Metoderapport til SKUP, 18. januar 2012

1. Navn på journalisten

Kjetil Stormark

2. Prosjektets navn

«På innsiden av hackermiljøet»

3. Publisert når

Magasinet PLOT, august 2011.

4. Redaksjon

Logos Media Ltd, Rostedsvei 12, 3610 Kongsberg. Tlf. 4177 5050.

5. Journalistens adresse og kontaktinformasjon

Frilansjournalist Kjetil Stormark. Ellers som ovenfor.

6. REDEGJØRELSE FOR ARBEIDET

Hvordan ideen blir til

8. april 2011 ringer mobiltelefonen. Det er fra et uregistrert nummer. En ung stemme i den andre enden spør om han snakker med Kjetil Stormark. Jeg kan knappest benekte. Motspørsmålet er enkelt.
«Kan du være med på en Skype-samtale med en liten gjeng?»

Det er noe av det første jeg lærer. Det er på skype det skjer. Skype blir opplevd som den sikreste kommunikasjonsarenaen akkurat nå.

Tre dager senere møter jeg 25 ungdommer, som dels snakker i munnen på hverandre. Jeg er kalt inn til et slags uformelt bakgrunnsintervju. Og det er jeg som blir intervjuet, rollene er byttet om fra hva jeg vanligvis er vant til. Norges fremste og yngste nettkrigere vil gjerne vite hvordan de hemmelige tjenestene kan finne på å utnytte datalagringsdirektivet (DLD).

Litt uti samtalen får jeg, trolig gjennom en forsnakkelse, vite at det er denne gjengen som for få dager siden angrep nettsidene til Arbeiderpartiet og Høyre, midt under Aps landsmøte.

Etter samtalen innser jeg at jeg sitter igjen med onlineidentitetene til Norges mest sentrale hackere. Det er en skjult verden som det er helt åpenbart at jeg er interessert i å utforske nærmere.

Men hackerne er bekymret: For få dager siden forsvant en av deres britiske venner. Hackeren «Topiary» er sporløst borte. Jeg bruker innledningsvis mye tid på å prøve å finne «Topiarys» reelle identitet. Teorien er at den unge briten kan ha blitt utsatt for en rendition, rett og slett blitt kidnappet, av noen av de sterke motkreftene han har vært med på å utfordre som medlem av hackergruppen LulzSec.

«Welcome to 2011.
The year of the Hacker».
DailyTech, 14. juni 2011

Prosjektet har hele tiden vært en kombinasjon av et sosialantropologisk og journalistisk prosjekt, der jeg ikke har hatt større ambisjoner enn å bare kartlegge hvordan hacktivismen foregår - hackere som bruker nettet som en aktivistarena. Bevegelsen ble i realiteten født på undergrunnsbevegelsens svar på finn.no, nettsiden 4chan. Men i noens øyne startet aktivismen på nettet også før dette.

Etterhvert som jeg kom tettere på hackerne, åpnet det seg en stadig større og interessant verden, der norske tenåringsgutter spilte ulike roller i forhold til dramatiske hendelser innenfor internasjonal politikk. Alt fra den arabiske våren til målrettede angrep mot de aktørene internasjonalt som hackerne mener står for maktovergrepene i verden: CIA, FBI, NATO, ulike lands politimyndigheter, Sony, Paypal, Visa, Mastercard mv. Ingen av de store aktørene kan føle seg trygge.

Da jeg kom inn i miljøet, var paranoiaen begynt å melde seg så smått, men vokste seg for alvor større underveis og mot slutten av arbeidet med saken. Dette kjennetegnes ved at mange av hackerne til å begynne med var fast bestemt på å stå fram. Det var helt uaktuelt da jeg satte siste punktum.

Nyhetssakene kom også trillende, så snart hackerne følte seg stadig tryggere på meg. Men også her ble de stadig mer forsiktige etterhvert som varmen ble skrudd opp i den internasjonale klappjakten på hackere i mange land.

Da jeg skjønte potensialet i prosjektet, kontaktet jeg dels PLOT og dels Dagbladet for å diskutere et mulig samarbeid. På grunn av muligheten til å presentere en sak over 30-40 sider i PLOT, falt valget på PLOT som samarbeidspartner.

Metode

Jeg har utelukkende brukt åpen observasjon og tradisjonelt kildearbeid. Dog har kildearbeidet vært svært krevende, fordi jeg i all hovedsak ikke har kjent identiteten på de hackerne jeg har forholdt meg til i arbeidet med saken.
Dialogen med ulike aktører har dels funnet sted på skype og dels på ulike irc-kanaler (irc - internet relay chat).

Jeg har vært opptatt av å selv ikke bryte loven. I flere tilfeller har jeg fått brukernavn og passord slik at jeg kunne ha tatt meg inn på lukkede servere, i ett tilfelle på en lukket brukertjeneste i Pentagon med reiseråd til ansatte og til opplæringsformål i forhold til antiterrorområdet.

I mange tilfeller har jeg i stedet bedt om å få tilgang til skjermdumper fra hackerne i etterkant, som jeg har benyttet i mine forsøk på å få verifisert ulike opplysninger.
Også her har det vært viktig for meg å ikke motivere til ulovlige handlinger, selv om jeg selvsagt ikke har noen garanti for at noen av de unge hackerne har ønsket å imponere meg.

For å kunne rekonstruere dialog underveis, har jeg tatt vare på de fleste chatloggene fra mine skypesamtaler og irc-samtaler. Jeg har også fått tilsendt kopier av andres logger.

I noen få tilfeller har jeg gjort observasjoner og intervjuer irl (in real life - i det virkelige liv).

Det har i prosjektet vært viktig at jeg kan forholdsvis mye om data og IT, samt behersker de viktigste uttrykkene og begrepene forbundet med onlinechatting. Dette har vært avgjørende for min troverdighet og mulighet til å bygge videre på den tilliten jeg ble vist innledningsvis.

Hva angår kilder, har jeg løpende supplert med omfattende mengder åpen kilde-research på nettet, basert på det jeg har fått tilgang til av muntlige opplysninger.

Underveis har det vært nødvendig å etablere gode mappe- og filstrukturer på laptopen, for å greie å manøvrere i de store datamengdene som jeg har kommet over i arbeidet med denne reportasjen. En ting er opplysningene som jeg har innhentet til denne reportasjen spesifikt.

Men jeg har også fått tilgang store mengder overskuddsinformasjon, i tillegg til at jeg vet om mange nye steder å finne informasjon. Dog insisterer jeg fortsatt på at jeg ikke ønsker å bryte loven, selv om mange av hackerne ikke tar slike, smålige hensyn.

Etiske avveininger

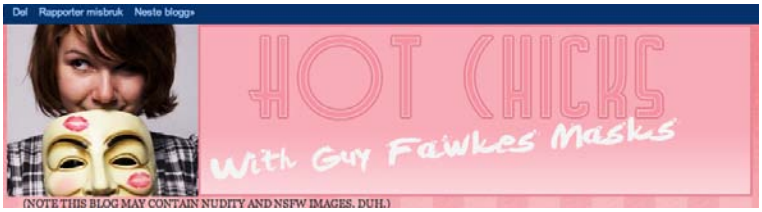
Prosjektet har reist flere etiske problemstillinger. Mange av hackerne har åpenbart vært mindreårige, noe som reiser problemstillinger ifht VVP 3.9. om å vise «særlig hensyn overfor personer som ikke kan ventes å være klar over virkningen av sine uttalelser». Mindreårige skal vanligvis ikke intervjues uten samtykke fra foreldre. Men i dette tilfellet

ville en slik skranke ha innebåret at det ikke lot seg gjøre å dokumentere hackernes verden, der mange ungdommer begår handlinger ofte uten at mamma og pappa har den fjerneste peiling på hva som foregår.

Underveis i arbeidet med PLOT-artikkelen, oppstod det i mai en uforsonlig krangel mellom medlemmer av hackergruppen Noria, som tidligere på våren brøt ut av Anonymous Norway. En 16-årig jente ble da utsatt for Face-rape, dvs at hun fikk lettkledde bilder av seg selv publisert på sin egen Facebook-profil.

Da jeg skjønte hva som hadde skjedd, og hackerne skrøt av hva slags ytterligere planer de hadde, valgte jeg å gå ut av min nøytrale reporterrolle og tok til motmæle. Jeg sa da at jeg anbefalte dem å ikke gjøre noe mer.
Jeg sa imidlertid ja til motta en dump/kopi av Facebook-siden til jenta, som dokumentasjon og bekreftelse på hva hackerne var i stand til å gjøre. Men det var aldri aktuelt for meg å bruke noe av den informasjonen som jeg fikk tilgang til og som var av privat karakter.

Underveis i prosjektet er jeg også blitt kjent med at det finnes egne blogger der lettkledde og nakne jenter blir avbildet med Guy Fawkes-masker. Også denne delen av prosjektet ble besluttet nedskalert, fordi det ville være en avsporing ifht hovedsporet i historien.



Jeg var mest opptatt av å vise hvordan norske og internasjonale hackere hevner seg på makthavere i ulike land, og hvordan de i stadig større grad opplevde å bli jaget vilt som en følge av dette.


Foto: Anonymous Norway

Bakmenn

Hackermiljøet spesielt internasjonal har noen likhetstrekk med etterretnings- og spesialstyrkemiljøene, som jeg kjenner vesentlig bedre og har mye mer erfaring med å jobbe opp mot. En viktig likhet, er at det er vanskelig å etablere tillit uten at noen går god for deg.

Gjennom de kontaktene jeg fikk i Norge, ble jeg etterhvert introdusert til noen av de viktigste, internasjonale bakspillerne i den relativt sammensatte hackerbevegelsen som går under kallenavnet «Anonymous».

Jeg ble fascinert over å oppdage at også her finnes det eldre personer, som regel menn, som trekker i trådene og som manipulerer massene av iltre tenåringer til å begå tjenestenektangrep og andre lovbrudd. Som resultat blir tenåringene jaktet på av FBI og andre lands myndigheter, mens bakmennene (ofte) slipper unna. Disse bruker i stedet

masse tid på å analysere den informasjonen som blir hentet inn. Anonymous har egne anlytikergrupper, som sammenstiller og gjennomgår opplysninger fra eposter, dokumenter og ulike informasjonskilder.

Det er en skjult krig som foregår på nettet, og der store nasjoner føler seg truet av det som i realiteten er en liten gruppe kunnskapsrike datahackere. Nøkkeluttrykket er at «informasjon er maktens råstoff». Det fascinerende med historien som jeg etterhvert greide å utvikle for PLOT, er at også de norske hackerne er tett sammenvevd i dette bildet.

Underveis i arbeidet med prosjektet, dro hackergruppen LulzSec (der Topiary var medlem) i gang en voldsom hackeroffensiv som raskt førte til at hackerne ble samtaletema på toppmøter i NATO. Saken blir ikke så mye større enn det.

Terrorangrepene 22. juli

På kvelden 22. juli har jeg hodet mitt hele andre steder enn i forhold til hackersaken som jeg egentlig har laget helt ferdig for PLOT. Topiary er pågrepet, på Shetlandsøyene av alle steder, og utviklingen er skrevet inn i saken.

Ved 22.45-tiden treffer jeg et medlem av den norske hackergruppen Noria på Skype.

<xxxxx> NORIA skal starte egen operasjon
<xxxxx> som svar på dette
<Kjetil Stormark> ok? hva da?
<xxxxx> usikkert enda
<xxxxx> vi må se hvordan situasjonen utvikler seg
<xxxxx> men om nødvendig
<xxxxx> vil vi bistå med å jakte ned de jævlene som sto bak
<Kjetil Stormark> så white hat til slutt, mao? (white hat: hackere som bare vil gjøre gode gjerninger)
<xxxxx> alt for Norge

Utover dette, var det ikke så mye «Fredrik» ville røpe. Om det bare var store og tomme ord, eller om det kom til å manifestere seg i noe mer, var umulig å vite.

En kompliserende omdreining

Torsdag kveld 28. juli har jeg og familien vært tilbake i Norge noen dager, etter å ha avbrutt ferien på grunn av hendelsene 22. juli.
Via mobiltelefonen min får jeg beskjed om at noen vil ha kontakt med meg på Skype.

Et medlem av hackergruppen Noria venter utålmodig når jeg logger på. Det første som slår mot meg når jeg logger på klokken 20.22, er et enslig ord.

<xxxxx> test

<Kjetil Stormark> der ja
<Kjetil Stormark> so, whats happening?
<xxxxxx> heh
<xxxxxx> har dumpet begge epostene

Noria-hackerne har funnet flere epostadresser som de mener Anders Behring Breivik har benyttet. Mens jeg arbeidet på spreng med første del av en mulig bok om terrorangrepene, hadde hackerne på eget initiativ, uten min innblanding, valgt å hacke to epostkontoer. De er også på sporet av flere kontoer og jager andre digitale spor.
Nå ber de meg om å overlevere materialet til politiet, slik at de selv slipper å eksponere hvem de er/var.

Etter å ha brukt natt til fredag 29. juli til å verifisere autensiteten av materialet, og noen få timer neste dag for å drøfte situasjonen med blant annet forlaget og PLOT-redaksjonen tok jeg neste dag kontakt med politiet for å opplyse at jeg satt på materialet og var villig til å overlevere dette til etterforskningsledelsen. Da hadde jeg ikke funnet opplysninger som kunne antyde planer om flere terroraksjoner, men det kunne jo hende at politiet satt med puslebiter jeg ikke kjente noe til.

For å sikre meg at situasjonen ble håndtert skikkelig fra politiets side, ringte jeg direkte til påtaleansvarlig i saken, politiadvokat Pål-Fredrik Hjort Kraby. Tidlig fredag kveld ble jeg ringt opp av en politikvinne, som antydet at det kunne bli aktuelt med avhør samme kveld. Halvannen time senere ringte hun tilbake, og slo fast at hun eller noen andre kom til å ta nærmere kontakt med meg.
Men først flere dager senere, seks dager etter at jeg hadde meldt fra til politiet om at jeg satt på materialet, kom det ny henvendelse. Da ble jeg spurt om jeg kunne komme til avhør på Manglerud politistasjon lørdag 6. august.
Tidspunktet fremstod som litt pussig.

En lørdag på Manglerud

Da jeg lørdag 6. august møtte opp til Manglerud politistasjon, hadde jeg tatt mine forholdsregler. En kollega ventet i bil på utsiden av politistasjonen. I tillegg hadde jeg nummeret til en advokat på speed dial.
Ingen sammenlikning forøvrig, men dagen før hadde politiet avhørt bloggeren «Fjordman», under alt annet enn harmoniske tilstander.
Jeg hadde ingen garantier for at mitt ønske om å hjelpe og formidle informasjon ville bli møtt på samme fredelige vis som mine intensjoner.
Men avhøret gikk greit.

PLOT-reportasjen blir oppdatert

På grunn av den nye omdreiningen, gikk jeg med på at magasinet PLOT kunne innarbeide opplysningene om hackingen av Anders Behring Breiviks epostkontoer i hackerreportasjen som skulle komme på gata 10. august.
Men tenåringene i hackergruppen var ikke enkle å stagge. De fortsatte på sitt plyndringstokt, og tok også kontroll over Breiviks twitterkonto. Da twitterkontoen til massemorderen plutselig begynte å gi lyd fra seg, ble det internasjonal oppstandelse, der nyheten ble formidlet som breaking news av CNN og andre på nettet.
Da nyheten om hackingen av også epostkontoene ble kjent, vakte dette også meget stor oppsikt.

Sikkerhetsmessige utfordringer

I perioden jeg arbeidet med å kartlegge hackernes verden, har jeg aldri noensinne - verken før eller siden - opplevd så store driftsmessige problemer med eget datautstyr. Mye

tyder på at jeg stadig ble forsøkt hacket, fordi det var et økende antall mennesker online som var nysgjerrige og bekymret over hva jeg arbeidet med.

Jeg innstallerte meget tidlig både kryptert nettforbindelse (vpn). Allerede før jeg påbegynte arbeidet med prosjektet, hadde jeg kryptert harddisk. Men noen dager var driftsproblemene like fullt så store at jeg måtte reboote maskinen fordi alt hang seg opp. Resultatet var at jeg hver gang mistet flere timers arbeidsinnsats. Det var derfor noen tunge øyeblikk, før jeg lærte meg noen grep for å takle disse praktiske utfordringene i hverdagen.

Kildevernmessige problemstillinger

Det er ekstremt mye dramatikk internt innbyrdes i og mellom de forskjellige hackermiljøene. Det er derfor viktig å være ekstremt forsiktig med hva slags kildeopplysninger man velger å gjengi, både i samtaler med ulike kilder og ikke minst ved publisering. Jeg tok tidlig et valg om at jeg kom til å anonymisere også hackernes nick, dersom det forelå et kildevernhensyn. Dette fordi det å bruke nicket til en hacker i mange tilfeller er likegodt med å identifisere med fullt navn.

Jeg måtte også tenke grundig gjennom bruk av alle illustrasjoner mv. mtp kildevernhensyn. Her hadde vi flere diskusjoner underveis, og der spesielt bildeleggingen av saken bød på mange avveininger som det var viktig at vi fikk løst på en tilfredsstillende måte.

Pågripelser i miljøet

Onsdag morgen 12. desember gjennomførte politiet i ulike deler av landet en koordinert aksjon mot fire forskjellige adresser i hhv Flekkefjord, Østfold, Romerike og Elverum. Etter nesten fem måneder, hadde lovens lange arm innhentet flere av medlemmene av Noria. Som grunnlag for aksjonen, forelå det en politianmeldelse fra den 16-årige jenta som er tidligere medlem av Noria og som fikk sin Facebook-konto angrepet.
Mye tyder imidlertid på at politiaksjonen er en «fisketur» på jakt etter informasjon om noe mer og større. Minst 20-30 politifolk og fem politidistrikter medvirket i aksjonen, som ble ledet av Oslo politidistrikt, samt med bistand fra både Kripos og Politiets sikkerhetstjeneste (PST). Ressursbruken er langt mer omfattende enn det som vanligvis følger av en nettmobbingsak.

I min nyhetsdekning av hendelsene (som jeg har dekket for Dagbladet) har jeg derfor valgt å opptre svært forsiktig med tanke på hva jeg skriver. Spesielt gjelder dette ifht krysskopling av hvem som er pågrepet vs det jeg har skrevet tidligere. Det er ikke min jobb å hjelpe politiet med etterforskningen. Men jeg har valgt å skrive det jeg med sikkerhet vet at politiet har fått vite/vet.

Det har gjort det litt krevende å håndtere at også andre journalister, av ulike årsaker, har fått inntak i deler av hackermiljøet. Det er derfor mer krevende å styre informasjonsflyten i offentligheten.

For meg er det helt avgjørende å ikke misbruke den tilliten jeg er vist ved å bruke all kunnskapen jeg sitter på fra tidligere. Som frilanser ville jeg nok ha tjent vesentlig mer på den løpende nyhetsdekningen dersom jeg ikke hadde lagt begrensninger på meg selv. Men samtidig ville jeg ha syndet grovt mot det kildevernet jeg lovet disse unge menneskene da jeg første gang møtte dem.

Tidsbruk

Siden jeg ble kontaktet i begynnelsen av april, har jeg hver eneste dag brukt minst to-tre timer, noen ganger 12-14 timer, på kontakt med hackerne. Jeg har hatt lange samtaler spesielt med hovedpersonen, som jeg valgte å kalle «Fredrik» på trykk. Da jeg nærmet meg deadline, brukte jeg rundt regnet tre uker på heltid på selve skrivejobben av saken.

Artikkelen endte på rundt 80.000 tegn, noe som er en fantastisk glede for en gammel journalist å få oppleve å få på trykk. Samtidig er det slik at dersom du skal få folk til å lese en så lang sak, må artikkelen virkelig holde mål. Det var derfor med stor ærefrykt og ydmykhet jeg satte meg til tastaturet for å prøve å sammenfatte flere måneder med research.

Spesielle erfaringer

Etter at saken stod på trykk i PLOT, har jeg fått utrolig mange hyggelige tilbakemeldinger fra en stor bredde av lesere. Veldig mange sier at de ved å lese saken har fått vesentlig ny kunnskap om hacktivisme og det lukkede hackermiljøet.

Jeg er også invitert til å snakke på sikkerhetskonferansen Hackcon. Der får jeg høre at mitt arbeid er den første saken i norske medier som de mener har greidd å behandle denne materien med dybde og det de mener er tilfredsstillende saksinnsikt.
Om det er riktig, aner jeg faktisk ikke.
Men det er uansett svært hyggelig sagt.

Jeg lærte utrolig mye av å møte hackerne og ved å få lov til å bli kjent med deres skyggeverden. Mange av hackerne er vanvittig gode researchere. Jeg tror faktisk jeg er blitt en mye bedre journalist av å ha skrevet denne saken.

De som behersker IT og den digitale verdenen, er den kommende herskerklassen. Å overleve digitalt, er viktig, nå som vi er på vei ut av «the information age» og er på vei over i «the draconian age», for å sitere en av bakspillerne i det internasjonale hackermiljøet.

Kongsberg, 18. januar 2012

Kjetil Stormark

FBI

HAN HAR SNOKET I PENTAGON, PLAGET DE RØD-GRØNNE OG HJULPET OPPRØRERNE I MIDT-ØSTEN. MEN RAZZIAER, FBI-AKSJONER OG EN INTERNASJONAL KLAPPJAKT TRUER DE NORSKE NETTAKTIVISTENE. HVEM KAN FREDRIK STOLE PÅ NÅ?

TEKST: KJETIL STORMARK

FOTO: HENNING CARR EKROLL

EN LITEN MINNEPINNE står plantet i den digre pc-en under bordet. Det gule lyset blinker og blinker. Det er på denne dingsen, ikke større enn en lillefinger, all programvaren ligger. Det er her alle de elektroniske sporene lagres. Og skulle det verste skje, at politiet kommer på døra, er det denne minnepinnen han kommer til å nappe ut av pc-en. Den unge gutten som sitter på kontorstolen kommer til løpe frenetisk opp en etasje og kaste den i mikrobølgeovnen. Og da kommer alle spor til å viskes bort, og foreldrene som sitter i etasjen over og ser tv vil aldri få vite hva han egentlig har holdt på med.

Ikke FBI heller.

Det er ikke uten grunn at Fredrik har klekket ut den planen etter alt som har skjedd de siste månedene. Han håper bare han slipper å følge den.

Grillukten henger tungt over boligområdet på det sentrale Østlandet. Det er vår, og ettermiddagen er varm. Lyden av lekende barn på grønne plener og summing fra terrasser sprer seg i de rolige gatene. Men nede i kjelleren stenges sollyset ute av de mørke gardinene. Midt i rommet står et skrivebord med to store høyttalere og en skjerm. Et par harddisker ligger slengt på bordet. Rommet fylles av summingen fra en hardtarbeidende datamaskin, og lysdiodene blinker og blinker. Som et hvilket som helst gutterom. Men dette er hovedkvarteret til en av landets fremste datahackere[1].

De lange, tynne fingrene raser over tastaturet. Klikk-klikk-klikk-klikk. Kommandolinjene på skjermen reflekteres i konsentrerte, men trøtte øyne. Kommunikasjonen mellom 17 år gamle Fredrik og de andre medlemmene av Anonymous, en av de mest beryktede hackergrupperingene i verden, går på nettbaserte programmer som Skype og IRC[2]. Lynraskt. Det er slik de koordinerer angrepene.

Foreldrene sitter foran tv-en i etasjen over. De vet ikke helt hva som foregår nede i kjelleren, men det kan hende de begynner å forstå mer etter hvert, tror Fredrik. Om noen måneder kanskje. Når ting begynner å dra seg til.

Om en liten time kommer Fredrik til å sovne i kontorstolen, som vanlig. Når han våkner igjen, med et rykk, kommer han til å fortsette der han slapp. Et lite tastetrykk så er han der igjen, ved frontlinjen i en elektronisk krig som virker så uendelig langt borte, men som er rett der nede, inne i kablene som forsvinner under pulten, gjennom veggen og ut i cyberspace[3].

FREDRIK ER EN normal norsk tenåring, men noe skiller ham fra jevnaldrende skolekamerater: Han lever i konstant frykt for at politiet skal dukke opp. Fra gutterommet driver han nettkrig mot norske myndigheter, mot diktaturer i Midtøsten, mot Pentagon, CIA og andre utenlandske etterretningstjenester. Med sin egen framtid som innsats, og det er framtiden han kjemper for.

17-åringen er en del av den voksende bevegelsen av norske ungdommer som sniker seg inn i datasystemer for å hente hemmelig informasjon. De utfører også såkalte tjenestenektangrep[1] for å vise sin misnøye med politiske vedtak. Det er ytringsfrihet dette handler om. Kampen mot diktaturer i Midt-Østen, og mot påfunn som datalagringsdirektivet[2].

Hackernes angrep er det siste halvåret blitt så alvorlige at NATO, CIA og FBI har iverksatt en internasjonal klappjakt. Bak Fredrik lurer også en garde av middelaldrende og innflytelsesrike menn, som har drevet krig på nett i mange år.

Denne vårdagen aner det Fredrik at folk i kretsen rundt ham er i ferd med å ryke i klørne på sine verste fiender. Han vet at de kan havne i fengsel i flere tiår. I alle fall hvis de utleveres til USA. Fredrik vet ikke lenger hvem han kan stole på. Noen av hans hackervenner er tatt allerede. Andre har gått i dekning, og han lurer på om de samarbeider med politiet, om de kommer til å tyste på ham. Månedene som kommer vil gi ham svaret på om han får bruk for mikrobølgeovnen.

FØR FREDRIK ER myndig opplever han å bli jaget av FBI og av selskaper innenfor den private sikkerhetsindustrien i USA. Han har allerede rukket å bli intervjuet av Al Jazeera, Sky News og andre internasjonale medier. Alltid iført den velkjente Guy Fawkes-masken, dette kjennemerket på Anonymous. Masken ble verdenskjent gjennom filmen V for Vendetta i 2006. Den gir etterlengtet beskyttelse mot de mektige fiendene Fredrik og hans allierte utfordrer. Katolske Guy Fawkes var sentral i planen om å sprenge det britiske parlamentet i 1605, i kampen for katolikkers menneskerettigheter under den britiske tronen. Symbolikken er ikke tilfeldig.

For noen måneder siden, i februar, var Fredrik én av tre personer som dro i gang en større nettbasert etterforskning. Målet var å avsløre amerikanske etterretningsprogrammer som etter sigende driver med overvåking og manipulering av millioner av mennesker, blant annet i den arabiske verden. De siste månedene er stadig flere nettsider til statlige, politiske og private aktører blitt angrepet.

Mens datahackerne tidligere representerte en subkultur på nettet, utgjør de i dag en sterkt voksende motstandsbevegelse - et tilsynelatende hodeløst troll - som skremmer vettet av regjeringer og makthavere verden rundt. Et troll som i nådeløs frekkhet ydmyker makten i all offentlighet. I tillegg er trollet i ferd med å vokse seg større og farligere.

Fredriks øyne er trøtte. Det er rett før han sovner nå. Men blikket slipper aldri skjermen. Fingrene hans er som limt til tastaturet. Kommer noen til å dolke ham i ryggen? Bør han slutte nå, før politiet banker på døra? Det begynner å bli farlig.

Skulle du komme i skade for å bli en fiende av Fredrik, svir det. Han har våpen vi vanlige mennesker ikke ser, og langt mindre forstår. Men om du ikke forstår det, merker du det. Blir ditt navn nevnt i et manifest fra Anonymous, er det som regel starten på en dårlig uke. Hackerne avslutter alltid sine meldinger slik:

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.

9. APRIL, NOEN uker før besøket hjemme på gutterommet, ble jeg oppringt fra et uregistrert nummer. Den unge stemmen i andre enden presenterte seg ikke. Noen dager tidligere var nettsidene til Arbeiderpartiet og Høyre blitt hacket av ukjente gjerningsmenn. Ap fikk sin nettside satt ut av spill midt under eget landsmøte, til stor ståhei i mediene.

- Kan du være med på en Skype-samtale med en liten gjeng?

Gruppen identifiserte seg som medlemmer av Anonymous. Dette var norske nettkrigere. Jeg hadde jobbet en del journalistisk med de hemmelige tjenestene, og de ville vite hva jeg trodde om mulighetene for at de hemmelige tjenestene og andre kan utnytte datalagringsdirektivet på ulovlig vis.

Tre dager senere begynte gruppesamtalen på Skype å bli en smule kaotisk. 25 ungsauer snakket

1> Hacker er en person som sniker i fremmede datasystemer for å oppdage hemmeligstemplet informasjon.

2> Skype er et nettbasert telefonprogram. IRC er det nettbaserte chatteprogrammet Internet Relay Chat.

3> Cyberspace er sammenkoblede datasystemer. Refererer til det fysiske nettet og den tenkte nettverdenen.

1> Tjenestenektangrep er angrep hvor man hindrer en person eller et system tilgang til informasjon eller ressurser de skal ha tilgang til.

2> EU-direktiv vedtatt av Stortinget den 4. april i år. Pålegger lagring av trafikkdata for e-post, ulike typer telefoni og internett. Tanken er å bruke informasjonen i bekjempelse av kriminalitet. Direktivet møter sterk motstand fordi mange betrakter det som et alvorlig inngrep i personvernet og frykter at personsensitiv informasjon kan misbrukes.

i munnen på hverandre. Men Fredrik holdt samtalen på sporet. Etter en liten stund forsnakket en av ungdommene seg. Han bestemte seg for ikke å prøve å bløffe seg ut av situasjonen.

– Ja, du skjønner vel at det var vi som hacket nettsidene til Arbeiderpartiet og Høyre.

Noen lo, andre forble tause, og ville ikke gi seg til kjenne mens jeg var pålogget. Men jeg satt igjen med alle nickene[1]. I løpet av kort tid hadde jeg god oversikt over deler av det norske hackermiljøet.

1> Et «nick» er en persons brukernavn på nett.

I DAG, HER HAN sitter på sitt anonyme gutterom, forklarer Fredrik noe av grunnen til at de stresset sånn den dagen. En 18-årig internasjonal hackervenn med nicket «Topiary» er nemlig sporløst borte. Fredrik vet ikke hvilket land han bor i. Få dager før Skype-samtalen hadde Topiary sagt at han hadde observert tre hvite vans ved huset sitt. Deretter ble tastaturet hans taust. I fraværet av nyheter om pågripelse og politiaksjon, frykter hackerne at kameraten er kidnappet av noen som opererer på vegne av amerikansk etterretning. Topiary var involvert i mye rart, mener Fredrik. Og nå er han forsvunnet.

– Topiary skrur alltid av ruteren[1] når han går ut. Men nå har ruteren hans stått på i to sammenhengende uker. Det har aldri skjedd før, sier Fredrik.

I Norge diskuterer hackerne hva som kan skje hvis noen banker på døren også hos dem. Fredrik og de andre beskytter seg bak krypterte nettforbindelser, såkalte VPN-tunneler[2]. Noen av dem bruker såkalte Tor-noder for å kamuflere trafikken sin. The Onion Routing project (Tor) ble utviklet allerede i 2002, men er de siste par årene blitt en stadig mer populær tjeneste. Programmet styrer internettrafikken din via en lang rekke servere, slik at det blir svært vanskelig, bortimot umulig, å finne ut hvor du fysisk holder til. For etterforskere som

1> Ruter er en maskin som distribuerer et nettverk til forskjellige datamaskiner.

2> VPN-tunnel er en sikker og privat forbindelse over et offentlig nett.

vil finne Fredrik, kan han befinne seg på et hvilket som helst gutterom i et hvilket som helst land.

Han kan kaste den svarte minnepinnen i mikrobølgeovnen hvis han må. Mikrobølgene ødelegger effektivt alt som er lagret. Men ingenting er godt nok hvis sikkerhetslekkasjen kommer innenfra, enten gjennom at noen tyster eller at gruppen blir infiltrert. Det skal ikke mer til enn at en eller annen ungdom dolker ham i ryggen.

PÅ NETT BRUKER Fredrik forskjellige kallenavn, og han gjør alt han kan for å skjule seg.

Det er ikke uten grunn han er paranoid. Det siste halvåret har hans motstand mot overvåking, og støtte til demokrati og åpenhet, ført ham inn i heftige konflikter. Flere av de mest kjente hackerne i verden bekrefter at de har samarbeidet med den norske 17-åringen. Mine neste møter med Fredrik; mitt forsøk på å forstå hvem han og vennene er, på å finne den sporløst bortkomne Topiary og på å undersøke våpnene og slagkraften til de unge nettkrigerne som har fått NATO og CIA på alerten, må derfor foregå elektronisk.

Jeg skrur på pc-en og finner Fredrik i cyberspace. Han taster meldinger om hvor forsiktig han hele tiden må være, om hvorfor vi må kommunisere her, gjennom kilometer med trygge kabler.

<Fredrik>: nå når jeg gjør snodigeting så booter[1] jeg fra en usb-stick[2]

<Fredrik>: ingen harddisk i det hele tatt

<Fredrik>: den stikken er ikke så vanskelig å ødelegge hvis noen skulle komme etter meg

<Plot>: hvordan fungerer det - å boote fra en usb-stick?

<Fredrik>: vel, noen hovedkort[3] har den muligheten at de emulerer en harddisk[4], altså lurer pc-en til å tro at usb-sticken er en harddisk

<Fredrik>:men det funker på samme måte

<Plot>: sånn at alle sporene er på sticken, ikke bare filer, men rubbel og bit, logger, osv.

1> Å boote er å TRENGER HJELP!
2> USB-stick er en minnepinne du kan lagre data på.
3> Hovedkort er datamaskinens hjerne og motor.
4> Harddisk er en datamaskins lagringsplass.

<Fredrik>: altså, jeg hadde planer for noen uker siden om å kjøpe meg en egen mikrobølgeovn for å ha under senga

<Fredrik>: jeg er litt paranoid

<Fredrik>: bare kaste inn stikken

<Plot>: mikro under senga - det er ganske heftige greier

<Plot>: Hvorfor velger du dette livet likevel da, når det blir så mye paranoia?

<Fredrik>: haha ja, men det er det eneste som faktisk ødelegger noe elektronisk helt.

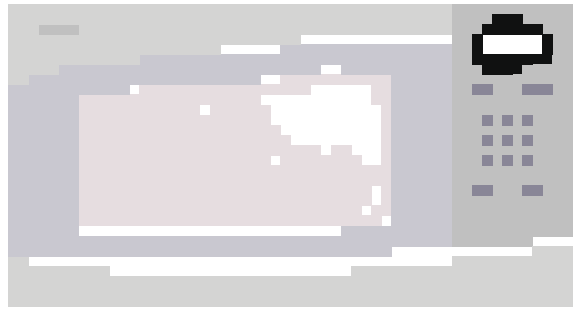
BARE NOEN MÅNEDER tidligere kunne administrerende direktør Aaron Barr i HBGary Federal fortsatt smile. Det private sikkerhetsselskapet han ledet arbeidet for den amerikanske regjeringen, og var spesielt på jakt etter lukrative kontrakter på etterretningsområdet. Etter kort tid i sjefstolen hadde Barr den perfekte pr-pakken klar. Intervjuet med Financial Times var spikret. Nyheten var at den nye toppsjefen hadde kartlagt lederskapet til hackergruppen Anonymous. Avsløringen ville gi Barr muligheten til å spise kirsebær med de store. Dette var ettertraktet informasjon.

Blant dem Barr hadde jaktet på informasjon om, var Fredrik i Norge.

«Hva gruppens størrelse angår, vil jeg understreke at lederskapet er på rundt 30, mens den operative gruppen er på flere hundre», skrev Barr i en e-post til Financial Times-journalisten i 18-tiden fredag 4. februar. Kort tid senere publiserte Financial Times nyhetssaken «Net closing on cyberactivists». Reaksjonen lot ikke vente å seg. Natt til lørdag sendte Barr en mail til en kollega: «Interessant dag. Jeg er blitt kontaktet av forsvarsministerens kontor (Rosemary), FBI, USG og nå DNI... alt sammen i dag. Jeg har et møte med FBI og OSD mandag klokka 11».

PR-stuntet til den ferske direktøren fungerte. Men det Barr ikke ante, var at hans angrep på Fredrik og hans venner var begynnelsen på slutten for ham selv som konsernsjef. Det var nemlig ikke bare forsvars- og polititopper i Washington D.C. som hadde rettet blikket mot HBGary Federal.

Ledelsen i selskapet hadde forberedt seg på motangrepet fra Fredrik og hans medsammensvorne. De var godt nok forberedt, trodde de, og TV-kanalen CBS sitt prestisjefylte program «60 Minutes» hadde allerede meldt fra at de ønsket å lage et nyhetsinnslag om Barrs suksess med å ta hackerne. Klokken 18.19 samme dag var lykkerusen ugjendrivelig over. Da hadde Fredrik og hans venner gått til angrep, og skjoldet Barr hadde satt opp lå knust tilbake.



En rasende Barr ble bare sintere utover helga, ettersom angrepet økte i styrke. «Denne gjengen tar ikke budskapet!!!! (...) Jeg kjenner ikke bare IRC-aliasene[1] deres, jeg kjenner de jævla navnene og hjemmeadressene deres!!!!!!», skrev han i en mail til markedssjefen og styrelederen i HBGary.

Straks etterpå måtte han melde til sine medarbeidere at et større angrep var under oppseiling. Han vedla en skjermpdump[2] fra en chat der en hacker prøver å rekruttere andre til en nært forestående operasjon. Skjermdumpen viser at Topiary, Fredriks medsoldat, unggutten som nå er sporløst forsvunnet, var en av arkitektene bak angrepet.

Topiary: Hello

CogAnon: Hi

Topiary: We're recruiting for a new operation in the Washington area; interested?

CogAnon: ok so what do you need from me?

Topiary: Our target is a security company. We may need local help on information gathering.

CogAnon: ok well just let me know.

Kilder i hackermiljøet sier Barr selv var «CogAnon» i denne dialogen. Da Barr logget på for å sende mailen med skjermdumpen fra samtalen, ante han imidlertid ikke at det som skjedde var en avansert lek der hackerne fikk med seg alt som foregikk.

Også passordet hans.

1> IRC-aliasene er navnene de bruker på chatteprogrammet IRC.
2> Å sende kopi av det du ser på skjermen.

BARRS STORE BRØLER var at han benyttet det samme passordet overalt. Hackerne sikret adgang til hele mailserveren, med muligheten for å bytte passord på en lang rekke andre brukere. De fikk tilgang til alt de ønsket seg, og mer til, uten å måtte anstrenge seg.

- Operasjonen var ganske banalt enkel, egentlig, sier en hacker som deltok i aksjonen.

Før Aaron Barr rakk å overlevere informasjonen om hackerne til FBI neste morgen, slik han hadde planlagt, sørget ungdommene for at han fikk en telefon fra en journalist i amerikanske Forbes Magazine. Barr var rystet da han fikk vite at hackere ikke bare hadde tatt ned nettsidene, men også lastet ned kopier av samtlige mailer på mailserveren, mer enn 60 000 mailer totalt. At de hadde slettet alle backup-filer, tatt over Barrs twitterkonto og lastet ned dokumentet Barr skulle overlevere til FBI neste dag.

I det 23 sider lange dokumentet er tre norske hackere identifisert ved navn. Fredrik som overvar angrepet fra orkesterplass, er ikke navngitt. I dag sier han at de tre navngitte er helt ukjente i det norske hackermiljøet. I tillegg inneholder dokumentet navn på to danske hackere, pluss navn fra 15 andre land. Topiary var naturlig nok ett av dem.

28. februar erklærte Aaron Barr at han forlot stillingen som konsernsjef etter bare ett år og fire måneder i sjefstolen. Han driver i dag et eget rådgivningsselskap. Når jeg kontakter Barr med tilbud om å kommentere saken, svarer han ikke.

Forsøket på å ta hackerne hadde feilet kapitalt. Fredrik kunne smile den februardagen. Han ble aldri navngitt, FBI fikk aldri has på ham og han kunne se fram til en ny vår med nettkrig fra gutterommet på Østlandet. Men den nagende usikkerheten slapp ikke taket. Var de på sporet av ham? Og hva skjedde egentlig med Topiary? Ble han tatt? Kom han til å tyste?

DET MASSIVE MATERIALET Fredrik og hans Anonymous-kolleger hadde hentet ut av mailserveren til Barrs selskap, viste at sel-

skapet utførte oppdrag for både det amerikanske forsvaret og etterretningstjenestene.

Gjennom en nettbasert etterforskning kalt «Operation MetalGear», fant Fredrik og medhackere ut at selskapet hadde utviklet programvare som gjør det mulig å administrere ti forskjellige falske personprofiler i sosiale medier samtidig. Slik kan det amerikanske forsvaret med letthet manipulere medier som Facebook og Twitter. Mailene satte dessuten Fredrik og de andre på sporet av et omfattende overvåkingsprogram: «Odyssey» har som formål å overvåke og manipulere bruken av sosiale medier i den arabiske verden. Tidligere ble programmet kalt COIN, et ord som vanligvis brukes som forkortelse for «counter insurgency», altså metoder for å slå ned folkelig motstand.

Fredrik var en av de tre initiativtakerne til etterfølgeren av «Operation MetalGear», som blir kalt «ProjectPM». Det er her de fleste hackerangrepene nå planlegges og koordineres. «ProjectPM» har tidvis fungert som basen til Anonymous-bevegelsen. Det som utad ser ut til å være et hodeløst troll, er i realiteten langt mer organisert og med et ganske tydelig hierarki.

I «ProjectPM» er det i praksis den amerikanske frilansjournalisten Barrett Brown som leder arbeidet. Brown er omstridt både innad i gruppen, og bortimot hatet blant sentrale aktører i Anonymous fordi han har valgt å stå fram som en form for uoffisiell talsmann i mediene. I mitt forsøk på å forstå hva hackere som Fredrik egentlig slåss for, hva som driver dem, kontaktet jeg tidligere i vår Brown. Han fortalte meg at han og hans gruppe blir tvunget til å bryte loven for å få tak i informasjon, på grunn av den manglende kontrollen av det amerikanske etterretningssamfunnet.

– Det er åpenbart at en del viktig informasjon om programmer som det offentlige finansierer, bare kan skaffes ved hjelp av metoder som inkluderer å bryte seg inn i selskapers servere. Hvis den amerikanske kongressen eller andre representanter for de stemmeberettigede var i stand til å faktisk kontrollere denne virksomheten, ville det ikke vært behov for å hacke seg inn i disse selskapene, sa Brown.

Brown var dessuten åpen på at han har samarbeidet tett med en 17 år gammel gutt i Norge. Fredrik. Og det er slike tanker – om behovet for å spre informasjon som hemmeligholdes av myndigheter og andre mektige aktører – Fredrik har når han noen måneder seinere skrur på maskinen og melder seg til tjeneste i den elektroniske skuddlinjen.

Men dessverre er det ikke bare fiender som FBI, og partiene som støtter Datalagringsdirektivet han må slite med for tiden. De interne konfliktene i det norske hackermiljøet er kraftig skjerpet de siste ukene, og risikoen for å bli tatt bare øker for Fredrik.

8. MAI EKSPLODERER det i IRC-kanalen «AnonOps», Anonymous-bevegelsens digitale forsamlingshus. Tre brukere, frontet av en person som kaller seg «Ryan», skyter plutselig og uforklarlig ned Anonymous-bevegelsens egen IRC-server. Jeg er flue på den elektroniske veggen

når en lang rekke ip-adresser[1] til brukere av «AnonOps» legges ut på nett. Plutselig er de indirekte navngitt. Bak en ip-adresse kan man ofte finne et navn, hvis vedkommende ikke har beskyttet seg godt nok. I et eksklusivt intervju med det britiske nettstedet «Thing» sier Ryan seinere at angrepet var en protest mot sentralisering av for mye makt innad i Anonymous-bevegelsen.

I realiteten var angrepet neppe spesielt krevende, fordi Ryan hadde eierskapet til domenene. Det var dermed en enkel sak å omdirigere trafikken til en annen server. Han var også administrator på IRC-serveren, og hadde derfor rutinemessig adgang til IP-loggene han publiserte.

Når Ryans angrep er over, popper Fredrik opp på Skype.

<Fredrik> Haha, det er ingenting, vi har ikke blitt hacket. Det var en admin som backstabbet[2] oss.

Ryan var sterkt uenig i at en mektig elite, de som var operatører på de to sentrale IRC-serverne fram til da, bestemte hvem som skulle bli angrepet. En elite som Fredrik hadde tilknytning til. Konflikten henger også sammen med en stadig sterkere todeling av makten innenfor Anonymous-bevegelsen, der en del av hackerne utviklet seg i en stadig mer radikal retning.

Igjen viser Fredrik og hans venner muskler.

Allerede samme dag blir Ryans egentlige identitet avslørt, i et rent hevnangrep. Ryan Cleary (19), får sin bostedsadresse i Essex i England publisert, sammen med telefonnummer, Skype-nick, ulike brukernavn, navn på andre familiemedlemmer og ytterligere private opplysninger. Det skal vise seg å være svært dårlige nyheter for den engelske 19-åringen.

I DAGER SENERE har Norge akkurat marsjert seg gjennom 17. mai da VG Nett melder at det norske forsvaret har vært utsatt for et massivt dataangrep, et angrep som «er blant de mest alvorlige i Norge hittil». Dagen etter følger papirutgaven opp, med forside og fire sider. Den ene overskriften lyder: «Massivt og målrettet», mens det andre hovedoppslaget har overskriften «- Kan lamme den norske økonomien».

I hackermiljøet blir nyhetsoppslagene og Forsvarets reaksjon møtt med en latter:

<Fredrik> haha, jeg ler litt av det jeg
<Fredrik>: de skrev noe om at det var det mest omfattende angrepet så langt ..
<Fredrik>: altså, en epost med en attachment[3]
<Plot>: så dette er neppe rettet spesifikt mot Forsvaret?
<Fredrik>: vel, jo, jeg tror det er rettet spesifikt mot forsvaret
<Fredrik> men jeg vil ikke si at det er noe .. "hardhacking"
<Plot>: Vil du karakterisere det Forsvaret snakker om her som hverdagslige IT-utfordringer?
<Fredrik>: vel, ikke hverdagslige, det skjer ikke hver dag, men det er SVÆRT vanlig
<Plot>: Dersom Forsvaret kaller dette det mest alvorlige angrepet noensinne, er det sannsynlig at de har vært utsatt for angrep som de IKKE har oppdaget?
<Fredrik>: Det er veldig sannsynlig, ja.

I stedet forteller Fredrik om langt mer alvorlige tilfeller av hacking.

<Fredrik>: for en liten stund siden ble det jo avdekket at en kar hadde adgang til mange servere som blant annet tilhører Pentagon og FBI.
<Fredrik>: og det visste ikke de noe om.
<Fredrik>: (prøver bare å si at om noen er erfaren nok og vil inn, så kommer han inn, uten at noen vet om det)
<Fredrik>: igjen, ingenting i media.
<Fredrik>: hvorfor skriver ingen om dette? :P

Plutselig kommer det en ny melding fra Fredrik på IRC-serveren vi kommuniserer gjennom.

<Fredrik>: https://www.fcg.pentagon.mil/
<Fredrik>: brukernavn Hoplite
<Fredrik>: passord xxxxxxx (fjernet av red)
<Plot>: tror ikke jeg tar sjansen på å logge på
<Plot>: da går jeg litt ut av journalistrollen min her ... men har du gått inn?

Få sekunder seinere sitter jeg med flere skjermdumper som viser ugraderte, men like fullt interne informasjonsskriv til ansatte i Pentagon. På nyhetsnettstedet jeg i tillegg er blitt henvist til, ser jeg dessuten eksempler på dokumentforsider med påskriften «Appended document contains special intelligence material» og «Defence Intelligence Agency», som er materiale fra andre hackerangrep mot Pentagon. Den norske 17-åringen er i ferd med å demonstrere hvor skarpe kniver han sitter med.

<Plot>: Men hva slags info er det man får tilgang til her?
<Plot>: er dette hoveddatanettverket til Pentagon?
<Fredrik>: hmm ser ikke ut som det var noe spesielt
<Fredrik>: DoD Foreign Clearance Guide
<Plot>: reiseråd
<Plot>: hva slags papirer du må ha med deg i forskjellige land

1> IP-adresse er datamaskinens unike adresse, som gjør det mulig å spore trafikken tilbake til den.
2> Admin backstabbet betyr at en administrator dolket dem i ryggen.
3> Attachment er vedlegg, her til en e-post.

<Fredrik>: jo og noe annet info

<Fredrik>: xxxx (link fjernet av red)

Ved å trykke på linken jeg akkurat har fått tilsendt fra Fredrik, befinner jeg meg plutselig og helt uforvarende inne på en nettside med overskriften «Level 1 Training System - ANTITERRORISM». For å unngå å gjøre meg skyldig i lovbrudd, lukker jeg raskt nettsiden. Når jeg siden forsøker å finne ut hvor dypt inne i dette nettverket Fredrik har beveget seg, spøker han det bort og begynner i stedet å snakke om hvor vanlig det er at nettverk blir angrepet. Det er i et slikt øyeblikk han betror meg at hackere tidligere har snoket i mailkontoen til statsminister Jens Stoltenberg. 17-åringen sier at han selv leste syv av disse mailene, som ble lagt ut på nettstedet 4chan. Fredrik lover å se om han kan få tak i kopier av mailene. Det klarer han aldri.

Noen dager senere melder han tilbake.

<Fredrik> det skjedde i fjor

<Fredrik> og de ble postet på 4chan, men siden det ikke var noe spesielt så var det ikke noen som tok vare på det, det kan også ha vært falsk

<Plot> leste du de forrige mailene selv? siden du sa det var syv mailer

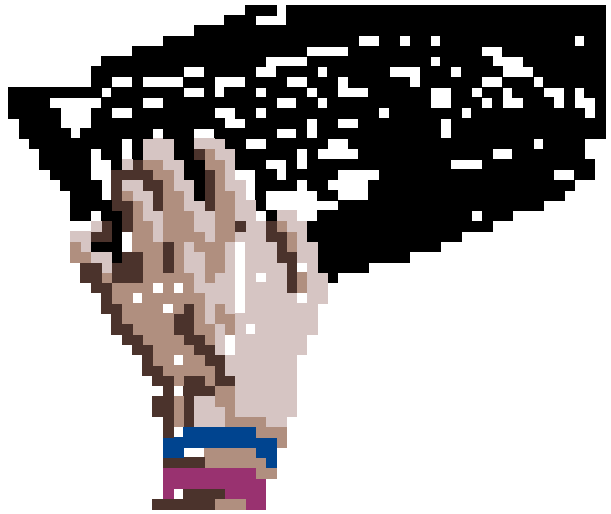
<Fredrik> jeg fikk bare høre at det var 7

<Plot> ok. Dere er ikke bare taktiske nå da?

<Fredrik> heh jo, vi er litt mer taktiske nå

De internasjonale hackernyhetene er blitt stadig flere de siste ukene, og Fredrik er nervøs. Mine forsøk på å bore ytterligere i Stoltenbergs mailer, fører bare til unnvikende svar. Er mailene bare en bløff, eller begynner miljøet å bli paranoid? Nettstedet der mailene til Jens Stoltenberg angivelig skal ha blitt lagt ut, er en slags oppslagstavle der mye av online-aktivismen har sitt historiske utspring. Mengden av informasjon som blir postet på 4chan gjør det krevende å følge med. Det er stedet der alt startet, men det er også et sted som med en viss berettigelse kan kalles for nettets avløpssystem.

I dag er det IRC-kanalen «AnonOps» som er møtestedet for hackere som slutter opp om Anonymous-bevegelsen. Norske hackere bruker mye tid her. Det gjør de også på den nasjonale varianten



«Opnorway».

FREDRIK ER SELV administrator for IRC-serveren der «Opnorway» er plassert. Det er herfra mange av de viktigste cyberangrepene i Norge den siste tiden er blitt planlagt, koordinert og gjennomført.

Etter hvert som paranoiaen har grepet om seg i hackermiljøet, i kjølvannet av de stadig mer høyprofilerte aksjoner og rykter om infiltrasjonsforsøk, er mange usikre på hvor trygt det er å bruke «AnonOps» og «Opnorway». Det er ingenting som hindrer politifolk og infiltratører å gå inn i IRC-kanalen og logge alt det som foregår der.

Miljøene blir derfor stadig mer lukkede, og diskusjonene tas i økende grad på Skype. Helst i form av samtaler som ikke kan rekonstrueres. Skype er langt tryggere enn IRC, og går for å være ganske avlyttingssikkert. Men det er hackere som ikke engang stoler på Skype. Disse ungdommene er paranoide med god grunn. De vet hvor hardt de kommer til å straffes hvis de blir tatt i å snoke i ting som er hemmelige.

Hackerne lurer fortsatt på hva som skjedde med Topiary. Nye forsøk på å få tilgang til informasjon om den savnede hackeren fører ikke fram. Ingen vil snakke.

<Fredrik> det er enkelte som har vært med oss i 2 år som plutselig gikk til FBI og snyltet på noen av oss

<Plot> såpass?

<Fredrik> vi har enda ikke sett eller hørt ifra han

<Fredrik> om han hadde blitt pågrepet så hadde det vært i media - det er derfor vi tror noen har snatcha han.[1]

<Fredrik> det ligger jo også noe i at hvis han bare har stukket av, og navnet hans kommer ut i det offentlige, så blir han jo tatt.

<Fredrik> han har gjort mye rart

DA JEG BEGYNTE å jobbe med denne reportasjen i begynnelsen av april ville flere av de norske hackerne stå fram. Det er helt uaktuelt i dag. I løpet av noen uker har frykten tatt over. I tillegg til politiet, kommer truslene på nett. Online-jungelen der hackerne ferdes, er et lovløst samfunn, der regelen om den sterkestes rett gjelder. Han du ler sammen med i dette øyeblikk, kan i neste sekund være din farligste fiende.

<Fredrik>: var noen som kjørte vulnerabilityscans på secnet[2] i går

<Plot>: hvordan gikk det?

<Fredrik>: en av de prøvde å utnytte en sårbarhet i IRC-en

<Plot>: vet du hvem?

<Fredrik>: nope, men han brukte ikke VPN[3].

<Fredrik>: han har ikke hatt internett siden jeg fant det ut

En norsk 17-åring har altså slått ut nettet til en person på andre siden av jordkloden. Fredrik sier han prøver å være forsiktig med slagkraften han kontrollerer. Men han nøler heller ikke med å bruke den. Hackerne som forsøkte å trenge seg inn på IRC-serveren var ikke norske, men fra Kina og USA.

<Fredrik>: kineseren scannet bare, fant ingen feil, så han hoppet sikkert til neste mål

<Fredrik>: amerikaneren ga ikke opp så lett

<Fredrik>: han brukte ikke tor[4] engang

1> Å snatche betyr ta/snappe.
2> Vulnerabilities på secnet betyr sårbarheter på et bestemt nett.
3> VNP refererer til VNP-tunnel, altså den sikre og private forbindelsen som hackerne bruker.
4> Tor refererer til Tor-noder, altså den andre formen for sikker forbindelse.

<Fredrik>: så det var han du tok ned?

<Fredrik>: yep

De fleste hackere med næringsvett og intakte overlevelsesinstinkter beskytter seg godt. De tekniske våpnene og skjoldene nettkrigerne utstyrer seg med, er så komplekse at det er vanskelig å henge med. VPN-tunneler er en vanlig form for beskyttelse. En slik tunnel gir deg en såkalt kryptert nettforbindelse og ruter trafikken din via en lang rekke forskjellige servere slik at det ser ut som om du sitter et helt annet sted i verden. I tillegg blir det vanskeligere å hacke deg. Dataprogrammet «Tor» gjør noe av det samme, og ble utviklet for å hjelpe opprørerne i den arabiske verden.

Fredrik bruker «Tor» ganske mye.

<Fredrik>: det er bare når man skal utføre skikkelige ulumskheter at man bruker begge.

<Fredrik>: forresten

<Fredrik>: for noen dager siden, så fikk en anon i USA FBI på døra

<Fredrik>: VPN'en som han brukte (en gratis og dårlig en, men det står klart at ingenting logges på nettsidene deres) ga IP addressen hans til FBI

<Fredrik>: det har vært snakk om noe angrep på dem (Cyberghost)

<Plot>: ah, ok. så det kan hende at FBI følger VPN-leverandørene ganske tett?

<Fredrik>: gratisvalgene ja

<Plot>: men betalingsløsningene er sikrere?

<Fredrik>: ja, "kjenner" en av de som driver VPNtunnel, de logger ingenting

<Plot>: Var det noen som var involvert i Metal Gear som fikk besøk?

<Fredrik>: vel .. topiary er jo borte

<Fredrik>: bortsett fra det, så nei.

<Plot>: hvor sentral var topiary i det som skjedde?

<Fredrik>: vi tror de samler opp info for å gjennomføre masse raids.

<Fredrik>: han vet mindre enn det jeg gjør

<Fredrik> men han deltok i angrepene på hbgary og en hack som kommer til å skje snart

<Fredrik>: de kommer til å hacke FBI

<Plot>: når da?

<Fredrik>: jeg vet ikke hvor og når, men jeg vet de kommer til å gjøre det

<Fredrik>: de hacket en nettside hvor du trengte FBI auth for å signe opp

<Fredrik>: og dumpet hele databasen med brukere og passord

<Fredrik>: jeg sier bare, om de gjør det så er helvete løs

<Fredrik>: det er også derfor jeg tar litt avstand fra anon akkurat nå

<Fredrik>: de har allerede hacket noen twittere osv til folk som er assosiert med fbi

Hackerne Fredrik refererer til, tilhører en ny gruppe som regnes som spesielt farlig. Gruppen heter LulzSec og har i løpet av de siste ukene laget voldsomme bølger internasjonalt. På kort tid fikk gruppen, som besto av seks-syv medlemmer, flere enn en kvart million følgere på twitter.

Og Fredrik får rett. Kort tid senere blir det kjent at LulzSec har gått rett i strupen på et selskap som gjør mye arbeid for FBI. En annen hackergruppe, som bistår amerikanske myndigheter med aktive mottiltak mot det som i økende grad blir karakterisert som «cyberterrorisme», la nylig ut en liste over det de mener er ledelsen i LulzSec, fem hackere med navnene «Sabu», «Tflow», «Kayla», «Joepie91» og Topiary.

Topiary skal ha vært ansvarlig for opprettelsen av twitterkontoen til LulzSec, samt en telefonlinje som gruppen kunne ta imot publikumstelefoner på. Begge deler var høyrisikotiltak. Topiary gjorde også mange medieintervjuer mens ting stod på. Han kan ha vært uforsiktig.

Fredrik frykter at han skal plapre.

I BYEN VARNA I Bulgaria har den 80 år gamle lorden Thomas Michael Jopling akkurat lagt fram sin rapport på vårsesjonen til NATOs parlamentarikerforsamling. I rapporten slår generalrapportøren fast at cyberterrorisme er i ferd med å bli en så stor trussel at NATO ikke kan utelukke at artikkel 5-forpliktelsene utløses dersom ett medlemsland angripes. Det betyr at et cyberangrep mot ett land kan bli oppfattet som et angrep på forsvarsalliansen som helhet. Lord Jopling tar til orde for harde mottiltak: «Jo lenger disse angrepene vedvarer, dess mer sannsynlig er det at mottiltak vil bli utviklet og etablert, der gruppene blir infiltrert og gjerningspersonene straffeforfulgt».

Svaret fra LulzSec er like kontant som det er barnslig frekt: «We accept your threats, NATO. Game on, losers», skriver LulzSec i en pressemelding, etter å ha angrepet en nettside indirekte tilknyttet amerikanske FBI.

Og hva har hackerne i LulzSec egentlig å frykte? I slutten av mai, som lyn fra klar himmel, dukker Topiary plutselig opp igjen, tilsynelatende i god behold. Ifølge Fredrik bekrefter Topiary at han har vært i varetekt, men han gir få detaljer utover det. Andre hackere forteller at de i denne perioden opplevde at Topiary oppførte seg på en helt annen måte enn tidligere. De følte det rett og slett som om personen bak nicket hadde skiftet personlighet, eller var en annen person enn før.

<Fredrik>: han sa at de vil gå etter de som vil gjøre mer

<Fredrik>: og... jeg har ikke helt gitt opp enda

<Plot>: men satt han i varetekt?

<Fredrik>: ikke hele tiden

<Fredrik>: han sa ikke hvor lenge

Noen mener pågripelsen av Topiary bare er et ubekreftet rykte. Topiary selv er imidlertid gått i såkalte hidemode[1], og beveger seg bare på nettet under andre kallenavn og uten å legge igjen spor. Lettelsen over å få en av sine onlinevenner tilbake blir hos Fredrik etter kort tid erstattet med den nagende usikkerheten: Er Topiary blitt informatør for FBI eller andre lands myndigheter? Er Topiary erstattet med en annen person, en infiltratør? Kommer myndighetene til å finne ut hva Fredrik gjorde med toppsjefen i HBGary? Kommer de til å følge med når han om noen dager skal angripe regjeringens nettsider?

GLOBALT ER DET en hard kjerne på rundt ti personer som står for mesteparten av den ekstreme hackingen. For å unngå FBI og andre lands politimyndigheter, opererer de under varierende navn. Ofte bruker de Anonymous-identiteten for ikke å bli sett på som én felles hackergruppe, men i realiteten pleier de tett kontakt med hverandre. Flere av dem kaller seg «internetfeds» – med referanse til det amerikanske uttrykket «feds», føderale agenter. Hvis det er tjenestenektangrep som er målet, kan de ved hjelp av koordinerte angrep oppnå en ganske formidabel kraft. Selv om de ikke er mange.

Spørsmålet er hva Fredrik vil være med på. I tiden som kommer, blir hackernes angrep hissigere. Det samme gjelder reaksjonene fra myndighetene. FBI begynner å få nok. Og NATO. Fredriks krets har politirazziaer og heftige fengselsstraffer i vente. Temperaturen stiger og stiger i dette miljøet, og akkurat nå står den norske 17-åringen helt i fronten.

En talsmann for grupperingen AntiSec som er tett knyttet til LulzSec, gjør det klart at det er mye mer bråk i vente. Han nekter meg å gjengi nicket hans på trykk. Han viser til LulzSecs første kunngjøring som slår fast at alle hackere bør slå kraftig ned på offentlige aktører som misbruker sin makt.

<Plot> Dere har fått både NATO og Department of Homeland security på tærne allerede?

<xxxxxxx> Ja, virkelig. Vel, de erklærte i realiteten krig mot oss.

<xxxxxxx> Vi bare pirket borti dem tilbake, for å se om de mente alvor. Fordi vi vet at de umulig kan være det.

<xxxxxxx> Tannløs tiger, etter vår mening.

<xxxxxxx> Nettet er vårt, og de får ikke ta det fra oss.

<Plot> Enkelte hacktivister er bekymret over at de høyprofilerte angrepene som dere har gjennomført, tvinger myndighetene til å innlede en global menneskejakt, som igjen fører til at mange må løpe i dekning, og tar avstand fra Anonymous og det dere gjør. Kommentar?

<xxxxxxx> Vel, det er alltid slik myndighetene opererer, de prøver å skape frykt. Det virker på de fleste innbyggerne, så langt, men antallet blir stadig færre.

<xxxxxxx> Vi har en ganske stor gruppe av mennesker som ikke er redde lenger og som blir dårlige av undertrykkingen, sensuren, propagandaapparatet og alle restriksjonene.

En langt mer myteomspunnet hackergruppe, kaller seg Peoples Liberation Front (PLF). Gruppen ledes av hackerlegenden «Commander X». Ifølge videoinnslag på YouTube, der kommandøren holder forelesninger med forvrengt stemme og skjult ansikt, blir lederfiguren presentert som en tidligere militær etterretningsoffiser. Det hevdes også at han deltok i CIAs forskningsprogram på såkalt «remote viewing», der det amerikanske forsvaret og CIA forsøkte å utvikle synske evner hos forsøkspersoner.

«Commander X» er medlem av en liten gruppe eldre mennesker som pleier uformell kontakt med hverandre, og som utgjør en slags hackerelite på nettet. De fleste foretrekker å operere i skyggene, usynlige, men like fullt mektige. Gjennom sin tekniske innsikt og livserfaring er det lett for dem å styre massene, uten at det blir for tydelig at det er akkurat det de gjør. Men i mange sammenhenger blir tenåringer som Fredrik for villstyrige. Derfor holder de eldre seg litt på avstand.

PLF spilte, sammen med Anonymous, en sentral rolle i tjenestenektangrep mot regjeringsnettsteder i både Tunisia, Iran, Egypt og Bahrain i vinter og vår. Målet var å hjelpe revolusjonsbevegelsene i disse landene. Nye aksjoner er nå under oppseiling for å hjelpe opprørere i Libya, Yemen og Syria. Dette blir organisert gjennom IRC-kanalen «Operation Freedom» på AnonOps.

PLF ble stiftet allerede i 1985, lenge før Anonymous-bevegelsen tok form rundt 2006. I et sjeldent intervju «Commander X» ga til «IT World» i februar i år, fortalte han hvordan de velger sine mål.

Det må være aktivister/demonstranter på bakken.

Demonstrantene må være ikke-voldelige.

Det må finnes håp om seier.

Det må eksistere en moralsk begrunnelse for å engasjere seg.

Dette er voksne menn. De styrer unge hackere i langt større grad enn mange tror, og de slåss, som Fredrik, for fri informasjon. En av toppene i PLF, en hacker med kallenavnet «Sepr», som også er «commander» og nummer tre i hierarkiet, sier at Fredrik er en av de han har samarbeidet tett med. Sepr er bekymret over klappjakten på hackere ver-

1> Hidemode betyr at han gjemmer seg på nett.

den rundt. Han er redd mange unge soldater kommer til å ryke.

– Menneskejakten de siste ukene har i sannhet blitt intensivert, i hovedsak på grunn av hackerangrepene som LulzSec har gjennomført. Hvis LulzSec ikke hadde lagt ut på et sanseløst plyndringstokt, ville menneskejakten ikke ha vært fullt så intens, tror jeg.

DET ER FORTSATT uvisst hva som skjer i mange av de arabiske landene, som Syria, Libya og Jemen. Fredrik har sagt lite eller ingenting om hvorvidt han selv har deltatt i hackernes forsøk på å støtte revolusjonen i den arabiske verden.

<Plot> Har du vært med på Operation Freedom? OpTunisia, OpEgypt og de greiene der?

<Fredrik> vel det jeg bidro til var «care-packagen» som ble sent ut.

<Fredrik> det er en pakke med diverse tools og guides som viser deg hvordan du forblir anonym på internett

<Fredrik> det var også noen guider der som fortalte deg hvordan man kjørte en protest

<Fredrik> og hvordan man kom seg vekk fra politiet

Fredrik forteller at han kom med i aksjonene ganske tidlig, allerede i januar, da ting for alvor begynte å skje i Tunisia. Deretter gikk det slag i slag.

<Fredrik> jeg vil ikke si at jeg var en av «fedrene» til operasjonene

<Fredrik> men jeg var der veldig tidlig

<Plot> hvordan vil du beskrive stemningen?

<Fredrik> vel, først virket det..

<Fredrik> det var veldig stille

<Fredrik> plutselig.. bare.. fikk det voldsom fart

DET ER MANDAG 23. mai. Tidlig kveld. IRC-kanalen «Opnorway» summer av aktivitet. I den digitale bikuben arbeider tenåringene på spreng. Fingrene flyr over tastaturene i gutterom over hele landet. Mange er rasende på datalagringsdirektivet som Arbeiderbartiet og Høyre til slutt sikret flertall for. Det er tid for nye cyberaksjoner, og målet i dag er nettsidene til Arbeiderpartiet og regjeringen.

Selv om hendelsene de siste ukene har gjort Fredrik usikker på hvor drøye aksjoner han vil være med på framover, klarer han ikke ligge unna. Han er rasende på datalagringsdirektivet.

Etter hvert som ungdommer kommer hjem fra skolen og fotballtreningen, kommer stadig flere til i IRC-kanalen. Samtalen mellom dem er teknisk og for de fleste av oss uforståelig. Våpnene de bruker for å utmanøvrere beksyttelsessystemene til den norske regjeringen og Arbeiderpartiet forteller historien om ungdommer med vanvittige ferdigheter, både om sin motstanders skjold og om sine egne sverd.

Den nesten uforståelige kommunikasjonen er lyden av en hackers våpen. Dette er lyden av et angrep på den norske regjeringen.

<Fredrik> DNS hijacking er morro

<Nick1> Det stemmer

<Fredrik> men

<Nick1> Det er simpelt, ja. Men elsker hvordan de fremfører den

<Fredrik> regjeringen.no kjører apache 2.2 (fortsatt sårbar for slowloris)

<Fredrik> samme med AP

<Nick2> woot 2.2

<Nick1> Var jo slik vi tok ned AP først

<Fredrik> Altså, dere tok ned AP ved å klikke på ei fil, tror ikke noen av dere visste hvordan. :P

<Nick2> Glad for eg har 40 mbit gjennom VPN <3

<Nick1> Eller, jeg klikka ikke :P så på jeg :D

<Fredrik> pff

<Fredrik> uansett

<Fredrik> hmm følg med nå

<Nick1> Fant en måte å doxe den på xx forresten

<Fredrik> huh ?

<Nick2> skjedde det noe?

<Nick2> http://httpd.apache.org/security/

<Nick1> Yeye, bare nevner det jeg :P

<Nick2> Det finnes flere måte å doxe folk på

<Nick2> Kravene er at du må ha tid og gidde det.

<Fredrik> hvor er xxx?

<Nick2> han er på trening

Om kort tid skal oppvarmingen begynne. En gang i kveldingen vil nettsoldatene teste ut hvor godt beskyttet datalagringsdirektivets forsvarere er i den elektroniske verden. Angrepet Fredrik planlegger denne kvelden er av den milde sorten. Under et DoS-angrep står én eller veldig få pc-er for angrepet ved å utnytte svakheter på enkelte servere til å sette et bestemt nettsted ut av spill. Fredrik og en av hans hackervenner kan altså klare dette alene, med bare en maskin eller to. Men skadevirkningene vil til gjengjeld være begrensede. Dette gjør de bare for å markere seg. Og for å plage.

Skal angrepet virkelig svi, måtte de ha gjennomført et såkalt dDoS-angrep. Dette er et massivt angrep der flere tusen pc-er gjerne er med på å overbelaste og sprenge en server. Det kan være store samfunn av hackere som stiller opp, men det kan også være folk som deg og meg, som ikke aner at vi er med på angrepet. Hackere kontrollerer nemlig pc-ene til tusenvis av intetanende amatører verden rundt. Ved å infisere pc-er med virus, såkalte trojanere, skaffer de seg i praksis kontroll over pc-en din og får den til å gjøre det de vil.

Er din pc infisert med en trojaner, kan du risikere at den er nyttig i hackeres angrep på mål både her og der. Pc-er de kontrollerer samles i et såkalt botnet, som kan brukes til å koordinere den samlede innsatsen. Slik kan du bli en bondesoldat på den digitale slagmarken. Kanonføde.

Flere norske hackere forteller at de kontrollerer såkalte botnet. Ett av botnettene som blir delvis kontrollert fra Norge, utgjør mer enn 70 000 fjernstyrte datamaskiner, kalt «zombier» innad i hackermiljøet. For å gjennomføre et effektivt masseangrep mot en nettside, trengs det sjelden mer enn rundt tusen datamaskiner på en gang. Men alt avhenger av båndbredden og maskinvaren på serveren som blir angrepet, samt av båndbredden på «zombiene» i botnettet.

Det er gjerne tidligere sentrale folk i dataspillbransjen som kontrollerer botnettene i hackermiljøet. Å få det norske hackermiljøet til å innrømme hvor stor «ildkraft» de faktisk besitter, har ikke vært enkelt. Innrømmelsene må lirkes ut av de jeg møter på nettet.

– Dette botnettet er ikke brukt mot mål i Norge så langt, presiserer en av de som har tilgang til botnettet på mer enn 70 000 maskiner.

Vedkommende, en norsk hacker, frykter reportasjen jeg holder på med skal føre til at norsk politi fatter større interesse for det de driver med.

Fredrik og hans hackervenner har ikke noe botnet for hånden i dag. Middagen er fortært, og de vil nøye seg med et enkelt DoS-angrep. Bare for å teste forsvaret til regjeringen.

<Fredrik> oy, testfire i kveld?

<Nick2> sure

<Nick2> oppvarming

<Nick1> Si når og hvor og jeg er inn

<Fredrik> må finne ut om det trenger mere kraft

<Nick2> botnet

<Nick2> xxxxxxx har d

<Nick1> Kan da heller ha det litt morsomt enn å kjøre pure død :P

<Nick1> <xx>, du er zer0 ja?

<Nick2> Hva?

<Nick2> snakker du om Zer02k?

<Nick2> <xx> fikk du skannet sida til regjeringa.no eller noe sånt?

<Fredrik> scanna med litt forskjellig

<Nick2> (Y)

<Fredrik> morpheus osv

<Nick2> 0h ..

<Fredrik> det e nån sårbarheta der, men ingen æ kan ta nytte av

<Nick2> hmm

<Nick2> der?

<Nick4> Da er jeg back AA

<Nick4> ladd

<Nick2> yes

<Nick2> im here sir

<Nick4> !aeeess add xxx vop

<Nick4> Det er kommandoen

<Nick2> tar litt tid 0 o

<Nick4> <xx>, husker du hva slags type ehanserv bot vi har?

<Nick4> begynte med a

<Fredrik> Anope

<Fredrik> nei

<Fredrik> atheme

<Nick4> takker AA

<Fredrik> gutar

<Fredrik> regjeringen.no - tango down

Fra min egen laptop kan jeg se at regjeringens nettsider er nede for telling. Men hackerne kjører i første omgang bare en sårbarhetstest, og slipper taket i nettsiden etter noen få sekunder. Hovedangrepet planlegges til klokken åtte samme kveld. Motstanderen er sterk og godt beskyttet, men Fredrik og hans hackervenn har planen klar.

DENNE KVELDEN MARKERER starten på fire dager med stadig mer aggressive angrep mot både Aps og regjeringens nettsider. Ungdom-

mene angriper også nettsidene til enkeltrepresentanter som stemte for innføringen av datalagringsdirektivet. Ingen av angrepene blir registrert eller rapportert av norske medier.

Hackerne sliter litt med Arbeiderpartiets nettsider, som åpenbart har forbedret sikkerheten vesentlig etter forrige angrep i begynnelsen av april. Sidene tar rett nok telling, og regjeringens nettsider går ned for telling hver eneste dag hackerne holder på, men det tar som regel bare kort tid før de er oppe igjen. Nettsidene er trolig satt opp med flere webserverspeil, konkluderer hackerne. På dag tre lykkes hackerne med å skyte ned regjeringens nettsider i mer enn én time, men IT-driftsavdelingen i regjeringskvartalet stanser omsider angrepet, etter alt å dømme ved å blokkere alle utenlandske ip-adresser.

Selv om hackerne sitter i Norge, blir de satt sjakk matt av dette trekket, fordi de benytter seg av Tor-noder eller krypterte VPN-tunneler – altså framstår det som om de er i utlandet.

Kanskje burde de hatt et botnet. Da hadde nok avisene fått det med seg, så kunne de fått oppmerksomhet om motstanden mot datalagringsdirektivet, som hackerne frykter vil rive i filler nordmenns rett til privatliv.

<Plot>: ser at det er litt frustrasjon over manglende medieoppmerksomhet

<Fredrik>: haha, jo, det er jo det som er målet

<Fredrik>: men medianorge gir jo blanke faen i de virkelige problemene som vi har her

<Fredrik>: jeg har bestandig levd med det at «folk bryr seg ikke før det går ut over dem personlig»

<Fredrik>: og det stemmer, for 99% av befolkningen

<Fredrik>: (nesten...)

Nå er kampen på nett i ferd med å gå utover Fredrik personlig. I slutten av mai er bølgene i ferd med å nå nye høyder innad i Anonymous-miljøet i Norge. Flere personer, som ønsker å beskytte sin anonymitet, blir identifisert – eller doxxet, som det kalles i disse kretser. Et kvinnelig medlem av gruppen rundt Fredrik opplever å få sin Facebook-side hacket, og høyst private bilder publisert på profilen sin. De som står bak, er trolig medlemmer av den samme gruppen.

En annen hacker som i begynnelsen av april deltok i flere tjenestenektangrep, blant annet mot Aps nettsider, blir også navngitt på nett. Her skal noe av uenigheten skyldes at hackeren på egen hånd, over flere dager, gjennomførte et tjenestenektangrep mot nettsidene til Folkets Info, et uavhengig nyhetsnettsted som er populært blant hackerne og onlineaktivistene. Årsaken til angrepet mot Folkets Info skal være at vedkommende ble provosert over at nettsiden publiserte bilder av medlemmer av Anonymous-bevegelsen uten at ansiktene deres var sladdet.

Fredrik står midt i stridighetene. Han vet at flere sysler med planer om å opprette en konkurrende hackergruppe. Han teller på knappene. Diskuterer med sine nærmeste venner. Og han blir med.

Fredriks nyetablerte gruppe kaller seg Noria. Den lille gjengen uttrykker mistillit mot Anonymous Norway, som de mener hovedsaklig består av useriøse personer som henger på og griner over hvor lite som gjøres. 90 prosent av Anonymous-gjengen synes bare det er kult å virke rebelsk, mener de. Dessuten skjønner de ikke det alvorlige i det de gjør og kan gjøre, mener utbryterne. Den nye gruppen vil slåss for de samme sakene som Anonymous kjemper for: Ytringsfrihet, personvern og fritt internett.

Men de er ikke mer enn rundt åtte personer, og tanken er bare å ha med folk som faktisk kan bidra med noe. Gruppen blir ikke fri og åpen, men lukket og kontrollert. Fredrik får en helt sentral rolle i gruppen, som begynner sin aktivisme med å hacke gamle venner i Anonymous Norway. I tillegg navngir de administratorene på nettsiden.

<Fredrik> hehehe nå er det krig her

<Plot> heisann, åssen da?

<Fredrik> vel, slapp dox[1] på noen admins i anonnorway

<Fredrik> nå skal noen randoms[2] gå til motangrep på oss

<Fredrik> så synd at vi doxxet en av dem

<Fredrik> og vi skal ringe han nå straks

<Fredrik> xxxxxx er ikke admin. han doxxet vi for the lulz[3]. xxxxx doxxet vi fordi han var irriterende

Litt senere på dagen forteller Fredrik at han og gruppen hans ringte opp to personer som de hadde valgt å identifisere.

<Fredrik> de sa at de satt på ubehagelig info om oss

<Plot> hva sa de ellers da?

<Fredrik> til slutt så fikk vi de til å stoppe

<Fredrik> eller de sa de skulle stoppe

<Fredrik> og de innrømmet at de ikke har noe på oss

<Fredrik> så.. #winning !

<Plot> stoppe med hva da?

<Fredrik> samle "ubehagelig info" om oss

<Plot> men de bare bløffet, mao?

<Fredrik> yep. de ville skremme oss

Som del av krigen mellom de forskjellige grupperingene innad i Anonymous Norway, blir det også publisert nakenbilder av minst ett norsk,

1> Dox og doxet betyr å identifisere, avsløre identiteten til.
2> Random er engelsk og betyr tilfeldige.
3> Lulz er flertallsform av LOL (laughing out loud), altså moro

mindreårig medlem av Anonymous på et internasjonalt nettsted som viser bilder av lettkledde og i noen tilfeller også helt nakne jenter, med ansiktene skjult bak Guy Fawkes-masker. Noen av dem er tilsynelatende meget unge. Mykpornosiden er publisert som en blogg. Etter at jeg begynner å stille spørsmål, fjernes flere av bildene, noe som kan tyde på at bloggen delvis styres fra Norge.

Og mens feidene herjer i Norge, får en 19-åring på andre siden av Nordsjøen merke hvor hardt det kan svi å gå til krig mot sine egne, slik Fredrik har gjort. Ryan, den unge gutten som navnga folk i Anonymous i februar, og som ble navngitt gjennom en hevn fra Fredrik og hans venner, får besøk på døren.

POLITIAKSJONEN MOT DET brunhvite murhuset i 10 South Beach Avenue i den slumrende småbyen Wickford i Essex i England er massiv. Ti politibiler ankommer stedet. Raidet ledes av Metropolitan-politiets avdeling for bekjempelse av cyberkriminalitet, men gjennomføres på bakgrunn av informasjon fra det amerikanske føderale politiet. FBI skal også ha vært med som observatører under selve aksjonen.

Grunnlaget for pågripelsen av Ryan Cleary (19), blir oppgitt å være cyberangrepene mot både CIA, FBI, Sony og Serious Organized Crime Agency (SOFA), det britiske FBI. Aksjonen pågår i fem timer. Politiet tar med seg alt som finnes av dokumenter, telefoner, datautstyr og annet elektronisk utstyr. I løpet av kort tid melder britiske medier at politiet har pågrepet et ledende medlem i LulzSec.

LulzSec svarer kjapt. Ironien i den første Twitter-meldingen er bitende: «Seems the glorious leader of LulzSec got arrested, it's all over now... wait... we're all still here! Which poor bastard did they take down?». Senere melder «LulzSec» i nye twittermeldinger at Ryan Cleary utelukkende har driftet en IRC-server der LulzSec lånte plass for å drifte en IRC-kanal. Utover det har det ikke vært noen forbindelse mellom gruppen og Cleary.

I første omgang er Cleary siktet for fem forskjellige forseelser av datakriminalitet. Men ifølge britiske medier kan 19-åringen i tillegg bli utlevert til USA, der han risikerer inntil 60 års fengsel hvis han blir funnet skyldig i dataangrepene. Da betyr det trolig mindre for Cleary at han også har angrepet mål i Norge.

Så sent som i desember i fjor gjennomførte hackeren som nå sitter i saksa et angrep mot VG Nett. Cleary benyttet et botnett som han hadde tilgang til, og som var på mellom 5 000 og 10 000 datamaskiner.

<Fredrik> ryan var litt... hva skal jeg si

<Fredrik> han var glad i oppmerksomhet

<Fredrik> han tok ned vg.no engang fordi jeg spurte

<Plot> såpass? Jøss

<Fredrik> jeg trodde ikke han var så dum

<Plot> når var det? vg.no mener jeg

<Fredrik> lenge siden

<Fredrik> i desember

<Fredrik> det var bare for 5min

Det sier Fredrik. Han var selv med på å doxxe, avsløre identiteten til, Cleary etter feiden i vinter. Det er det Cleary betaler prisen for nå. Fredrik har selv fått seg en del fiender på nettet. Og hva skjer hvis Topiary faktisk er blitt rekruttert som tyster og sladrer på ham?

Fredrik begynner å lure på hvilken retning hans store lidenskap skal ta. Stadig vekk dukker nyhetssaker opp om hackere som er pågrepet, om folk som havner i klørne på fienden. Han vet så lite om de han må stole på, om Topiary, for eksempel. Hvordan kan han vite at ingen kommer til å sladre? Uansett hva han gjør nå, hvor mye han roer seg, kan fortiden alltid innhente ham. Dolkes han i ryggen kan han lide samme skjebne som Ryan Cleary.

DE FLESTE SOM passerer Hasle torg i Oslo denne fredags ettermiddagen er på vei hjem fra jobben eller ute for å handle til helga. Det regner. Men det hindrer ikke et 20-talls demonstranter fra Anonymous Norway å lufte hodet. Det finnes en verden der ute også, utenfor cyberspace.

Plakatene er klare. Demonstrantene har også med seg mat, anleggsradio og fem store, grønne flagg med Anonymous-logo. Snart flyter rytmene ut i trafikken. Plakaten som vises fram til de passerende bilistene. «Scientologi er en farlig kult». Hackerne i Anonymous har i flere år nærmest ført et vendetta mot Scientologi-kirken, som de mener fungerer som en sekt, med hjernevasking og utnytting av medlemmer.

En tenåringsgutt i dress og flosshatt patter på en sigar. Han holder fram en plakat med påskriften «Tut mot scientologi». Og taxisjåfører, trailersjåfører og vanlige bilister tuter.

På andre siden av veien, hos Scientologi-kirken, øker irritasjonen. Et medlem av trossamfunnet går fra rom til rom, og begynner frenetisk å trekke for gardinene. En ung jente danser i veikanten, iført røde knestrømper, en rød boa som er hengt opp som en hale og ellers ganske minimal bekledning, været tatt i betraktning. Det vrimler av unge demonstranter på Hasle Torg.

Men en mann mangler. En 17 år gammel gutt.

FREDRIK SA DET ikke passet, rent praktisk; at det var derfor jeg ikke kom til å finne han her i dag. Han ville egentlig, sa han. Selv om han hadde fått beskjed, via omveier, om at en av de tilstedeværende ville drepe ham dersom han viste trynet sitt.

Men en av Fredriks nærmeste allierte er her. For å unngå at noen av de andre hører ham, trekker han meg til side og hvisker lavt at han er tilknyttet utbrytergruppen til Fredrik, han er med i Noria.

Ved 17.30-tiden svinger en politipatrulje fra Grønland politistasjon inn Grenseveien, og kjører opp på fortauet ved siden av demonstrantene. En demonstrant viser fram polititillatelsen, som gir dem lov til å demonstrere.

Mens politiet er på stedet dukker en illsint, middelaldrende mann opp. Det er Niels Syvander Baardseth, lederen for Scientologikirken i Oslo. I løpet av få sekunder går han til fysisk angrep på en av demonstrantene, og prøver å rive til seg en av plakatene. De to politifolkene må fysisk trekke med seg Baardseth noen meter bort fra demonstrantene. Til tross for flere beskjeder om å forlate stedet, nekter han å følge påleggene. Han krever å få med seg plakaten før han går noe sted. Til slutt mister politiet tålmodigheten og pågriper 41-åringen. Hos Anonymous-demonstrantene blir det feststemning når Baardseth blir geleidet inn i den parkerte politibilen. På alle bauger og kanter blir det tatt bilder og filmet. Like etter kommer en demonstrant smilende bort til meg.

- Kan jeg få kopier av de bildene du tok nå?

- Skal du lage plakater?

- Nei, jeg skal tatovere de på ryggen, svarer han med et smil som nesten går fra øre til øre.

BLANT HACKERNE FINNES det både «white hats» og «black hats». De hvite hattene hacker for å avdekke svakheter, men uten å ødelegge noe. De svarte tar ikke slike hensyn. De bruker den brente jords taktikk.

De aller farligste aktørene er de som leter etter unge og håpefulle i hackermiljøene, tenåringer som kan rekrutteres til fullblods spionasjeoppdrag.

Også norske tenåringer er gjennom årenes løp forsøkt rekruttert. I noen tilfeller har de latt seg lure til å gjennomføre hacking der de har hentet ut «top secret»-graderte dokumenter fra servere i det amerikanske regjeringsapparatet.

Iran og Nord-Korea er blant statene som har rekruttert mange hackere, som dels driver spionasje og dels driver med cyberkrigføring, forteller kilder. Jeg får kontakt med en norsk hacker som fortsatt er i tenårene. Han forteller at han selv er blitt forsøkt rekruttert til livsfarlige spionasjeoppdrag. Hans historie forteller hvilke karriereveier Fredrik står overfor.

<xxxxxx>: iran har noen jævlig gode hackere

<Plot>: som jobber for staten?

<xxxxxx>: ja

<Plot>: åssen vet du det?

<Plot>: har du fått noen av dem etter deg? ;-)

<xxxxxx>: ikke personlig

<xxxxxx>: men jeg veit at iran driver og romsterer mye rundt i blant annet amerikanske servere og sånt

<xxxxxx>: jeg har liksom gjort ting som kan putte meg bak lås i mange år

<xxxxxx>: du kan si at jeg har hengt med feil personer

<xxxxxx>: jeg hang med en gruppe som drev veldig store botnets og mye kredittkortsvindling og sånt i stor skala

<xxxxxx>: de var russiske/kinesiske, noe sånt, det er det eneste jeg vet om de

<xxxxxx>: de hadde botnets på over 2 millioner pcer og sånt.. det her er seriøse jævler

To millioner «zombies» er nok til å ta et mellomstort land offline. Hackeren forteller at han ble «lurt opp i stry», til å gjøre det farlige arbeidet på vegne av andre. Han tilbrakte en periode mye tid på en lukket IRC-server, hvor det foregikk mye kriminell aktivitet. Det var der rekrutteringsforsøket skjedde.

<xxxxxx>: en av de sa plutselig at de trenger noen, og jeg var jo ganske fresk akkurat da så jeg tenkte hvorfor ikke

<xxxxxx>: jeg så de siste gang for 2 år siden

<Plot>: hva var det de trengte folk til?

<xxxxxx>: en dag viste de meg en jobb de hadde utført på noe amerikanske servere, husker ikke helt hva det var, men de ga meg brukernavn og passord til noe accessystem, de sa til meg at jeg skulle få snoke så mye rundt som jeg ville

<Plot>: hva slags system var det?

<xxxxxx>: jeg skjønte jo ikke at de ville at jeg skulle utføre snokinga for de

<xxxxxx>: det var noe kommunikasjonssystem av en eller annen rar type

<Plot>: ok - hva da, husker du noen detaljer?

<xxxxxx>: de ville at jeg skulle laste ned noen filer

<Plot>: hva slags type filer da?

<xxxxxx>: de var stemplet top secret, da pisset jo jeg nesten på meg

<xxxxxx>: da skjønte jeg med en gang at her bør jeg jo ikke være

<Plot>: såpass. husker du hva temaet var, bortsett fra graderingen?

<xxxxxx>: jeg leste ikke, jeg så CIA-logoen og noe USAR (US Army Reserves, red. anm) tekst på førstesiden, jeg var jo bare 15 år da

<xxxxxx>: da fikk jeg panikk når jeg så det

<xxxxxx>: det var ikke noe god følelse skal jeg si deg

<xxxxxx>: de hadde gitt meg nødvendig beskyttelse, selvfølgelig

<Plot>: VPN mv?

<xxxxxx>: men ja, jeg hadde bare ikke nerver til det, det skremte meg

<Plot>: men hvor kommer Iran inn i bildet i denne historien?

<xxxxxx>: en av de sa det at det er veldig mye iranske hackere som snoker rundt på servere til andre land

<Plot>: er det andre land som er veldig dyktige på cyberkrigføring?

<Plot>: eller snoking

<xxxxxx>: nordkorea tror jeg

DET FINNES OGSÅ «white knights» – hvite riddere – som kan mobiliseres på nettet til innsats for en god sak. Men saken må være god. Forsøk på å bruke nettets riddere til egne, private formål blir som regel hardt slått ned på. Har du private gjøremål eller motiv, må du betale for jobben. Og da må du ofte gå til helt andre miljøer for å rekruttere villige «leverandører». «Black knights»-hackere, spesielt fra Ukraina og andre deler av den tidligere østblokken, tar gladelig slike oppdrag. Enten det er hevn eller informasjonsinnhentning du har i tankene; alt lar seg levere.

Bak fasaden av utagerende hackergrupper som begår stadig mer spektakulære cyberangrep, finnes det flere hardtarbeidende researchgrupper. Disse bruker åpent tilgjengelig informasjon, men også dokumenter og annet materiale som er kommet til veie gjennom dataangrep mot ulike aktører. LulzSec, som skapte de voldsomme bølgene i mai og juni, har en egen researchgruppe som arbeider med analyse av både innhentet informasjon og med tanke på framtidige aksjoner.

For kortere eller lengre varighet oppretter små eller større grupper elektroniske notisblokker der alle kan jobbe med det samme dokumentet samtidig. I løpet av ganske kort tid kan en gruppe mennesker – fra forskjellige steder i verden – gjennomføre granskinger med oppsiktsvekkende resultater. Dette kalles «crowdsourced investigations». Gruppebaserte etterforskninger. Når samarbeidet er ferdig eller tar pause, fjernes notatblokkene.

Det er slikt arbeid Fredrik engasjerer seg mest i når skoleåret er omme. Han har nesten sluttet å logge på AnonOps og jobber heller videre med informasjon andre har samlet inn. Han har trappet ned nå, han har logget av en kriminell løpebane – i god tid før han er voksen nok til å drikke øl og kjøre bil.

Han definerer seg som en «White Hat», selv om en statsadvokat kanskje vil være uenig. Fredrik har holdt seg unna de drøyeste angrepene i det siste. Nå frykter han bare at fortiden innhenter ham. At folk som Topiary gjør noe dumt. De som ønsker å profilere seg som den fremste spesialstyrken i disse dager er LulzSec. De vet i alle fall hvordan de skal skape bølger og nyhetsoverskrifter.

ETTER Å HA angrepet CIA, FBI, det amerikanske senatet, britiske politimyndigheter og en lang rekke andre nettsteder, er turen i slutten av juni kommet til NATO selv. LulzSec har bestemt seg for å vise hvem som er den tannløse tigeren, og at selv ikke forsvarsalliansen kan forsvare seg mot det nye årtusenets nye krigføringsmetoder.

Innledningsvis leter hackerne etter sårbarheter og svakheter i IT-infrastrukturen til NATO. Hos forsvarsalliansens online-bokhandel, finner de muligheten til å komme seg på innsiden. 25. juni avslører LulzSec at de har lastet ned 12 000 kunders navn, brukernavn og passord fra denne bokhandelen og lagt disse ut på nettet. I den nedlastbare filen ligger navnene på minst 18 nordmenn, herunder flere ansatte i Forsvarsdepartementet og Forsvaret forøvrig, samt en ansatt i Direktoratet for samfunnssikkerhet og beredskap. Dersom disse har falt for fristelsen, som Aaron Barr og veldig mange andre databrukere, til å bruke samme brukernavn og passord mange forskjellige steder, fungerer dataangrepet mot NATOs bokhandel. Og LulzSec finner mulige bakdører inn i datasystemene til det norske forsvaret.

Kommunikasjonsrådgiver Marita I. Wangberg i Forsvarsdepartementet er blant ofrene. Hun får sitt passord avslørt når LulzSec går til aksjon. Wangberg får en mail fra IT-avdelingen på jobben som gjør henne oppmerksom på det som har skjedd.

LulzSec legger kort tid seinere ned virksomheten, i alle fall tilsynelatende. En søkemotor opprettes, der alle brukernavn fra samtlige dataangrep legges ut samlet. Poenget med tjenesten er å gi folk muligheten til å finne ut om passordene deres var på avveie. Passordene er ikke tilgjengelige gjennom denne tjenesten. På søkemotoren ligger det i midten av juli mer enn 250 brukernavn med e-postadresser som sluttet med .no. I tillegg kommer nordmenn som bruker internasjonale mailtjenester som slutter på .com og .org.

SECRET SERVICE-AGENTENE FØLGER med på folkemengden. Det er 1. juli, og den amerikanske statsråden Janet Napolitano er i Østerrikes hovedstad Wien for å delta på toppmøtet i Organisasjonen for sikkerhet og samarbeid i Europa (OSSE).

Den største trusselen i dag, ifølge Napolitano, nå som Osama bin Laden er død og USA planlegger uttrekning fra både Afghanistan og Irak, er en fiende livvaktene ikke kan se. Napolitano, som er ansvarlig for Departement of Homeland Security, er mest opptatt av cyberterrorismen, som hun kaller den. Hackingen som nesten daglig rammer amerikanske myndighetsorganer.

- De fleste land har ikke engang et juridisk rammeverk som styrer nettvirksomheten. Dette er et såpass nytt fenomen at de juridiske systemene, både nasjonalt og internasjonalt, ikke har greid å holde tritt med den teknologiske utviklingen vi har sett, sier Napolitano til en gruppe pressefolk.

- Det er det enkle faktum. Vi må trappe opp vår innsats som et svar på dette, legger hun til.

Ifølge ubekreftede nyhetsmeldinger skal en vesentlig del av strategien til amerikanske etterretningstjenester og FBI være å forsøke å rekruttere så mange informanter på nettet som mulig. Ved å true hackere med lange fengselsstraffer, er håpet at de skal velge å angi andre og større hackerfisk enn seg selv. Verdens maktelite i ferd med å kaste seg rundt. Noen av de beste hodene i verden mobiliseres for å få stoppet Fredrik og hans hackervenner.

Den britiske avisen Daily Mail skrev 17. februar i år at nettbasert kriminalitet hvert år koster Storbritannia mer enn 27 milliarder britiske pund. Dataangrep, industrispionasje på nettet og tyveri av fortrolig selskapsinformasjon koster alene mer enn 21 milliarder.

DEN NAGENDE USIKKERHETEN plager fortsatt Fredrik når fellesferien begynner. Sist Topiary ga livstegn fra seg var 23. mai. Han sendte bare ut en avskjedsmelding på twitterkontoen sin. Noen av svarene han fikk, var spottende. Andre takket «atopiary», som er nicket han bruker på twitter, for innsatsen. Så forsvant Topiary.

Men 7. juli våkner Twitter-kontoen hans plutselig til liv igjen. Plutselig tvitrer den bortkomne hackeren som om ingenting har skjedd. Den ene kommentaren er mer rappkjeftet enn den andre.

Stilen er påfallende lik tvitringen fra den offisielle LulzSec-kontoen. Nå er det Fredrik som spør meg om jeg vet hva som egentlig foregår. En mulighet er at Topiary, for å skjule sin aktivitet i perioden som medlem av den utagerende LulzSec-gruppen, valgte ikke å bruke sine vanlige brukerkontoer og nicks. Parallellbruk ville gi cyberkrim-jegerne muligheten til å bevise at Topiary var medlem av LulzSec. Den såkalte pågripelsen i april kan derfor være et rykte han selv plantet på nettet for å forvirre og røyklegge.

Andre sentrale aktører som har gått med på å snakke med meg under avtale om full anonymitet, er ikke overbevist.

– Da Topiary kom tilbake fremsto han som en helt annen person enn før. Enten hadde han skiftet personlighet, eller så var det noen andre som brukte nicket hans.

EN MELDING MED overskriften «50 days of lulz», 50 dager med moro, oppsummerer LulzSec sine plyndringstokt verden rundt. Problemene for regjeringene verden rundt er ikke over ennå. Etter nedleggelsen av LulzSec har den tidligere gruppen «AntiSec» gjenoppstått. På nettet er det alltid et liv etter døden.

IT-ansvarlige verden rundt har på langt nær sett siste tastetrykk fra hackernes side. Når jeg besøker kommandosentralen til «AntiSec» på AnonOps i begynnelsen av juli, oppholder rundt 550 forskjellige brukere seg i IRC-kanalen. Som i en kube der biene summer rundt og venter på neste oppdrag. Mange er allerede i gang med konkrete aksjoner.

I Orlando, Florida, lekte hackerne nylig katt og mus med ordføreren og det lokale politiet. Bildene av en Guy Fawkes-maske, hengende på et gateskilt med ordførerens private hjem i bakgrunnen, ble oppfattet som en trussel. Orlando-politiet kontaktet FBI og ba om hjelp. Andre ungdommer jobber videre med å støtte revolusjonene i den arabiske verden, selv om det her råder en tilsynelatende usikkerhet rundt valg av mål og videre strategi. I chatgruppene på AnonOps råder den totale paranoia. Dersom noen av aksjonistene har vært offline i bare et døgn, går spekulasjonene høyt om de har gått i garnet til FBI.

FREDRIK HAR BEGYNT å tenke på voksenlivet. På om han vil være en hvit eller en svart hatt. Det er sommer i Norge. Et skoleår er omme, og 17-åringen trenger jobb. Noen kroner inn hadde vært fint, men aller helst vil han ha en jobb der han kan fortsette med sin altoppslukende interesse: Å følge med på hva makteliten driver med og avsløre dette.

<Fredrik>: hmm, dette har gått mye ut over skoleåret mitt :P

<Plot>: ligger du dårlig an?

<Fredrik>: ikke dårlig an, men har brukt mye skoletid til dette, hehe

Han forklarer at Anonymous for ham ikke er viktig, det er bare en identitet, et felles ikon, som han og andre bruker for å vise at det er en stor gruppe mennesker som bryr seg og aksjonerer. Fredrik mener hele det politiske systemet, også i Norge, har sviktet. Han kaller det «ett dags-demokratiet» - fordi han mener at velgernes innflytelse forsvinner helt etter at de har stemt på valgdagen. Men han nekter å avsløre hvilke metoder Noria kommer til å bruke i kampen for omfattende samfunnsendringer i Norge.

<Fredrik> Jeg selv bruker ikke anon som identitet lengre, men jeg fortsetter å bruke det som et ikon.

<Fredrik> Altså, anon er viktig, men det er personene bak som betyr noe.

<Plot> Men hvorfor er det dere gjør riktig og viktig?

<Fredrik> Du tenker på aktivismen?

<Plot> Ja.

<Fredrik> Det er jo utrolig viktig at folk står opp og sloss for hva de synes er rett (og feil.)

(Jeg er ikke så flink til å ordlegge meg)

<Fredrik> Om noen for eksempel er for en ting, betyr ikke det at alle andre er for det. Vi er et løst samfunn / folkesamling.

<Fredrik> Jeg vil på en måte peke til at aktivisme generelt er viktig, gjør en forskjell!

<Plot> Men for at en aksjon skal være gjennomførbar, f eks et DDOS-angrep, må jo mange nok være enige om at angrepet er riktig og kan rettferdiggjøres?

<Fredrik>Vel, en person med et botnet kan sette igang en operasjon selv, helt alene og fyre løs på hva han sjøl vil, ingen kan stoppe han. Alle kan gjøre alt i Anonymous sitt navn, på en måte. Hacker noen Sony og sier de at de er Anons, så gjorde anon det.

<Fredrik> I operation payback så var det «folkeavstemning» på hvilke mål vi skulle angripe. Du kan si at det fungerer på følgende måte: Person A har en idé/mål. Han forklarer idéen for alle andre, så kommer de med innspill. Liker de det, så kjører de igang.

<Plot> Er det ofte de samme folkene som har ideer om aksjoner?

<Fredrik> Vel, de fleste operasjonene har blitt arrangert av de samme personene og den samme gruppen med folk. Det er ofte slik at noen har et mål/en plan, de sprer informasjonen på Facebook osv, folk ser det og tenker «Oi, dette er jo en sak jeg støtter» og hiver seg på

<Fredrik> jeg sier ikke at alle operasjonene har blitt arrangert av de samme personene, men det er nesten sånn.

<Fredrik> Folk er late og vil ha instruksjoner, det er derfor slike operasjoner som operation payback har blitt en så stor suksess, de fulgte en 1-2-3 prosedyre.

<Plot> Så Aaron Barr hadde egentlig rett, det finnes faktisk noen som kan defineres som et slags lederskap?

<Fredrik> altså, du kan si det finnes et lederskap i AnonOps, ja.

TIRSDAG 19. JULI får verden vite at hackerne har overgått seg selv. De har angrepet hjemmesiden til avisen The Sun i England, og lagt ut en fiktiv nyhet om at mediemogulen Rupert Murdoch er funnet død, med den lakoniske kommentaren: «I det minste rakk han å si unnskyld først». Murdoch-imperiet rystes i grunnvollene etter avsløringene om konsernavisen News of the Worlds bruk av telefonhacking og ulovlig avlytting av mer enn 4000 personer gjennom flere år. Flere sjefer har de siste ukene forlatt sine stillinger. Det samme har sjefen for New Scotland Yard og pressesjefen for den britiske statsministeren, Andy Coulson, som tidligere arbeidet som nyhetsredaktør i News of the World. På nett triumferer hackerne med følgende strofe: «We have joy, we have fun, we have messed up Murdoch's Sun».

Og det foregår mer i kulissene. Mye mer.

Da hackerne gikk inn på webserveren til The Sun via en kompromittert maskin i kontorlandskapet i avisen, skal de også ha lastet ned kopier av et ukjent antall mailer fra mailserveren. LulzSec, der Topiary fortsatt fremstår som et sentralt medlem, forbereder en snarlig publisering av materialet. Fra

twitter-kontoen til LulzSec, mottar followerne – nå flere enn 336.000 personer – følgende melding: «Arrest us. We dare you. We are the unstoppable hacking generation and you are a wasted old sack of shit, Murdoch. ROW ROW FIGHT THE POWER!».

NESTE KVELD ER porten til helvete åpnet på vid gap. I løpet av dagen slår FBI til mot minst 35 forskjellige adresser i USA alene. Minst 16 personer pågripes. Et betydelig antall personer er trolig satt under etterforskning, uten at det ennå foreligger noen siktelser. Tflow, som er medlem av LulzSec, meldes pågrepet i en tilsvarende politiaksjon i England. Tflow er bare 16 år. Sentrale hackere er plutselig tause. Også tre hackere i Nederland går i garnet. IRC-serveren AnonOps går i tillegg offline. Mange går i dekning. De som ikke dukker opp på de avtalte skjulestedene, blir omtalt som MIA: Missing in action.

På nettet driver hackerne en intens klappjakt på tystere i egne rekker, i tillegg til å forsøke å finne ut om de selv er i faresonen eller ikke. Også jeg blir møtt med svært nærgående spørsmål om hvem jeg egentlig er og hva jeg driver med. Mye tyder på at den omfattende og internasjonale politiaksjonen denne dagen bare er forsmaken på det som er i vente.

Politiaksjonene har utgangspunkt i det som skjedde i oktober-november-desember, med hevnangrepene på blant annet Paypal, Visa og Mastercard, i kjølvannet av støtteaksjonene for Wikileaks. Betalingstjenestene nektet å ta imot donasjoner til Wikileaks etter den voldsomme lek-

kasjen før jul i fjor, på oppfordring fra den amerikanske regjeringen. Det aksepterte ikke hackerne, som slo tilbake mot nettsidene. Nå slår makta tilbake igjen. Det er loggene fra IRC-serveren til Ryan Cleary som danner mye av grunnlaget, mener hackerne å vite. I tillegg tyder mye på at Cleary har angitt flere av sine tidligere hackervenner.

Topiary tok æren for angrepet mot PayPal i desember i fjor, mener kildene mine. Men i virkeligheten var det en skandinavisk gruppering som skaffet Topiary informasjonen han trengte for å komme på innsiden av PayPal-systemet. Trolig en svensk gruppe, sies det. Det er også mulig hackerne var fra Norge.

– Jobben ble gjort av helt andre enn LulzSec. Slik er det ofte. De som gjør jobben forholder seg tause, og lar andre ta æren. Det er mye tryggere sånn, sier en.

På grunn av de sterke, skandinaviske koplingene, tyder mye på at det kan være politiaksjoner under oppseiling også her hjemme, tror flere. Norske ungdommer som har vært aktive som hackere i perioden sitter ikke nødvendigvis trygt.

TO DAGER ETTER alle politiraidene, får jeg til slutt Topiary i tale, over den trygge nettbaserte Skype-linjen. I likhet med FBI, har også jeg drevet klappjakt på ham siden begynnelsen av april. Innad i hackermiljøet er det åpen krangel om hvorvidt Murdoch-mailene skal publiseres eller ikke. Dersom materialet publiseres i sin helhet, kan det ødelegge alle muligheter for vellykkede straffesaker i kjølvannet av hackerskandalen. Og på toppen av dette har Anonymous fra en annen twitterkonto tidligere på dagen meldt at hackerne sitter på 1 gigabyte, 1000 megabyte, med hemmelige NATO-dokumenter som de har stjålet fra en NATO-server.

Topiary avviser alle ryktene om at han er blitt tatt av det britiske politiet, han vil ikke engang bekrefte at han befinner seg i England. Og han avviser på det sterkeste at han noen gang vil tyste på sine venner.

– Jeg har aldri bistått politiet på noe vis, og det kommer jeg heller aldri til å gjøre. Jeg kan ikke snakke for alle andre, svarer Topiary.

Hackeren som har gjort det til et varemerke å være velformulert og bråkjekk, er påfallende nøktern og lavmælt.

– Hva er neste skritt for LulzSec?

– Dette kan stanse på et hvilket som helst tidspunkt. Når det gjelder LulzSec, kommer vi ikke til å gjennomføre ytterligere aksjoner, men i stedet vende tilbake ved helt spesielle anledninger, når det er verdt det, sier Topiary.

Mer konkret vil han ikke være.

Før Topiary forsvinner ut i cyberspace igjen, slår han fast at påstandene om at LulzSec har deltatt i et angivelig tjenestenektangrep mot Telenor, som hevdes å ha vært den egentlige årsaken til at tre millioner nordmenn mistet mobilforbindelsen i pinsen, er feilaktige.

– Det høres i så fall ut som et ganske stort tjenestenektangrep. Men det er ikke oss, i så fall, sier Topiary.

Det er sommer på Østlandet. Flere måneder har gått siden Aaron Barr ble felt av Fredrik og hans venner, og regjeringen har fått en liten forsmak på hva en 17 år gammel gutt er i stand til. Mens cyber-etterforskere fra FBI forsøker å finne nye brikker til puslespillet, sitter Fredrik hjemme på gutterommet og håper han er trygg; at han ikke lider samme skjebne som Ryan Cleary og andre onlinevenner. Hackere verden rundt har røket i klørne på etterforskere de siste månedene. Nato og FBI har begynt å vise muskler. Fredrik har begynt å undersøke navn på hvilke advokater som kan være aktuelle å bruke. I tilfelle politiet skulle banke på. Han har en uggen følelse.

FREDAG 22. JULI, klokken 15.26, hører alle lyden av et virkelig angrep. Fredrik er i sjokk og sjokket går snart over i sinne. Flere hackere begynner å kartlegge Anders Behring Breiviks liv på nettet. Fredrik og hans gruppe varsler at de kommer til å prøve å ta seg seg inn i Breiviks mailkontoer. Men Fredrik sier han ikke vil gå i veien for politietterforskningen. Får han tilgang til noen av epostene vi han gi dem til politiet.

Hans nye gruppe kaster seg også med den internasjonale operasjonen Unmanifest, som jobber for å fjerne alle referanser til Breiviks manifest. Det er slike ting Fredrik vil jobbe med framover. De gode gjerninger i cyberspace.

Men han er nervøs. Siden angrepet på Paypal i desember i fjor, er minst 79 hackere i åtte forskjellige land pågrepet av timyndigheter. FBI og andre lands poli-

Fingrene hans slår takten, pc-en summer en melodi under pulten hans. Noe har skjedd med 17-åringen. Meldingene tikker inn; nye razziaer, nye pågripelser. Minnepinnen er fortsatt plantet i den kraftige maskinen, og den blinker som før. Oppe på kjøkkenet står mikrobølgeovnen. Så skjer noe. Noen roper fra etasjen over.

Middagen er ferdig.

EPILOG: I SLUTTFASEN av arbeidet med denne reportasjen ble jeg kontaktet av en person jeg aldri tidligere har møtt, en kvinne fra Sør-Afrika, som insisterte på å sende meg et bilde av seg selv. Først trodde jeg det kunne være en tidligere kilde som forsøkte å kontakte meg på en litt klossete måte. Men da personen forsøkte å sende meg en fil, blokkerte jeg profilen umiddelbart. Dette likte jeg svært dårlig.

<Fredrik>: Virker som et vanlig infeksjonsangrep.

Da jeg dagen etter tok kontakt med Topiary, som er kjent for å elske practical jokes, for å høre om dette var noe han hadde hørt om, fikk jeg negativt svar. Men etter få minutter i Skype-samtalen, ba han meg om å kopiere noe av dialogen og lime den inn i dialogfeltet igjen. Teksten han skrev, ble da ugjenkjennelig. Kort tid etter kom det til syne et mønster som liknet på binær kode, bare i forvrengt form. I frykt for at jeg var i ferd med å bli hacket, selv om jeg selv surfet på en kryptert VPN-linje, tastet jeg raskt følgende beskjed:

«Is now a good time to remind you I come in peace?».

Etter å ha lest svaret bestemte jeg meg for å dra ut nettverkskabelen, skru av maskinen og reise hjem:

«The Matrix has you dear Norwegian».

Tirsdag 26. Juli, et drøyt døgn før Plot gikk i trykken, pågrep New Scotland Yard, i en lenge planlagt politiaksjon på Shetlandsøyene, enda en 19-åring. Topiary.

Enkelte nicks og andre detaljer som kan virke identifiserende er fjernet eller endret av redaksjonen.

HACKERFAR: - ALREIT AT DEN STØRSTE BØLLA FÅR JULING

De fleste foreldre til hackere er uvitende om det som foregår. Det er ikke tilfellet for en far til en av de norske hackerne. Sønnen samarbeider med LulzSec og har fått status som semi-moderator i chatrommet der LulzSec-medlemmene vanligvis henger på IRC. Faren er i 40-årene, har mangeårig IT-bakgrunn og er tidligere etterretningsoffiser i Heimevernet. På den tiden hadde han kontakt med daværende Forsvarets etterretningstjeneste. Mannen som i dag arbeider i det private næringsliv, har også tidligere utført IT-oppdrag for det norske regjeringsapparatet. I motsetning til også Fredriks foreldre, vet denne mannen godt hva tenåringssønnen driver med. I tillegg er faren selv med noen ganger, ikke på angrepene, men han er til stede på IRC-serverne og observerer hva datahackerne driver med. Faren innrømmer at han heier på sønnen og hackervennene hans når de går til angrep på mektige aktører.

– Noen ganger er det ålreit at den største bølla i skolegården får juling, at han blir satt litt på plass. Vi elsker jo det, at underdogen vinner. Men samtidig er det jo sånn at mindretallet har alltid rett. Det er ganske mye som disse gutta og jentene tenker og gjør ...hensikten er god. De ønsker oppriktig å endre verden slik at de gjør den til et bedre sted for de fleste, også for alle sauene der ute, vanlige folk, sier faren.

Han understreker at han ikke selv støtter tjenestenektangrep, og at han forsøker å gi sønnen råd om å unngå å være med på ting som er direkte ulovlig. Faren mener at hans indirekte deltakelse gir sønnen langt bedre veiledning enn om han hadde stukket hodet i sanden. Altfor mange foreldre aner lite eller ingenting.

– Jeg har fått vite at 625 personer var med på tjenestenektangrepet mot Aps nettsider i april. De aller færreste beskyttet seg. Det er foreldrene til disse som virkelig burde vært bekymret. Det er jo utrolig lett å beskytte seg mot å bli sporet, sier faren.