samfunn – eller, som fokus her, et høyteknologisk fenomen som hacking og IKTs samfunnsmessige og kulturelle rolle. Dette er spesielt viktig, fordi hacking har ikke bare en tett kobling til utvikling av IKT. Forklaringer av hva hacking er, spriker. Dette reflekterer vel så mye de forskjellige analytikeres holdninger til IKT og brukere/skapere av IKT, dvs. analytikernes egen fortolkningsfleksibilitet. I forlengelsen av det siste ligger det muligens grunnsyn om hvordan samfunn skal være, dvs. et normativt fundament som fargelegger brillene til den som analyserer – og heri – fortolkningsrammen for hva IKT er – og hva slags rolle den bør ha i samfunnet.

I denne rapporten vil jeg sette fokus på de forskjellige forklaringene av hacking. I gjennomgangen av den omfattende litteraturen, som også omfatter opplysninger og diskusjoner man finner i aviser, tidsskrifter (både på papir og på nettet) om hackere er det mulig å identifisere minst tre forklaringstyper på fenomenet hacking:

- *Juridisk-moralske forklaringer*, hvor hackeraktiviteter karakteriseres som kriminelle og subversive, fordi hackere ofte ulovlig tar seg til rette i IKT-systemer og begår andre handlinger av kriminell art, dvs. at hacking er en spesiell, til tider farlig form for ungdomskriminalitet, noen ganger med forbindelser til organisert kriminalitet,
- *Psykologiske forklaringer*, som ser på hackere som mistilpassede, umodne og emosjonelt mangelfullt utviklede individer organisert i subkulturer, der de utfolder hacking som en form for kompensasjon, dvs at både hackerne og deres aktiviteter kan forklares patologisk (slektskap med autisme antydes av noen), men at de kan volde stor skade på sine omgivelser, noe som forsterkes av at de ofte er intellektuelt svært begavede og derfor i stand til å være mer utspekulerte enn ”vanlige” kriminelle,
- *Kultur-idealistiske forklaringer*, som tar utgangspunkt i at hacking er en form for lek, den er intellektuelt og estetisk krevende, men som lek er den en av mange leketyper som særlig gutter i senpuberteten har en tendens til å oppsøke og dyrke intenst i en periode, så intenst at de noen ganger mister perspektivet på moralen og lovligheten av det de gjør.

I tillegg til disse tre forklaringstypene vil jeg prøve å utvikle en fjerde, en forklaringstype som tar utgangspunkt i hacking i et *politisk perspektiv*. Utgangspunktet for dette, som skal utdypes i et eget kapittel, er den slående likheten mellom hacking og tidligere tiders protopolitiske opprørsbevegelser, spesielt det som av Eric J. Hobsbawn har blitt betegnet som ”sosial banditvirsomhet”. ”Sosial banditvirksomhet”, med Robin Hood-skikkelsen

som mest kjente eksponent ("Ta fra de rike og gi til de fattige"), oppstår fordi en maktelite begår overgrep mot bondebefolkningen, ved å krenke dypfølte oppfatninger om rettferd, ære og eiendom. Både i hackere og i den klassiske sosiale banditt er et mulig å se klare fellestrekk i motiver, berettigelse, rekruttering og adferdsmønstrer. Det er også fellestrekk ved konteksten og omgivelsene. Hensikten med denne sammenligningen er å se om det er mulig å isolere noen politiske fellesfaktorer – dette for å undersøke om ikke den sterke gjennomsyring av IKT som foregår i mange samfunn i dag, når det kommer et stykke, skaper fellestrekk i reaksjonsmønster og dermed forteller oss mye om hvordan samfunnsutviklingen oppleves – og hvordan forskjellige grupper med ulike interesser i IKT ønsker at den skal være.

Fremstillingen i denne rapporten er organisert slik:

- i neste kapittel (kapitel 2) vil jeg beskrive hacking som et idealtypisk fenomen, med utgangspunkt i dens historiske opprinnelse,
- kapitel 3 vil presentere og utdype tre vanlige forklaringstyper av hacking, dvs de juridisk-moralske, de psykologiske og de kulturidealistiske,
- kapitel 4 tar for seg hacking i et politisk perspektiv, og som ledd i dette om hacking kan forklares som en protopolitisk bevegelse,
- til slutt, i kapittel 5, vil jeg oppsummere og drøfte de forskjellige forklaringstypene, samt skissere noen implikasjoner av disse for vår forståelse av IKT og samfunnsutviklingen.

2 IKT-hacking

«Hacking» har i løpet av de siste 10-15 årene fått en spesiell betydning i IKT-sammenheng. For folk flest betegner det den intense - noen ganger illegale - bruken av PC'er og data/telenett, oftest utført av unge menn og tenåringsgutter. Forestillingen om en «hacker» kan være ensbetydende med en «datanerd» - en noe keitete, meget skolebegavet mager unggutt med kviser og tykke briller som p.g.a. av sin IKT-lidenskap både er sosialt ubehjelpelig og går kledd deretter. I IKT-sammenheng er det imidlertid riktig å skille mellom en «klassisk», opprinnelig betydning og en annen, mer samtidig og populær betydning. Fokus her vil være på den siste betydningen av betegnelsen, dvs hacking som en intens lek, utforskning og utvikling av IKT som til tider kan anta ulovlige former p.g.a. ureglementert bruk av, og inntreden i, IKT-systemer. Fordi disse to betydningene ikke alltid er så lett å skille fra hverandre vil det innledningsvis være nyttig å belyse disse. Samtidig er det viktig å understreke stor likhet mellom disse to betydningene av hacking. Men viktigst er det at begge formene for hacking - og de subkulturene de utøves i - kan være et inntak til å fortolke IKT som en fenomen som kanskje har en dypere, grunnleggende politisk og kulturell forankring enn man kan ane på overflaten.

2.1 Klassisk hacking

Ifølge Steven Levy (Levy 1984) oppsto betegnelsen hacking[1] slik vi forstår det i dag, på MIT i USA, en gang på slutten av 1950-årene. Betegnelsen ble skapt av de unge, mannlige ingeniørstudentene som var medlemmer av MITs Tech Model Railroad Club (TMRC) - nærmere bestemt i klubbens «Signals and Power Subcommittee». TMRC disponerte et rom hvor de hadde plassert en stor modelljernbane. Mange av delene som modeljernbanen besto av hadde klubben fått som gaver, blant annet fra Western Electric, på denne tiden USAs gigant innen produksjon av teleutstyr og -komponenter. TMRC var organisert i forskjellig grupper og en av disse - «Signals and Power Subcommittee» - hadde ansvaret for «systemet» i modelljernbanen, dvs. sporveksler, signaler, releer, lys, svitsjing og hele kablingen som lå under bordet som den enorme modelljernbanen var plassert på. Levy skriver: «While someone might call a clever connection between relays [i modelljernbanen] a «mere hack», it would be understood that, to qualify as a hack, the feat must be imbued with innovation, style and technical virtuosity» (Levy 1984, s.23). Levy forteller at de mest ivrige av disse modelljernbaneentusiatene kalte seg selv for «hackers», altså på et tidspunkt som kan nærmere tidfestes til slutten av 1950-årene. Dette

[1] Avledet av verbet «to hack», har «hacking» følgende betydninger på engelsk:

- å hugge, hamre, slå eller skjære i stykker noe ved gjentatte, uregelmessige eller klossete slag,
- å ergre eller irritere noe(n)
- å bane seg vei ved å hugge eller skjære vekk hindringer, som i en jungel eller tett kratt,
- å mestre eller lykkes i et forsett.

Etymologisk er det nærliggende å tro at det norske ordet «hakke» har samme germanske opprinnelse som det engelske «hack» - i alle fall er det et visst overlapp i betydningen på moderne norsk og engelsk.

var omtrent samtidig som MIT fikk sine første datamaskiner. Hackerne fra TMRC fattet interesse for en av disse maskinene, TX-0, som de snart beleiret, særlig om kveldene og nettene, når maskinen ble lite benyttet av andre, mer "normale" brukere. Året 1959 går igjen som et viktig tidspunkt for grunnleggingen av det Levy kaller hacker-bevegelsen og den tilhørende uskrevne kode eller credo for hackere - «Hacker Ethics» - grunnreglene for hackeres forhold til datateknologi (Levy 1984, s. 39-49):

- *Tilgang til datamaskiner og berøring/mekking («The hands-on imperative») bør være ubegrenset og total - og overordnet alt.*
- *All informasjon bør være fri, dvs fullt tilgjengelig og gratis.*
- *Ikke stol på autoriteter - desentralisering bør oppmuntres.*
- *Hackere bør vurderes ut fra sine prestasjoner, ikke «falske» kriterier som akademisk grad, alder, hudfarge eller stilling.*
- *Du kan skape kunst og skjønnhet på en datamaskin.*
- *Datamaskiner kan gjøre livet ditt bedre.*

Det mest slående med Hacker Ethics er de politisk-ideologiske normene og de estetiske idealene. Dette skal utdypes nærmere nedenfor.

I Levys fremstilling (Levy 1984) skiller han mellom tre generasjoner av hackere som i grove trekk har til felles normene som er angitt ovenfor, men hvor teknologien de benyttet - dvs hacket på - var forskjellig:

- *«De sanne hackerne»* - Første generasjon av hackere, som tidfestes til slutten av 1950-årene og de tidlige 1960-årene - i hovedsak konsentrert til MIT-miljøet, med opprinnelse i TMRC, hvor programmering i maskinkode utgjorde en viktig aktivitet,
- *«Maskinvare-hackerne»* - Annen generasjon av hackere - i området rundt San Francisco - hvor bygging av de første små datamaskinene, forløperne til dagens personlige datamaskiner, var en dominerende aktivitet, tidlig i 1970-årene,
- *«Spill-hackerne»* - Tredje generasjon av hackere, tidlig 1980-tall også med hovedtyngde i California, men også andre steder i USA - hvor utvikling av dataspill var det viktigste.

Felles for disse klassiske hackerne var deres sterke ideologiske-estetiske overbevisning om IKT, slik Levy har formulert dette i «Hacker Ethics». Dette kombinert med en spesiell livsstil preget av total hengivelse til IKT gjør det mulig å spesifisere følgende kjennetegn:

- unggutt eller ung mann i senpuberteten, typisk i 16-20 års alderen,
- i en hackers forhistorie vil man finne at han fra tidlig alder (småbarn) utviste nysgjerrighet og interesse for teknisk/mekaniske/elektroniske innretninger og komponenter,
- stor lærenemhet i matematikk og naturvitenskap, ofte student på tekniske ingeniørhøyskoler eller ved universitetene, med naturvitenskapelige fagkretser,
- ofte fra hjem hvor en av foreldrene (oftest faren) hadde interesse for teknologi, som ble delt med sønnen,

- eksentriske interesser og adferd sammenlignet med til jevnaldrende barn og ungdom, sjeldent interessert i jenter og idrett - ofte isolert i forhold til jevnaldrende og deres ungdomskultur,
- oftest liten interesse for ungdomskulturens moter og konformitetspregede normer for utseende/forfengelighet.

2.2 Hacking som idealtype

Svært mange av disse kjennetegnene finner vi igjen også blant de mer moderne, samtidige hackere, slik at det er mulig (fristende) å betegne hackere som en *type* sosial kategori eller ungdom. Det finnes få *voksne* hackere - hackere vokser fra dette i løpet av 20-25-årsalderen - typisk overgang markeres ved at de inngår forhold til kvinner, får jobb og karriere, dvs. fanges av hverdagslivets tvang når de etter hvert kommer over i «ansvarlige» posisjoner i det bestående.

Foruten disse iøynefallende trekkene, er et annet kjennetegn deres sterke ideologiske og estetiske holdning til IKT - og mer indirekte - til samfunnet ellers. «Hacker Ethics» som Levy har utesket kan leses som et politisk manifest, men også som et estetisk manifest. Det politiske aspektet kommer sterkest til uttrykk som en dyp skepsis til autoriteter og hierarkiske organisasjoner med maktbruk, spesielt de som kontrollerer IKT-ressurser og informasjon.

Gitt hackeres primære fascinasjon og tiltrekning til IKT er det naturlig at enhver hinder for dette fremstår som et onde, noe som begrenser deres frihet til å få nærkontakt med alt som inngår i IKT, enten dette er maskinvare, kabling, selve systemet og nettverket, programvare - eller informasjons- og kommunikasjonsflyten i IKT-systmer. Systemadministrasjon - spesielt bruk av passordbeskyttelse som regulerer adgang - blir av hackere oppfattet som et onde - noe som legger kontroll og hindringer i veien for den frie utfoldelsen og muligheten til total teknologisk hengivelse. Sammenhengen mellom politiske og estetiske idealer er overlappende og flytende. Det er klart at hackeres primære motivasjon er tilfredsstillelsen, gleden og spenningen de får av å hacke. Dette inneholder mange aspekter, slik som mestring av kompleksitet, evnen til å «avluse» - finne feil i programvare, rette på disse - og forbedre dem, forenkle og dermed effektivisere eksisterende løsninger, lage tillegg og utvidelser som anriker en eksisterende funksjon eller teknologi, eller gir mulighet til helt nye anvendelser - eller, mest attråverdig, å skape noe helt nytt - noe som ikke har eksistert før - noe som er «new to the world», dvs en virkelig «oppfinnelse» som kan bli en innovasjon. Dette fordrer kombinasjon av tekniske og teoretiske IKT-ferdigheter og kreativitet, evnen til å skape og formgi - samt konsentrasjon og overnormal utholdenhet og arbeidskapasitet.

I beretninger om hackere fortelles det om hvordan de bokstavelig talt bor over eller i umiddelbar nærhet av sin terminal eller datamaskin - og arbeider til de stuper i søvn etter 30 timers arbeidsøkter. En konsekvens av dette er utvikling av arbeidsstil og døgnrytmer

som fort kommer helt ut av fase med «normale» dagsrytmer - noe som i seg selv kan være kilde til konflikt, f.eks. i bevoktede, offentlige bygninger som er stengt om natten, evnen til å følge studieprogresjon ved universitetskurs, oppmøte, ta eksamener, etc. Tidligere, da tilgang til datamaskiner var en begrensning, var dessuten det å hacke om natten gunstig, fordi da var maskinene oftest ledige og man kunne sitte uforstyrret.

I likhet med andre former for besettelse (f.eks. spillegalskap, narkomani, etc) vil en hacker oppfatte alle hindringer eller sperrer/begrensninger som et onde og trussel mot den utfoldelse hvor bare kroppens mest basale behov (søvn, mat og drikke og toalettbesøk) setter de eneste begrensningene. Hindringer blir dermed kilde og motivasjon for deres politiske ideologi: Full frihet, åpenhet og likestilling er idealet - enhver begrensning eller hinder for dette er et onde, slik som:

- passord,
- åndsverkbeskyttelse
- hemmelighold av kildekoder i programvare,
- betaling for telekommunikasjon når dette er nødvendig for å nå andre datamaskiner,
- tilgang til maskinvare,
- tilgang til verktøy,
- alle former for sensur eller begrensninger av ytringsfrihet.

Den estetiske dimensjonen er vanskeligere å definere, men sannsynligvis den mest grunnleggende. Problemet med å karakterisere estetikk er et generelt problem, slik man kjenner dette fra bl.a. kunstkritikk. Estetikk gjelder vage, lite definerbare faktorer som «skjønnhet» og «attraktivitet», dvs både er kvalitative og høyst subjektive. Estetikk har basis i hvordan en gjenstand eller hendelse oppleves - og er dermed flyktig. Men estetikk er også et sosialt fenomen og dermed gjenstand for forhandlings- og fortolkningsfleksibilitet for de som berøres eller ønsker å ta stilling til et estetisk spørsmål. Slik vil en estetisk standard eller kode bli etablert som en fellesverdi. For hackere - som utøvere av en ekstrem form for ingeniørkunst - synes det å være en del felles komponenter som inngår i deres estetiske kode. Disse er ikke spesielt unike fordi man vil finne disse som vanlige normer for hva som oppfattes som godt ingeniørarbeid - de skiller seg mest ut i intensiteten, dvs grad av ekstremitet og kompromissløshet, slik man ofte påtreffer blant utøvende kunstnere. Hva som øyensynlig skiller hackere fra «vanlige» ingeniører og andre skapende utøvere er - foruten intensiteten og utholdenheten i selve utøvelsen av aktiviteter og de spesielle sosiale kjennetegnene - den tette koblingen mellom deres estetiske kode og de moralsk-politiske idealene de forfekter. Man vil kunne si at hackere kombinerer ekstrem teknologisk estetikk og håndteringsvirtuositet med idealer om teknologisk anarko-kommunisme innen IKT. Videre er det mulig å hevde at de moralsk-politiske idealene til hackere er en konsekvens av deres kompromissløse estetiske standard og utfoldelsen av denne teknologiske besettelsen. Den estetiske koden kjennetegnes av følgende attributter:

- grunnleggende nysgjerrighet og fascinasjon av kunstige, menneskeskapte innretninger, spesielt elektroniske og elektromekanisk teknologi (releer, svitsjer, transistorer, mikroprosessorer, kretskort, programvare, etc),
- et begjær etter å forstå hvordan og hvorfor teknologi og programvare virker, både enkeltelementer og komplekse sammensetninger av disse, som i et telenett eller datasystem,
- begjær etter å manipulere og styre/mestre teknologi og programvare - og leke seg frem til slike ferdigheter gjennom taktil kontakt (hands-on),
- higen etter å perfeksjonere eksisterende tekniske elementer eller systemer, typisk gjennom:
    - «avlusning» (debuging) av programmeringsfeil eller,
    - forbedringer som kan øke effektiviteten av programvare, f.eks ved forenklinger,
    - øke funksjons- eller informasjonsmengden ved å legge til nye elementer,
- higen etter å skape noe helt nytt - en oppfinnertrang,
- eleganse, stil og kløktighet i utførelsen av det nyskapte, ofte med forbilder i spill, litteratur, musikk, film, tegneserier, billedkunst, etc.

De siste punktene, hvor de estetiske aspektene er særlig fremtredende, er også de som er vanskeligst å definere, men synes å kjennetegnes av følgende:

- *minimalisering (økonomi) og forenkling*, f.eks. forkorte en subrutine i et program fra 10 til 5 linjer og samtidig forbedre den,
- *elaborering og artikulasjonsutvidelse*, ved å finne frem til nye anvendelser eller uttrykksformer,
- *spektakulære effekter og uttrykksformer* - å skape sensasjonelle (bokstavelig talt) grafiske eller lydmessige effekter, slik som i utvikling av lek og spill på datamaskiner,
- *eksplorative bragder* mht omgå hindringer og stengsler for adgang til IKT-systemer,
- *vanskelighetsgrad og kløkt* mht prestasjonen

I tillegg til disse aspektene inngår det et sosial element, for i hacker-beretninger er anerkjennelse og omdømme fra andre utøvere (og et eventuelt publikum) en viktig faktor. Det siste er et kjennetegn man vil finne i svært mange prestasjonsorienterte utøvelsesformer, i kunst, idrett, vitenskap, håndverk og ingeniørkunst generelt. I de fleste grupper av utøvere («peer groups») vil man finne at disse forvalter et felles - om enn flyktig - sett av koder og standarder for hva som er verdifullt, aktverdig, vakkert - og, ikke minst, hva som representerer utfordringer og prestasjoner i forhold til disse. Slik er det også blant hackere - et gjennomgangstema i litteraturen om hackere er at de skryter uhemmet om det de oppfatter som egne bragder - og, noen ganger, er tilsvarende kritiske om andre utøvere, kolleger innen hacking.

3 Forklaringer av hacking

I innledningskapitelet ble det hevdet at i diskursene om hacking er det mulig å identifisere tre forklaringstyper. Det kan selvsagt ikke utelukkes at det finnes flere forklaringstyper – klassifikasjonen er, selv om den bygger på et omfattende materiale i litteraturen om hacking, basert på et kvalitativt skjønn. De tre forklaringstypene var:

- *Juridisk-moralske forklaringer*, hvor hackeraktiviteter karakteriseres som kriminelle og subversive, fordi hackere ofte ulovlig tar seg til rette i IKT-systemer og begår andre handlinger som oppfattes som avskyelige og kriminelle,
- *Psykologiske forklaringer*, som ser på hackere som mistilpassede, umodne og emosjonelt mangelfullt utviklede individer organisert i subkulturer, der de utfolder hacking som en form for perversjon,
- *Kultur-idealistiske forklaringer*, som tar utgangspunkt i at hacking er en forms for lek, den er intellektuelt og estetisk krevende, men som lek er den en av mange leketyper som særlig gutter i senpuberteten har en tendens til å oppsøke og dyrke intenst i en periode.

I tillegg til disse tre ble det bebudet en fjerde forklaringstype, der hacking forklares i et politisk perspektiv. I dette kapittelet vil jeg utdype de tre førstnevnte – den fjerde blir tatt opp og drøftet i neste kapittel.

3.1 Juridisk-moralske forklaringer

Denne forklaringstypen betrakter hacking som en type datakriminalitet – noen ganger sidestilles hacking med en form for terrorisme, dvs. som en særdeles ondsinnet, sadistisk og samfunnsfiendtlig aktivitet. Begge forklaringsvariantene synes å ha til felles at hackerens illegale aktiviteter, i mangel av et åpenbart økonomisk vinningsmotiv, best kan forstås som et ondsinnet, sadistisk og sykelig begjær etter ”noe”. Felles for disse variantene av denne forklaringstypen er at de demoniserer hackere.

Denne type forklaring er utbredt når hacking får mediaomtale. Typisk er sensasjonspregede oppslag om hackere som har snoket i databaser til NASA og CIA, eller ”tagget” hjemmesidene til New York Times. Gjennom reportasjer blir det skapt et bilde av hackere som konspiratoriske og farlige, ondsinnet, slik som i den såkalte ”HotMail”-skandalen i august/september 1999, som skal omtales nærmere i neste kapittel. I disse oppslagene er det ikke bare kategorien ”hackere” og deres aktiviteter som demoniseres – de mest aktive hackere fremstilles og blir behandlet som demoner som besitter særdeles ondsinnet magiske evner. Et eksempel på dette er Kevin Mitnick[2] som i sin tid figurerte på FBIs liste over ”Most Wanted” sammen med andre avskyelige kriminelle. Mitnick ble tillagt magiske evner, evnen til å forvandle vår fysiske verden ut fra en ond hensikt,

[2] Jfr. Aftenposten, 11/8-99, artikkel ”Kjendis-hacker soner til neste år”.

gjennom sine fingerferdigheter med PC'er og telefontastaturet. Da han ble arrestert i 1995, etter at han gikk i en mye omtalt felle satt opp av Tsutomu Shimomura[3], fikk han ikke lov til å slå nummeret på telefonen da han skulle ringe sin forsvarsadvokat – polititet var redd at han via telefontastaturet skulle slå et tall som ville forårsake ubotelig skade (for eksempel utløse en bombe, etc.). I denne forklaringstypen inngår ofte forestillingen om at hackere skaper og sprer sykdom – datavirus – som de med ondsinnet overlegg og list sprer i cyberspace, dvs. en form for biologisk, virale terrorisme som ødelegger datafiler, sletter hukommelsen på minnelageret, eller – mest alvorlig – får telefonsentraler til å bryte sammen. Fordi slike anslag er skapt og iverksatt ut fra overlegg, blir denne form for hacking forklart som grunnleggende samfunnsfiendtlig. Kjernen i den juridisk-moralske forklaringstypen er imidlertid at hacking er en type kriminalitet. Et typisk eksempel er teleoperatører som oppdager at noen har hacket telefonsentralen slik at bruken av telenettet ikke blir registrert eller er belastet en annen kunde. De vil mene at dette er kriminelle handlinger, at hackere (hvis de står bak) utfører aktiviteter som er svindel, tyveri og – i ekstreme tilfeller – terrorisme som på forskjellig vis underminerer teknologiske systemer av vital betydning for samfunnet. I deres beskrivelser av hvordan hackere arbeider brukes ofte benevnelsen "social engineering" om hackeres arbeidsmetoder. Dette vil si at de lurer godtroende folk i "systemet" til å oppgi passord, kontonummer, viktig teknisk informasjon, etc. ved å utgi seg for å være noe annet enn det de er – for så å bruke denne type informasjon til å trenge seg inn i ulovlig i databaser, telesystemer, etc. – ved bruk av falske identiteter. I likhet med demoner, inngår misbruk av ærlige, tillitsfulle folk i attributtene som kjennetegner en hacker.

En eksponent for denne type juridisk-moralske forklaringstype der hackere får demoniske attributter finner vi i Katie Hafner og John Markoffs bok (Hafner & Markoff 1993) om hackere, som utkom i 1994. I denne boken er det tre fortellinger om hackere, skrevet i en dokumentar-romanstil. Felles for disse hackerne er at de ble dømt til fengsel for sin virksomhet. Ved hjelp av opplysninger fra rettssakene (vitneavhør, uttalelser fra sakkyndige, etc. - dette har også vært kilde til grundige tekniske detaljer om hvordan den illegale hackingen ble utført), tegnes det et bilde av hackerne og deres gjerninger. Typisk for karakterbeskrivelsene av hackerne er at de har hatt en vanskelig, spesiell barndom og oppvekst (skilte eller sære foreldre, tidlig debut som lovovertredere, rotløs ungdomstid, etc) preget av ensomhet og normløshet – eller eksentrisitet. Med dette som mal tar boken oss med inn i de tre fortellingene.

I den første fortellingen er Kevin Mitnick hovedfiguren, men fortellingen omfatter også hans nærmeste sammensvorne Susan (som forrådte Kevin) og Roscoe. I fortellingene blir deres metoder og moralske gangsyn beskrevet – særlig fenomenet "social engineering". Forfatterne tegner bl.a. et bilde av Susan – som de påstår opererte som prostituert i tillegg - var flink med telesvindel og «social engineering»: «As a teenager, Susan had employed the technique she called psychological subversion, otherwise known as social engineering, to

[3] Shimomura har selv skrevet en artikkel om denne hendelsen, jfr. "Catching Kevin", *Wired*, februar,

talk her way into backstage passes at dozens of concerts». (Hafner & Markoff, 1993, s. 29). Boken utkom før den siste arrestasjonen av Mitnick, den som ble omtalt ovenfor. Det er nærliggende å tro at boken har medvirket til de forestillingene som ble skapt om Mitnicks magiske evner – det som gjorde at han ikke fikk lov til å slå telefonnummeret selv til sin forsvarsadvokat da han ble arrestert.

I den andre fortellingen blir handlingen lagt til Tyskland og omhandler en gruppe unge, tyske hackere, med Pengo som hovedperson, tidlig på 1980-tallet. Pengo var aliasnavnet på en hackerunggutt fra Berlin. Kjernen i denne historien var at ca 1986 dro en av guttene i gjengen til Øst-Berlin og prøvde å selge databaseinnhold, programvare, etc til Soviet-representanter der. Dette hadde de skaffet seg bl.a. ved ulovlig inntrenging i databaser, via datakommunikasjon. Fortellingen beskriver hvordan de forskjellige i denne gjengen jobbet - og at salgene til Sovjet hadde et tynt visir av en privat aksjon for å skape IKT-«balanse»-mellom supermaktene, dvs. et slags fredsskapende initiativ. Fortellingen dramatiseres med en parallell historie om Stoll, edb-ansvarlig ved Lawerence Berkely Laboratories, som overvåket alle innbruddsforsøkene, satte opp feller og bidro til å avsløre gutta i Berlin.

Den siste fortellingen omhandler RTM, dvs aliasnavnet (initialene) for hackeren Robert Tappan Morris - sønn av en NSA krypteringsekspert med fortid fra Bell Labs - som lagde en programsnutt (agent - også benevnt virus) som fikk over halvparten av Internett til å gå i spinn i november 1988 (Hafner & Markoff 1993, s. 382-443) . Denne rettssaken var særlig pikant p.g.a. farens posisjon og tilknytning til NSA. I fortellingen virker det som forfatterne har en viss sympati for RTM - at de ble sjarmert av ham, i motsetning til de andre de har skrevet om. De prøver å tegne et bilde av RTM som en meget begavet, men eksentrisk unggutt, som i en hackingrus mistet besinnelsen og moralsk dømmekraft – og at dette forklarer hans ugjerning. Altså mer enn en demon, en forvillet, overivrig unggutt som skapte en familietragedie for en meget respektabel slekt.

En annen variant av den juridisk-moralske forklaringstypen skiller mellom ”god” og ”ond” hacking, for så å beskrive teknisk detaljert hvordan de onde hackerne arbeider – om deres metoder og arbeidsstil – dette ut fra et motiv om å skjerpe It-ansvarlige årvåkenhet m.h.t. sikkerhetsrutiner og beskyttelsestiltak. I en lederartikkel i Scientific American (oktober 1998) ble det hevdet at man må kjenne til hvordan onde hackere arbeider for effektivt å kunne beskytte seg selv: ”Smart corporations, law enforcers and the military are listening. /…/ Vigilance and prudence can keep malicious hacking in check”. Ut fra dette publiserte Scientific American en artikkel av Carolyn P. Meinel[4] (Meinel 1998), hvor hun i en novelleform gir en teknisk detaljert beskrivelse av en ”krig” mellom en ond hacker, som kalles ”Abednego” og en ”god” hacker, ”Dogberry”. Dogberry er IT-ansvarlig i et stort firma og som hacker kjenner han alle triksene. Dette gjør det mulig for ham å sette inn

1996.

[4] Meinel blir i nevnte artikkel omtalt som øverste leder for en ”non-profit organization” som heter Happy Hacker Inc., som har til formål ”..to teaching people how to hack responsibly and legally”, jfr (Meinel 1998), s. 77.

mottiltak etter hvert som Abednego trapper opp sine anstrengelser for å trenge inn i de IT-systemene som Dogberry er ansvarlig for. Fortellingen avsluttes med at Dogberry får FBI til å storme Abednegos leilighet, hvor de beslaglegger utstyr (bevis i harddisken) – for til slutt å bli dømt til to års fengsel (uten å fortelle hvorfor Abednego ble dømt). I denne instrumentelle måten å forholde seg til hacking ligger det under at hacking kan være ”god” eller ”ond” – og om den er ”ond”, så beror dette på hackernes personlige egenskaper. Dette er en forklaringstype som leder hen mot neste forklaringstype: de psykologiske forklaringene.

3.2 Psykologiske forklaringer

De psykologiske forklaringene har hovedfokus på hackere som personlighetstyper og deres mentalitet. Bildet som tegnes av hackere er at de best kan forstås som sosialt og emosjonelt mangelfulle individer. Slike forklaringer synes å innta en sentral posisjon i kretser som er generelt skeptiske til den teknifiseringen av samfunnet som IKT-utviklingen innebærer. For disse fremstår hackere som representanter for en utviklingstrend – de representerer en skremmende avantgarde. Hackere representerer dermed en tendens – en tendens de frykter også fordi de fleste hackere er menn – og dermed bærere av en undertrykkende mannskultur. Allerede i 1984 utga Sherry Turkle en bok (Turkle 1984) som målbærer denne form for forklaring. Boken er bygget rundt studier av tre grupper av edb-brukere/skapere: barn og tenåringer, hackere og kunstig intelligens-miljøene - alle enten på eller i nærheten av MIT. Data om dette ble innsamlet i fra slutten av 1970-tallet og begynnelsen av 1980-årene. Boken er av spesiell interesse fordi den omhandler muligens de samme hackerne som var kilden til Levys bok (Levy 1984) – Levys bok utkom omtrent samtidig med Turkles. Turkles bok regnes fortsatt som banebrytende og autoritativ – og hennes forklaringer tillegges betydelig vekt. En sammenligning av Levys og Turkles bøker viser i all tydelighet hvor ulikt samme fenomen kan oppfattes. Dette gjør at Turkles bok er av spesiell interesse.

Sherry Turkles hovedpåstand er at hackere - i mer ekstrem grad enn «vanlige» ingeniører - har et dårlig selvbilde og at hacking må forstås som en kompensatorisk aktivitet. At hackere har et dårlig selvbilde underbygger hun bl.a. med informantrefleksjoner hvor en hacker forteller at han ser på seg selv som stygg. Ut fra dette spør hun: «Why are the computer-science students seen as the ugliest men or, when they are women, women who are somehow suspect?» (Turkle 1984, s. 200) For å forklare dette lager hun en dikotomi av begrepene ”science” og ”sensuality”. Hun mener at et viktig kjennetegn med hackere er at de identifiserer seg selv mest (mye mer enn andre) med ”science”. Dette kan forklare hvorfor de har avstengt seg fra omverden, til fordel for maskiner som «..demand perfection and are compelled by the controllable» (Turkle 1984, s. 201). Et kjennetegnet med hackere utdypes slik: «Most hackers are young men for whom at a very early age mastery became highly charged, emotional, colored by a particular desire for perfection, and focused on triumph over things». Og videre at de derfor «…are the holders of an esoteric knowledge, defenders on the purity of computation seen not as a means to an end but as an artist’s material whose internal aesthetic must be protected» (Turkle 1984, s. 207).

Mestring av datamaskiner og programvare inntar ifølge Turkle en helt sentral rolle i hackeres liv – de er besatt (addicted) av det å leke med spørsmålet om mestring og kontroll. Denne trangen forklares ut fra at hackere har problemer med å forholde seg til andre mennesker – hun beskriver hackeres tette forhold til sin teknologi som et forførende asyl, en kompensasjon for nederlag i den "normale", sosiale verdenen. Samtidig gir Turkle hackere anerkjennelse for at de har en ekstrem toleranse for stilavvik mht folks utseende, påkledning og væremåte (renslighet) - og at denne toleransen er grunnlag for fellesskap - og noe som ytterligere skiller dem fra de «normale». Dette blir oppsummert som hackeres respekt for hverandres «radikale individualisme».

Turkle forklarer hackeres dragning mot datamaskiner som deres eneste mulighet til å bli elsket: «The hacker culture appears to be made up of people who need to avoid complicated social situations, who for one reason or another got frightened off or hurt too badly by the risks and complexities of relationships» (Turkle 1984, s. 216). Hun bygger dette på informasjon fra hacker-gutter som har hatt dårlige forhold til jenter og mange nederlag: «..fundamental issue at the heart of the hacker's relationship with sexuality: the insistent antisensuality of the hacker culture» (s. 219). Samtidig anerkjenner Turkle at hackere oppebærer det hun kaller «computational aesthetic» og en enorm intensitet og nytelse knyttet til det. Men hun mener at dette er mekanisk, ikke-innlevende, «uekte» og asensuell. Hun mener dette aspektet kjennetegner et vidt spekter av hackeres aktiviteter og følelser (i den grad de har det). Dette kan forklare hvorfor hackere vil bryte seg inn i alle avlåste systemer - de dirker mekaniske låser (s. 232-234) og gjør skade på databanker. At hackere har det hun kaller ".. the fantasy of an electronic Robin Hood» (Turkle 1984, s. 235) er også et utslag av deres sosiale og emosjonelle ubehjelpelighet. Ut fra de observasjonene hun velger å fremlegge – og de tolkningene hun tilbyr om disse – er det i og for seg ikke overraskende at hun mener å se sterke fellestrekk mellom autisme og hacking. Hun sier ikke dette i klartekst, men benytter i stedet en kasusbeskrivelse fra psykologen Bruno Bettelheim av en autist – for så å peke på det hun mener er fellestrekk med de hackerne hun har analysert.

De to forklaringstypene vi har sett på – den juridisk-moralske og den psykologiske – har til felles en dyp bekymring over fenomenet hacking. I den første er det datakriminalitet og samfunnsskadelige aktiviteter som står i fokus. Den psykologiske forklaringstypen, foruten å inngå i teknologi- og fremtidsskeptiske diskurser, benyttes ofte for å forklare mannskultur. Argumentasjonen man ofte ser er at hackere skremmer vekk kvinner fra IKT, at især unge jenter som ønsker å utdanne seg i informatikk mobbes vekk av de ekstreme kravene og særhetene som hackere stiller til de ønsker å omgås. Ut fra dette kan det hevdes at hacking ikke bare er et utslag av sosial og emosjonelle mangler, men også er kvinnefiendtlige. Fordi hackere er en dominerende kraft i IKT-utviklingen betyr denne formen for ekskludering av kvinner at hacking i sin konsekvens diskriminerer kvinner, samtidig som de skaper en teknologi som reproduserer mannsdominans. Dermed ser man at to helt forskjellige forklaringstyper – den juridisk-moralske og den psykologiske, om

enn fra forskjellige premisser, kan være enige om en ting: En sterk skepsis til hacking og hackere. Imidlertid er det mulig å analysere fenomenet hacking på helt andre måter, og dette skal utdypes nedenfor, i det neste avsnittet og i neste kapittel.

3.3 Kultur-idealistiske forklaringer

I litteraturen om hacking finnes det en forklaringstype som prøver å fremstille hackere som primært kreative og intenst lekende i sitt forhold til datateknologi – og at dette er det viktigste utgangspunktet for å forstå hacking som fenomen. I disse fremheves de positive egenskapene ved hackervirksomhet, særlig hackernes intense og kreative eksperimentering og utvikling av datateknologi. Selv om dette er så intens og altoppslukende at det kan betegnes som et avvik som tiltrekker særlig eksepsjonelt begavede unge menn, så forsøker denne forklaringstypen å vise at hackervirksomhet er grunnleggende legitimt som prosjekt. Hackernes "feil" er at de – uten å være seg særlig bevisst de politiske perspektivene i dette – skaper en helt ny kultur, cyberspace. Hackernes innovasjonsevne kan virke som en provokasjon og trussel i konvensjonsbundne, konservative omgivelser – og mot etablerte maktbastioner som ønsker å definere IKT på sin måte, for å vedlikeholde sitt hegemoni og makt. Der de andre forklaringstypene ser hackervirksomhet som et arnested for datakriminalitet, så vil denne forklaringstypen peke på at hackere sjeldent blir dømt for de monstrøse anklagene som påtalemyndighetene, oftest i ledtog med gigantene i dataindustrien og teleselskapene, reiser mot dem. Når det kommer et stykke, så er de fleste hackere ganske uskyldige og harmløse. Videre, der hackere blir forklart som sosialt og emosjonelt mangelfullt utviklede unge menn som kompenserer for alle sine kvinne- og følelsesnederlag, så vil denne diskursen peke på at hackere – i likhet med andre unge idealister og aktivister – er så oppslukt av sine aktiviteter at utenforstående lett kan misforstå og patologisere dette engasjementet. De vil derimot hevde at hackere er idealister og utgjør en positiv og kreativ kraft i utviklingen av cyberspace, dvs. en helt ny kultur.

En analytiker som har prøvd å fremstille hackervirksomhet ut fra denne forklaringstypen, som man kan kalle en kultur-idealistisk forklaringstype, er Bruce Sterling, i en bok han utga i 1992 (Sterling 1992)[5]. Han ser mange likhetstrekk mellom hackere og de tidligere opposisjonelle (dissenterne) i de kommunistiske, østeuropeiske regimene – og han mener at hackere på samme måte er blitt forfulgt og demonisert, dvs. at de er blitt behandlet slik essensen i den juridisk-moralske forklaringstypen tilsier, dette p.g.a. en maktkamp om utformingen av cyberspace. Til tider har denne maktkampen vært en forfølgelseskampanje eller hekseprosess rettet mot hackere.

Utgangspunktet for Sterlings forklaring er fortellingen om massearrestasjonene som politimyndigheter gjennomførte i USA, tidlig i 1990 og 1991. Ofte skjedde arrestasjonene etter anvisning fra teleoperatøren AT&T. En hendelse som utløste dette var et omfattende

[5] Denne boken er også utgitt elektronisk – sommeren 1998 var den å finne på web: http://www.lysator.liu.s…ests/hacker/. Det er denne versjonen som ble benyttet i foreliggende arbeid og derfor blir sidehenvisningene ganske forskjellige fra bokens.

sammenbrudd av USAs telefonnett, 15. januar i 1990. Toppledelsen i AT&T, sikkerhetsfolk og påtalemyndigheter hadde mistanke om at sammenbruddet skyldtes hackervirksomhet, dvs elektronisk sabotasje. Senere viste årsaken seg å være en programeringslus i en sentral i Manhattan, som forplantet seg utover i telenettet og skapte sammenbrudd i halvparten av alle AT&Ts sentraler. Undersøkelsene viste at sammenbruddet skjedde i forbindelse med oppgraderingen av programvaren i en 4ESS-sentral (digital), under installasjon av ny programvare for signaleringssystemet (CCITT SS nr 7), hvor det var en logisk feil, en «break»-kommando som henførte til en «switch»-kommando. Dette fikk hele sentralene til å slå seg av og på hvert 4 sekund. Dermed forplantet feilen seg til andre sentraler, og 15. Januar i 1990 satte dette halve telenettet i USA ut av spill. Hackerne hadde ikke noe med dette å gjøre – det var programmererne i AT&T som hadde begått tabben. Disse opplysningene ble kjent først lenge etterpå, etter massearrestasjonen av hackerne.

I følge Sterling var massearrestasjonene tidlig på 90-tallet mest et symptom på en grunnleggende og skjult maktkamp om eierskapet til cyberspace og hvordan man skulle formgi dette, eller som Sterling selv formulerer det: ”Hacking had become too improtant to be left to the hackers. Society was now forced to tackle the intangible nature of cyperspace as property, cyberspace as privately-owned unreal-estate.”

Sterling gjetter på at det til enhver tid finnes ca 5.000 personer som kan kalles for hackere i USA – og av disse er det ca 200 personer han mener kvalifiserer til status som ”elitehackere”, dvs at de har så store datateknologiske ferdigheter at de fritt og ubemerket kan vandre inn i tungt beskyttede tele- og datasystemer. Men det er en konstant gjennomstrømning av folk i hackersamfunnet; en hackerkarriære starter gradvis, men vanligvis tidlig i tenårene, for så oftest å få en brå slutt i 22-års alderen, dvs. når unge i USA oftest fullfører sin college-utdannelse. «Hackers are generally teenagers and college kids not engaged in earning a living. They often come from fairly well-to-do middle-class backgrounds, and are markedly anti-materialistic (except, that is, when it comes to computer equipment)” (s 11 i utskriften). Sterlings definisjon av hacking er ”..a non-profit act of intellectual exploration and mastery”. Dette som en kontrast til elektronisk svindel, for eksempel tyveri av tellerskritt eller kloning av et mobiltelefonabonnement, dvs. lovbrudd begått i vinnings hensikt, som et kriminelt levebrød. For en hacker gjelder prinsippet om fri informasjon, noe ganger vil «fri» bety at «forbudt informasjon» er av spesiell interesse:

> *«..hackers are very serious about forbidden knowledge. They are possessed not merely by curiosity, but by a positive lust to know....the intensity of this desire, as mainfested by these young technophilic denizens of the Information Age, may in fact be new, and may represent some basic shift in social values - a harbinger of what the world may come to, as society lays more and more value on the posession, assimilation and retailing of information as a basic commodity of daily life.» (s. 21 i utskriften - Sterlings uthevelse).*

Videre, i tråd med Steven Levy tankegang, skriver Sterling at: «Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit», og at hackere «…of all kinds are absolutely soaked through with heroic anti-bureaucratic sentiment. Hackers long for recognition as a praiseworthy cultural archetype, the postmodern electronic equivalent of the cowboy and mountain man». (s 6 i utskrift). Hackere selv betrakter seg som en elite. De kan være beskjedne, men «..when they do talk, hackers tend to brag, boast and strut.» Dette fordi omtrent alt de gjør er usynlig, så hvis de ikke skryter, så vil ingen få greie på hva de har gjort. Og at hackere «..suffer from a strange obsession to *teach*» - (Sterlings uthevelse) - og de som blir arrestert, tilstår absolutt alt, selv hallusinasjoner - at det kan virke som de ber om å bli arrestert.

Etter massearrestasjonene av hackere i USA i 1990 oppsto det en debatt hvor hackere ble omfavnet av borgerrettsforkjempere, særlig de som forfekter et utvidet informasjons- og yttringfrihetsoppfatning. Et resultat av dette var stiftelsen av organisasjonen ”Electronic Fronier Foundation” (EFF) – med aktivisten og ex-rockeartisten (fra ”The Grateful Dead”) John Perry Barlow, han som populariserte begrepet ”cyberspace”. Blant mesenene for EFF finner man ”gamle” hackere som senere hadde skapt seg store, private formuer på sine innovasjoner, slike som Steve Wozniak (Apple Computer), John Gilmore (Sun Microsystems) og Mitchell Kaper (oppfinner av Lotus 1-2-3). Men hackerne selv, ifølge Sterling, har utvist lav bevissthet omkring disse prinsipielle, politiske perspektivene omkring hvordan cyberspace skal utformes: «Hackers do propagandize, but only among themselves, mostly in giddy, badly spelled manifestos of class warfare, youth rebellion or naive techie utopianism» (s.1)Videre: «As a political force, the digital underground is hamstrung».

Massearrestasjonene førte til en del tiltaler, med etterfølgende rettssaker. I en slik sak, den såkalte ”Neidorf-saken” gikk anklagen bl.a. ut på at hackeren, Craig Neidorf, hadde videreformidlet hemmelig teknisk informasjon, et ”E911”-dokument fra telefonselskapet Bell South, et selskap i AT&T-sfæren. Aktoratet stilte i rettssaken med representanter fra Bell South som sine kronvitner. Craig Neidoft var medredaktør av en elektronisk oppslagstavle/nyhetstjeneste for hackere som het *Phrack*. Nærmere analyse av dette dokumentet (9 sider) viste at det var en beskrivelse av, og administrative retningslinjer for, en nødtelefontjeneste med oppkallsnummer 911 (tilsvarende 113 i Norge). Dokumentet inneholdt ikke noe teknisk informasjon, langt mindre informasjon som kunne brukes til ulovlig inntrenging i telesystemer. Men dokumentet var bedriftsinternt og Bell Souths intellektuelle eiendom – og det hadde på en ureglementert måte havnet hos *Phrack*, som av prinsipielle grunner lot den ligge fritt tilgjengelig i databasen sin. I følge Sterling, som gjengir hele E911-dokumentet, var det helt andre ting som sto på spill enn innholdet i dokumentet: «The real struggle was over the control of telco language, the control of telco knowledge» - at teleselskapene som establishment i sine bestrebelser på å beholde total hegemoni, overhode ikke ønsker noen form for innsikt, og hadde greid å overbevise påtalemyndighetene om at hackernes videreformidling av E911 var en trussel.

Noen år etter massearrestasjonene var de fleste hackerne frikjent eller straffet med milde, symbolske straffer. I følge Sterling blamerte politi og etterretningsvesen seg med de voldsomme razziaene og arrestasjonene - at når "bevisene" ble lagt frem for domstolene hadde anklagene blitt betydelig redusert og banalisert i forhold til opprinnelige anklager. Sterling mener at hackere har en apolitisk bevissthet – at de ikke forstår, eller bare i liten grad evner å artikulere den politiske dimensjonen i det de gjør. Dette fordi deres primære prosjekt er å leke, utforske og skape nye anvendelser av datateknologi. Denne oppfatningen finner vi igjen i en analyse av norske hackere, utført av Tove Håpnes (Håpnes 1996), i det hun kaller de enkelte hackeres *scenario'er,* som betegnelse på hackerens visjon og ambisjon om sine aktiviteter. Håpnes beskriver en gruppe informatikkstudenter, muligens ved NTH, som tilbringer mye tid i skolens Software Workshop. Håpnes fant at hackere var intenst opptatt av konkurranse og lek, spesielt spill. Hackere betrakter seg selv som skapende edb-brukere, og at de derfor etterstreber så stor frihet som mulig – og at de betrakter seg selv som "designers of technology" (s 139). Dette fenomenet kaller Håpnes for *domestisering*[6], for å betegne den kreative prosess som hacking er, eller som hun selv skriver: "…our hackers say it is important to have an artistic approach, to be creative, to proceed tentatively, to look for what fits, to experiment..." (s.139-140). Hun mener at hackere oppfatter seg som et fellesskap (s. 140) – som hun betegner som en "anarchistic subculture" - en sosial habitat. Dette, som tilsynelatende kan stå i et motsetningsforhold til de sterke innslagene av individualisme, lek, skapende utfoldelse og eksperimentering hos hackere, forklarer hun som "..a more complex male machine-culture than that we may find described ..."(s.146). P.g.a. dette og andre faktorer som bidrar til kompleksiteten velger hun å kalle hacking som et tvetydig (ambigious) prosjekt. Slik sett ser vi at de kulturidealistiske forklaringene peker på at hacking, som et prosjekt, til tross for sin eksplosive kreativitet, livsstil og energi, kan forklares som et fenomen uten sterke politiske ambisjoner og blottet for kriminelle motiver. Dette kan forklare hvorfor Håpnes mener at hacking er tvetydig – og dermed egentlig er i overensstemmelse med Sterling og hans observasjon om lav politisk bevissthet blant hackere, men som, nettopp p.g.a. sin virksomhet, blir dratt inn i det politiske – fordi de uforvarende har vandret inn i et territorium der makt og politikk er viktig.

3.4 Oppsummering av forklaringstyper

Dette kapittelet har tatt for seg tre forklaringstyper som man kan finne i diskursene om hacking som fenomen. De tre var:

---

6 Domestisering som begrep brukes vanligvis for å betegne den foredling/videreutvikling som utføres når en art overføres fra en "vill" tilstand til en samfunnskontrollert tilstand, slik som domestisering av kyr, ris, etc. – at noe som er vilt blir tamt. Det kan diskuteres om denne analogien er fruktbar for teknologiutvikling, som i utgangspunktet er kunstig og menneskeskapt, men intensjonen er kanskje å betegne den sosiale overtakelsen, appropriering, som skjer når nye grupper tar i bruk teknologi som de tidligere ikke har brukt, for så å videreutvikle den.

- *Juridisk-moralske forklaringer*, hvor hackeraktiviteter karakteriseres som kriminelle og subversive, fordi hackere ofte ulovlig tar seg til rette i IKT-systemer og begår andre handlinger som oppfattes som avskyelige og kriminelle,
- *Psykologiske forklaringer*, som ser på hackere som mistilpassede, umodne og emosjonelt mangelfullt utviklede individer organisert i subkulturer, der de utfolder hacking som en form for perversjon,
- *Kultur-idealistiske forklaringer*, som tar utgangspunkt i at hacking er en form for lek, den er intellektuelt og estetisk krevende, men som lek er den en av mange leketyper som særlig gutter i senpuberteten har en tendens til å oppsøke og dyrke intenst i en periode.

Det interessante med disse tre forklaringstypene er hvordan samme empiriske utgangspunkt kan lede til helt forskjellige fortolkninger. I den psykologiske forklaringen ser vi hvordan Sherry Turkle tegner og fortolker de samme hackerne som sannsynligvis dannet basis for Steven Levys beskrivelse av de klassiske hackerne (jfr. kap.2) – hans forklaringer ligger nærmest det vi har klassifisert som den kultur-idealistiske forklaringstypen. Der en analytiker (Turkle) ser emosjonelt og sosialt mangelfullt utviklede sære unggutter – ser andre de samme unggguttene som kreative og intenst lekende – og at de nærmest uforvarende sprenger grenser. Grensesprengning kan også oppfattes som noe kriminelt og moralsk forkastelig – fordi etablerte normer, hegemonier, lover og koder trues. Det som i et innovasjonsperspektiv vil kunne oppfattes som paradigmeskiftende kan altså også oppfattes som noe subversivt og et patologisk avvik. Dermed ser vi hvordan et fenomen som hacking – avhengig av analytikeren og hans/hennes ståsted – ikke bare skaper forskjellige forklaringer av samme empiriske representasjon, men at disse forklaringene også sier mye om hvordan de mener verden bør være – og hva som skal være retningsgivende for dette. Dette betyr at forklaringstyper som betoner de politiske aspektene er av interesse, at de politiske perspektivene må trekkes inn i forklaringen av hacking som fenomen. Dette er spesielt utfordrende fordi, som Sterling påviste, er den politiske bevisstheten til hackere ikke på et ideologisk artikulasjonsnivå som man forventer i et politisk program. Allikevel er det opplagt at hackere, ut fra det de gjør og mener er viktig her i verden, har et politisk budskap og utfører politiske handlinger. Dette blir tema for neste kapittel.

4 Hacking som politisk fenomen og protopolitisk bevegelse

4.1 Innledning – kan hacking være politisk?

I dette kapittelet skal fokus settes på hacking som politisk fenomen. Fremgangsmåten som vil bli benyttet er først å presentere et case – den såkalte "HotMail-skandalen" som utspilte seg i august/september 1999. Hensikten med dette er å vise et typisk eksempel på en hackeraksjon. Dernest vil jeg presentere en analytisk tilnærming som forklarer det protopolitiske fenomenet "sosial bandittvirksomhet". Dette etterfølges av en analyse og drøfting av om hacking som politisk fenomen – belyst med eksempler fra HotMail-skandalen og andre eksempler. Til slutt vil jeg drøfte om denne tilnærmingen er fruktbar.

Makthavere og etablerte sosiale grupper har til alle tider oppfattet at "andre" som på forskjellige måter prøver å unndra seg deres maktutøvelse, regler, kontrollstrategier og normer, er subversive eller destruktive. Mange karakteristikker brukes om disse: Kriminelle, asosiale avvikere, terrorister, etc. Som vi så i forrige kapittel er dette kjernen i den moralsk-juridiske forklaringstypen, altså en forklaring basert på et bestemt maktperspektiv, sett fra de som innehar makt eller forvalter makt, dvs. deres ståsted. Men det er også mulig med helt andre politiske perspektiver og utsiktspunkter. En tilnærming er å lytte til hva hackere selv sier og analysere deres budskap og handlinger. Det bildet man da får fortoner seg ganske forskjellig fra det man finner i de moralsk-juridiske forklaringene. Det ligger også helt utenfor det man finner i den psykologiske forklaringstypen. I de kultur-idealistiske forklaringene så vi hvordan lek og kreativitet ble fremhevet som det viktigste med hackeres virksomhet – og at hackernes politiske ambisjoner ble bagatellisert som ubehjelpelige fordi de mangler en eksplisitt ideologi og er blottet for plan, strategi og konkrete politiske ambisjoner. Om enn ubehjelpelige er det allikevel påfallende at hackere nettopp har sterke politiske budskap og handler politisk. I stedet for å overse dette kan det være fruktbart å undersøke nærmere hva slag politiske aspekt som ligger i hacking – dette som et grunnlag for å karakterisere hacking som et politisk fenomen.

4.2 HotMail-skandalen

I månedsskiftet august/september 1999 brakte media nyheten om at hackere igjen hadde slått til – denne gangen mot HotMail – noe som raskt ble forklart som et anslag mot MicroSoft og Bill Gates, som eier HotMail. Under overskrifter som "Terroristangrep på MicroSoft"[7] ble leseren fortalt – i ingressen – at "Den kybernetiske terrorismen har rettet sitt hittil kraftigste og mest vellykkete angrep på den digitale tidsalderens mest totalitære

[7] Dagsavisen, 1.9.1999

regime, MicroSoft". En annen overskrift fortalte at "HotMail-hackere presser MicroSoft"[8]. I de første meldingene forklarte media at hackerne hadde fjernet passordbeskyttelsen og andre hindringer i påloggingsprogramvaren, slik at de enkelte brukerområdene kunne åpnes av alle og enhver – dvs. at de som ville, kunne fritt gå inn i andres postkasser og lese alle meldinger der. HotMails eposttjeneste er meget populær fordi den er gratis for brukerne (reklamefinansiert) og den har ca 50 millioner brukere fra hele verden, hvorav 280.000 brukere er i Norge. HotMail var altså vid åpen. I følge en melding i *Wired News*[9] var det en hittil ukjent gruppe som kalte seg "Hackers Unite" som påsto at de hadde manipulert HotMail. Gruppen hadde via sin talsmann, en 21 år gammel svensk mann (i andre meldinger ble han omtalt som 18 år gammel) bosatt i Gøteborg med navn Lasse Ljung, alias "DarkWing", uttalt til den svenske avisen Aftonbladet at hensikten med "innbruddet" i HotMail var å avsløre hvor dårlig MicroSofts sikkerhet egentlig er – og at MicroSoft har et tilnærmet monopol på all programvare. Hensikten var altså både å ydmyke og avsløre giganten MicroSoft. Etter hvert som det kom frem mer informasjon, ble det kjent at Hackers Unite besto av åtte personer fra USA, Israel, Filippinene, Sverige og Norge – og at disse tilhørte "internasjonale hackerorganisasjoner"[10]. De hadde ifølge samme melding greid å trenge seg inn i en av serverene (databasemaskinene) til HotMail to uker før saken ble kjent i media. Både inntrengningen i HotMail og samarbeidet mellom medlemmene i Hacker Unite hadde foregått via Internett, på et såkalt "chat-network" – altså i cyberspace.

I "HotMail-skandalen", som enkelte aviser straks døpte denne hendelsen, ble det etter hvert sådd tvil om "sikkerhetshullet" i loginprogrammet var resultat av hackernes manipulasjoner, dvs. om de hadde omprogrammert denne programvaren, eller om det "bare" var et "smutthull", dvs en eksisterende, men lite kjent loginprosedyre uten vanlige beskyttelsessperrer, som hackerne hadde oppdaget. MicroSoft fremsatte en påstand, via sitt talerør i webavisen *MSNBC.com*, om det siste – med antydninger om at hackernes bragd var betydelig overdrevet – at sikkerhetshullet hadde vært der hele tiden og skyldes en tidligere, hittil ukjent programeringstabbe hos MicroSoft/HotMail[11], dvs. dårlig kvalitetssikring fra HotMails side. Dette utspillet fra MicroSoft var opplagt beregnet på avdramatisering og trivialisering av det som ble utlagt som en hackerbragd utført av Hackers Unite.

---

8 Nettavisen, 1.9.1999.

9 jfr. http://www.wired.com/news: "HotMail Hackers: "We did it"" (30.8.1999, kl 1600).

10 jfr. Nettavisen, 2.9.1999, kl 0610: "HotMail lå åpen i 14 dager".

11 Jfr. http://www.msnbc.com/news/307118.asp – "Hotmail: Case of the phantom hacker" – 2.9.1999, kommentarartikkel av Kevin Poulsen.

4.3 "Klassisk" sosial banditvirksomhet som protopolitisk bevegelse

Eric J. Hobsbawns klassiske analyse fra 1960-tallet (Hobsbawn 1972) kastet et nytt lys på fenomenet banditvesen – og hans perspektiver kan danne utgangspunkt for et nytt perspektiv på hacking. Hans påstand var at banditvesenet er universelt – man finner det i så og si alle land, og at banditten som sosial person kan forklares ut fra politisk protest og opprør/aksjon rettet mot det som oppfattes som en dyp urettferdighet og krenkelse av menneskelige og kulturelle verdier. Den mest kjente prototypen på denne skikkelsen finner vi i legenden om Robin Hood[12] – han som ved å "ta fra de rike og gi til de fattige", fremsto som den egentlige godhet og frigjører. Dette i kontrast til de grådige og hjerteløse godseierne, prestene (kirken), kremmerne (ågerne), etc – med sheriffen som den verste av alle skurker. Fra norsk historie kjenner vi Gjest Baardsen som en lignende figur og folkehelt.[13] I likhet med tusenårsbevegelser, oppstår sosial banditvirksomhet i perioder med samfunnsmessig omveltning, typisk ved overgang fra enkle, egalitære bondesamfunn til føydale eller stratifiserte nasjonstater. Fra Peter Worselys studier av tusenårsbevegelser (Worsely 1970), særlig de såkalte cargo-cultene, ser vi at også disse kan ha et politisk siktemål – befrielse fra undertrykkelse og gjenskaping av det gamle, det opprinnelige – det som forsvant da "utviklingen" kom. Eller som Eric Hobsbawn selv sier: "Social banditry and milleniarism – the most primitive forms of reform and revolution – go together historically" (Hobsbawn 1972, s.29). Det er når slike bevegelser vokser – øker i antall aktive deltakere, utøvere og støttespillere – at bevegelsene kan få en klarere politisk målsetning. Hvis de lykkes, blir de seierherrer og kan selv bestemme sitt omdømme; de forvandles fra å være "banditter" til å bli "revolusjonære helter" (f.eks. Castro i Cuba), eller "frigjørere" (UCK i Kosovo), eller fra "religiøse fanatikere" til "nasjonens redningsmenn" (for eksempel muslimske presteskapet i Iran, etter at Shan av Persia ble styrtet). Et slikt utviklingsforløp – fra opprør til maktovertakelse – enten opphavet kalles banditvirksomhet eller religiøse bevegelser – kan historien gi mange eksempler på.

Det første og mest entydig kjennetegn på sosial banditvirksomhet er rekrutteringen, hvem som blir og er banditter. I følge Eric J. Hobsbawn (Hobsbawn 1972, s.31) er det menn i alderen 17 til 20 år som utgjør hovedtyngden av rekruttene – dvs. de fleste blir banditter på et tidspunkt i deres livssyklus mellom pubertet og familiedannelse. Dette er et tidspunkt i livet hvor unge menn er mobile – i de gamle bondesamfunnene var ungdom i denne aldersgruppen stadig på flyttefot, på jakt etter jobber, i lære, etc. Foruten denne primærgruppen av eldre tenåringer, ser man en annen, men ikke fullt så viktig rekrutteringskilde: Avvikere, som av forskjellige grunner var utstøtt eller marginalisert – og derfor hadde en mobilitet som var gunstig for rekruttering til banditvirksomhet, slik som desertører, arbeidsløse leiesoldater, gjetere, krypskyttere, etc. Eric J. Hobsbawn

---

[12] Robin Hood har en gang levd, men man vet ikke med sikkerhet hvem den historiske Robin Hood egentlig var og hva som er fakta og fiksjon om hans liv.

[13] Jfr. Gjest Baardsens selvbiografi (Baardsen 1966)

.

(Hobsbawn 1972, s. 35) mener også at personlighetstypen spiller en rolle i rekrutteringen – at de som blir banditter har et mer opprørsk, opposisjonelt vesen; de er oppsetsige og ærekjære og vil ikke la seg "tråkke på". Mange vil oppfatte dem som simple bøller, og det er ikke rart fordi de i klesveien, kroppsspråk og væremåte fremstilles nettopp slik – utfordrende og provoserende, dvs det motsatte av ydmykhet og underdanighet i sitt ytre. Ut fra dette har Eric J. Hobsbawn (Hobsbawn 1972, s. 42-57) utdypet ni kriterier som særpreger sosiale banditter – og som skiller dem fra "vanlige" kriminelle bøller og tyver. Disse ni kriteriene skal utdypes i neste avsnitt, i forbindelse med analysen der hackere sammenlignes med sosiale banditter.

Et sentralt aspekt med sosial bandittvirksomhet er hevnen – og måten den fullbyrdes på. Historisk sett er det unektelig slik at bandittvirksomhet - uansett om den forklares som "ren" kriminell eller som politisk/sosial protest – så er den både voldelig, brutal og grusom. I følge Eric J. Hobsbawn (Hobsbawn 1972, s.63) må en banditt vise rå styrke – og at de kan, om nødvendig, være skånselsløse. Dernest, så ligger det i det å bøte på urett – hevnen, eller den folkelige straffen – at den nødvendigvis må være brutal fordi banditten og hans allierte vanligvis ikke har noe rettsapparat eller system som kan utøve andre former for straff – de må ta loven i egen hånd. Videre, de samfunn og tidsepoker hvor banditter har operert, har generelt vært brutale, sett i lys hvordan vi i dag ser på vold. Vår tids hackere er fredelige og helt ikkevoldelige i sin virksomhet. En annen forskjell er deres økonomiske stilling og tilpasning. Som all annen virksomhet, så har bandittvirksomhet et økonomisk – og derigjennom et annet, tilleggspolitisk – fundament, for, som Eric J. Hobsbawn påpeker (Hobsbawn 1972, s.83), så må jo banditter ha mat – og de trenger forsyninger, særlig våpen og ammunisjon. Deres viktigste "inntektskilde" er selvsagt røverutbyttet, men for å leve av det må disse godene inn i den økonomiske sirkulasjonen – ransbyttet må konverteres til andre goder. Banditter trenger kjøpere, transport, formidling og mellommenn – det siste også i forbindelse med forhandlinger om løsepenger for fanger de har tatt (kidnapping) eller krøtter og hester som de har "berget". De økonomiske mekanismene i dette kjenner vi fra moderne kriminalitet i forbindelse med helerivirksomhet og hvitvasking av svarte penger. Dette nettverket av forbindelser som banditter er avhengige av i sin økonomiske tilpasning gjør at banditter er en del av et "normalt" samfunnsliv – men dimensjonene på disse aktivitetene (store summer røvet penger, verdigjenstander, krøtterbølinger, etc.) gjør at banditene sidestilles med de velstående, for eksempel hacienda-eierne, den lokale adelen, etc. Samtidig er de p.g.a. virksomhetens illegale natur – også utenfor samfunnslivet, men som en maktfaktor med et økonomisk fundament viser bandittvirksomhetens historie og sosiologi at banditter inngår i et avhengighetsforhold med sine omgivelser, særlig med den etablerte, lokale makteliten. Denne dobbeltheten – at de er "utenfor" samfunnet (illegal virksomhet) fordi de kjemper for en aktverdig sak ("ta fra de rike og gi til de fattige", gjenopprette rettferdighet, plage og terrorisere undertrykkende myndigheter, etc.) - samtidig som de økonomisk og politisk er avhengig av et etablert samfunnssystem og dens elite, er et skjørt balanseforhold som sjelden lar seg vedlikeholde over tid: Enten blir banden en del av eliten og integreres på forskjellig vis - banditten blir godseiere selv, eller en del av godseierens maktsystem,

som ”vokter” eller godseierens private armé. En variant av dette er at banditten utvikler og etablerer selvstendige organisasjoner som opererer i det skjulte. Eksempler på dette er utviklingen av mafiaen i Italia. Eller – i noen få, sjeldne tilfeller – vokser banden og blir del av brede, politisk-militære bevegelser, som, hvis de lykkes, etablerer et nytt regime. Eksempeler på dette finnes i mange revolusjonære frigjøringsbevegelser, slik som på Kuba og i Kina. Imidlertid, den vanligste utviklingen i følge Eric J. Hobsbawn er at banden oppløses fordi de på en eller annen måte blir forrådt eller militært knust.

Essensen i analysen av den klassiske, historiske sosiale banditten er at han (det er nesten utelukkende menn) som sosial person er en unggutt i opprør mot maktutfoldelse og samfunnsendringer som krenker eller truer dype, rotfestede verdier og idealer i bondesamfunnet. Ungguttene har – i motsetning til andre – en type frihet fordi de ikke har så mange hensyn å ta – og de føler seg lite sårbare, med tilhørende mulighet til å ta risiko, dvs. modighet og dristighet. Ungdomstidens overmot gjør dem fryktløse – de kan dyrke en lidenskapelig interesse, overbevisning eller hat med uforbeholden intensitet og oppmerksomhet – kun kroppens mest påtrengende biologiske behov (minimum av mat, søvn, etc.) setter noen få grenser. Distinksjonene mellom den sosiale banditt – en unggutt med ”sense of mission” og et moralsk, sosialt ideal – og mer ungdommelig eventyrere/opportunister/misfits er vag og flytende – de har mange fellestrekk. I en tidsalder da IKT i økende grad er en faktor i samfunnsutviklingen, kan det være fruktbart å analysere om ikke hacking kan forstås som en type moderne sosial bandittvirksomhet – dvs. som en protopolitisk strategi – og bevegelse. På samme måte som man kan se klare paralleller mellom historiske tusenårsbevegelser og politiske aksjoner innen IKT (for eksempel parallellen mellom ”cargo-cults” og etablering av s.k. ”science-parks” som Fornebu-IT) kan man se tilsvarende paralleller mellom hacking og sosial bandittvirksomhet. En måte å undersøke dette nærmere på er å se om Eric J Hobsbawns kriterier for sosial bandittvirksomhet er anvendbare for hacking.

4.4 Hackeren som protopolitisk aktør

4.4.1 Hacking som politisk opprør

Eric Hobsbawns hovedtese er at en sosial banditthandling i det gamle bondesamfunnet begås som en reaksjon på en (eller flere) urettferdige handlinger begått av en personer og organisasjoner i maktposisjon. Hos hackere kan man se en parallell aksjonsform, begrunnet ut fra at IKT-industriens store aktører med sine maktmidler, undertrykker og begår urettferdighet. MicroSoft fremstår som en viktig representant for denne type allmektighet: Monopol, proprietarisering og privatisering av noe som burde være allmenning, vasallisering/slavebinding av brukere, etc. Et attributt som inngår i denne oppfatningen er både store mangler og begrensninger med de tekniske løsningene og programvaren i MicroSofts produkter og bedriftens egenrådighet – begge deler virker undertrykkende og fordummende. Å ”avsløre” MicroSoft er derfor viktig – en rettferdig sak. Opp gjennom hackervirksomhetens historie har kampen mot ”byråkratisk-

kapitalistiske" IKT-systemer vært en rød tråd. Hackere har alltid vært forkjempere for full åpenhet og tilgjengelighet – alle former for stengsler, enten de er legale, tekniske eller økonomiske, har vært betraktet som et onde. I Steven Levys (Levy 1984) beretning om pioner-hackerne på MIT på 60-tallet, begynte hackeres opposisjonsvirksomhet da MITs administrasjon og etablerte edb-forskere prøvde å innføre begrensninger på, og kontroll av, bruken av MITs datamaskiner – dette ved innføring av passordbeskyttelse, adgangskontroll til bygningene, avlåsing av enkelte rom, konto for brukerområder på maskinene, etc (Levy 1984). Etter hvert som datakommunikasjon via telenettet ble vanlig, utvidet hackere sin virksomhet til målsetningen om gratis og ubegrenset bruk av telenettet – dette også begrunnet med at telesystemenes priser var en hindring/diskriminering av grunnleggende menneskerettigheter – retten til yttringsfrihet, forsamlingsfrihet og ubegrenset meningsutveksling og eksperimentering med programvare, etc. Hackerne forfektet, slik credoet om "Hacker Ethics" viser, et demokratisk frihetsideal – som de mente ville kunne utvikles enda bedre med en "fri" tilgang til IKT-ressurser. Dette førte dem på kollisjonskurs med eiendomsrettighetsnormer, foruten generelle byråkratiske prinsipper om kontroll. Særlig konfliktskapende og uforløst er konflikten mellom hackeres idealer og idealer om beskyttelse av åndsverk og intellektuell eiendom (typisk betegnet i begrepet "copyleft"), noe som er grunnleggende for mange i IKT-sammenheng, for eksempel retten til eiendom av programvare. I hackernes frihetsideal ligger noe som kan betegnes som en kommunardistisk oppfatning av almenningsrettigheter til informasjon, bruk av IKT-ressurser og teknologiske løsninger. Følgelig er alle former for proprietarisering, stengsler og inngjerdinger et overgrep – og "alle" har en hellig rett til å bekjempe dette.

4.4.2 Hackere bøter på urett

Et viktig kjennetegn med sosial bandittvirksomhet er at den bøter på urett, og er, i motsetning til andre former for banditteri, ikke utført i vinnings hensikt, med et rent økonomisk motiv. Motivet ligger i en oppfatning av hva som er rettferdig – og banditthandlingen retter seg mot å gjenskape en rettferdighet. Et kjennetegn med hackervirksomhet er rettferdiggjøring ut fra nettopp en målsetning om å bøte på urett som begås av "systemet". I HotMail-saken uttalte den svenske unggutten DarkWing at de ville avsløre hvor dårlig MicroSoft egentlig er, samt at MicroSoft har et monopol, dvs at MicroSoft er omnipotent, diktatorisk overfor det folk egentlig trenger eller fortjener. Både dårlig kvalitet og monopol-misbruk er vederstyggeligheter i hackeres øyne. Det er opplagt at Hackers Unite, hvis de hadde hatt "rene" kriminelle motiver, lett kunne ha utnyttet sin posisjon med oppdagelsen av ubegrenset adgang til HotMail på svært mange økonomisk lukrative og malisiøse måter, hvis de hadde ønsket det. Men de valgte en "avsløring" rettet mot MicroSoft, dvs. formidling av et politisk budskap.

4.4.3 Hackere vil deprivatisere IKT

Den "klassiske" sosiale banditten kjennetegnes ved at han "tar fra de rike og gir til de fattige" (Robin Hood-prinsippet), dvs. gjennom sin handling omfordeler et gode som de onde urettmessig har tilegnet seg. For en hacker fremstår proprietariseringen av

programvare, IKT-systemer, samt utestengingen/inngjerdingen som noe som må åpnes og gjøres tilgjengelig for alle. Ut fra dette kan man si at de "fattige" er alle de som begrenses eller lider under kontrollen og eiendomshåndhevelsen som systemet har eller prøver å innføre. For en hacker er "frigjøringen" av de undertrykte ved å oppløse en urettmessighet som noen få privilegerte sitter på, målsetningen. Slik sett er det mulig å likestille de som er "fattige" i IKT-sammenheng, dvs. undersåtter i et monopolistisk, autoritært og grådig IKT-system, som slaver som utnyttes grovt og fantasiløst av store bedrifter som IBM, MicroSoft, AT&T, etc. De hackerne som lever nærmest opp til Robin Hood-prinsippet er de som teleselskapene beskylder for å stjele tellerskritt. Piratkopiering av programvare kommer også i samme kategori. Imidlertid, på dette området er det mange tyver på torget – ikke bare hackere i den forstand de er definert her. Mafiaen og andre profesjonelle kriminelle er betydelige – sannsynligvis de største – operatørene på disse områdene. For de yrkeskriminelle, de som selger tellerskritt som enhver heler selger sølvtøy eller annet stjålet gods, er det den økonomiske vinningen som er hovedmotivet – men metodene de bruker har de ofte til felles for de mer idealistiske hackerne. Piratkopiering er avslørt som en betydelig industri – blottet for den type motiver som man finner hos hackerne: Store piratfabrikker som forfalsker MicroSofts emballasje og autentisitetssertifikater og masseproduserer CD-plater med programvare er bl.a. avslørt i England og i Kina.

4.4.4 Hackernes handlinger og metoder er aktverdige

Eric J. Hobsbawn skriver at et kjennetegn i identiteten til en sosial banditt er at han bare begår grusomme handlinger (for eksempel drap) i et minimum av omfang – og da ut fra aktverdige motiver, som selvforsvar eller fullbyrding av rettferd. Hackere dreper aldri – fysisk vold inngår ikke i deres arbeidsmetoder – deres modus operandi er preget av ikkevoldelig adferd. På denne måten skiller de seg fra "klassiske" sosiale banditter, som opererte i historiske og politiske sammenhenger som var preget av voldsbruk, hvor bruk av våpen og fysisk straff var mer utbredt som en del av myndighetsutøvelsen. Den moderne, sivile IKT-verdenen er utpreget ikkevoldelig og sivilrettslige, dvs. at den sivile orden preges av åndsverksrettigheter, salgskontrakter og –vilkår, edb-administrasjon – og ikke minst – av adgangskontroll og forskjellige former for nøkkeladministrasjon. En hacker ville ikke oppnå noe som helst om han drepte en systemansvarlig; voldelige, fysiske konfrontasjoner i form av ran og overfall forekommer ikke i deres metodiske repertoar. Derimot er ulike former for innbrudd og inntrenging en vanlig modus operandi for en hacker. Dette kan omfatte innbrudd i konkret, fysisk forstand, for eksempel lirke opp en lås til et koblingsskap eller skuff, eller mer virtuelle innbrudd, slik som typisk dekkes av benevnelsen "cracking". Eksempler på sistnevnte tilfelle kan være å snike seg inn i en passordfil på et system, ved at hackeren utgir seg for å være systemansvarlig, for så å opprette en ny, fiktiv bruker med vide fullmakter, som danner basis for hacker-raiding videre, for å trenge inn i IKT-ressurser som vanligvis ikke er tilgjengelige. I likhet med den klassiske banditt begås slike ulovligheter ut fra det de selv oppfatter som aktverdige motiver – og hvor selve handlingen ikke oppfattes som destruktiv, ut over det at det utfordrer systemets maktfullkommenhet.

4.4.5 Hackerne har støtte og goodwill i sine omgivelser

Den klassiske sosiale banditten har en forankring i sitt lokalsamfunn – han er en del av det og støttes, om enn i de skjulte, av krefter her som sympatiserer med ham – og som beskytter ham mot øvrigheten. For hackere – som lever i urbane, komplekse sammenhenger – er en tilsvarende lokalsamfunnsforankring som de tradisjonelle banditten har i bondesamfunnet, ikke tilstede. Derimot vil man finne at mange hackere opererer fra, eller har base i, i IKT-miljøer, som indirekte og direkte gir ham støtte og utfoldelsesmuligheter. En slik base har tradisjonelt vært universitetenes informatikkmiljøer, blant unge, mannlige informatikkstudenter og ellers i elektroteknologiske studentmiljøer. Videre finner man stor sympati for hackeraktiviteter i et utall av organisasjoner, både virtuelle og mer ordinære. Hackervirksomhet kan følgelig karakteriseres som en subkultur, men idealene som de forfekter har en sterk basis i vide kretser utenfor denne hard kjernen. At det finnes en grobunn for de synspunktene som hackere forfekter, er vanskelig å måle eksakt, men er klart synlig i tilslutningen som gis i "alternative" bevegelser, slik som i utviklingen av operativsystemet Linux og i utviklingen av internett.

4.5 Hackeres økonomiske tilpasning

I likhet med sosiale banditter – og andre mennesker – trenger hackere mat, søvn og et minimum av kroppspleie – og de trenger utstyr: PC'er, harddisker, modemer, printere, CD-spillere, og – telekommunkasjonslinjer. De trenger også et sted å være, en operasjonsbase. Gutterommet i barndomshjemmet fremstilles ofte som en slik base – og utstyret de trenger har de, som andre moderne tenåringer – oftest fått av sine foreldre – foreldre som tror at IKT er god pedagogikk som dessuten holder den unge, håpefulle vekk fra gatene. I hackerbiografier ser man at de debuterer gradvis fra sine gutteværelser inn i andre miljøer hvor hacking kan dyrkes mer intenst. Et typisk forløp er å gå videre som informatikkstudent på universiteter og høyskoler, ofte kombinert med deltidsarbeid i bedrifter som trenger IKT-kyndige i sitt arbeid, for eksempel edb-avdelinger, konsulentfirma, reklamebyråer, butikker som selger og har vedlikehold på datautstyr, etc. Det siste gir i sin tur adgang til enda større IKT-ressurser og muliggjør at man kan dyrke hacking i kombinasjon med "vanlig" arbeid. Web-design er et område som har sugd til seg et stort antall unggutter av denne typen – og skapt nettverk og kontakter mellom likesinnede. Et kjennetegn ved hackere er deres kompetanse og ferdigheter i å håndtere IKT. Dette opparbeider de ved en intenst og altoppslukende tilværelse foran skjermen – eller bak skjermen, langt nede i maskineriet, hvis vedkommende har en mer hardwareorientert legning. På arbeidsmarkedet er de attraktive – og deres teori- og teknologibegavelser gjør at de besitter en intellektuell kapital som er høy. Slik sett passer de inn i det Eric J. Hobsbawn beskriver om de sosiale banditten tilpasning til samfunnet – at de er avhengige av det, men samfunnet har også interesser i dem, særlig deres kompetanse og ferdigheter. I likhet med banditter som blir rekruttert av godseierne som "vaktmenn", ser man at hackere kan bli legalisert som "sikkerhetskonsulenter". Men det vanligste er at hackere, i likhet med sosiale banditter (som ikke blir drept) og politiske aktivister ellers "vokser ut" av denne tilværelsen – de får kjærester, etablerer familier

og/eller blir opptatt av å ”gjøre” karriære, dvs. lar seg kooptere eller blir konvensjonalisert og ”normalisert”. Et lite antall hackere etablerer seg som grundere og noen få av disse har bygget seg opp store private formuer basert på en teknisk innovasjon de har hacket. Men en slik posisjon ligger langt vekk fra det opprinnelige startpunktet.

4.6 Oppsummering

Gjennomgangen i dette kapittelet har vist at hackere deler mange fellestrekk med klassisk, sosial bandittvirsomhet. De åpenbare fellestrekkene er:

- Omtrent identiske m.h.t. sosiodemokratiske kjennetegn: Begge rekrutterer ressurssterke ung menn, med hovedtyngde i 17-20 års alderen – menn i senpubertet og tidlig voksen alder som er villig til total hengivenhet og er altoppofrende for en bestemt sak.
- Begge kjennetegnes av å være uredde (overmodige?) og dristige på de områdene de opererer i, selv om disse er ganske forskjellige.
- Begge har en opposisjonell legning, en trang til uavhengighet og skepsis til etablerte autoriteter.
- De rettferdiggjør sine handlinger ut fra en overbevisning om systemurettferdighet, som et opprør rettet mot øvrigheten, enten denne er offentlig eller privat.
- Hensikten med handlingen er å bøte på en urett eller å prøve å skape en situasjon i samsvar med egne idealer for rettferd og likeverd. Dette antar forskjellige former i cyberspace, sammenlignet med bondesamfunn. Men begge har til felles opprør mot myndigheter og institusjoner (for eksempel eiendomsrett) som etter deres mening urettmessig diskriminerer, depriverer eller utestenger folk fra deres rettigheter.
- Begge mener at de i sin framferd, fordi de er aktverdige, ikke bruker mer makt og midler enn det de må for å oppnå sine målsetninger. Banditter dreper ikke flere enn de ”må” – hackere ødelegger eller manipulerer ikke mer enn de må for å få frem sitt budskap eller oppnå en målsetning.
- Både hackere og sosiale banditter har til felles at de har støttespillere i sine omgivelser som gir dem legitimitet og goodwill, slik at de kan fortsette sin virksomhet.

Hackere og sosiale banditter er forskjellige på en rekke områder. Det mest opplagte er den historiske konteksten de opererer i, slik som:

- Tidsperioden og sosio-økonomisk sammenheng – hvor sosiale banditter er et typisk rural fenomen i bondesamfunn med svak politisk organisering og styring, og hacking, som er et fenomen fra høyteknologiske moderne samfunn.
- Metodene som benyttes, der sosiale banditter bruker våpen og fysisk vold, mens hackernes metoder er utpreget ikkevoldelige og basert på IKT-ferdigheter.
- Oppfatning av hva som er rettferd – der hackere synes å ha en sterk forankring i en borgerlig, liberalistisk frihetsideal og estetiske verdier, mens de sosiale banditten har basis i bondesamfunnets verdikodeks knyttet til oppfatninger om eiendomsrett, ære, likverdighet og rettferd.

- Forhold til omgivelsene – og omgivelsenes oppfatninger av hva hackere og sosiale banditter står for: Sosiale banditter har et nært forhold til de lokalsamfunnene de kommer fra, oftest nære slektskaps- og familiebånd til disse. De sosiale banditten reflekterer lokalsamfunnets grunnleggende verdinormer og oppfatninger av hva som er rett og galt. Hackere har derimot liten lokalsamfunnsforankring – de tilhører moderne, komplekse samfunn, preget av spesialisering og fragmenterte sosiale systemer. Hackernes arenaer er cyberspace og de IKT-miljøene de fysisk oppholder seg i, f. eks. på informatikkrommene ved universitetene. I slike sammenhenger ser man ofte at de har støtte og goodwill fra sine omgivelser.

Selv om historisk kontekst kan forklare forskjeller som skiller hackere fra sosiale banditter, så er det allikevel kontekstuelle fellestrekk som også er viktige. Den mest opplagte er at begge fenomenene blomstrer opp i situasjoner preget av samfunnsendring. I følge Hobsbawn er sosial banditvirksomhet et universelt fenomen fordi det opptrer på steder som undergår sterke endringer av samfunnet – uansett tid og sted. Det tar form av et opprør mot at en sosial klasse prøver å få makt over en annen. Opprøret, den sosiale banditts virksomhet, rettes mot de som utøver denne makten og representerer ”systemet”, slik som jordeiere, lensmenn, etc. – og dermed fremstår som agenter for innføring av en ny, undertrykkende samfunnsorden: De pålegger dem nye byrder, fratar dem hevdvunnene rettigheter, krenker deres rettferdsfølelse, ydmyker dem og er brutale, etc. Hos hackerne finner vi at deres opprør retter seg mot de som prøver (og oftest lykkes) i å formgi IKT-utviklingen og –systemer på måter som strider mot deres idealer av frihet, åpenhet, fellesskap, etc. Hackere gjør opprør mot en utvikling – mot en bestemt tendens i hvordan sterke maktgrupperinger ønsker at fremtiden skal bli, ut fra hvordan makten utfoldes i dag. Hackere har en overbevisning om frihet og åpenhet som de mener at IKT kan virkeliggjøre, men som forskjellige maktgrupper undertrykker fordi de vil ha økonomiske eller politiske monopoler. I følge Sterling er hackere politisk ubehjelpelige. Hobsbawn sier omtrent det samme om sosiale banditter – begge har til felles at de mangler politiske visjoner og strategier – og at deres handlinger er basert på reaksjon, på konkrete objekter som symboliserer deres misnøye. Begge har til felles at deres politiske gjennomslagskraft oftest er marginal i den forstand at de sjeldent får til de egentlig ønsker gjennom sine aksjonsformer – når de lykkes med sine aksjonsformer fører dette bare til at det etablerte forsterker sitt forsvarsverk. Like fullt er de politiske i sine motiver og målsetninger for aksjoner – og de har mange fellestrekk. Dermed ser vi at det er mulig å forklare hacking som også et politisk fenomen, som en politisk aksjonsform, med forankring i en politisk oppfatning, dvs. hacking fremstår som en protopolitisk bevegelse.

5 Hacking og kampen om IKTs fremtid

Analyse av hacking har vist at det er mange måter å forstå og forklare dette fenomenet på – og det finnes sikkert flere enn de som er blitt presentert i dette arbeidet, slik at analysen er langt fra uttømmende. Innledningsvis ble det påstått at hacking er av interesse fordi den er nært tilknyttet IKT-utviklingen, og fordi det i økende grad synes som samfunnsutviklingen er påvirket av IKT-utviklingen. Hacking kan analyseres som en type konflikt eller en form for avvik, som påvist i de tidligere kapitlene. Ved å forstå *hvorfor* et avvik oppstår eller en konflikt skapes er det lettere å forstå *hva* det avvikes fra, eller *hva* som er konfliktgrunnlaget. Dermed kan analysen av hacking som en konflikt eller et avvik gi verdifull innsikt – en slik analyse kan by på forskningsstrategiske fordeler.

5.1 Forklaringer og teknologisyn

Som påvist fortoner hacking seg svært forskjellig avhengig av analytikeren: Der enkelte er på hackere som subversive og kriminelle, ser andre mistilpassede unge menn – og andre igjen valpete unggutter i fri (noen ganger helt uhemmet), kreativ utfoldelse. Det er også mulig å analysere hacking som et politisk opprør, med enkelte klare likhetstrekk til tidligere tiders protopolitiske bevegelser. Alle forklaringstypene har til felles at de kan sannsynliggjøre sine fortolkninger og forklaringer med å peke på empirisk materiale. Forklaringsmangfoldet kan derfor bero på empiriske forhold – hacking omfatter et stort antall mennesker med et høyt og variert aktivitetsnivå, noe som også skaper en empirisk flytktighet. Det vil si at forskjeller i forklaringer kan tilbakeføres til analytikernes seleksjon og avgrensning i utvelgelse av empirisk materiale. En slik situasjon av forklaringsmangfold er ikke uvanlig – forskere er forskjellige; selv om de stirrer på samme fenomen vil deres blikk feste seg på ulike punkter.

Går vi tilbake til analysen i de foregående kapitlene og de forklaringstypene som ble presentert der, er det mulig å kategorisere disse ut fra to dimensjoner:
- *analytisk fokus*, hvor det skilles mellom personlighetsfokus og handlingsfokus,
- *syn på hacking*, hvor det skilles mellom positivt og negativt syn.

Dette kan skjematisk representeres som vist i diagram 5.1, der forklaringstypene er plassert i forhold til de to dimensjonene. Diagrammets skjema forsterker kontraster som ikke nødvendigvis er så uttalte i forklaringene, slik de ble analysert tidligere. Men selv om nyanser tapes byr diagrammet allikevel på fordeler fordi kontrastene tydeliggjør forskjellene. For å utdype dette: I de psykologiske forklaringene er det hackeres personlighet som står i fokus. I disse fremstår aktivitetene eller handlingen som utføres av hackere, som et tegn på unge menn med alvorlige problemer. Denne forklaringstypen er i mindre grad bekymret over hva hackere gjør eller skaper, om det de gjør er aktverdig, forkastelig, kreativt, etc. er av mindre interesse. Dette fordi *hva* de gjør er resultat av

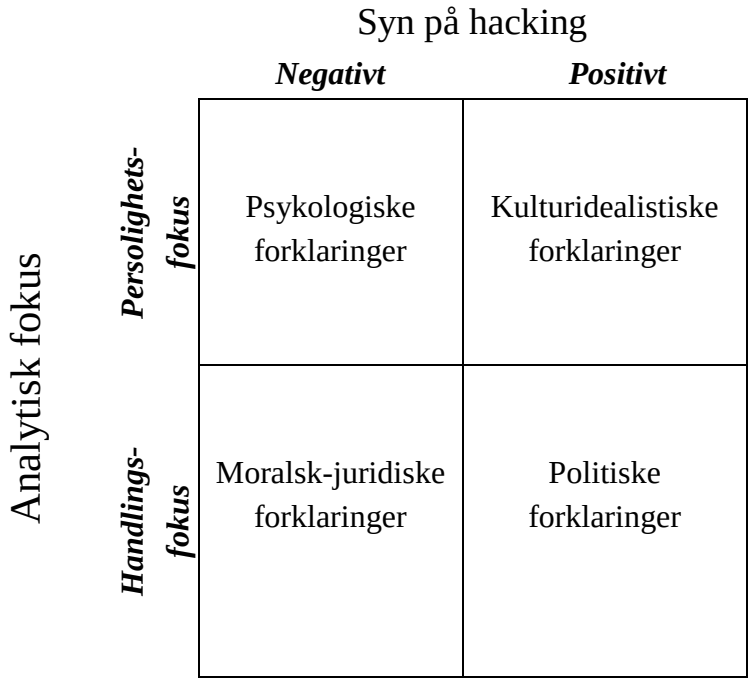

Diagram 5.1: Forklaringstyper vedrørende hacking

hvem hackeren er, dvs. i hovedsak unge menn som er mistilpassede og har et dårlig selvbilde. I den moralsk-juridiske forklaringstypen er forklaringskjeden reversert i forhold til den psykologiske: Her er det handlingen og aktivitetene som er primærfokus. I disse forklaringene opptrer personlighetsfaktoren som en mulig, bakenforliggende faktor som kan belyse hvorfor slike handlinger begås, slik man ofte ser i kriminalreportasjer (f.eks.: ”moderen/bedrageren/voldtektsmannen/hackeren (stryk det som ikke passer) vokste opp i et trist hjem uten far og med en alkoholisert mor”). Til tross for forskjellige forklaringer og fokus har begge til felles at de er negative eller skeptiske til hackere og hacking.
I den moralsk-juridiske forklaringstypen er det opplagt at hackere oppfattes som en trussel mot det bestående, de etablertes interesser. I hvilken grad dette også gjelder den psykologiske typen, er ikke opplagt. Sherry Turkle motiverer sine forklaringer med at IKT er en kultur i støpeskjeen og at det derfor er viktig å forstå hvordan IKT skapes og brukes. Ut fra dette kan man si at hennes skepsis til hackere er hva de representerer av utviklingstendenser – dvs. en frykt for fremtiden. I det hun mener å se hos hackere – deres intense behov for mestring, ekstreme individualisme og dårlige, usensuelle selvbilde – ligger det et skremmebilde av hvordan fremtiden kan bli, dersom hackere får prege utviklingen. Implikasjonene av dette er å advare mot en kreativ kraft – en kraft som andre, med andre analytiske briller, vurderer med motsatt fortegn. En konsekvens – om enn muligens utilsiktet – er at den psykologiske forklaringstypen understøtter den moralsk-juridiske, som et forsvar for de etablertes syn på hvem som skal styre og ha kontroll over

IKT-utviklingen, altså en form for forklaringsallianse p.g.a. komplementariteten i det som forklares: Der den moralsk-juridiske forklaringen ser datakriminalitet og subversivitet, der kan de psykologiske forklaringene supplere med forklaringer om at disse handlingene begås av mistilpassede unge menn med store personlige problemer.

I den kulturidealistiske forklaringen er skillet mellom diagrammets handlingsfokus og personlighetsfokus ikke så skarpt, fordi analytikere kobler disse to tett sammen. Hovedresonnementet i forklaringen er at hacking best kan forstås som et pubertetsfenomen – en aktivitet som dyrkes intenst av en liten gruppe unge menn i noen år, når de har behov for å leke uhemmet, slik mange ungdommer, særlig gutter, gjør, f.eks. innen ekstremsport, biler, etc. Her er det spill, lek, estetikk, kreativitet og skaperglede som er hovedmotivasjonen – og dette er noe helt annet enn kompensasjon for sosial og emosjonell ubehjelpelighet. I tråd med dette bagatelliseres hackernes politiske utspill og ambisjoner – på lik linje med deres handlinger. I den grad hackere bryter lover – så er dette uten den vinnings hensikt som kjennetegner en kriminell handling. I den politiske forklaringen er det handlingen som står i fokus – og likhetstrekkene med sosial bandittvirksomhet som protopolitisk bevegelse – begge som uttrykk for opprør mot en undertrykkende samfunnsutvikling. For, i motsetning til den moralsk-juridiske forklaringstypen, er det mulig å se på hacking som kamp om utformingen av IKT – både i nåtid og for fremtiden. Hackernes mål er emansipatorisk og estetisk – begge deler undertrykkes av hvordan IKT utvikles og forvaltes av de som har kontroll og makt – dvs. de store dataindustrielle foretakene, teleselskapene og myndighetene. I den kulturidealistiske forklaringstypen er dette også anerkjent som en faktor, men hackernes politiske handlinger blir vurdert som overflatisk, ubehjelpelig og patetisk – uten strategi og organisasjon som en politisk bevegelse krever. IKT-industriens og myndighetenes maktfullkommenhet gjør at de overreagerer overfor hackere – de oppfatter hackere som en trussel uten at de har grunn til dette – deres nulltoleranse for avvik gir seg utslag i hekseriforestillinger om hackere og en formidable mobilisering av makt for å undertrykke dette.

I den politiske forklaringstypen – hvor det sannsynliggjøres at hacking har mange protopolitiske egenskaper – vil det være naturlig å forvente en overgang til mer politisk målrettede handlinger. Dette kan tenkes å skje på minst to forskjellige former:

- *assimilasjon:* synspunkter og ideologiske resonnementer som hackere har utviklet vil bli fanget opp eller på andre måter blir integrert i de etablerte politiske organisasjonenes programmer og agenda'er, på lik linje med andre strømninger i samfunnet, slik som likestilling mellom kjønnene, naturvern, rasemessig likestilling, rettigheter for seksuelle avvik, etc.
- *videreutvikling:* fra protopolitiske aksjoner til selvstendige, mer målrettede og målbevisste, systematiske aksjoner, med tilhørende organisasjon og strategi.

Assimilasjon av hacker-ideologi i etablerte politiske systemer er vanskelig av to grunner: Dels fordi det ikke er noen uenighet/inkompatibilitet mellom de idealene som hackere forfekter m.h.t. åpenhet, deltakelse og likhet i IKT – og etablert politisk ideologi.

Hackernes motstand mot MicroSofts monopolstilling er noe de har til felles med en bred, anti-monopolistisk opinion. Likeledes er det en bred opinion om at IKT bør være et redskap for demokrati. Den andre grunnen – hackernes "hands-on"-imperativet – er for spesialisert til å kunne oppfattes som en interessant og legitim menneskerettighet. Bortsett fra enkelte, private borgerrettsorganisasjoner som EFF har hackeres teknologiske hjertesak liten interesse.

Videreutvikling som en hypotese er interessant fordi fra protopolitiske bevegelsers historie ser man at noen få av disse – slik som tusenårsbevegelser, "banditorganisasjoner", etc. – gradvis forvandles til brede politiske bevegelser med klar målsetning, strategi og organisasjon – og har dermed større mulighet for å oppnå målsetninger. Innen hackerbevegelsen er det mye som tyder på at dette har skjedd, f.eks. utviklingen av operativsystemet Linux, som en del av "Open Source"-bevegelsen (Moody 1998), som har sitt fundament blant unge og eldre hackere. I følge Eric S. Raymond (Raymond 1999) som har brukt fremgangsmåten til Thorvald Linus fra Linux-utviklingen til å utvikle en email-applikasjon "Fetchmail", er det mulig å få hackere – via internett – til å utvikle programvare til en meget høy standard, til en pris og pålitelighet som ikke er mulig i konvensjonelt, kommersiell programvareutvikling. Raymond henter ideologisk begrunnelse fra en russisk anarkist, Kropotkin – om betydningen av å få en rekke "frie" hackere til å samarbeide ut fra en felles forståelse og "…their own ego satisfaction and reputation among other hackers" (Raymond 1999). Det kan selvsagt diskuteres om det å skape et operativsystem (f.eks. Linux) er en politisk handling, fordi for den vanlige bruker av IKT vil ikke dette være helt opplagt. Svært mange vanlige brukere vet ikke engang at det finnes noe som heter operativsystem, langt mindre hva slags funksjon den har. Imidlertid, for aktørene inne IKT-sektoren er Linux-utviklingen teknologipolitkk i høyeste grad, både ideologisk (programvare som er gratis, lett tilgjengelig og billig i bruk) – men også kommersielt.

Gjennom Linux og lignende programvareutviklingarbeider har hackerne greid å etablere noe som i gavnet er en ny måte å utvikle standardisert programvare – og samtidig skape noe som er helt nytt, dvs med et betydelig innovasjonsapekt . Dette gjelder både organisatorisk og teknologisk. Teknologisk betyr dette at hackernes kreativitet nå blir kanalisert til å skape innovasjoner i mer organiserte former. Linux er et godt eksempel på dette, et operativsystem som kvalifiserer som en innovasjon innen programvare. Organisatorisk og politisk videreutvikling av hacking, fra protopolitiske bevegelse med mange likhetstrekk med de historiske, sosiale banditten – til en ny type innovasjonsregime, har skjedd i løpet av 1990-årene. I følge Eric S. Raymond (Raymond 1999) er det Web'en og internett som i stor grad har fungert som mekanisme og kanal for dette. Hvis dette vedvarer som en bevegelse betyr det at hackere er blitt en faktor, og kan dermed sidestilles med liggende og mer formaliserte standardiseringsorganisasjoner innen IKT-sektoren som kan få betydning for den videre IKT-utviklingen. Samtidig, nettopp fordi hackerne har lykkes i å få gjennomslag, slik man kan se i Linux, betyr denne suksessen en åpning for kommersiell kooptering av hackerbevegelsen. Mange

kommersielle programvareutviklere legger nå kildekoden til sine programmer åpent ut på nettet, med invitt til hackere om å bidra til avlusning og forbedringer. Denne kimen til en ny modus operandi, både blant hackere og mellom hackere og de etablerte, betyr at hacking som faktor har blitt konstituert – og kan tenkes å bli en avgjørende kraft i den videre IKT-utviklingen. Samtidig ligger det i hackingens vesen – dens trang til frihet og aversjon mot autoriteter – at de mer "tradisjonelle", protopolitiske handlinger vil fortsette, slik vi så i den såkalte HotMail-skandalen.

5.2 Hacking som antiprogram

En åpenbar forklaringsstrategi m.h.t. hacking som hittil ikke er drøftet finnes innenfor den sosialkontruktivistiske skolen av teknologiteori. Hacking som fenomen kan tenkes å passe inn i det som betegnes som "anti-program" innen ANT – aktør-nettverk-teori. I denne varianten av sosialkontruktivistisk teori vil man finne beskrivelser av empiriske tilfeller hvor nettopp er bruken av teknologi tilpasses slik at den "saboterer" eller underminerer teknologieierens eller makthavers hensikt. For å illustrere dette har Bruno Latour gitt en innlevende skildring av en spesiell nøkkeltype som benyttes på portdørene i leiegårder i Berlin – og kalles derfor "Berlinernøklen". Denne nøkkeltypen er konstruert[14] slik at brukeren[15] tvinges til å låse portdøren etter seg – først når portdøren er låst blir nøkkelen frigitt (Latour 1992), s. 252-254. Latours poeng er at den tekniske formgivingen av denne nøkkeltypen, som all annen teknologi, har støpt inn – eller skrevet inn, som han velger å kalle dette – en anvisning om brukerens adferd, eller program, som har til hensikt å tvinge frem en bestemt type adferd. Latour forklarer at det er en form for delegering av et maktforhold til en teknisk innretning – nøkkelen utfører den kontrollfunksjonen som et menneske (f.eks vaktmester) skal gjøre. Anti-programmer er tilpasninger som folk utfører for å slippe unna denne typen anvisninger eller påbud. I tilfellet berlinernøkler består anti-programmet i at brukeren filer nøkkelen til, slik at han/hun slipper ekstrabryderiet med å låse etter seg – programmet blir dermed sabotert/lurt og delegasjonen av kontroll mister betydning. Samtidig forblir portdøren ulåst – hvem som helst kan nå vandre inn i gården. For hackere kan man si at i den grad de utfører handlinger som går på tvers av de etablerte programmene, så er hacking en type anti-program. Slik sett kvalifiserer store deler av aktivitetene som hackere utfører som anti-program. Man kan også beskrive forholdet mellom hackere og de etablerte som en maktkamp der teknologi er en viktig alliert for begge parter.

Latour bruker "program" og "anti-program" i et omfattende begrepsmessig rammeverk hvor bruk av metaforer inngår i analyse- og forklaringsstrategien, under en parole om "teknologi som tekst". Dette er en parole som mange andre innen den sosialkontruktivistiske retningen også benytter, men fortolker og anvender på litt

---

[14] Korrekt sosialkontruktivistisk terminologi ville være å si "skrevet" i stedet for "konstruert" – altså teknologisk formgiving er inskripsjon, ikke konstruksjon.

[15] I sosialkontruktivistisk terminologi ville man si "leseren" i stedet for "brukeren" – noen (Akrich) er så konsekvent at leseprosessen kalles for "de-scription".

forskjellig måte. I Latours anvendelse av denne tilnærmingen benyttes det han kaller en lingvistisk/semiologisk tilnærming, dette ved å skille mellom en syntagmatisk og en paradigmatisk dimensjon (jfr. (Akrich and Latour 1992), s. 260-261. I den syntagmastiske dimensjonen avdekkes programmets struktur, slik man i lingvistikken analyserer en setnings oppbygging i substantiver, verb/predikater, objekter, osv. I den paradigmatiske dimensjonen analyserer man hvordan et element kan byttes ut med et annet, f. eks. hvordan et substantiv kan skiftes ut med et annet – hos Latour vil dette si hvordan en aktant (f.eks. en teknologisk gjenstand) kan byttes ut med en annen. Ideen med dette er at man i analyse av teknologi skal kunne blottlegge aktør-nettverkets struktur, slik Latour tror man gjør i lingvistikken, i analyser av setninger. Videre mener Latour at denne tilnærmingen gjør det lettere å blottlegge både programmer og anti-programmer innen teknologi, dvs. forklare hvordan teknologi skapes og tillempes i utviklingen. I denne tilnærmingen blir det nedlagt forbud mot å bruke kategoridistinksjoner som ”natur”, ”samfunn” – alle er aktanter som er kjedet sammen i et nettverk – ideen er at man skal ha samme kategorinøytralitet i forhold til fenomener i ”virkeligheten” (Latour kaller det agnostisk) som lingvister har til ord og utsagn i språkanalyse. Ut fra dette mener Latour og hans tilhengere at det byr på analytiske fordeler å ta utgangspunkt i teknologi som tekst.

Latours ide om ”anti-program” er imidlertid attraktiv på et abstrakt nivå, hvis man løsriver begrepet fra det såkalte lingvistiske analyseapparatet og parolen om ”teknologi som tekst”. Det er opplagt mulig å si at hacking representerer en form for anti-program, fordi hackernes idealer og handlinger ofte er klart opposisjonelle, preget av et opprør mot et etablerte. Vurdert som et anti-program vil hacking passe fint inn i den juridisk-moralske forklaringstypen som ble utdypet i kapittel 3. Men hacking er noe mer enn bare anti-program – det er også et program, eller for å gå lengere, et konglomerat av programmer fordi hacking har en ideologi og estetikk, en form for organisasjon som kan kalles en bevegelse og mange andre kjennetegn som er noe langt mer signifikant enn noe som avgrenses til en tekst eller antiprogram. Vi kommer dermed fort tilbake til de spørsmålene som ble stilt innledningsvis: Er hacking *bare* et ”normalt”, pubertertsrelatert ungdomsfenomen? Eller er det noe mer alvorlig: Er det et sosialt avvik, eller er det en mer grunnleggende politisk konflikt og motsetningsforhold i en teknologipreget samfunnsutvikling som utspiller seg? Representerer hacking en trussel i kampen om hvordan fremtiden skal se ut?

Litteratur

Akrich, M. and B. Latour (1992). A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies. *Shaping technolgy/Building society - Studies in sociotechnical change.* W. Bijker and J. Law. Cambridge, Massachusetts, The MIT Press**:** 259-264.

Baardsen, G. (1966*). Mitt liv : forfattet av meg selv på Akershus festning 1827-1835.* Trondheim, Nordenfjeldske forlag.

Ferguson, E. S. (1993). *Engineering and the mind's eye*. Cambridge, The MIT Press.

Henderson, K. (1991). "Introduction: Social studies of technological work at the crossroad." *Science, Technology and Human Values* 16(2): 131-139.

Hobsbawn, E. J. (1972). *Bandits*. Harmondsworth, Penguin Books.

Håpnes, T. (1996). Not in their machines: How hackers transform computers into subcultural artefacts. *Making technology our own? - Domesticating technology into everyday life*. M. Lie and K. H. Sørensen. Oslo, Scandinavian University Press**.**

Keith Grint and S. Woolgar (1997*). The Machine at Work*. Cambridge, Polity Press.

Latour, B. (1992). Where are the missing masses: The sociology of a few mundane artifacts. *Shaping technology/Building society - Studies in sociotechnical change*. W. Bijker and J. Law. Cambridge, Massachusetts, The MIT Press**:** 225-258.

Levy, S. (1984). *Hackers - Heros of the computer revolution*. New York, Dell Publishing.

Meinel, C. P. (1998). "How hackers break in...and how they are caught*." Scientific American* 280(October): 70-77.

Moody, G. (1998). "The wild bunch", *New Scientist*, (2164): 42-46.

Raymond, E. S. (1999). The Cathedral and the Bazaar, http://www.netaxs.com/~esr/writings/cathedral-bazaar/. 1999.

Sterling, B. (1992). *The Hacker Crackdown*. New York, Bantam Books.

Turkle, S. (1984). *The second self - Computers and the human spirit*. New York, Simon & Schuster.

Worsely, P. (1970*). The trumpet shall sound : a study of "cargo" cults in Melanesia*. London, Paladin.