Metoderapport, SKUP 2016

Teppefall

Hovedsak, 18. juni 2015:

http://www.adressa.no/pluss/magasin/2015/06/18/Teppefall-11219093.ece

Jonas Alsaker Vikan, 928 28 316
Jonas.Vikan@adresseavisen.no

Ole Martin Wold, 986 31 898
Ole.Martin.Wold@adresseavisen.no

Adresseavisen, Postboks 3200, Sluppen 7003 Trondheim Sentralbord: 07200

Sammendrag

TEPPEFALL-prosjektet følger spor fra organisert dopsalg på det mørke nettet og frem til en 29 år gammel finansutdannet mann i Oslo. Mannen har i årevis brukt svært avansert teknologi som Tor, PGP-kryptering og Bitcoin til å begå grov kriminalitet i internetts skyggeland.

Det er første gang i norsk sammenheng, og antakelig også internasjonalt, at journalister har avdekket identiteten til personer som bruker denne teknologien som en usynlighetskappe.

Vi finner sporet som dokumenterer hvordan 29-åringen knytter sin reelle identitet til aliaset DEEPLOVE den 13. mars 2013 og hvordan han og andre bruker aliaset til omfattende dopsalg. Mot slutten av 2013 endres aliaset til ALFA&OMEGA og salget fortsetter frem til 8. juni 2015. Våre undersøkelser viser at 29-åringen og en eller flere medskyldige har stått for over 1500 salg av dop ved hjelp av minst sju skjulte nettsider til kunder i Norge, Sverige, Danmark og Finland. Vi har fulgt og dokumentert aktiviteten ved hjelp av tilgang til salgslogger, slettede opplysninger og vanlig kildearbeid.

TEPPEFALL kartlegger i tillegg virksomheten til en 31 år gammel mann bak aliaset KVALITETSBEVISST fra det ble registrert høsten 2012 og frem til kvelden 7. juni.

5. november 2014 publiserte vi saken SILKEVEIENE som avslørte at flere grupper eller nettverk av nordmenn hadde stått for minst 5500 salg av narkotika. Blant de som ble kartlagt i SILKEVEIENE var ALFA&OMEGA og KVALITETSBEVISST. Noen måneder senere startet OPERASJON MARCO POLO i hemmelighet på Kripos. Etterforskningen er den første i sitt slag i Norge og førte til pågripelsen av 29-åringen Adresseavisen identifiserte som mannen bak DEEEPLOVE og ALFA&OMEGA. Da vi fulgte 29-åringens bevegelser i Oslo i mars, var han enda ikke under etterforskning.

Kripos arresterte i tillegg en 31-åring bak KVALITETSBEVISST-aliaset i OPERASJON MARCO POLO.

Både 29-åringen og 31-åringen var ustraffet. De satt i varetekt helt frem til 21. desember, siktet for grovt salg av narkotika og organisert kriminalitet. Forholdene har en strafferamme på 15 år i fengsel. Etterforskningen OPERASJON MARCO POLO skal fortsette utover i 2016.

Innhold

1. Mål og problemstilling

Selv om alvorlig narkotikakriminalitet var høyt prioritert i Riksadvokatens rundskriv til politi og statsadvokater både i 2014 og 2015 så ikke politiet ut til å ta omfanget av kriminaliteten som SILKEVEIENE-saken dokumenterte på det mørke nettet særlig alvorlig. Derfor bestemte reportasjeleder Ann-Inger Borstad og jeg (Jonas) at jeg skulle se om det lot seg gjøre å avdekke identiteten til personene som skjulte seg bak dopnettverkenes dekknavn:

- *Er det mulig å trenge gjennom anonymiseringsteknologien Tor, PGP-kryptering og Bitcoin for å finne bakmenn? Hvor befinner de seg? Er de vanlige kriminelle?*
- *Er det mulig for pressen å få dokumentert denne lyssky aktiviteten i den virkelige verden, og vise at dette faktisk foregår i norske byer?*

Jeg satt allerede på en oversikt over narkotikanettverkene og to ble valgt ut:

MÅL A) ALFA&OMEGA spilte en hovedrolle i SILKEVEIENE-saken fordi jeg kunne vise at A&O hadde stått for 1500 dopsalg på litt over et år. A&O fremsto som en av, hvis ikke den største norske aktøren.

MÅL B) KVALITETSBEVISST var den norske aktøren som hadde vært aktiv over lengst tid på det mørke nettet, ifølge mine undersøkelser. I tillegg fremsto KVALITETSBEVISST som mer teknologisk avansert enn de andre nordmennene.

For å svare på problemstillingene har vi jobbet etter tre hovedspor:

Spor 1) Vi følger digitale spor som personene bak aliaset DEEEPLOVE legger igjen på det mørke nettet til hundrevis av innlegg på finansnettsteder og blogger på åpent nett til vi avdekker navnet på en av mennene som står bak.

Spor 2) DEEEPLOVE forsvant høsten 2013. Hvor? Vår hypotese er at personene fortsetter med dopsalg, men under et nytt alias: ALFA&OMEGA. Hamskiftet dokumenteres ved en omfattende gjennomgang av åpne og lukkede datakilder på det mørke nettet. Mye av materialet var slettet da arbeidet pågikk.

Spor 3) Vi kartlegger KVALITETSBEVISSTs dopsalg fra 2012 til 2015 og forsøker å identifisere personen som står bak dekknavnet.

Denne rapporten redegjør for metoder, spesielle erfaringer, problemer som oppsto, utfordringer med teknologi samt presseetiske vurderinger som forsinket publiseringen av TEPPEFALL og førte til en omarbeidelse av det som var en ferdig sak.

1.2 Oppstart og utgangspunkt

Arbeidsperioden var midten av januar (2015) til midten av mars, og fra 1. april til midten av mai. Jeg (Jonas) og fotograf Ole Martin har deltatt i hele veien mens Jonas Nilsson begynte med programmering og design i mai. Espen Rasmussen og Christer S. Johnsen har bidratt med desking av den ferdige saken.

Jeg jobbet med SILKEVEIENE hele høsten 2014 og bidro ikke til vanlig nyhetsarbeid. Reportasjeleder Ann-Inger Borstad tydeliggjorde at TEPPEFALL var verdt å satse på, selv for et regionalt mediehus som Adresseavisen og skjermet meg i ny periode. Det står til

redaksjonsledelsens (og spesielt til Borstads) ære. Undersøkende journalistikk på det mørke nettet er ikke mulig å gjøre innimellom blålysjakt og generell nyhetsdekning.

Jeg hadde noen tråder å jobbe etter, men liten tro på å lykkes. I Sverige har etterforskeren Jimmy Arkenheim avslørt flere personer tilknyttet slike dopnettverk. Hans erfaring er at kombinasjonen av alias, Tor, PGP og Bitcoin gir de kriminelle ekstraordinært gode muligheter til å skjule seg. Arkenheim betegner sikkerhetsnivået som «skyhøyt».

Denne saken fra 2011 var den første saken om dopsalg fra skjulte nettsider. I 2015 opererer enkelte internasjonale medier med egne reportere på stoffområdet. Joseph Cox er en av dem og skriver for for Wired og Motherboard. Cox kjenner ikke tilfeller hvor undersøkende journalistikk har avdekket identiteten til personer som skjuler seg på det mørke nettet:

- Jeg kan ikke tenke meg et tilfelle hvor et journalistisk arbeid har identifisert en dopselger før politiet, sier Joseph Cox.

Nærmest kom en reportasje fra BBC Newsnight fra 13. november 2013. Saken er bygd på en enorm datalekkasje fra den skjulte nettsiden BLACK MARKET RELOADED. Dataeksperter hjalp Newsnight til å omforme rådataene til 330 000 e-postadresser. Fra det antallet var kun én adresse mulig å knytte til en amerikansk narkotikalangers virkelige identitet. Newsnight forfulgte ikke det sporet videre.

Jeg fant ingen norske saker hvor journalister hadde avslørt hvem som står bak dekknavn på det mørke nettet. Aftenposten skrev om noen norske «nettlangere», som de ble kalt, på den skjulte nettsiden SILK ROAD (stengt i 2013). Flere norske alias ble nevnt, blant dem DEEPLOVE og KVALITETSBEVISST. Hvis avisen gjorde forsøk på å spore opp og avsløre personene bak, så har jeg ikke funnet et publisert resultat av det arbeidet.

Under SILKEVEIENE-saken hadde jeg identifisert flere kunder, men jeg hadde ingen angrepsvinkel for å finne ut hvem som sto for salgene. Kundene visste ikke hvem de kjøpte av. Redaksjonsledelsen aksepterte ikke kjøp av narkotika som metode. Jeg hadde ingen datalekkasje fra skjulte nettsider (som BBC hadde). Jeg måtte finne andre metoder.

2. Arbeidet med saken: Metoder og kildebruk

I TEPPEFALL-prosjektet er det kombinasjonen av ulike metoder, tradisjonell og utradisjonell journalistisk tilnæring på åpent og lukket nett og feltarbeid i Oslos gater, som har gitt gjennombrudd. Rapporten redegjør for metodebruken i en så kronologisk rekkefølge som mulig. Et metodekart synliggjør hvordan de ulike tilnærmingene har overlappet (vedlegg 1).

Deler av saken handler om avansert teknologi og derfor har jeg brukt ekspertkilder til å få vurderinger og til å hjelpe meg å forstå hva materialet jeg hadde samlet inn betød. Like viktig var det å få hjelp til å forstå hva funnene ikke betød for å unngå å gjøre feil.

Spaning har vært en viktig og en ressurskrevende metode som var avgjørende for å få viktige svar. Adresseavisen har valgt ikke å identifisere 29-åringen som våre undersøkelser knytter til et av de største norske narkotikanettverkene (se punkt 3.3). Følgelig er konkrete navn og adresser er anonymisert i metodeforklaringene i rapporten. Jeg kan lite om IT, men lærte underveis. Med tiden fant jeg ut at dette ikke handler om ufeilbarlig teknologi, men om menneskelig adferd. Mennesker gjør feil. Det gjelder bare å finne feilene.

2.1 Mål A

Like før SILKEVEIENE-prosjektet skulle publiseres i november 2014, fikk jeg tilgang til en kopi av den skjulte nettsiden SILK ROAD (SR1), som FBI slettet fra det mørke nettet 1. oktober 2013. Jeg studerte SR1-kopien og sammenlignet med det jeg visste fra min egen kartlegging høsten 2014 som viste at ALFA&OMEGA var den kanskje største norske aktøren. Det var ingen DEEEPLOVE i mine funn, og ingen spor etter A&O i SR1-kopien. Det skurret, for SILKEVEIENE viste at A&O skrev dette i 2014:

«Vi har nesten 1000 transaksjoner bak oss på de tidligere markedene som SR1, Sheep, BMR»

Jeg så likheter i kundebehandling og kommunikasjon mellom DEEEPLOVE og A&O. Hva om samme personer sto bak DL i 2013 og A&O i 2014 og 2015, og bare hadde byttet alias? Kunne det stemme?

For å undersøke en eventuell sammenheng, var den første oppgaven å se nærmere på hvilke opplysninger jeg kunne finne om DEEEPLOVE i kopien av SR1.

2.1.1 METODE 1: Databasesøk 1

I TEPPEFALL har jeg søkt i to PGP-databaser, en på det mørke nettet og en på åpent nett (se vedlegg 2 og 6). Det første, viktige funnet i saken ble gjort da jeg søkte opp DEEEPLOVE i ALL MARKETS VENDOR DIRECTORY (AMVD), som er en PGP-database på det mørke nettet. Kopien min av SILK ROAD viste at DEEEPLOVE (DL) var aktiv i 2013, men kunne jeg finne mer informasjon ved å søke etter dekknavnets krypteringsnøkler i AMVD?

1) ALL MARKETS VENDOR DIRECTORY (AMVD)

SR1 var navet for dopsalg på det mørke nettet i 2011-2013. Da SR1 ble stengt, ble 150 000 brukere spredt over mange nye skjulte nettsider. Fragmenteringen gjorde det vanskelig for kundene å finne selgerne de stolte på. I kaoset ga databasen AMVD orden. Der lå 4500 offentlige krypterings-nøkler til 6000 dekknavn fra åtte skjulte nettsider mellom 2011 og 2015. Slik kunne kunder søke seg frem til den offentlige nøkkelen til selgeren de stolte på.

En bonus med AMVD-søk er at databasen kan fortelle når og på hvilken skjult nettside en selgerkonto ble registrert, hvor mange dopsalg som er gjort, hvilke offentlige nøkler dekknavnet opererer med og e-postadressene de er knyttet til.

For journalister, politi eller forskere som gjør research på det mørke nettet er AMVD en kjemperessurs. I TEPPEFALL-prosjektet var det spesielt muligheten til å gå bakover i tid som var viktig i jakten på personen (e) som sto bak DEEEPLOVE. Men jeg satt kun på *en* e-postadresse som DL brukte våren 2013. Kunne AMVD avsløre andre ting om DEEEPLOVE?

A) Hva var målet?

Se om DEEEPLOVE aktiv på andre skjulte nettsider (i tillegg til SR) i 2013. Finne ut når DL registrerte seg på de ulike sidene og med hvilke e-postadresser. Hente ut salgsloggen for å se omfanget av dopsalget og laste ned DEEEPLOVEs offentlige krypteringsnøkler.

B) Hva ble funnet?

DEEPLOVE var på SILK ROAD fra mars 2013, og på BLACK MARKET RELOADED (BMR) og på SHEEP MARKETPLACE fra oktober. På BMR sto DL for 17 salg og på SHEEP var det 289 loggførte salg av narkotika. DL brukte to forskjellige e-postadresser.

Spesielt to opplysninger fra AMVD var viktige: Databasen avslørte at DL var aktiv på BMR, SHEEP og SR1 (samme steder som ALFA&OMEGA oppga å ha stått for 1000 dopsalg på). Samtidig viste AMVD at A&O-aliaset ikke eksisterte der.

E-postadressen som DEEEPLOVE brukte til kundekontakt på SR1 var utgangspunktet mitt. AMVD ga meg en adresse til. Jeg visste at det var vanlig å bytte adresser, men den jeg fant var til en gmail-konto, og ikke til en kryptert e-posttjeneste. Det var et lovende spor for det ledet ut av «boblen» hvor all informasjon var kryptert, og til det åpne internettet.

2.1.2 METODE 2: E-postspor 1

Jeg ser alltid etter opplysninger som leder bakover i tid fordi jeg har utnyttet at digitale spor kan være veldig vanskelig å fjerne i andre saker. I 2015 var de norske dopnettverkene veldig profesjonelle. Men det er krevende å leve et dobbeltliv over lang tid. Hadde de alltid vært så sikkerhetsbevisste? Gmail-adressen kunne være en avgjørende tabbe, tenkte jeg. Heretter omtales gmail-sporet omtales som ALIAS1@GMAIL.COM, av hensyn til identifisering.

A) Hva var målet?

Se om det gikk an å spore ALIAS1@GMAIL.COM til noe, eller noen

B) Hva ble funnet?

ALIAS1@GMAIL.COM hørte til en brukerkonto (videre kalt ALIAS1) som hadde skrevet hundrevis av innlegg på norske forum for finansnyheter mellom 2010 og 2013, blant annet HegnarOnline og Stocktalk. ALIAS1 og ALIAS1@GMAIL.COM hørte til en finansblogg på blogspot.com i 2010 som opphavspersonen brukte til å gi investeringsråd til nordmenn. Bloggen er slettet. I 2010 var bloggens adresse og ALIAS1@GMAIL.COM knyttet til enda en brukerkonto på Stocktalk. Kontoen var under et nytt pseudonym (ALIAS2). Jeg fant ALIAS2 på Stocktwits, et tredje nettsted for finansfolk. På Stocktwits var ALIAS2 registrert i 2009 og på kontoen var et ekte navn oppgitt som kontoeeier.

Jeg tok skjermbilder fortløpende mens jeg manøvrerte gjennom forum og gamle innlegg. I midten av februar stoppet rekken av spor fra gmail-adressen til DEEPLOVE opp ved det ekte navnet på Stocktwits-kontoen. I 2015 var mannen 29 år gammel. Da jeg så navnet gikk det kaldt nedover ryggen på meg. Jeg hadde sett det før:

På høsten i 2014, da jeg forberedte SILKEVEIENE-saken, sendte jeg en henvendelse til Länskriminalen i Skåne om etterforskningsdokumentene fra en av sakene til superspaneren Jimmy Arkenheim. Jeg fikk utlevert 1200 sider som jeg gikk gjennom. I materialet lå det bilder av sju konvolutter som skulle til norske kunder av det svenske nettverket som Arkenheim jaktet på. Jeg hadde merket meg navnene og notert de ned. En av de sju konvoluttene skulle til den samme 29-åringen, som bodde i Oslo.

Gmail-sporet viste at 29-åringen var en av de som sto bak DEEEPLOVE, en av Norges største selgere av dop fra det mørke nettet (se skjermbilder i vedlegg 3 og 4).

2.1.3 METODE 3: E-postspor 2

Den andre e-postadressen som kunne knyttes til DEEEPLOVE ble funnet i AMVD. Adressen pekte til en leverandør som tilbød kryptert sending. Jeg måtte undersøke den selv om jeg hadde funnet et navn fra gmail-adressen. Adresse 2 kalles nå: SALG@HUSHMAIL.COM

A) Hva var målet?

Se om det gikk an å spore SALG@HUSHMAIL.COM til noe, eller noen

B) Hva ble funnet?

Adressen ga ingen treff på det åpne nettet, men førte til at jeg fant seks forskjellige krypteringsnøkler knyttet til DEEEPLOVE i AMVD- og PGP.MIT.EDU-databasene

Nøklene var brukt med flere e-postkontoer som DEEEPLOVE hadde disponert i 2013.

2.1.4 METODE 4: Analyse av krypteringsnøkler

En krypteringsnøkkel ser ut som en meningsløs samling bokstav og tall, se vedlegg 2. Jeg var usikker på om det var mer å hente, men jeg analyserte DEEEPLOVEs nøkler elektronisk.

A) Hva var målet?

Se etter skjult informasjon eller spor i de seks nøklene

B) Hva ble funnet?

En registreringsdato for hver nøkkel og hvilke e-postleverandører DL benyttet seg av

Jeg lagde et Excel-dokument med en tidslinje hvor registreringsdato på hver adresse ble ført inn. Dokumentet kunne vise om bytte av krypteringsnøkler og e-poster sammenfalt med hendelser på det mørke nettet og i den virkelige verden. Jeg så en utvikling:

Nesten umiddelbart etter at DEEEPLOVEs krypteringsnøkkel ble knyttet til e-postadressen ALIAS1@GMAIL.COM i mai 2013, byttet DL nøkler. Et nøkkelbytte skjedde også etter FBI beslagla SILK ROAD i oktober 2013. Mennene bak DL-aliaset var oppmerksomme på egne feil og på ytre farer. Krypteringsnøklene fortalte i tillegg hvilke e-postleverandører DL brukte. Samtlige krypterer innholdet for brukeren og krever minimalt med IT-kompetanse:

@hushmail, @safe-mail, @tormail, @countermail

Jeg sjekket hvor leverandørene holdt til, og om de ville levere ut innholdet ved rettsanmodning fra norske myndigheter. Svarene ble en del av en interaktiv grafikk som vi presenterte med TEPPEFALL for å vise de digitale sporene. Jeg ville synliggjøre at nettverkene ikke var umulige å avsløre selv om de teknologiske verktøyene virket å være ugjennomtrengelige. Grafikken fins under mellomtittel *Til røttene*.

Den sjuende nøkkelen DL hadde hatt hørte til gmail-adressen. Analyse av nøkkelen viste at den var registrert 13. mai 2013 og at den antakelig var opprettet ved hjelp av programmet GnuPG (se informasjon i vedlegg 3.1). Kanskje fordi DEEEPLOVE hadde behov for å svare på kundenes henvendelser fra en sine personlige e-postkontoer for situasjoner det ikke passet å logge inn på krypterte tjenester.

Noen dager senere fant DEEEPLOVE ut at det ikke var noen god idé, sluttet med GnuPG og gikk tilbake til krypterte tjenester på @hushmail, @safe-mail og så videre. DEEEPLOVEs vurdering var riktig, men skaden hadde skjedd: 13. mai 2013 ble gmail-adressen liggende igjen i AMVD-databasen slik at jeg kunne finne den nesten to år senere, følge sporet ut på åpent nett, gjennom finansforum til jeg hadde navnet på hovedpersonen bak DEEEPLOVE.

2.1.5 METODE 5: Databasesøk 2

Jeg hadde lært en del om PGP, men så ikke for meg at det var databaser for offentlige nøkler utenfor det mørke nettet. Noen uker etter at jeg hadde funnet 29-åringens ekte navn fra søk i AMVD, fikk jeg et spørsmål fra en kilde som ikke fant min offentlige nøkkel i noe kilden kalte PGP.MIT.EDU. Kilden forklarte at det var en database hvor offentlige nøkler var søkbare, akkurat som AMVD. Forskjellen var at denne databasen lå ute på vanlig nett.

Databasen hentet informasjon fra en server på Massachussetts Institute of Technology (MIT). PGP.MIT.EDU ble også synkronisert automatisk mot andre servere. Det betyr, ifølge MIT, at nøkler som lastes opp ikke kan slettes fra systemet.

- Det er litt som en frivillig telefonkatalog, sier Runa Sandvik, ekspert på digitale sikkerhetsverktøy, om databasen.

Jeg hadde ingen mulighet til å sjekke funnet fra databasen AMVD mot andre kilder på det mørke nettet. Og selv om jeg fant støtte for at 29-åringen var DEEEPLOVE, blant annet i de svenske dokumentene, var jeg ute etter å få verifisert PGP-funnet. PGP.MIT.EDU, som lå på et prestisjeuniversitet, fremsto som en mer solid datakilde. Jeg tenkte imidlertid at det var usannsynlig at jeg skulle finne noe om DEEEPLOVE i en database på åpent nett.

2) Søk i PGP.MIT.EDU

PGP.MIT.EDU fungerte som AMVD, og jeg kunne søke etter en bestemt nøkkel, på navn, i fritekst eller på alias som DEEEPLOVE / ALFA&OMEGA.

A) Hva var målet?

Se etter spor etter DEEEPLOVEs epostadresser i PGP.MIT.EDU

B) Hva ble funnet?

Se søkeresultatet i vedlegg 6. Krypteringsnøkkelen fra ALIAS1@GMAIL var også brukt med to andre adresser: DLs salgsepost fra SR og den private e-posten som tilhørte 29-åringen

PGP.MIT.EDU fortalte at 29-åringen sto bak DEEEPLOVE-aliaset fordi han hadde brukt den samme krypteringsnøkkelen til en e-postkonto i sitt eget navn og i e-posten som DL brukte til omfattende dopsalg. Jeg visste at for å få lest meldinger kryptert mot nøkkelen som var felles for de tre adressene, måtte vedkommende bak sitte på den private (og hemmelige) dekrypteringsnøkkelen. Som digitalt spor var funnet som en smoking gun.

For meg er dette et eksempel på at de som bruker avansert teknologi for å skjule seg, ikke nødvendigvis har tilsvarende avansert teknologisk kompetanse. DL var ikke klar over hvor stor sikkerhetsrisiko lemfeldig omgang med offentlige nøkler og PGP.MIT.EDU var. Mennene bak visste ikke at nøkler og informasjon kan bli liggende igjen.

2.1.6 METODE 7: Åpne søk

Da jeg hadde koblet et ekte navn til DEEEPLOVE, sørget jeg for å finne ut mest mulig om vedkommende ved hjelp av åpne nettsøk.

A) Hva var målet?

Skaffe mer informasjon om 29-åringen og hans bakgrunn

B) Hva ble funnet?

Mannens bakgrunn var fra finansbransjen. Han hadde uttalt seg i aviser om aksjetrading og hadde vært involvert i flere selskaper. Jeg fant oppføringer i Storbritannia, Norge og Kina.

En del av problemstillingen var å finne ut om de som solgte narkotika på det mørke nettet var «vanlige» kriminelle. Fra 29-åringens yrkesbakgrunn fremsto han som ressurssterk, initiativrik og intelligent. Dette var ikke «pusheren på plata».

2.1.7 METODE 8: Kartlegging sosiale medier

Jeg forventet ikke å finne noe av betydning på 29-åringens kontoer i sosiale medier. Men jeg hadde jo dokumentert at han hadde gjort tabber så jeg måtte se hva jeg kunne finne.

A) Hva var målet?

Kartlegge 29-åringens aktivitet på sosiale medier

B) Hva ble funnet?

Fra Facebook så jeg at 29-åringen hadde studert i et av landene hvor han var registrert med et selskap. På Instagram delta han innlegg om Bitcoin. Det er et legitimt, digitalt betalingsmiddel, men også det primære betalingsmiddelet på det mørke nettet. Bitcoin-innleggene beviste ingenting, men bekreftet at 29-åringen hadde lang erfaring med slike transaksjoner. Mannen disponerte enda en Instagram-konto, registrert under et alias. To kontoer på Soundcloud viste at han likte musikksjangeren DEEP HOUSE.

Både Facebook- og Soundcloud-kontoene var åpne. Instagram-kontoen i 29-åringens navn var låst. Vi ville ikke at mannen skulle lure på hvorfor journalister fra Trondheim ønsket å følge ham, så vi opprettet en falsk konto og sendte en følgeforespørsel som han aksepterte. Da fikk vi tilgang til over 100 av 29-åringens innlegg over tre år. I tillegg så vi at han hadde enda en konto, under et pseudonym. Vi brukte informasjonen vi fikk fra sosiale medier til å forberede bruken av spaning som metode i Oslo.

2.1.8 METODE 9: Geolokalisering fra SoMe

Da jeg var på SKUPs graveskole i 2013 lærte jeg om programmet Geocreepy på et kurs med sikkerhetseksperten Tor Andre Breivikås. Geocreepy lokaliserer personer geografisk ut fra GPS-spor som deles i sosiale medier. Programmet kan gi informasjon om dato og tidspunkt for aktiviteten. I 2014 brukte Jan Gunnar Furuly Geocreepy til å kartlegge bevegelsene til norske politikere.

A) Hva var målet?

Se etter steder 29-åringen besøkte ofte og som vi måtte være obs på.

B) Hva ble funnet?

Undersøkelsene avslørte et bevegelsesmønster i flere bydeler (og land).

Geocreepy finner GPS-spor på Google+, Instagram, Flickr og Twitter. I vår sak var kun Instagram aktuelt, men jeg hadde til gjengjeld to kontoer som mannen brukte. 29-åringen hadde sperret GPS-data på kontoen hvor han brukte sitt ekte navn. På pseudonym-kontoen hadde han glemt å gjøre dette noe som ga GPS-posisjoner fra 44 innlegg, og data om når de var publisert. Informasjonen ble brukt i spaningsforberedelsene.

2.2 METODE 10: Spaning

I løpet av våren hadde vi to opphold i Oslo som varte i en arbeidsuke hver gang. Selv om vi hadde funnet og verifisert en link mellom 29-åringens identitet og DEEEPLOVE, så ville vi observere mannen, for å få bekreftet eller avkreftet flere hypoteser og skaffe mest mulig bildedokumentasjon.

Spaning som metode krever mye forberedelser (forklart i punkt C). Vi hadde brukt metoden i SILKEVEIENE-sakene, men på postkasser og statiske mål. Nå skulle vi følge en 29-åring rundt i travle Oslo sentrum. Det var noe helt annet. Redaksjonsledelsen var spesielt opptatt av sikkerheten rundt dette. Vi visste ingenting om hva slags person vi hadde med og gjøre og hva som kunne skje hvis vi ble oppdaget.

A) Hva var målet?

Følge 29-åringens bevegelser, observere hvem han traff og hva han gjorde. Bekrefte eller avkrefte at han hadde en normal jobb. Skaffe bildedokumentasjon og få bilde av brevposting. Konfrontere 29-åringen med våre funn og sikre samtidig imøtegåelse.

B) Hva ble funnet?

Vi skaffet mye bildedokumentasjon. Ingenting tydet på at mannen hadde en normal jobb. Vi observerte kjøreturer rundt om i Oslo sentrum på underlige tidspunkt. Vi observerte møter med flere forskjellige personer som vi ikke kjente identiteten til.

C) Hvordan ble spaningen forberedt?

Bydelen ble studert i Google Earth. Nærmiljøet, gater, enveiskjøringer, parkering og mulige posisjoner ble vurdert med Google Street View. Informasjon fra sosiale medier og geolokalisering ble analysert med samme verktøy. Vi utstyrte leiebilene med flere barneskjermer, slik at de skulle passe bedre inn i området og gi noe kamuflasje for oss som måtte sitte der dagen lang. Fotograf Ole Martin rigget bilene med flere forskjellige kamera (se vedlegg 8), slik at han kunne få sikret bilder uansett om vi var stasjonære eller ute i trafikken. Under hvert opphold skiftet vi leiebil tre eller fire ganger, som et sikkerhetstiltak. Søk i Postens nettsider fortalte hvor det var innleveringspostkasser. Vi antok at det å gå på postkontor var uaktuelt, siden de er videoovervåket

Det var tydelig at 29-åringen ikke hadde en vanlig jobb. Hva han egentlig gjorde om dagene, ga ikke spaningen et entydig svar på. Men mannens bevegelser og rutiner styrket hypotesen om hans tilknytning til ALFA&OMEGA og eller DEEEPLOVE.

Vi fikk ikke et bilde av 29-åringen som postet brev, men fordi vi ikke var gode nok til å følge ham på kjøreturer rundt om i byen kunne vi ikke utelukke at det skjedde. Samtidig så vi flere

møter mellom mannen og andre personer, som fremsto som spesielle. I et tilfelle skjedde møtet i mannens bil, mens 29-åringen kjørte samme runde rundt et kjent landemerke i Oslo sentrum to ganger.

Spaningen er en ressurskrevende metode. For å utnytte spaningsoppholdene bedre burde vi hatt to team. Altfor mange ganger mistet vi 29-åringen under kjøreturer rundt om i trafikken. Da mistet vi også muligheten til å gjøre flere funn. En tredje tur til Oslo var planlagt for å dokumentere en konfrontasjon med 29-åringen. Turen skulle legges nært opptil publiserings-dato. Da Kripos gikk til aksjon 8. juni måtte vi ta tilsvar på vanlig måte via forsvarer.

2.3 ALFA&OMEGA-hypotesen

Som søk i ALL MARKETS VENDOR DIRECTORY hadde avslørt så eksisterte DEEEPLOVE kun i 2013, på SILK ROAD, BLACK MARKET RELOADED (BMR) og SHEEP. ALFA&OMEGA dukket først opp i midten av oktober 2013, like før DL forsvant. Mageføelsen sa at samme person (er) sto bak begge aliasene og AMVD viste at navnene ikke hadde sameksistert, men overlappet. Hvordan kunne jeg finne ut om det stemte, og dokumentere navnebyttet?

PGP.MIT.EDU viste at noen registrerte en krypteringsnøkkel til ALFA&OMEGA 17. oktober 2013, to uker etter at SILK ROAD ble stengt av FBI. Samtidig gikk jeg gjennom hundrevis av A&Os forumposter i 2014 og 2015, et materiale jeg hadde arkivert etter SILKEVEIENE-saken. I en av postene, på forumet knyttet til den skjulte nettsiden AGORA, skrev en kunde 5. januar 2015 en tilbakemelding og fortalte om handel med ALFA&OMEGA våren/sommeren 2013, et tidspunkt hvor A&O ikke eksisterte. Rotet kunden med datoer?

Jeg kunne ikke utelukke det, men innlegget forsterket hypotesen om at folkene bak A&O bare hadde byttet navn. Men var det fra DEEEPLOVE eller noe helt annet? For å få svar på om A&O virkelig var DL, måtte jeg forsøke å rekonstruere «karrieren» dopnettverket hadde hatt på det mørke nettet.

2.3.1 METODE 11: Analyse av datasett fra 2013-2015

SILKEVEIENE-sakene bygget på undersøkelser av fem skjulte nettsider i 2014:

AGORA, EVOLUTION, SILK ROAD 2 (SR2), PANDORA, og CLOUD-NINE

ALFA&OMEGA solgte dop fra de tre første, DEEEPLOVE eksisterte ikke på noen mens KVALITETSBEVISST var på SR2. Jeg måtte skaffe materiale fra 2012 og 2013 for å finne ut mer om DEEEPLOVE. Problemet var at det var slettet.

Våren 2015 fikk jeg tilgang til kopier av tre skjulte sider som forsvant i 2013: SHEEP MARKETPLACE, TORMARKET og BLACK MARKET RELOADED (BMR). Fra før haddes jeg en kopi av SR1. Nå fikk jeg tilgang til enda en kopi. Da den første SR1-kopien min ble tatt på forsommeren, hadde DEEEPLOVE så vidt kommet i gang. Kopi nummer to var tatt 15. september, da SR1 hadde to uker igjen av «levetiden». Kopi2 hadde fanget opp langt mer av DLs aktivitet. Spørsmålet var om kopiene jeg skaffet av SR1, SHEEP, TORMARKET og BMR kunne gi ny kunnskap om ALFA&OMEGA og DEEEPLOVE?

A) Hva var målet?

I 2014 oppga ALFA&OMEGA at nettverket hadde stått for 1000 salg i 2013 da aliaset ikke eksisterte. Å inkriminere seg selv virket underlig, og enda rarere var det dersom det ikke var grunnlag. Var det sant at personen (e) bak hadde stått for «nesten 1000» salg av narkotika i 2013? Hadde A&O eksistert før 17. oktober 2013. Hvis ja, under hvilket alias? Var DEEEPLOVE det første aliaset som A&O opererte med? Kunne jeg finne eldre profiler på A&O? Jeg ville undersøke alle innlegg og profiler på DL for å kartlegge antall salg og vareutvalg fra mars til oktober 2013. Var det sant at DL la ned dopsalget i oktober 2013?

B) Hva ble funnet?

ALFA&OMEGA eksisterte ikke før 17. okt. 2013. Salgslogg fra den andre SR-kopien fra 15. september 2013 viste at DEEEPLOVE hadde over 300 dopsalg på noen måneder. DL skrev selv at personene bak hadde sendt narkotika i posten i ti år. Det fortalte mye om omfanget av virksomheten jeg hadde sporet til en 29-åring i den virkelige verden og hvor effektiv beskyttelse teknologi ga. Begge SR-kopiene dokumenterte at DL hadde produktnavn som kun en annen norsk selger brukte: A&O. I kopien av SHEEP fant jeg en DL-profil hvor det var registrert ytterligere 289 narkosalg. Profilen hadde samme krypteringsnøkkel som DLs SR-profil: Samme person (er) sto bak profilene. Fra kopien av TORMARKET fant jeg A&Os profil med 17 registrerte salg. Jeg så at A&O-profilen var identisk med DEEEPLOVEs profil på SHEEP: Vareutvalget var det samme, HTML-formatering av tekst var lik og formuleringene var en ordrett kopi. I tillegg oppga A&O et fiktivt navn og adresse på TORMARKET som eksempel på hvordan kundene skulle skrive sine mottaksadresser. Eksempelet var identisk med det DL brukte på SHEEP. Ingen andre brukte disse (vedlegg 9).

Kopiene ga noen praktiske problemer. Materialet var uforholdsmessig stort, på mange tusen sider. Informasjonen var komprimert til *.tar* og *.xz*-filer, som var helt ukjente for meg. Jeg måtte få hjelp av programmerer Jonas Nilsson for å få lest filene i SUBLIME, som har en søkefunksjon som gjør det egnet til store datamengder. Jeg søkte på nøkkelord som «Norge», «DEEEPLOVE», «ALFAOMEGA» og «KVALITETSBEVISST» og fikk ut salgsprofiler, kundeorientering, salgslogger og vareutvalg fra 2013 og 2014. Oversikt over hvilke skjulte nettsider som har vært datakilder ligger i vedlegg 10.

Gjennomgangen av kopiene var tidkrevende, men gjorde meg sikker på sammenhengen mellom DEEEPLOVE og ALFA&OMEGA. Det var sannsynlig at bakmennene hadde skiftet navn i tiden etter FBIs aksjon mot SILK ROAD 1. oktober 2013.

Selv med støtte i disse nye opplysninger kunne jeg ikke utelukke at jeg så sammenhenger fordi jeg ønsket å se dem. Jeg måtte ha ytterligere dokumentasjon. Nye funn, fra tradisjonelt kildearbeid, ble avgjørende for resultatet av prosjektet.

2.4 Kildearbeid

Kildearbeidet pågikk gjennom hele prosjektperioden. Det var rettet mot data- og sikkerhetseksperter, politi og påtalemyndighet, forskere og kjenner av det mørke nettet i Norge og andre land. Kildearbeidet avklarte sentrale forhold rundt 29-åringen bak DEEEPLOVE, skaffet meg tilgang til datasett som ga saken et bredere fundament, førte til ny informasjon om KVALITETSBEVISSTs skjulte side og sørget for at jeg unngikk å gjøre feil på felt hvor min egen datatekniske kompetanse ikke strakk til.

2.4.1 Offentlige kilder

Selv etter mye jobbing satt jeg med en følelse av at det mørke nettet var noe abstrakt og ikke helt «ekte». Følelsen ble forsterket av resultatene fra kartleggingen av 29-åringens kontoer i sosiale medier som ga inntrykk av en ressurssterk person med en vennekrets bestående av tilsvarende ressurssterke personer. Det var vanskelig å skulle forstå at 29-åringen styrte omfattende narkotikasalg til hele Norge, slik funn fra det mørke nettet viste.

Jeg hadde sjekket at 29-åringen ikke var domfelt. For å få fjernet min egen tvil måtte jeg få dokumentert at mannen var eller hadde vært involvert i kriminell aktivitet. En tilleggs-avklaring var også nødvendig: Utgangspunkt for TEPPEFALL-prosjektet var å finne bakmenn fra narkosalget fordi politiet ikke tok problemet på alvor. Hvis det pågikk en etterforskning mot 29-åringen, så kunne det fått innvirkning på vår dekning.

A) Hva var målet?

Var 29-åringen under etterforskning? Hadde han vært involvert i kriminalitet, i så fall hvilken type og alvorlighet? Få sjekket om noen av landets største politidistrikt hadde etterforsket dopsalg på det mørke nettet og om KRIPOS hadde igangsatt etterforskning etter SILKEVEIENE-saken som ble publisert 5. november 2014 hvor ALFA&OMEGA spilte en hovedrolle og hvor KVALITETSBEVISST fikk bred omtale?

B) Hva ble funnet?

Det pågikk ingen etterforskning mot 29-åringen (Se merknad i vedlegg 11). Tre brev med dop ble sendt til hans adresse i 2013 og Tollvesenet stoppet samtlige, i april, oktober og november. Over 300 brukerdoser ecstacy lå i konvoluttene, men sakene ble henlagt. Et fjerde brev kom gjennom tollen. Det ble sendt fra Sverige 11. september 2013. Brevet ble fotografert av svensk politi som etterforsket avsenderen, nettverket SWEEXPRESS. Brevet inneholdt hasj eller lykkepiller. De tre største politidistriktene i Norge (Oslo, Hordaland, Rogaland) hadde ingen saker på dopsalg fra det mørke nettet etter SILKEVEIENE ble publisert. Det hadde heller ikke Sør-Trøndelag. KRIPOS svarte 17. desember 2014 at de ikke utelukket at en henvendelse ville bli rettet til internasjonale samarbeidspartnere for å få tilgang til databeslag (som blant annet kunne ramme A&O / DL og KB) «på et eller annet tidspunkt». Direkte spørsmål om en etterforskning var påbegynt forble ubesvart, men jeg fikk opplyst at det var sjelden politiet ville si noe offentlig slikt. Våren 2015 slo en bacheloroppgave ved Politihøgskolen fast at ingen norske selgere var tatt. Kilden, som politistudenten oppgir i fotnotene i oppgaven «Narkotikahandel på dypnettet», var et besøk hos Kripos 16.04.2015.

Selv med så mye ecstasy i, ble sakene med brevene til 29-åringen henlagt en etter en. Det overrasket meg ikke, en del avSILKEVEIENE-saken handlet om statistikk som viste at over 90 prosent av saker som handlet om narkotika sendt med post ble henlagt i Oslo i 2013.

Bildet av det fjerde brevet fikk jeg fra Skåne-politiets etterforskning av nettverket SWEEXPRESS høsten 2013. I motsetning til i Norge kan journalister i Sverige be om innsyn i etterforskningsdokumenter når det tas ut tiltale i en sak. Det skal motvirke maktovergrep. Jeg hadde fått innsyn under arbeidet med SILKEVEIENE-saken.

Informasjonen om tre narkobrev stoppet i tollen samt det svenske bildet av dopkonvolutten med 29-åringens navn- og adresse på var funnene som gjorde at jeg ikke lenger tvilte på at mannen hadde drevet en virksomhet fra skyggene på det mørke nettet.

2.4.2 Slettede bevis

Jeg visste at ALFA&OMEGA / DEEELOVE-dekknavnene hadde vært aktive siden mars 2013, og på flere skjulte nettsider. Men jeg begynte ikke å samle informasjon før høsten 2014. Hva hadde foregått i de 18 månedene før jeg koblet meg opp første gang?

Søk i AMVD viste at DL og A&O hadde solgt stoff fra fire skjulte sider som var slettet, og fra SILK ROAD som FBI hadde beslaglagt. Det måtte ligge svært interessante opplysninger om aliasene på de skjulte nettsidene, men var det i det hele tatt mulig å få tilgang til slettet info?

Det viste seg at det er et lite internasjonalt miljø av forskere og sikkerhetseksperter som følger utviklingen på det mørke nettet. Jeg måtte komme tett på miljøet og få oversikt over hvem det gikk an å snakke med, men jeg hadde dårlig tid. Utfordringen lå i å finne kilder som satt på informasjon, og oppnå nok tillit til at de ville dele materialet med meg.

A) Hva var målet?

Skaffe kopier av SILK ROAD, SHEEP MARKETPLACE, BLACK MARKET RELOADED (BMR), TOR MARKET og forumene til hver skjulte nettside

B) Hva ble funnet?

Jeg fikk kopi av SR1 fra 15. september og medhørende forum. Her var DL og KB aktive. Jeg fikk kopier av SHEEP, TORMARKET og BMR.

Kopiene fylte inn hullene i tidslinjen min. Jeg kunne følge utviklingen fra DEEEPLOVE til ALFA&OMEGA og ha oversikt over KVALITETSBEVISST. De slettede sidene avdekket også nye feil som bakmennene hadde gjort, som å kopiere profiler ordrett mellom ulike sider.

2.4.3 Ekspertanalyse 1: Skjulte nettsider

23. oktober 2013 tok personen bak KVALITETSBEVISST et stort steg mot å profesjonalisere virksomheten sin og åpnet sin egen skjulte nettside. Å opprette en egen skjult nettside ved er for teknisk viderekomne. Det er en svært krevende oppgave å kode og konfigurere dette slik at siden ikke «lekker» informasjon som kan brukes til å identifisere bakmannen eller hvor serveren befinner seg. Jeg fikk en dataekspert til å se på KBs side. Rammene ble avgrenset til at eksperten skulle se på overflaten, det var uaktuelt å gjøre seg skyldig i datainnbrudd, selv om siden ble brukt til salg av dop.

A) Hva var målet?

Få mest mulig informasjon om siden, og se hvilke tekniske løsninger som lå til grunn. Hente ut en IP-adresse til serveren, eller andre identifiserende opplysninger.

B) Hva ble funnet?

KVALITETSBEVISST hadde brukt en variant av operativsystemet Linux som heter Gentoo, som lar brukeren skreddersy program og operativsystem til sin egen datamaskin. I 2014 var Gentoo på 38. plass av populære Linux-varianter. Scriptspråket var PHP, siden kjørte på en nginx-server mens det visuelle innholdet ble matet inn via en wordpress-plattform. Nettsidene var profesjonelt satt opp. Det lot seg ikke gjøre å lese av en IP-adresse.

Det finnes firma som tar betalt for å opprette skjulte nettsider, men sidene som selges er generiske og lite fleksible. Alt tydet på at personen bak KB hadde gjort jobben selv.

Dataeksperten som så på den konkluderte med at personen som hadde satt opp KBs side måtte ha svært god kjennskap til IT-sikkerhet.

Eksperten ba om å bli anonymisert på grunn av frykt for represalier fra kriminelle elementer på det mørke nettet. Jeg hadde selv blitt utsatt for ubehageligheter etter SILKEVEIENE-sakene, og visste at miljøet kunne slå tilbake. Jeg gikk med på å anonymisere eksperten.

2.4.4 Ekspertanalyse 2: PGP-sporene

PGP er et avansert sikkerhetsverktøy med lav brukervennlighet. Samtidig presenteres resultatene fra søk i databasen PGP.MIT.EDU på en måte som er rettet mot «datafolk».

Jeg har ikke teknisk bakgrunn, eller spesiell kunnskap om IT. For å sikre meg mot feil ba jeg om hjelp til å forstå funn jeg hadde gjort, blant annet fra Runa Sandvik. Hun er ekspert på digitale sikkerhetsverktøy og har det siste året holdt flere kurs for norske journalister og redaktørforeningen, blant annet på SKUP-konferansen i 2015.

A) Hva var målet?

Kvalitetssikre funn fra søkene jeg gjorde i databasen PGP.MIT.EDU

B) Hva ble funnet?

Sandvik bekreftet at funnene jeg hadde gjort på DEEEPLOVEs identitet stemte. Samtidig hadde jeg misforstått det jeg hadde funnet i krypteringsnøklene til KVALITETSBEVISST.

Hennes innspill var avgjørende for TEPPEFALL og stoppet meg fra å gå i bekreftelsesfella.

2.5 Mål B

Mål B var å avdekke identiteten til personen (e) bak aliaset KVALITETSBEVISST.

2.5.1 METODE 12: Analyse av skjulte nettsider

Under SILKEVEIENE-saken fant jeg KBs egen skjulte nettside. Jeg gikk gjennom innholdet og lagret skjermbilder. Etter hvert oppdaget jeg at KB i tillegg hadde satt opp et hemmelig forum kun for nordmenn. Til TEPPEFALL er to utgaver av KBs salgsside og kundeforum analysert. Skjermbilder ligger i vedleggene til rapporten.

A) Hva var målet?

Lære mest mulig om KBs aktivitet: Antall narkotikasalg, vareutvalg, pakkerutiner, postrutiner og tilgang til dop. Få kartlagt epostadresser og PGP-nøkler

B) Hva ble funnet?

KVALITETSBEVISST hadde ualminnelig god tilgang til ulike marihuana-typer. KB sendte post på faste dager og stoffene ble vakuumpakket flere ganger. KB var nærmest sykelig opptatt av sikkerhet og svarte ikke på beskjeder som ikke var krypterte. Etter hver utviklet KB et automatisert bestillingssystem hvor stoff, kunder og beløp var erstattet med tallkoder. Systemet var svært avansert, og et av sikkerhetstiltakene som gjorde at kundene stolte på KB. I tillegg til marihuana hadde KB tilgang til kokain, såkalt «magic mushrooms» og MDMA. På KBs sider var salgsloggen fjernet slik at det ikke gikk å dokumentere omfanget av salget slik jeg hadde gjort i SILKEVEIENE-saken. KB hadde skrevet over 400 meldinger på et forum som KB opprettet for nordmenn. Analyse av innleggene viste at KB satt ved tastaturet på

kveldstid og dette ble presentert i en grafikk i TEPPEFALL. Samme analyse fortalte at KB ble pågrepet på kvelden 7. juni. Siste melding ble publisert klokken 21.43. Bildene av narkotika på KBs side ble lagret og jeg undersøkte metadata uten å finne noe. Bildene ble imidlertid avgjørende litt senere. Jeg fant mange PGP-nøkler som KB brukte i 2012-2015. De var knyttet til epostadresser hos @lelantos @yahoo @safe-mail @tormail. KBs avatar, profilbildet som personen (e) bak viste kundene, sporet jeg til et obskurt kunstverk laget av to amerikanere som maler i kaffe. KB hadde naturligvis ikke fått tillatelse til å bruke bildet som har tittelen «connoisseuren» (kjenneren) og kunstnerne har varslet søksmål (se vedlegg 12.1).

Salgslogger har siden 2011 vært en sentral del av skjulte sider hvor det selges dop. Tanken bak er at kunder kan lese tilbakemeldinger fra andre kunder. Salgsloggen fungerer som en veiledning til hvem man skal handle fra.

I SILKEVEIENE-sakene brukte jeg salgslogger til å dokumentere antall dopsalg som norske aktører sto bak, blant annet ved å telle antall tilbakemeldinger. Tilsvarende metodikk har blitt brukt av påtalemyndigheten i Sverige til å få avsagt svært strenge dommer mot personer som har omsatt narkotika fra det mørke nettet. KB var langt mer sikkerhetsbevisst enn DEEEPLOVE, og hadde skjønt at salgsloggen var en risiko. På sin egne skjulte nettside eliminerte KB trusselen og publiserte ikke salgsloggen.

Fra 2012 og frem til KBs skjulte side dukket opp i starten av 2014 kunne jeg se at over 600 dopsalg skjedde. Etter det er det umulig å si hvor mange salg KB har gjort, men det er rimelig å anta at totalantallet er oppunder 2000 siden aktiviteten økte underveis. Det var også stor aktivitet på kundeforumene til KB. Her la KB i tillegg ut bilder av stoffer som var på vei inn i butikken. Jeg lagret kopier av hele forumet på ulike tidspunkt.

Hensynet til sikkerhet var viktig for KB, også på kundeforumene. Den eneste informasjonen som var synlig var antall brukere, over 500, som var KBs kunder mellom 2012 og 2015.

2.5.1 METODE 13: Utarbeidelse av profil

PGP-nøklene og e-postadressene til KVALITETSBEVISST ga ingen opplysninger som identifiserte personen (e) bak. Jeg hadde 400 innlegg som KB skrev på sitt eget forum mellom oktober 2013 og juni 2015. I tillegg satt jeg på to kundeforum KB opprettet på SILK ROAD 1, helt tilbake til oktober 2012. Det burde være mulig å lære noe fra så mye informasjon skrevet av KB selv. Jeg bestemte meg for å lage en profil på personen bak skjermen.

A) Hva var målet?

Gå gjennom alt det skriftlige materialet på KB for å «bli kjent» med personen bak skjermen. Jeg så etter kjennetegn, vaner, egenskaper og ortografiske tendenser.

B) Hva ble funnet?

I motsetning til DEEEPLOVE / ALFA&OMEGA, som fremsto som flere personer, virket det som én person var bak KB-aliaset. De sterkeste indikasjonene var skrivemåte og konsekvent bruk av entallspronomen. KB var ingen vanlig bruker av det mørke nettet. Personen bak måtte ha en form for høyere teknologiutdannelse for å kunne sette opp en skjult side uten å frykte at den skulle være sårbar. Jeg fikk en følelse av at KB var over 30 år. Vurderingene i innleggene viste en viss modenhet. KB lot også til å ha en slags politisk motivasjon, eller i det minste en politisk rettferdiggjørelse av dopsalget han sto for. Andre innlegg bar preg av libertariansk tankegods om uregulerte markeder. KB messet om legalisering, personvern og kontrakultur.

Etter å ha gått gjennom materialet mitt, noterte jeg følgende trekk på KVALITETSBEVISST:

- KB var én person som var over 30 år med høy IT-kompetanse
- Personen hadde en form for høyere teknologiutdannelse
- Politisk orientert mot tema som overvåkning, individuell frihet og legalisering

Jeg er usikker på hvor klokt det var å opprette en profil. Selv om de fleste karakteristikkene stemte, førte profilen til mye tidsbruk og enda verre: Jeg gikk nesten i bekreftelsesfella.

2.5.2 Falsk positiv identifisering

Metoden jeg brukte på ALFA&OMEGA og DEEEPLOVEs epostadresser ga meg til identiteten til 29-åringen i Oslo. Jeg prøvde samme fremgangsmåte på alle epost-adressene som hadde tilhørt KVALITETSBEVISST mellom 2012 og 2015.

A) Hva var målet?

Finne identiteten til KB

B) Hva ble funnet?

Identiteten til en mann i midten av 30-årene på Vestlandet

KB hadde mange e-postadresser og kun en ga treff. PGP.MIT.EDU viste at en annen e-postadresse var knyttet til KBs krypteringsnøkkel den 27. november 2013. Jeg fulgte spor etter adressen på det åpne nettet og fant identiteten til eieren, en mann i midten av 30-årene bosatt på Vestlandet. Funnet førte til en systematisk gjennomgang av denne personens kontoer i sosiale medier og han ytringer. Jeg ville se om personen matchet profilen jeg hadde på KB.

En etter en stemte punktene med mannens personlige detaljer og karakteristikker. Jeg trodde jeg kunne ha funnet mannen bak KB og begynte å se for meg spaningsturer til hans hjemsted. Før jeg gjorde mer sjekket jeg e-postfunnet mot tre kilder som arbeidet med PGP og data-sikkerhet. Se funnet i vedlegg 13 og svaret fra Runa Sandvik, som var en av kildene. De to andre var enig med Sandvik. Den nedslående beskjeden var at jeg hadde misforstått betydningen hva jeg hadde funnet. Jeg satt med en falsk positiv:

Det var ikke sammenheng mellom funnet og identiteten til personen bak KB. Runa Sandvik kunne heldigvis bekrefte at fremgangsmåten jeg hadde brukt til å finne identiteten til 29-åringen bak DEEEPLOVE (og A&O), hang sammen både teknisk og logisk.

Det var frustrerende at jeg hadde tolket KB-funnet feil. Jeg trodde jeg hadde løst begge målene jeg hadde satt meg for saken. Samtidig var det trygghet i at kildene kunne bidra til å forhindre feil. Jeg var ydmyk på at jeg arbeidet med et teknologisk felt som var nytt for meg.

2.5.3 Identifisering av Mål B

På tross av at jeg brukte metodene som fungerte på Mål A til å lete etter personen bak KB, så lykkes jeg ikke. Heller ikke andre metoder eller et stort innsamlet ga meg et navn. Jeg måtte konstatere at jeg mislykkes med mål B. Personen bak KB var for dyktig til å holde sin persona på det mørke nettet adskilt fra sin virkelige identitet.

Da jeg skrev saken ferdig i mai var fokuset på 29-åringen bak DEEEPLOVE og A&O-aliasene, og funnene som viste at de største politidistriktene og Kripos ikke tok tak i kriminaliteten. Jeg leverte saken som ble liggende med behov for avklaringer fra redaksjonsledelsen rundt bildebruk og identifisering.

Så skjedde det noe. 10. juni sendte KRIPOS ut denne pressemeldingen, hvor det gikk frem at fire «sentrale» personer innen salg av narkotika fra det mørke nettet var pågrepet. Alle de store norske mediene siterte meldingen. Mens jeg forsøkte å komme i kontakt med de som etterforsket saken, oppdaget jeg noe i pressemeldingen som jeg kunne bruke.

2.5.4 Pressemeldingen

Pågripelsene måtte stamme den første norske etterforskningen mot dopsalg fra det mørke nettet. Det var tydelig at KRIPOS hadde en strategi om ikke å dele informasjon med media. De skulle beskytte etterforskningen, og ville ikke kommentere hvilke alias som var tatt.

Men i den magre pressemeldingen la jeg merke til noe. KRIPOS viste til tre bilder på Flickr-kontoen sin. Bildene var av en pc, en marihuana-plante og en pakke hasj som pressen kunne illustrere sakene med. Da jeg åpnet Flickr så jeg umiddelbart at KRIPOS-fotografen bare kunne ha tatt to av de tre bildene, av marihuana-planten og pcen.

Jeg kjente igjen det siste bildet, som viste en mørkebrun pakke med hasj, og var helt sikker på at det var hentet fra varesortimentet på den skjulte siden til KVALITETSBEVISST. Bildet viste hasj-varianten «hangman», som KB solgte våren 2015. Var KB pågrepet?

Siden bildet ikke var tatt av KRIPOS fryktet jeg at det kunne være et slags illustrasjonsfoto, og at KRIPOS publiserte det som et eksempel på hva som lå til salgs på det mørke nettet. Jeg måtte få luket vekk den feilkilden før jeg kunne være sikker på at KB satt i varetekt.

A) Hva var målet

Jeg hadde alle opplysningene om KBs aktivitet, utenom identiteten. For å bruke dette i TEPPEFALL måtte jeg få bekreftet at en eller flere av de pågrepne var KB.

B) Hva ble funnet?

KVALITETSBEVISST var en av de fire pågrepne, en 31 år gammel mann.

I omfattende og pågående saker er det en viss (berettiget) frykt hos politiet for at for mye informasjon blir delt i media før de pågrepne er varetektsfengslet. Hvis det skjer, vil forsvarerne kunne bruke det som et argument mot hensynet til bevisforspillelse – som er påtalemyndighetens sentrale argument for å få varetektsfengslet de siktede. Denne taktikken kjenner jeg fra andre saker og visste at jeg ikke ville få svar på direkte spørsmål. Løsningen ble å bruke kunnskapen jeg satt på til å få svaret jeg trengte: Se skjermbilde i vedlegg 14.

Siden Kripos bekreftet at alle de tre bildene dreide seg om *beslag* i den aktuelle saken, var det logisk at KB var en av de fire pågrepne. En bakgrunnssjekk bekreftet at KB var mann på 31. Han passet inn i profilen. Over tretti, med høyere utdanning fra et teknisk universitet. Da han ble pågrepet jobbet han som foredragsholder i datasikkerhetsbransjen – noe som gjorde at han skilte seg ut fra de tre medsiktede.

Da jeg fant navnene på de pågrepne gikk det kaldt nedover ryggen på meg for andre gang: En av dem var den 29 år gamle mannen som vi hadde spanet på og som jeg hadde identifisert som mannen bak DEEEPLOVE og ALFA&OMEGA. Det var overraskende fordi jeg hadde avklart at 29-åringen ikke var under etterforskning da vi forberedte første oslotur i februar.

3. Presseetiske vurderinger

3.1 Falsk identitet

Jeg, eller vi, har operert med flere forskjellige falske identiteter på det mørke nettet, og i enkelte sosiale medier, som Instagram. Vær Varsom-plakaten sier følgende:

> 3.10. Skjult kamera/mikrofon eller falsk identitet skal bare brukes i unntakstilfeller. Forutsetningen må være at dette er eneste mulighet til å avdekke forhold av vesentlig samfunnsmessig betydning

Sakene har avslørt at nordmenn har begått over 5500 uoppklarte narkotikaforbrytelser ved hjelp av det mørke nettet. Videre er identiteten til en mann knyttet til kanskje Norges største salgsnettverk avdekket.

Dette er et miljø hvor anonymitet er hellig og forbrytelsene vi har dokumentert har høye strafferammer. Det har vært avgjørende at vi ikke har identifisert oss som journalister under innsamling av dokumentasjon. Jeg mener at funnene forsvarer bruken av falsk identitet og er ikke i tvil om at forholdene som er avdekket er av vesentlig samfunnsmessig betydning, jamfør VVP. Opplysningene ville ikke kunnet bli fremskaffet ved annen metodebruk.

3.1.1 Det mørke nettet

Både hemmelige forum og skjulte sider stiller krav om innlogging. Dette er steder hvor journalister ikke er populære fordi miljøet som er samlet her, ikke setter pris på noen form for søkelys eller kritisk blikk på handelen med ulovlige varer og tjenester. Det var skjerpende at SILKEVEIENE-saken hadde avslørt omfanget av dophandel, og skapt sinne i miljøet.

På et hemmelig forum var jeg navngitt og omtalt som «i fare» noe Adresseavisen var i kontakt med politiet om. Dersom jeg hadde identifisert meg ville jeg mistet tilgang til informasjon.

3.1.2 Sosiale medier

I SoMe-gjennomgangen av 29-åringen fant vi en Instagram-konto hvor han var svært aktiv. Tilgangen var begrenset slik at vi måtte sende en forespørsel om å følge mannen.
Det var grunn til å tro at 29-åringen ville kjenne igjen navnet mitt og derfor opprettet vi en falsk profil, som ikke oppga personalia, men som var interessert i samme musikksjangre som ham. Interessen hadde vi sett i hans profiler, og vi tok sjansen på at musikklinken gjorde at han godtok forespørselen. Det gjorde han og vi fikk tilgang til innlegg som vi kunne bruke til geolokalisering. Her oppdaget vi også at han hadde enda en Instagram-profil under et alias.

3.2 Identifisering

Det ble klart relativt tidlig at jeg lykkes i å avdekke identiteten til en 29-åring bak DEEEPLOVE og A&O. På dette tidspunktet, i midten av februar, viste vårt kildearbeid at det ikke pågikk en etterforskning mot mannen. Han var heller ikke tidligere straffet. Vær Varsom-plakatens paragraf 4.7 sier blant annet følgende:

> Vær varsom med bruk av navn og bilde og andre klare identifikasjonstegn på personer som omtales i forbindelse med klanderverdige eller straffbare forhold. Vis særlig varsomhet ved omtale av saker på tidlig stadium av etterforskning
>
> (...) Det kan eksempelvis være berettiget å identifisere ved overhengende fare for overgrep mot forsvarsløse personer, ved alvorlige og gjentatte kriminelle handlinger, når omtaltes identitet eller samfunnsrolle har klar relevans til de forhold som omtales (...)

Adresseavisens etiske retningslinjer legger disse føringene for identifisering:

> I Adresseavisen bruker vi som hovedregel ikke navn og bilde ved omtale av kriminalsaker.

Avgjørelsen fra redaksjonsledelsen var at 29-åringen ikke skulle identifiseres i tekst eller bilde. Da mannen ble pågrepet av Kripos 8. juni ble det gjort en ny vurdering. Selv om 29-åringen nå var siktet i en alvorlig sak med høy strafferamme var konklusjonen lik. Samme vurdering gjaldt for 31-åringen som knyttes til KB-aliaset.

3.3 Bildebruk

Spaningsperiodene i Oslo gjorde at vi satt på et omfattende bildemateriale av 29-åringen som var tatt uten at han visste det. Fem bilder ble publisert etter at bildene hadde vært vurdert ut fra hensyn til identifisering. Det ble bestemt at 29-åringens ansikt og andre identifiserende kjennetegn skulle anonymiseres. På et sjette bilde, som jeg skaffet fra svensk politi, ble mannens navn og adresse sladdet på en konvolutt med narkotika.

3.4 Samtidig imøtegåelse

Planen var at vi skulle konfrontere 29-åringen. Han ble pågrepet av Kripos før dette ble gjort og muligheten til samtidig imøtegåelse falt bort. 29-åringen ble varetektsfengslet i fullstendig isolasjon og vi måtte kontakte mannens forsvarer for å sikre tilsvar gjennom å stille konkrete spørsmål rundt de ulike opplysningene vi satt på. Samme fremgangsmåte ble brukt til forsvareren for 31-åringen som skal ha vært KB. Advokatene kunne si svært lite fordi de var underlagt strenge restriksjoner av retten på grunn av de alvorlige siktelsene.

4. Spesielle erfaringer

4.1 Detaljer og dokumentasjon

Historien i TEPPEFALL bygger på store og små biter med informasjon som er samlet inn fra et stort antall lukkede og åpne kilder. Jeg opplevde flere ganger at opplysninger som fremsto som ubetydelige da de ble funnet, ble svært viktige senere. To Excel-ark, for mål A og B, ble brukt for å holde orden. Jeg laget en sammenstilling av sentrale funn som saken bygde som redaksjonsledelsen kunne bruke som hjelpedokument i presseetiske vurderinger (vedlegg 15).

4.2 Liggetid

Jeg leverte en versjon av tekst og bilder til vurdering 12. mai. Spørsmålet var hvorvidt vi skulle bruke anonymiserte bilder av 29-åringen som vi tok under spaningen. I midten av mai var Adresseavisen preget av omorganisering med en sjefredaktør på vei ut og en annen inn. Saken ble liggende hos ledelsen, uten de nødvendige avklaringene ble tatt. Jeg var frustrert, men opplevde ikke det som noe stort problem fordi jeg var trygg på at ingen andre medier satt på den informasjonen jeg hadde funnet. 8. juni kom KRIPOS- aksjonen.

4.3 Kripos-aksjon og omarbeidelse

Da TEPPEFALL ble skrevet ut var et premiss at politiet ikke foretok seg noe mot kriminaliteten vi hadde dokumentert. Dette ble holdt opp mot våre undersøkelser som ledet til 29-åringens identitet. Jeg hadde jobbet med å avdekke organisert narkosalg fra det mørke nettet nærmest på heltid mellom august 2014 og juni 2015. Da KRIPOS sendte ut pressemelding 9.juni var det en spesiell opplevelse. Jeg hadde levert en sak, ventet og purret for å få publisert den. Nå hadde rammebetingelsene endret seg. Saken måtte endres.

Etter SILKEVEIENE pekte jeg på det jeg flåsete kalte «Norsk impotens» (se punkt 7.4 i rapporten), og varslet oppfølging rundt hvorfor KRIPOS ikke ba om å få utlevert tilgjengelig materiale fra internasjonale samarbeidspartnere som min journalistikk viste at var tilgjengelig. Nå hadde noe endelig skjedd.

SILKEVEIENE ble publisert 5. november 2014, og i slutten av februar 2015 opprettet Kripos OPERASJON MARCO POLO i all hemmelighet. Bevis fra internasjonale politimyndigheter var en av flere metoder som ble brukt i saken. Mens det kokte brukte jeg pressemeldingen metodisk før jeg kastet meg på et fly til Oslo for å rekke varetektsfengslingene, selv om jeg visste at KRIPOS kom til å be om restriksjoner for å beskytte den pågående etterforskningen.

Premisset om at norsk politi satt på hendene, falt vekk. De gode nyhetene var at jeg kunne inkludere materialet jeg hadde samlet på KVALITETSBEVISST. Og at myndighetene tok tak i problemet Adresseavisen hadde brukt mye ressurser på å løfte frem. Etter fengslingsmøtene omarbeidet jeg saken og TEPPEFALL ble publisert 18. juni.

4.4 Etterspill

Mens vi satt i en bil i Oslo og observerte 29-åringen som vi knyttet til DEEEPLOVE / ALFA&OMEGA 1. mars 2015, var OPERASJON MARCO POLO i oppstartsfasen. 29-åringen var enda ikke mistenkt eller siktet.

Etter TEPPEFALL ble det i enkelte lukkede miljøer på nettet spekulert i om Adresseavisen hadde overlevert opplysninger eller funn til OPERASJON MARCO POLO. Dette kan vi selvfølgelig avkrefte. Metoderapporten fra SILKEVEIENE-saken har imidlertid blitt lest av etterforskningslederen på saken.

Et av hovedpoengene med sakene har vært at narkotikasalget utgjorde grov og organisert kriminalitet hvor flere jobbet sammen. Etter å ha etterforsket i 9 måneder opplyste Kripos 27. oktober at tre av de fire som ble pågrepet 8. juni, var siktet etter den såkalte «mafiaparagrafen». Samtlige knyttes til KVALITETSBEVISST. 16. november ble en 26 år gammel slektning av 29-åringen pågrepet. Mannen (26) jobbet som regnskapsfører. Etterforskningsleder Richard Beck Pedersen sier at «mafiaparagrafen» fortløpende vurderes opp mot mennene bak DL og A&O .

Per 19. november var totalt 16 personer pågrepet i tre fylker som følge av OPERASJON MARCO POLO. Sakens dokumenter er fortsatt klausulerte, men i slutten av desember bekreftet Beck Pedersen hvem KRIPOS ville ramme med pågripelsene:

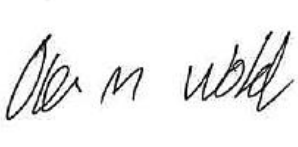
- Vi knytter de fire pågrepne i sommer til aliasene Alfa&Omega, Deeep love og eller Kvalitetsbevisst, sa etterforskningslederen. Operasjon Marco Polo fortsetter utover i 2016.

Jeg har fått forespørsler om å holde foredrag om SILKEVEIENE / TEPPEFALL fra et bredt antall etater og organisasjoner. Innlegg har blitt holdt for Direktoratet for samfunnssikkerhet og beredskap, etterforskere og påtalejurister i Sør-Trøndelag politidistrikt, Seksjon for organisert kriminalitet ved Sentrum politistasjon i Trondheim, Psykofarmakologisk forum ved St. Olavs Hospital, Tollvesenets etterretningskonferanse, Psykiatriveka 2016, Vårmøtet for Sør-Trøndelag legeforening og påtalemøtet til Oslo statsadvokatembeter som våren 2016 omfatter gamle Oslo, Asker, Bærum, Romerike, Follo og Østfold politidistrikt. Sakene er brukt som kilde i en akademisk oppgave på Politihøgskolen, og forskning fra SIRUS.

I slutten av oktober 2015 oppsto Norges andre etterforskning av dopsalg fra det mørke nettet da et miljø i Telemark ble avslørt. Skule Worpvik er leder for seksjon for organisert kriminalitet i Telemark politidistrikt og har ansvaret for saken. Worpvik deltok også i Kripos' pågripelser av KVALITETSBEVISST sommerne 2015.

- Denne narkohandelen er utbredt i et perspektiv som politiet aldri har sett i retning av. Vi hadde ikke vært i stand til å rulle opp vår sak hvis ikke vi hadde hatt kunnskapen fra Adresseavisens saker, sier Skule Worpvik.

Trondheim, 18. januar 2016, Jonas Alsaker Vikan og Ole Martin Wold



5. Publiseringsliste

Se vedlegg 18.