Metoderapport:

Silkeveiene_

Basert på saker i Adresseavisen mellom 5. november 2014 og 15. januar 2015

Innsendere:

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

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

Adresseavisen, Industriveien 13, 7003 Trondheim
Sentralbord: 07200

1.Sammendrag

Adresseavisen avslørte at profesjonelle norske nettverk har stått for minst 5500 salg av kokain, amfetamin, MDMA, ecstasy, hasj og marihuana til norske kunder i løpet av det siste året, uten risiko for å bli pågrepet fordi narkotikasalget skjer fra en skjult del av internett

«Det mørke nettet» fanges ikke opp av søkemotorer. For å få adgang kreves kunnskap om avansert teknologi, kryptering og den digitale valutaen Bitcoin

Vi har avdekket hvordan organiserte norske aktører opererer på det mørke nettet, dokumenterer nettverkenes modus, metoder, priser og utvalg dop, og størrelsen på den norske delen av et internasjonalt marked verdt milliarder av dollar årlig.

Sakene viser hvordan nettverkene utnytter et smutthull i det norske postsystemet og gjør intetanende postmenn og kvinner til narkokurerer. Dette skjer fordi manglende kompetanse og prioritering i politiet har ført til at nettverkene har bygd seg opp over flere år

Avsløringene fikk to statsråder til å rykke ut for å innføre et nytt kontrollregime for Posten og love at kriminaliteten skal gis prioritet i 2015

2.Innhold

3.Innledning

Denne rapporten beskriver arbeidet med prosjektet kalt «silkeveiene», hvor vi i en dokumentar og flere nyhetssaker har avslørt et hittil ukjent norsk narkotikamarked med profesjonelle aktører som skjuler seg på et ukjent område av internett kjent som det mørke nettet (se pkt. 3.2 om Skjulte tjenester).

Prosessen frem mot publisering inneholdt en bratt teknologisk læringskurve. Jeg måtte forstå TOR-systemet og teknologien bak Bitcoin, lære begrep som Operations Security (OPSEC, se pkt. 7.2), og Open-Source Intelligence (OSINT).

Arbeidet har vekslet mellom tradisjonelt journalistisk arbeid, og utvikling av nye metoder for å utvinne informasjon fra skjult materiale på det mørke nettet. Store mengder innsamlede opplysninger har blitt gjennomgått og analysert (se pkt. 5.1 og 5.5).

Rapporten vil drøfte metodebruken og resultatene den ga. Den vil redegjøre for de presseetiske problemstillingene som har oppstått, og de spesielle erfaringene prosjektet har gitt.

Sakene avslører grov narkotikakriminalitet med strafferammer på over ti år i fengsel begått av organiserte miljøer. Politiet har ikke etterforsket disse miljøene som fortsatt er på frifot og i virksomhet. Det har ført til at jeg har måttet ta flere grep for å ivareta sikkerhet og kildevern i denne rapporten. Utfyllende opplysninger kan oppgis til jury ved konkrete forespørsler rundt enkelttema.

3.1 Oppstart

Arbeidet som skulle ende opp i «silkeveiene», begynte for Jonas med en uforståelig nettlenke i begynnelsen av 2014.

Lenken dukket opp i forbindelse med research til en annen sak. Lenken fremsto som ulogisk, den førte til «page not found» - og at jeg ble nysgjerrig:

`http://hj4ndbfe2vhvauck.onion/`

Ved å søke på hele lenken i Google forsto jeg at den var adressen til en skjult nettside som befant seg på det som, for meg, var en ukjent del av internett. Programmet som kamuflerte nettsiden ble også brukte av personer som ønsket å opptre helt anonymt på nettet. Å lære seg å bruke programmet ble den første utfordringen i prosjektet (se pkt. 3.2).

På grunn av andre forpliktelser og saker, ble det med sporadisk research fra lenken ble oppdaget og til jeg gikk ut i foreldrepermisjon i april. I løpet av permisjonen, da jeg fikk litt avstand til jobben og mulighet til å samle tankene, bestemte jeg meg for å gjøre et prosjekt på dette ukjente nettet.

Arbeidet pågikk på heltid mellom 5. august og 5. november 2014, og pågår fortsatt. Ole Martin er fotograf, og ble koblet i september. Mot slutten av arbeidet ble Adresseavisens

utviklingsdesk koblet inn. Fra midten av oktober og frem til publisering, arbeidet Jonas Nilsson, Christer S. Johnsen og Espen Rasmussen med den digitale presentasjonen på hovedsaken.

Jeg (Jonas) jobber i nyhetsavdelingen. Det er antakelig ingen mellomleders drøm at en av nyhetsjournalistene blir opptatt på fulltid med et prosjekt som i hvert fall i begynnelsen fremsto som litt uklart. Jeg har imidlertid blitt møtt kun med velvilje fra reportasjeleder Ann-Inger Borstad som har gitt meg den tiden som har vært nødvendig for og utforske det mørke nettet og de skjulte tjenestene som befinner seg der.

3.2 Skjulte tjenester og TOR

Programmet som skjulte nettsiden jeg fant lenken til, het The Onion Router. TOR er et anonymitetsnettverk som bruker avansert kryptografi for å kamuflere digitale spor, slik at brukerens IP-adresse ikke skal kunne spores av etterretningsorganisasjoner, politi – eller journalister.

Jeg lærte at anonymiteten oppnås ved at TOR sender brukerens nettrafikk gjennom tre lag med servere. Hver server krypterer trafikken før den sendes til neste server og til slutt ut på det åpne internettet vi kjenner.

Nettsider som er satt opp ved hjelp av TOR er kjent som såkalte «hidden services» (skjulte tjenester). De skjulte tjenestene utgjør et område som kalles «dark web», det mørke nettet, som Googles søkemotorer klarer å finne. Jeg skjønte at for å følge lenkene og få opp innholdet, så måtte jeg kjøre en nettleser med TOR.

Det var overraskende lett å lære seg TOR: Det er et gratis system som er tilgjengelig for nedlasting fra det åpne nettet. Etter å ha installert det, fungerer TOR som en nettleser. Etter en kort testperiode kunne jeg surfe fra det åpne nettet og inn på det mørke nettet for første gang.

Jeg følte meg litt som Alice i det hun tumlet ned kaninhullet mot eventyrland.

3.3 Kryptomarkedene

«En nettside hvor varer utveksles mellom parter som bruker krypteringstjenester, spesielt Bitcoin og TOR, til å skjule identiteten sin.» *(Dr. James Martin, Universitetet i Sydney)*

Kryptomarkeder har eksistert siden januar 2011, men holdt en lav profil i flere år. I oktober 2013 ble det største kryptomarkedet raidet av FBI etter en to år lang etterforskning. Begrepet oppsto på ulike hackerforum, ifølge dr. James Martin ved Universitet i Sydney, en av svært få som har publisert forskning om det som foregår på kryptomarkedene.

Da jeg begynte med prosjektet fant jeg over 30 forskjellige kryptomarkeder på det mørke nettet. De tilbyr en lang rekke varer og tjenester, de aller fleste av dem er ulovlige: Hackertjenester, stjålne kredittkort, infisert programvare, falske pass, personopplysninger, sjeldne dyr (!), våpen. Og alle tenkelige former for narkotika.

Jeg hadde ikke jobbet med problemstillingen lenge da jeg skjønte at narkotika var den viktigste varen på det mørke nettet. Tusenvis av ulike former for dop ligger ute for salg på hvert eneste kryptomarked. Narkotika er den desidert største produktkategorien. Stoffene er noen få tastetrykk unna russøkende kunder i hele verden.

Retriever-søk viser at begrepet kryptomarked ikke har blitt brukt i saker av norske journalister. I Norge har narkotikasalg fra det mørke nettet vært omtalt i noen få enkeltstående artikler basert i hovedsak på sitering fra amerikanske medier.

Selv om det var flere nyhetssaker i amerikanske medier, fant jeg imidlertid ingen forsøk på å gå dypere inn i systemene til kryptomarkedene for å beskrive hvordan de fungerte. Det var heller ingen journalister som hadde gjorte en kartlegging av aktører, nettverk og omfang i forskjellige land.

De norske nettverkene jeg fant på kryptomarkedene, hadde imidlertid bred kjennskap til norsk samfunnsstruktur og smutthull som eksisterer.

3.4 Problemstilling

Da jeg kom tilbake på jobb etter permisjon og sommerferie i august, spilte jeg inn ideen om et prosjekt som skulle handle om det mørke nettet. En arbeidsplan ble utformet. Jeg fikk tid til å lete etter opplysninger for å svare på denne problemstillingen:

- *Hva er det mørke nettet? Hva foregår der?*

Problemstillingen var generell fordi verken jeg eller andre i redaksjonen hadde kunnskap om det mørke nettet. I løpet av de første ukene ble problemstillingen endret. Dokumentasjon fra de første undersøkelsene viste at det gikk an å angripe mer konkrete fenomen og forhold ved de skjulte tjenestene.

3.5 Problemstilling v. 2.0

Kjøp og salg av narkotika driver handelen på kryptomarkedene opp i milliarder av dollar hvert år. Formen for narkotikahandel fremsto som ny, og i voldsom økning. Jeg tenkte at narkoflyten måtte bli fokus for prosjektet og stilte meg selv følgende spørsmål:

- Forsyner nordmenn seg fra de internasjonale godteributikkene med narkotika?

Svaret var ja. Det eksisterte et marked hvor også nordmenn opererte. Nye spørsmål:

- Hvor stort var det norske miljøet? Hva var omfanget på narkotikasalget?
- Var nordmenn kunder, eller også selgere? Var norske narkotikaselgere organiserte?
- Hvem er kundene? Hvor befinner de seg?
- Hvilke stoffer selges? Hvordan skjules stoffene?
- Hvordan distribueres narkotikaen? Hvor blir pengene av?

Jeg innså at i tillegg til å finne svar, så måtte jeg forklare det teknologiske bakteppet for det mørke nettet: TOR, kryptomarkeder og Bitcoin. Ideen var å lage en dokumentar som skulle gi

svar på spørsmålene over og samtidig beskrive utviklingen i det norske markedet gjennom 2014.

Adresseavisen har ikke tradisjon for å trykke lengre dokumentarer så jeg ba om at saken kunne publiseres først på Adressa Pluss før kortere versjoner av funn samt oppfølgingssaker skulle gå på nyhetsplass i papirutgaven.

Dokumentaren kunne ikke bare inneholde informasjon fra det mørke nettet, eller handle om noe som skjer på et sted få har hørt om. Det ville bli for abstrakt. Jeg måtte sette det inn i norsk virkelighet og noterte flere spørsmål:

- Hva vet norsk politi om det usynlige norske narkotikamarkedet? Hva vet Kripos?
- Hva vet internasjonalt politi og hva gjør de med narkosalget? Hva gjør norsk politi?
- Har politiet tilgang på riktig kompetanse og metoder?
- Hva sier forskning, internasjonalt og nasjonalt, om problematikken?
- Er politikerne orientert? Gjør de noe med det som foregår?

Etter å ha endret problemstillingen gikk jeg i midten av august i gang med å lete etter svar på spørsmålene.

4. Dette er nytt

- Organiserte, norske nettverk har det siste året stått for minst 5500 salg av kokain, ecstasy, amfetamin, LSD og andre stoffer til norske kunder på det mørke nettet. Omsetningen er på mange millioner kroner. Pengene forsvinner med en anonym digital valuta som ikke kan spores av banker eller myndigheter. Nettverkene har vært aktive i flere år

- Narkotika sendes i vanlig A-post med innenrikspost. I Norge er det ingen kontroll av brev som går på kryss og tvers av landet. Brevene kan heller ikke spores gjennom postsystemet. I tillegg selger nettverkene dop fra Norge og sender det til kunder over store deler av verden. Nettverkene vet at Norge ikke er ansett som et land som produserer narkotika, og forsendelser blir sjelden stoppet. I tillegg har ikke Tollvesenet regelmessige kontroller av brev som går ut av landet. Alt dette vet nettverkene, som bruker opplysningene aktivt i markedsføring

- Nettverkene pusher kokain, ecstasy, amfetamin og andre stoffer på kunder de ikke aner hvem er. Vi dokumenterer at barn er blant kundene. Samtidig tilbyr nettlangerne gratis stoff mot at brukerne skriver en rusrapport om virkningen av stoffet. Rusrapporten brukes i markedsføring, som bevis på narkoens kvalitet

- Påtalemyndigheten henla i fjor 87 prosent av alle saker som oppsto etter beslag av utenlandske narkotikabrev adressert til nordmenn. Antall beslag er i sterk økning, ifølge Tollvesenet. Men antallet slike saker som endte i påtaleavgjørelse i 2013, er over fem ganger lavere enn antallet narkotikasalg som vi dokumenterer på det mørke nettet. Den narkoposten får reise fritt, så lenge langerne betaler porto

- Norsk politi har ikke kjennskap til det norske markedet som vi har kartlagt. Politiet kjenner ikke til omfanget på narkotikaforbrytelsene som begås der daglig. Det har ikke vært en norsk etterforskning av den organiserte kriminaliteten som styres av og rettes mot nordmenn på det mørke nettet

- To dager etter publisering av de første sakene gikk 16 land til en koordinert aksjon mot narkotikasalget på det mørke nettet. Mens Finland og Sverige deltok, sto Norge utenfor det internasjonale samarbeidet. Kripos oppgir at internasjonalt samarbeid er svært viktig for å oppdage slik kriminalitet, men selv om bevis på de norske nettverkenes aktivitet, kommunikasjon, modus, kundeidentiteter og vareutvalg ligger tilgjengelig hos Europol, har ikke Kripos bedt om å få det utlevert

- 3 uker etter at dokumentaren silkeveiene ble publisert, gikk samferdselsministeren og justisministeren sammen med konsernsjef i Posten for å bruke politiet til å kontrollere innenriksposten. Endringen i postsystemet skal stoppe narkoflyten fra de norske nettverkene. Ifølge samferdselsminister Ketil Solvik-Olsen skjedde dette fordi narkosalget ikke hadde «fått den oppmerksomhet og prioritet som det bør ha»

5. Metoder og kildebruk

Da jeg begynte med prosjektet, innså jeg raskt at det ikke eksisterte en oppskrift jeg kunne følge. Jeg måtte etablere egne metoder for å samle inn informasjon fra data som var tilgjengelig på det mørke nettet.

Jeg brukte erfaring fra tidligere saker og kursing til å følge spor fra det mørke nettet ut på det åpne nettet, og gjennom flere sosiale medier.

Parallelt jobbet jeg mer tradisjonelt mot kilder i politiet, nasjonalt og internasjonalt, skrev begjæringer om tilgang på rettskilder i Norge og utlandet, søkte etter svar hos forskere i Australia, Canada og England, og holdt etter hvert adresser fysisk under oppsikt flere steder i Midt-Norge.

For å gjøre metodikken så oversiktlig som mulig er hver metode gitt et tall i denne rapporten. Tallet angir cirka når arbeidet den ble brukt for første gang. Noen av metodene ble brukt i en kort periode, mens andre var relevante gjennom hele prosjektet. I vedleggene finnes også et metodekart (se pkt. 10.2) som viser tidsbruk og forholdet mellom metodene så presist som jeg kan huske. Jeg har måttet lære meg å ta i bruk flere verktøy som jeg ikke kjente til fra før. Dette er redegjort for i punkt 10.1.

Skriftlige kilder er inndelt i avsnitt om datagraving (pkt. 5.1) og dokumentgraving (pkt. 5.5).

5.1 Datagraving

Internasjonale og norske narkoselgere som er aktive på det mørke nettet er i utgangspunktet skjult av TOR-systemet. De bruker i tillegg dekknavn og sender krypterte beskjeder til hverandre. Mye tid og ressurser går med på å opprettholde anonymiteten.

Likevel var det mulig å finne konkrete opplysninger som kunne brukes. Den største overraskelsen for meg som journalist, var at jeg kunne «misbruke» infrastrukturen på det mørke nettet til å finne konkrete opplysninger om modus og omfang på svært alvorlig narkotikakriminalitet. Det avgjørende her, var at jeg brukte nok tid til å skjønne hvordan infrastrukturen var bygd opp. Se flere betraktninger i pkt. 7, «Spesielle erfaringer»).

I denne fasen brukte jeg fire hovedmetoder: Lenkefarming, informasjonsinnsamling, analyse av omdømmesystemet, søk i krypteringsnøkkeldatabaser.

5.1.1 Metode 1: Lenkefarming

Jeg hadde forstått at adressene til de skjulte tjenestene (kryptomarkedene) besto av et ulogisk utvalg bokstaver og *.onion*.

Ettersom de skjulte tjenestene ikke fanges opp av Google, måtte jeg ha lenkene til de sidene jeg skulle undersøke. Jeg strevde med å få oversikt, og i oppstartsperioden føltes det hele som å famle rundt i blinde.

Innhenting av lenker ble gjort i to omganger: Det var den første metoden jeg brukte i august, og funnene lå til grunn for alt arbeid som fulgte. I september var det nødvendig å bruke samme metode igjen.

August:

A) Hva var målet?

- Finne lenker til kryptomarkeder
- Finne lenker til eventuelt andre mulige kilder som undergrunnsforum
- Se etter informasjon om aktører
- Finne opplysninger om hvordan systemene fungerte
- Var det mulig å forstå noe av narkonettverkenes modus?

B) Hva ble funnet?

- Jeg så at det var over 30 kryptomarkeder i sving, og samlet lenkene i et dokument
- Jeg fant ut at hvert kryptomarked var knyttet til et eksternt undergrunnsforum
- Jeg identifiserte de fem største og viktigste kryptomarkedene
- Jeg forsto at kryptomarkedene og undergrunnsforumene hadde forskjellig funksjon (beskrevet detaljert i punkt 1 og 2 under)

C) Forholdet til andre metoder

- Lenkeinnhenting foregikk parallelt med alle de andre metodene fordi selv om jeg etter hvert skaffet meg bred oversikt over det mørke nettet, fortsatte jeg å finne relevante lenker som ga ny informasjon helt frem til publisering

Utgangspunktet jeg hadde var en lenke til kryptomarkedet SILK ROAD 2 (SR2) som jeg fant gjennom åpne søk etter saker om det mørke nettet.

Fra SR2 fant jeg lenker videre til et undergrunnsforum, som lå på en egen adresse fristilt fra SR2. Selv om undergrunnsforumet hadde en egen adresse, var det myntet på kunder og selgere på SR2.

Jeg opprettet to profiler med falsk identitet begge steder for å få tilgang til alt innholdet (se pkt. 7.1 «Falsk identitet»). Fra de to første lenkene lærte jeg hvordan handelen på det mørke nettet foregikk. Funnene viste at kryptomarkedet og undergrunnsforumet oppfylte forskjellige formål:

1) Kryptomarkeder

- Er salgskanal for narkotika og en rekke andre ulovlige varer og tjenester. Tusenvis av narkotikalangere og kunder er registrert på hvert kryptomarked.
- Sidene er et utstillingsvindu hvor kunder ser seg ut varer, og selgere
- En selgerkonto koster opp mot 3500 NOK. I tillegg krever kryptomarkedene en prosentavgift av hvert salg som gjøres. Kundekonto er gratis
- Narkotika betales i Bitcoin, en nær anonym, digital valuta
- Pengetransaksjoner og hvitvasking skjer ved utnyttelse av avanserte, tekniske funksjoner som er bygget inn i kryptomarkedene
- Selgere og kjøpere kan kommunisere med et kryptert meldingssystem

Jeg fant mest informasjon på undergrunnsforumene, men på kryptomarkedene lå det to svært viktige element: Narkotikanettverkenes profiler, hvor de presenterte dopet sitt med tekst og bilder og omdømmesystemet (se pkt. 5.1.3). I tillegg sa langerne gjerne noe om sine karrierer og erfaring. Det ble delt enkelte opplysninger som viste meg veien videre til andre funn (se pkt. 5.1.4 om krypteringsnøkkelsøk).

2) Undergrunnsforum

- Er knyttet til et kryptomarked, men ligger fysisk adskilt på egen URL
- Fungerer som et anonymt torg hvor titusenvis av brukere diskuterer aktuelle tema og utveksler erfaringer om bruk av krypteringsverktøy, innkjøp og betaling med Bitcoin, postens rutiner i ulike land, dosering, virkning og pris på narkotika
- Sikkerhetsmanualer og tips deles systematisk med andre brukere etter beste praksis-metoden
- Vestlig ruspolitikk angripes heftig og ofte. Journalister er uglesett

Undergrunnsforumene var diskusjongrupper for brukerne av kryptomarkedene. Her var det mye å hente for en person som var helt ny i denne skjulte verdenen. Jeg brukte tid på å lese meg opp, samle skjermbilder og analysere innholdet på undergrunnsforumene. Informasjonen som lå her var helt uvurderlig for å forstå kulturen, metodene, internjustisen og sjargongen som rådet i miljøet.

I begynnelsen av september tok jeg i bruk lenkeinnsamlingsmetoden på nytt da problemstillingen ble endret.

September:

A) Hva var målet?

- Finne lenker til norske langere og nettverk på kryptomarkedene
- Finne lenker til relevante norske diskusjoner i undergrunnsforumene

B) Hva ble funnet?

- Jeg fant kontoene til rundt ti norske narkotikanettverk og langere
- Jeg fant ut at en av nordmennene hadde satt opp sin egen side på det mørke nettet
- Jeg fant lenker til en norsk diskusjontråd som var lest 15 000 ganger i 2014
- Jeg fant en hemmelig diskusjonsgruppe som eksisterte uavhengig av kryptomarked og undergrunnsforumene

C) Forholdet til andre metoder

- Jeg jobbet med å samle informasjon basert på lenkefarmingen både før og etter problemstillingen ble endret (se pkt. 3.5). Lenker som jeg opplevde som relevante tok jeg skjermbilde av. Alt videre arbeidet, bygde på lenkene jeg hadde funnet i denne fasen

Den systematiske lenkefarmingen ga meg mulighet til å sikre et bredt utvalg av opplysninger om det organiserte systemet som jeg begynte å se omrisset av. Et system hvor nordmenn gjorde store penger på dop – uten at de så ut til å ofre risikoen for politiets innblanding en tanke.

5.1.2 Metode 2: Informasjonsinnsamling og analyse

Selv om det var over 30 kryptomarkeder i virksomhet identifiserte jeg fem som størst og viktigst: EVOLUTION, AGORA, PANDORA, CLOUD-NINE OG SILK ROAD 2. Jeg gikk nøye gjennom alle sammen på jakt etter opplysninger.

Fra selgernes butikker kunne jeg se bilder, utvalg av narkotika, priser og tonen de brukte til å presentere seg mot kundene. Jeg fikk også tak i krypteringsnøklene, som ble brukt til kommunikasjon og identifisering.

Deretter saumfarte jeg undergrunnsforum og brukte søkeord som «Norge», «narkotika», «Norway», «shipping to Norway» for å finne diskusjoner med nordmenn. Herfra fikk jeg lastet ned en norsk diskusjonstråd som gikk over hele 2014. Diskusjonen var lest over 15 000 ganger.

Jeg skrev den ut i helhet, og den besto av rundt 90 sider med tre-fire innlegg på hver side. I tillegg fant jeg en rekke forskjellige sikkerhetsmanualer som «Narkotikahunder – hva de kan og ikke kan lukte» og «Hvordan pakke narkotika».

I midten av september satt jeg på hundrevis av skjermbilder som inneholdt informasjon som jeg ikke visste var viktig. Men det kunne helt klart vise seg å være det. Jeg innså at jeg var avhengig av å systematisere materialet før det ble for uoversiktlig til å bruke.

Jeg opprettet et skjermbildearkiv (1), og deretter bygde jeg et excel-register (2) av de viktigste opplysningene jeg satt på.

1) Skjermbildearkiv

Mappearkivet ble delt inn etter navn på kryptomarked og navn på norske aktører. Skjermbildene ble sortert etter relevans i mappen som passet. Volumet ble stort, veldig fort, men opplysningene som lå samlet i dette arkivet ble sentralt for sakene.

A) Hva var målet?

- Se om det gikk an å få ut informasjon om kryptomarkedenes ulike funksjoner
- Finne opplysninger om norske nettverk og / eller enkeltpersoner
- Se priser og utvalg av stoffer tilgjengelig for nordmenn
- Lete etter mest mulig informasjon om de norske aktørene og deres modus
- Sortere alle innsamlede opplysninger
- Bygge en bank over opplysninger som jeg ikke umiddelbart kunne si at var sentrale

B) Hva ble funnet?

- Omdømmesystemet på kryptomarkedene: Jeg skjønte hvordan kundenes tilbakemeldinger til selgerne var fundamentet for narkotikatrafikken på kryptomarkedene. Analysen av omdømmesystemet ble (se pkt. 5.1.3) nøkkelen til å få dokumentert omfanget av de norske nettverkenes narkotikasalg
- Forretningsideen til de norske nettverkene: Narkosalg fra det mørke nettet utnyttet et hull i postvesenets system. Fordi det ikke var kontroll av innenlandsbrev i Norge kunne nettverkene sende narkotikaen til kundene i A-post med tilnærmet null risiko for å bli tatt. Siden de i tillegg var anonymisert av TOR, og brukte krypterte e-poster for å beskytte kommunikasjonen sin, fremsto aktiviteten som svært vanskelig å oppdage
- Nettverkenes modus: Brevene som ble sendt inneholdt narkotika som var vakuumpakket en til tre ganger, for å fjerne lukt. Det ble brukt forseglede mylar-poser for å unngå fukt. Både masker og hansker ble brukt i pakkingsprosessen, for ikke å etterlate DNA-spor. Alle adresser som sto på brevene ble skrevet ut på lapper slik at ikke håndskrift skulle kunne avsløre nettverkene
- Kunder ble coachet i hvordan de skulle nekte befatning med brevene, dersom de ble kalt inn til politiavhør. Det skulle føre til mer krevende arbeid for politiet, og tvinge frem henleggelse

C) Forholdet til andre metoder

- Arkivet ble brukt til å analysere omdømmesystemet (pkt. 5.1.3), til å hente ut krypteringsnøkler, til å finne opplysninger for gjennomgang på sosiale medier (se pkt. 5.2) og til å sjekke andre detaljer helt frem til publisering

Forretningsideen forsto jeg umiddelbart, men det tok lengre tid før jeg skjønte hvor viktig omdømmesystemet var. Da det gikk opp for meg, var det enkelt å gå tilbake til arkivet og hente ut informasjonen jeg hadde samlet om omdømmesystemet.

Det skjedde for øvrig flere ganger at jeg gikk tilbake til arkivet for å sjekke opplysninger. Systematiseringen av opplysninger ga meg oversikt over kryptomarkedene, de viktigste funksjonene, men også forskjellen mellom dem og noen unike detaljer:

PANDORA satset tungt på kundeservice, og ga publikummet hjelp på tysk, fransk og engelsk, AGORA hadde ekstrem sikkerhet, mens EVOLUTION ga kundene mulighet til å holde igjen selgernes penger til varene var mottatt.

Jeg fikk flere ganger bevis på hvor viktig det var å ha kontroll på dokumentasjonen mens jeg arbeidet med sakene. Det kunne det skje ting som påvirket tilgangen min på informasjon. Plutselig ble et kryptomarked utilgjengelig i lengre perioder, og samtidig opplevde jeg at en narkolanger jeg undersøkte forsvant fra det mørke nettet sammen med sporene han hadde lagt ut.

2) Excel-register

Opplysninger i arkivet som jeg oppfattet som sentrale ble matet inn i Excel. Jeg ville at registeret skulle fungere som et støttedokument, slik at jeg hele tiden hadde oversikt over hvor opplysningene mine stammet fra.

A) Hva var målet?

- Lage en profil over norske nettverk og norske aktører
- Profilen skulle samle de mest konkrete opplysningene om salg, e-poster, krypteringsnøkler, utvalg dop, tidligere dekknavn, hvilke kryptomarkeder nettverket var tilstede på og lenker til kontoene

B) Hva ble funnet?

- Antall narkotikasalg totalt (5500) og individuelt for hvert nettverk / langer
- Jeg så hvor de ulike aktørene var aktive, hvilke stoffer de solgte og prisene
- Krypteringsnøklene til nordmennene
- Hvor lenge noen av aktørene hadde vært i virksomhet på det mørke nettet
- Bilder av vareutvalget som nettverkene selv publiserte
- Priser på dopet

C) Forholdet til andre metoder

- Registeret ble opprettet parallelt med skjermbildearkivet. Researchen har blitt brukt som referanse i forbindelse med utskriving, til å kontakte nettverk og kilder (se pkt. 5.4) og for å kartlegge personer via sosiale medier (pkt. 5.2)

Å opprette arkivet og Excel-registeret var en tidkrevende drittjobb som bremset fremgangen min. Jeg satt i dagevis og grupperte informasjonen. Jobben sparte meg imidlertid for masse arbeid senere i prosjektet. Informasjonen som lå i lenkene og skjermbildene var viktig for å forstå systemene som var i sving.

Excel-registeret ga i tillegg oversikt over hvilke opplysninger og detaljer jeg satt på om de norske nettverkene og narkotikalangerne. De viktigste opplysningene ble presentert i en omfattende, interaktiv grafikk som var et av element i dokumentaren:

http://spesial.adressa.no/darkweb/DarkGrafikk.html

5.1.3 Metode 5: Analyse av omdømmesystemet

Da jeg begynte å arbeide med omdømmesystemet på kryptomarkedene hadde informasjonsinnsamlingsfasen (se pkt. 5.1.2) gitt svar på flere spørsmål fra problemstillingen til prosjektet, og jeg visste at det eksisterte norske nettverk og langere på det mørke nettet. De viktigste spørsmålene var ubesvart:

Hvor utbredt var dette egentlig? Dreide det seg om noen få teknisk avanserte personer som solgte mindre mengder narkotika til hverandre? Eller kunne det være noe større?

Analysen av omdømmesystemet skulle svare på det, og gi en av de mest oppsiktsvekkende avsløringene i sakene, at nordmenn har stått for over 5500 narkosalg på ett år, uten at kriminaliteten har blitt oppdaget.

A) Hva var målet?

- Forstå hvordan omdømmesystemet fungerte
- Se om omdømmesystemet kunne brukes til å måle omfanget av narkotikasalget på det mørke nettet
- Se om omdømmesystemet kunne si noe om hvor store de ulike norske aktørene var
- Se om omdømmesystemet kunne si noe om de norske aktørenes modus og anseelse i markedet

B) Hva ble funnet

- Omdømmesystemet var kryptomarkedenes måte å skape tillit i et økonomisk marked hvor anonymitet rådet. De fleste som vil kjøpe noe, uansett bransje, ønsker at selgeren vet hva han / hun driver med. Det var dette omdømmesystemet fortalte kundene.
- Norske aktører hadde stått for 5500 narkotikasalg på ett år, uten at kriminaliteten hadde blitt oppdaget av norske myndigheter
- De mest aktive nordmennene hadde over 1000 salg hver
- De mest aktive nordmennene scoret himmelhøyt på kundetilfredshet

C) Forholdet til andre metoder

- Analysen av omdømmesystemet foregikk parallelt med at jeg jobbet med analyse av OPERASJON LARVEN (se pkt. 5.5.1), innhenting av politirapporter (pkt. 5.5.5) og internasjonal forskning. Summen av opplysningene jeg fant her, bidro til at jeg forsto viktigheten av funnene fra analysen av omdømmesystemet. Resultatene ble i tillegg holdt opp mot søk i krypteringsnøkkeldatabaser (pkt. 5.1.4)

Dokumentasjonen bak tallene bygger på tredelt tilnærming: Analysen av omdømmesystemet, søk i krypteringsnøkkeldatabaser og nettverkenes egne opplysninger. De to siste bidro til å gi et bredere grunnlag, men analysen av omdømmesystemet var helt klart viktigst.

Hvordan kan mennesker stole på hverandre og gjøre forretninger med store beløp når alt de har å forholde seg til er et dekknavn, en Bitcoin-konto og en kryptert e-postadresse?

Svaret på spørsmålet skulle vise seg å være omdømmesystemet:

Omdømmesystemet er sider hvor kundenes tilbakemeldinger til en narkolanger blir publisert slik at enhver som er innom selgerens konto kan se dem. Selv om kryptomarkedene har forskjellige funksjoner og tjenester, har alle en variant av omdømmesystemet.

rating	feedback	item	freshness
★★★★★	great smoke! fast shipping and a good price! my new favorite vendor!	item	157 days
★★★★★	i love it! finally a domestic vendor that got my poison! clean and dry to a deasent price.		157 days
★★★★★	sterk som faen, rask levering og god kontakt	item	160 days
★★★★★	Really good stealth :) Jeg anbefaler!!!	item	161 days
★★★★★	speed S-class :D will be back soon	item	161 days
★★★★★	Levering neste dag! Amazing! Min favoritt leverandører nå!	item	161 days
★★★★★	Great Product, Great Shipping, Great Communication, my primary vendor now.	item	162 days
★★★★★	Quality all the way, order to delivery to product - incredible!	item	162 days
★★★★★	Super dense, frosty, and strong as fuck :D	item	162 days

Figur 1 Utdrag fra omdømmesystemet hos det norske nettverket Norwegian. Skjermbilde tatt i oktober 2014 på Silk Road 2.

Kunden bruker omdømmesystemet til å gi en karakter til selgeren. Karakteren er gjerne et tall mellom 1 og 5. Den baseres på service, pris og kvaliteten på stoffet som kjøpes. Kundene kan se tilbakemeldingene, og hvor lenge det er siden de ble publisert

Jeg skjønte ikke umiddelbart hvor viktig systemet var, fordi jeg var farget av egne er faringer fra tidligere saker med digitale markedsplasser på det åpne nettet.

I forbindelse med oppfølging av Dagens Næringslivs avsløringer av et dopingnettverk i Trondheim var jeg flere ganger innom de åpne nettsidene som nettverket brukte. Der kunne hvem som helst skrive tilbakemeldinger til selgerne, noe som førte til at selgerne selv opprettet flere falske profiler for å gi seg selv rosende omtale. De ekte kundene kunne ikke vite det, men dopingselgerne bygde opp et falskt bilde av kvaliteten på sin egen virksomhet.

På det mørke nettet er omdømmesystemet er en låst del av selgerens profil slik at narkotikalangere ikke selv kan redigere, manipulere eller forfalske tilbakemeldingene som publiseres. Omdømmesystemet skal motvirke svindel.

Tilbakemeldingene legges inn av kundene, og forutsetningen for å få adgang til å skrive tilbakemelding er at man har bestilt og betalt narkotika gjennom kryptomarkedets infrastruktur. Slik representerer en tilbakemelding ett kjøp.

Tidlig i arbeidet hadde jeg gjort en grovtelling av tilbakemeldingene til de norske nettverkene. Hvert nettverk hadde alt fra 1 til 30 sider med 30 tilbakemeldinger på hver side. Jeg hadde tenkt å bruke opptellingen som et anslag på det norske omfanget fordi jeg var bekymret for at tallet ikke var troverdig (basert på de tidligere erfaringene jeg hadde gjort meg).

I slutten av september skjønte jeg hvordan omdømmesystemet fungerte, og hvor sentralt det var. Samtidig jobbet jeg parallelt med andre, mer tradisjonelle metoder. Etter å ha sett at omdømmesystemet ble lagt til grunn som bevis i to svenske rettsinstanser (se pkt. 5.5.2) og gått gjennom forskning på kryptomarkedene (se pkt 5.5.6) så følte jeg meg overbevist om at metodikken min holdt vann:

Tallene omdømmesystemet ga meg, var et faktagrunnlag og ikke bare et anslag. De fortalte meg hvor store de norske narkonettverkene var, og ved å legge sammen alles tall kunne jeg si noe om hvor stort dette usynlige dopmarkedet var.

Siden jeg satt på skjermbilder fra hver enkelt side med tilbakemeldinger til alle de norske aktørene kunne jeg gå inn i arkivet jeg hadde etablert (pkt. 5.1.2).

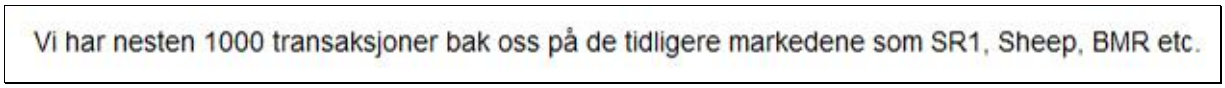
Det var en grei operasjon å telle over slik at jeg kunne svare på problemstillingen om et norsk omfang, og slå fast at det var begått mer enn 5500 salg av narkotika fra nordmenn til nordmenn i løpet av det siste året.

At alt dette hadde fått foregå ved hjelp av Posten, uten innblanding fra politiet, synes jeg var oppsiktsvekkende. Det synes også politiet (se pkt. 8).

Tallene fra analysen av omdømmesystemet ble i tillegg holdt opp mot tall jeg fikk hentet etter å ha søkt i databaser over krypteringsnøkler. I enkelte tilfeller la jeg tall som nettverkene selv oppga til kundene til grunn.

Jeg så at nettverkene hadde det med å publisere antall salg som en del av markedsføringen mot nye kunder. Tallene fant jeg i data lagret i skjermbildearkivet mitt. Her er to eksempler:

1)



Figur 2 Det norske nettverket «Alfa&Omega» oppgir salgstall fra nå nedlagte kryptomarkeder. Skjermbilde hentet fra kryptomarkedet Evolution i slutten av august 2014.

2)

Figur 3 Det norske nettverket «Foxhound Norway» oppga salgstall på et undergrunnsforum sommeren 2014. Skjermbilde tatt i slutten av august.

Det virket usannsynlig at noen skulle oppgi et høyere salgstall enn de hadde faktisk stått for, og dermed seg selv for en langt strengere straffereaksjon enn det var grunnlag for. Likevel kunne jeg ikke utelukke det, og derfor rangerte jeg denne metoden som den minst viktige av de tre jeg brukte for å komme frem til totalantallet 5500.

5.1.4 Metode 6: Søk, krypteringsnøkkeldatabaser

Selv om jeg nå kunne telle opp antall narkotikasalg nordmennene hadde gjennomførte på de fem kryptomarkedene som jeg hadde identifiserte som størst og viktigst i 2014 (se pkt. 5.1.1), så var det tydelig at flere av aktørene hadde vært i sving på det mørke nettet en god stund. De hadde etablert rutiner for sikkerhet og kundebehandling, og utviklet modus for salg, pakking og sending av narkotika. Slikt tar tid.

A) Hva var målet?

- Var det mulig å se hvor lenge nettverkene hadde vært aktive?
- Kunne jeg finne opplysninger om hvor høye salgstall de hadde hatt tidligere?

B) Hva ble funnet?

- Måned og år for når nordmennene registrerte seg på de største kryptomarkedene. En av de mest aktive hadde holdt på siden 2012
- Salgstall til norske selgere og nettverk på kryptomarkeder som hadde blitt beslaglagt, nedlagt eller hacket i tiden før jeg begynte på mitt prosjekt

C) Forholdet til andre metoder

- Søkene foregikk parallelt med analysen av omdømmesystemet

Under informasjonsinnsamlingsfasen (beskrevet i pkt. 5.1.2) gikk jeg gjennom mange diskusjonstråder på flere undergrunnsforum. Jeg nærmet meg det mørke nettet som et

fenomen, og ville danne meg et inntrykk av menneskene, kulturen og historien til det internasjonale miljøet som opererte her.

Jeg kom stadig vekk over diskusjonstråder som handlet om det opprinnelige kryptomarkedet SILK ROAD 1 (SR1), som ble bredt omtalt i internasjonale medier da det ble beslaglagt av FBI i oktober 2013. SR1 hadde spilt en viktig rolle for fremveksten av miljø og utviklingen av systemer på det mørke nettet. I etterkant av FBI-aksjonen etablerte BLACK MARKET RELOADED og SHEEP MARKETPLACE seg som de største kryptomarkedene.

Begge ble lagt ned i løpet av det neste halve året, men det måtte jo ha vært norsk aktivitet her og?

Tidlig i arbeidet kom jeg over en database på det mørke nettet som samlet de offentlig tilgjengelige krypteringsnøklene til store narkotikalangere. Jeg fant lenken til databasen på et av undergrunnsforumene. Databasen hadde knyttet 4500 offentlige krypteringsnøkler til selgerprofiler på kryptomarkedene, og gjort nøklene søkbare.

Databasen tjente samme hensikt som omdømmesystemet: Den skulle bygge tillit i et helanonymt miljø.

Jeg så at mange av nettverkene hadde utviklet et eget varemerke og bygd sin kundegruppe over lang tid på samme måte som i vanlig forretningsdrift. Databasen var et verktøy som publikum kunne bruke til å sjekke identiteten til en narkotikaselger ved hjelp av den offentlig tilgjengelige krypteringsnøkkelen som langeren brukte til å identifisere seg med overfor kundene.

Kryptomarkedene på det mørke nettet var utsatt for «force majeure», noe FBI-aksjonen i oktober 2013 var eksempel på. Andre ganger kunne et kryptomarked bli hacket, eller rett og slett forsvinne.

Selv om kundene beveget seg videre til nye kryptomarkeder etter hver hendelse, var det vanskelig for dem å vite at personene bak dekknavnet FOXHOUND NORWAY på kryptomarkedet EVOLUTION, var de samme personene som hadde stått bak dekknavnet på SHEEP MARKETPLACE noen måneder tidligere.

Hver selger publiserte sin offentlige krypteringsnøkkel på profilen sin på kryptomarkedene. Kundene brukte nøkkelen til å sende krypterte beskjeder til selgeren, og de krypterte beskjedene kunne bare dekrypteres ved hjelp av en hemmelig nøkkel selgeren selv satt på.

En offentlig krypteringsnøkkel så slik ut:

Figur 4 Dette er den offentlige krypteringsnøkkelen til det norske nettverket Foxhound Norway. Skjermbilde tatt i september 2014 på Silk Road 2.

Beskjeder kryptert med den offentlige krypteringsnøkkelen til det norske nettverket FOXHOUND NORWAY kunne bare dekrypteres med nettverkets egne, hemmelige nøkkel. Hvis dekknavnet var stjålet, og noen utga seg for å være FOXHOUND NORWAY (for å dra nytte av det etablerte varemerket til nettverket) så var det en smal sak å sende en kryptert beskjed ved hjelp av den offentlige krypteringsnøkkelen. Hvis det ikke kom et svar, så var det et bevis på at personene som nå opererte som FOXHOUND NORWAY, ikke var personene som de utga seg for å være. Og det betød at det var fare for å bli svindlet.

Nøkkeldatabasen var et slags identifikasjonssystem som kunne følge personer og nettverk over tid gjennom virksomhet på flere kryptomarkeder. Da jeg forsto det, skjønte jeg at jeg satt på tilgang til en tidsmaskin.

Jeg hadde tidligere samlet inn alle mulige opplysninger om de norske aktørene. I arkivet mitt lå også de offentlige krypteringsnøklene som jeg kunne søk med i systemet. Databasen svarte med å gi viktige opplysninger som i utgangspunktet ikke var tilgjengelig for meg under informasjonsinnsamlingsfasen.

Krypteringsnøkkeldatabasen utvidet altså tidshorisonten for undersøkelsene mine av den kriminelle aktiviteten på det mørke nettet. Samtidig fikk jeg datoer for når de enkelte nettverkene og selgerne begynte virksomheten sin.

Virksomheten på det mørke nettet var ikke så ny. Nordmennene var i gang med å selge narkotika allerede i 2012. Dette var over ett år tidligere enn jeg trodde.

5.1.6 Metode 7: Søk i html-arkiv

Etter å ha søkt i krypteringsnøkkeldatabasen visste jeg at flere av de norske nettverkene og selgerne hadde vært aktive SILK ROAD 1 (som ble beslaglagt av FBI i oktober 2013). Jeg ville finne ut mest mulig om aktiviteten deres her, men kildematerialet lå nedlåst hos FBI.

Fra undersøkelser av undergrunnsforum fikk jeg tilgang til et arkiv over alle selger-kontoene fra SILK ROAD 1.

A) Hva var målet?

- Lete etter opplysninger om norske selgere på SILK ROAD 1

B) Hva ble funnet?

- Det var minst 6 aktive nettverk og enkeltselgere på SR1
- Flere av dagens nettverk og langere var aktive på SR 1
- Flere av dagens nettverk og langere sto for hundrevis av salg på SILK ROAD 1
- Enkelte av dem opererte under andre navn

C) Forholdet til andre metoder

- Tilgangen på opplysningene fikk jeg fra innsamlingsfasen (se pkt. 5.1.2)

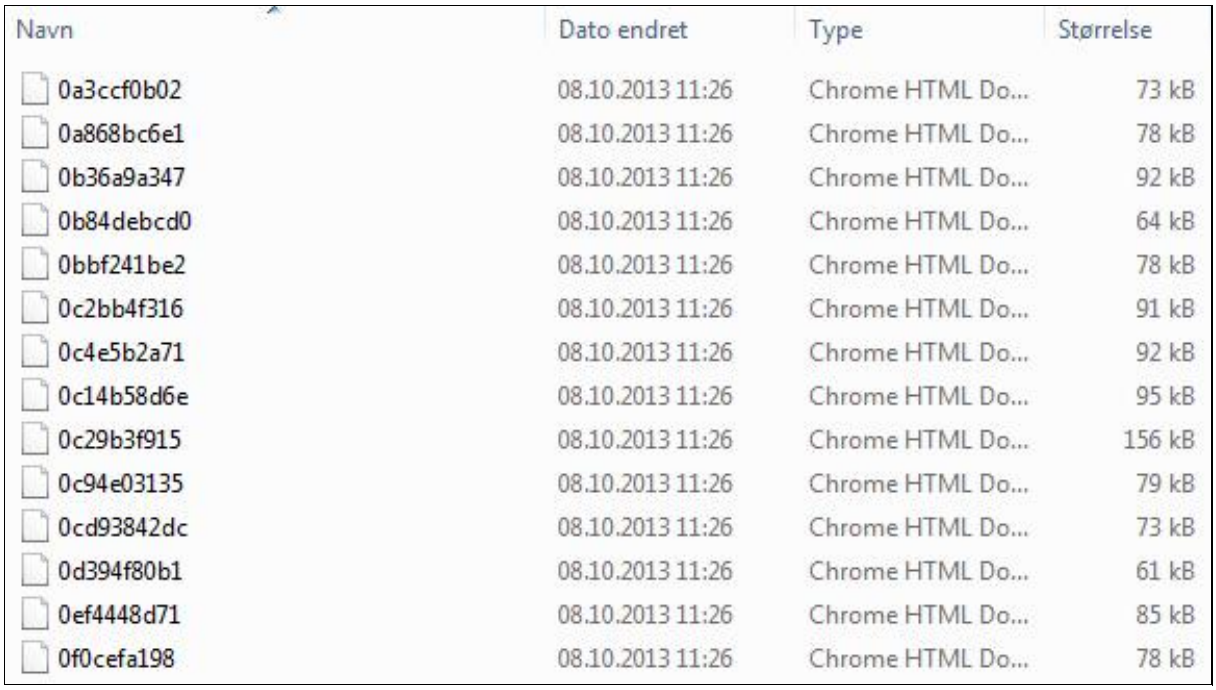
Backupen av filene var tatt av en i den innerste kretsen av administratorer på SR1. I materialet lå det lagret informasjon om over 1200 narkotikanettverk og langere fra hele verden. De norske måtte også finnes her, tenkte jeg.

Utfordringen besto i at arkivet hadde lagrede nettsider i html-format. Filene hadde ikke navn etter selgerkontoer, men besto av tilfeldige bokstaver. Jeg måtte åpne en og en fil for å lese innholdet. Dette var svært upraktisk. Jeg var kun interessert i nordmenn, og på jakt etter kanskje ti av 1200 oppføringer i arkivet.

Løsningen på problemet fikk jeg fra Jonas Nilsson ved Adresseavisens utviklingsdesk. Nilsson er designer og programmerer og hadde ansvaret for den digitale utformingen av dokumentaren vår. Han foreslo å kjøre filarkivet inn i programmet Sublime Text.

Sublime Text er et tekstredigeringsprogram som ofte brukes av programmerere til å skrive kode. En av programmets mange nyttige funksjoner er muligheten til å kjøre fritektssøk på hele mapper med dokumenter.

Programmet viste all koden som lå i de 1200 lagrede nettsidene, og det var svært uoversiktlig, men heldigvis kunne jeg bruke søkefunksjonen. Det gjorde at jeg med letthet kunne lete meg frem i kode og tekst ved å søke på "Norge" eller dekknavnene jeg kjente til fra før. Det lot meg følge de norske aktørene enda lengre bakover i tid.



Navn	Dato endret	Type	Størrelse
0a3ccf0b02	08.10.2013 11:26	Chrome HTML Do...	73 kB
0a868bc6e1	08.10.2013 11:26	Chrome HTML Do...	78 kB
0b36a9a347	08.10.2013 11:26	Chrome HTML Do...	92 kB
0b84debcd0	08.10.2013 11:26	Chrome HTML Do...	64 kB
0bbf241be2	08.10.2013 11:26	Chrome HTML Do...	78 kB
0c2bb4f316	08.10.2013 11:26	Chrome HTML Do...	91 kB
0c4e5b2a71	08.10.2013 11:26	Chrome HTML Do...	92 kB
0c14b58d6e	08.10.2013 11:26	Chrome HTML Do...	95 kB
0c29b3f915	08.10.2013 11:26	Chrome HTML Do...	156 kB
0c94e03135	08.10.2013 11:26	Chrome HTML Do...	79 kB
0cd93842dc	08.10.2013 11:26	Chrome HTML Do...	73 kB
0d394f80b1	08.10.2013 11:26	Chrome HTML Do...	61 kB
0ef4448d71	08.10.2013 11:26	Chrome HTML Do...	85 kB
0f0cefa198	08.10.2013 11:26	Chrome HTML Do...	78 kB

Figur 5 Slik så filarkivet fra Silk Road 1 ut. Skjermbilde tatt i januar 2015.

Opplysningene jeg fant her ble en del av oppfølgingssakene. Jeg fant ut at enkelte av nettverkene hadde byttet dekknavn etter SR1 ble beslaglagt, men ved å sammenholde opplysninger om e-postadresser og krypteringsnøkler (pkt. 5.14) klarte jeg å identifisere dem igjen. Takket være arkivet var det mulig å se at et av de mest aktive nettverkene i 2015, FOXHOUND NORWAY, opererte under LOYAL SUCCESS sommeren 2013.

5.2 Kartlegging sosiale medier

Alle som handler narkotika på det mørke nettet tror de er hundre prosent anonyme. Men anonymiteten fungerer kun dersom man bruker teknologien og de ulike verktøyene riktig. I tillegg må man være forsiktig slik at man ikke røper identifiserende opplysninger.

I løpet av arbeidet med saken brukte jeg sosiale medier på det åpne nettet til å søke etter personer jeg fant spor etter på det mørke nettet. Det lykkes noen ganger. Samtidig var det ikke gull alt som glimret.

I jakten etter kunder og selgere har jeg gått gjennom rundt tjue profiler på disse sosiale mediene: Facebook, Google+, Twitter, Youtube og Steam.

5.2.1 Deanonymisering: BRUKER123 til ØYSTEIN

I rettsdokumenter fra Sverige (se pkt. 5.5.2) går det frem at en narkolanger sto for 1880 salg på det mørke nettet. Kundene var i alderen fra 18 til 50 år. Etterforskerne fortalte meg imidlertid at de var overbeviste om at systemene på det mørke nettet også ble brukt til å pushe narkotika på barn.

Selv om etterforskerne hadde rullet opp tre saker fra det mørke nettet i løpet av et par år, så hadde de ikke klart å avsløre salg til barn under 18 år. Hvis det var så enkelt å bruke det mørke nettet at barn kan sitte hjemme og ha tilgang til alle mulige typer narkotika, så ville det være svært bekymringsfullt.

A) Hva var målet?

- Kunne jeg finne spor etter barn som handlet narko på det mørke nettet?
- Var det mulig å få noen til å stille opp og fortelle om det?
- Var det mørke nettet kjent blant russøkende ungdom?

B) Hva fant jeg?

- 16 år gamle BRUKER123 / ØYSTEIN var 15 da han hørte om narkokjøp på det mørke nettet fra en kompis (14)
- ØYSTEIN skaffet seg digitale penger, Bitcoin, ved hjelp av kontantkort kjøpt i kiosker
- Deretter kom han inn på et undergrunnsforum hvor han fikk opplæring i kryptering, og andre verktøy
- Han kjøpte narko flere ganger, og klarte å få saken henlagt, også etter opplæring fra andre, erfarne brukere
- Ifølge ØYSTEIN var det flere i kretsen hans i ungdomsmiljøet i Midt-Norge som kjente, og brukte det mørke nettet til å kjøpe flere typer narkotika

BRUKER123 og ØYSTEIN er samme person, men det er ikke det ekte dekknavnet eller det virkelige navnet til personen bak. Jeg har valgt å anonymisere både dekknavnet og personens virkelige identitet siden denne rapporten skal publiseres. Dette er gjort av hensyn til kildevernet.

Historien om BRUKER123 / ØYSTEIN ble publisert i Adresseavisen torsdag 6. november, som del av papirutgaven av dokumentaren «silkeveiene». Jeg måtte bruke flere metoder for å fjerne lagene med sikkerhet som han hadde omgitt seg med på det mørke nettet. Metodene ble brukt kronologisk, slik de er forklart under. Se også metodekart i vedleggene til rapporten (pkt. 10.3).

5.2.2 Metode 8: Analyse, undergrunnsforum

I forbindelse med informasjonsinnsamlingsfasen (se pkt. 5.1.2) lastet jeg ned, og skrev ut en diskusjon mellom norske brukere på et av undergrunnsforumene, som er knyttet til kryptomarkedene.

Diskusjonstråden, som var lest over 15 000 ganger av nordmenn, gikk gjennom hele 2014 og besto av rundt nitti sider med tre-fire innlegg på hver side. Informasjonen som brukerne delte her, hjalp arbeidet mitt på flere områder. Teksten, innlegg og de ulike brukerne ble analysert flere ganger.

I et av innleggene dukket det opp en person som jeg i denne rapporten kaller BRUKER123.

A) Hva var målet?

- La BRUKER123 igjen spor om hvem han var?
- Var det mulig å se hvor BRUKER123 befant seg i landet?
- Var det mulig å beskrive hans bruk av det mørke nettet dersom jeg ikke fikk tak i ham?

B) Hva ble funnet?

- BRUKER123 var 16 år og bodde et sted i Midt-Norge
- BRUKER123 het ØYSTEIN
- BRUKER123 beskrev hvordan han hadde kjøpt narkotika, blitt oppdaget av politiet før han senere klarte å få saken sin henlagt
- Erfarne brukere av det mørke nettet drev med opplæring av yngre og uerfarne

Jeg hadde fortsatt bare tilgang til BRUKER123s anonyme profil på undergrunnsforumet på det mørke nettet. Jeg vurderte om jeg skulle kontakte ham på forumet, men landet på at det var uaktuelt. Jeg visste for lite, og hadde ikke kontroll over omstendighetene:

Det er lett og ikke svare på meldinger. Det er enda enklere å slette brukeren for å komme tilbake med et nytt dekknavn, som da ville være ukjent for meg. Dette ville føre til at jeg mistet de få sporene jeg hadde etter ham før jeg hadde noe håndfast som jeg kunne følge ut i den virkelige verden.

5.2.3 Metode 9: Profilanalyse, det mørke nettet

Det neste jeg gjorde var å analysere profilen til BRUKER123 på undergrunnsforumet.

A) Hva var målet?

- Finne identifiserende opplysninger
- Se spor som jeg kunne følge ut av det mørke nettet

B) Hva ble funnet?

- BRUKER123 var forsiktig. Han publiserte ingen opplysninger på profilen
- Jeg fant den offentlige krypteringsnøkkelen hans som viste meg e-postadressen til BRUKER123

På dette tidspunktet i prosjektet hadde jeg lærte en del om krypteringsnøkler.

Den offentlige krypteringsnøkkelen ble brukt av andre personer til å kryptere e-poster og meldinger til BRUKER123. Jeg visste at jeg kunne bruke den offentlige krypteringsnøkkelen til BRUKER123 til å vise meg hvilken e-postadresse den var knyttet opp mot. Da fikk jeg ut et spor jeg kunne jobbe videre med.

Jeg sjekket krypteringsnøkkelen hans mot databasen hos e-postleverandøren Countermail, som er markedsledende på krypterte e-posttjenester. Analysen viste at BRUKER123s krypteringsnøkkel var knyttet til BRUKER123@hotmail.com.

5.2.4 Metode 10: Åpne søk

Håpet mitt var at BRUKER123 hadde slurvet med sikkerheten og brukt den samme e-postadressen også på det åpne nettet. Jeg hadde flaks, BRUKER123 hadde ikke vært nøye nok:

BRUKER123 hadde samme dekknavn på undergrunnsforumet og i e-postadressen sin. Det kunne bety at han ikke hadde rukket å bli like proff på sikkerhet, slik mange på kryptomarkedene var.

Jeg googlet både dekknavnet og e-postadressen.

A) Hva var målet?

- Hadde «BRUKER123» brukt dekknavnet eller e-postadressen sin på det åpne nettet?
- Var det mulig å følge sporene videre til mer identifiserende opplysninger?

B) Hva ble funnet?

- BRUKER123 brukte både e-posten og dekknavnet i flere forskjellige sosiale medier
- Jeg fant spor etter BRUKER123 på Youtube, Steam, Google+, Instagram og Facebook

Dekknavnet i seg selv ga meg ingen fornuftige treff, men e-postadressen ledet til de ulike kontoene i sosiale medier.

5.2.5 Metode 11: Profilanalyse, det åpne nettet

Funnene kom etter å ha fulgt brødsmuler mellom forskjellige sosiale medier. Jeg måtte bruke informasjon på kontoene til å komme videre.

BRUKER123 la tilsynelatende litt tilfeldige opplysninger ut på hver konto, basert på hvilket sosiale medium han brukte. På Youtube var han for eksempel mest opptatt av hvilke dataspill han spilte, og hvilke nicknames han hadde i forskjellige spill.

A) Hva var målet?

- Samle flest opplysninger om hvem BRUKER123 egentlig var
- Finne ut hvor han bodde, og hvordan jeg kunne kontakte ham

B) Hva ble funnet?

- At BRUKER123 faktisk var 16 år, og bodde i Midt-Norge
- Flere bilder av BRUKER123
- BRUKER123s ekte navn (her kalt ØYSTEIN)

E-postadressen BRUKER123@hotmail.com ledet meg først til Google +-kontoen. Det var ikke et ekte navn på profilen, men et bilde av en ung gutt, noe som støttet hypotesen om at BRUKER123 faktisk var 16 år.

E-postadressen ledet i tillegg til en Youtube-konto, også opprettet med et dekknavn. Under «info» hadde imidlertid personen bak kontoen oppgitt riktig alder (16 år) og i tillegg et fornavn. Det viktigste funnet var at Youtube-kontoen var koblet opp mot BRUKER123s kontoer i andre sosiale medier, Google +-kontoen og i tillegg: En konto på Facebook.

Facebook-kontoen viste samme fornavn, ØYSTEIN, som på Google + og som ble oppgitt på Youtube-kontoen. Det var også samme bilde som på Google + og et etternavn. Jeg følte meg nå sikker på at det var samme person bak kontoene.

Jeg hadde i tillegg tilgang til kontoen hans på Steam, som er en blanding av en online spillbutikk og et sosialt medium for ulike spill. Der var det også mulig å kontakte ham ved å ringe kontoen hans.

5.2.6 Metode 12: Facebookanalyse

E-postadressen, som var utgangspunktet for undersøkelsene mine, lå ikke på Facebooksiden til ØYSTEIN / BRUKER123:

Jeg ville ikke ha funnet 16-åringens fulle navn hvis jeg ikke gått nøye gjennom de andre profilene hans. Men jeg var egentlig ikke nærmere å kontakte ham enn tidligere og hadde fortsatt kun mulighet til å bruke nettet.

A) Hva var målet?

- Finne et telefonnummer til BRUKER123 / ØYSTEIN
- Finne adressen hans i den virkelige verden

B) Hva ble funnet?

- Morens Facebookprofil
- Morens adresse
- Tre telefonnummer registrert på moren

16-åringen oppga ikke e-post, telefonnummer eller adresse på Facebook. En gjennomgang av ØYSTEINs offentlige innlegg på Facebook førte til at jeg fant morens Facebook-profil.

Moren hadde et annet etternavn så det var først etter at jeg hadde sett gjennom en del bilder at det var mulig å stadfeste hennes identitet, og slektskapet. Moren hadde ikke tatt særlige hensyn til anonymitet: Hun hadde oppgitt 16-åringen som sin sønn (slik Facebook ber brukerne gjøre).

5.2.7 Metode 13: Søk «bak» Facebookprofil

Jeg hadde funnet 3 telefonnummer på moren. Jeg vurderte det som uaktuelt å ringe henne for å spørre etter sønnen. Da måtte jeg ha presentert meg, og sagt noe om hvorfor jeg skulle ha tak i ham. Jeg måtte løse problemet på en annen måte. Jeg tok i bruk et søkeverktøy jeg fikk tilgang til etter å ha deltatt på et av kursene på SKUPs graveskole i 2012.

A) Hva var målet?

- Finne riktig telefonnummer til ØYSTEIN
- Oppnå kontakt med ham

B) Hva ble funnet?

- Opplysningene BRUKER123 kom med om alder og hjemsted stemte
- ØYSTEIN hadde kjøpt narko flere ganger, og fått saken henlagt
- Flere i ungdomsmiljøet rundt ØYSTEIN hadde kjennskap til det mørke nettet og til avanserte teknologiske konsepter som PGP-kryptering og TOR
- Barn helt ned i 14 års alder var aktive på kryptomarkedene

Open-Source Intelligence (OSINT) er etterretningssjargong for søk gjort i offentlig tilgjengelige kilder. Ved å utnytte et OSINT-søk utviklet av den tidligere FBI-agenten Michael Bazzell kunne jeg sjekke morens tre telefonnummer opp mot «baksiden» av kontoer på Facebook.

OSINT-søket bruker Facebooks egen graph-search til å gå gjennom, eller sjekke opplysninger som navn, telefonnummer og e-postadresser. Verktøyet muliggjør søk etter informasjon som ikke er direkte delt på Facebook-kontoenes «about» eller «contact» sider. Mer om Michael Bazzell her.

Det er mulig å sperre denne typen søk, men da må brukerne ha endret personverninnstillingene sine i tiden etter at Facebook graph-search ble introdusert i Norge (2013).

Verken ØYSTEIN eller moren hadde endret disse innstillingene. Dermed brukte jeg OSINT-søket på de tre numrene jeg satt på.

Det første fikk opp profilen til moren. Det andre nummeret hørte til en jente som antakelig er søsteren til ØYSTEIN. Det tredje nummeret viste 16-åringens profil.

Endelig var jeg sikker på at jeg hadde direkte kontaktinformasjon. Jeg tok sjansen på at han ikke ville sjekke nummeret mitt og hvem jeg var, og brukte min egen telefon til å ringe ham. Før jeg tok kontakt med 16-åringen diskuterte jeg fremgangsmåte med redaksjonsledelsen. Se redegjørelse for problemstillingene under pressetiske vurderinger (se pkt. 6.1)

Da ØYSTEIN tok telefonen fryktet han først at jeg var politi. Da det gikk opp for ham at jeg var journalist, ble han satt ut.

- Hvordan fant du meg, spurte han da jeg sa jeg ønsket å møte ham for å høre hans historie.

Etter å ha avklart at han ville være anonym i saken og beskyttet av kildevern, gikk han med på å treffe meg og fotograf Ole Martin.

Noen timer senere fortalte han oss hvordan han hadde registrert seg og fått opplæring på undergrunnsforumet. Jeg kunne verifisere opplysningene, fordi jeg hadde analysert diskusjonstråden hvor han hadde vært aktiv.

16-åringen hadde hørt om kryptomarkedene, og det mørke nettet, fra en kamerat som var 14 år. Kameraten satt da allerede på «et lager av hasj og viagra» som han hadde kjøpt og fått i posten. Fra 16-åringens historie ble det tydelig at også barn var aktive på kryptomarkedene, og at de brukte det mørke nettet til å kjøpe stoff fra norske narkotikanettverk.

Å høre ham fremstille det som relativt normalt, var rystende.

5.2.8 Deanonymisering: SELGER123

Jeg oppdaget under informasjonsinnsamlingsfasen (pkt. 5.1.2) at et norsk/svensk nettverk av hasjselgere skjuler seg bak dekknavnet SELGER123. Opplysningene er en del av pågående arbeid, og personen er ikke pågrepet av politiet, derfor er dekknavnet byttet ut med SELGER123.

Nettverket har gjennomført hundrevis av transaksjoner, og har vært i virksomhet i flere år.

Utgangspunktet mitt var e-postadressen nettverket brukte til kundepleie.

A) Hva var målet?

- Bruke e-postadressen til å komme nærmere SELGER123
- Deanonymisere personen, eller personene bak SELGER123

B) Hva ble funnet?

- E-posten var brukt til å opprette en Facebookside til SELGER123
- SELGER123 publiserte adressene til butikken sin på det mørke nettet på Facebook-kontoen

Jeg brukte e-posten til diverse søk på samme måte som jeg gjorde da jeg fant BRUKER123 (se pkt. 5.2.1-5.2.7).

Kartleggingen jeg hadde gjort av nordmennene viste at ingen av narkotikanettverkene eller de enkelte langerne brukte e-postadressen de oppga på det mørke nettet ute på det åpne nettet.

Unntaket til denne regelen var SELGER123. E-postadressen nettverket fortsatt opererer med, pekte til en Facebookside som hadde samme navn som nettverket. Det gjorde at jeg kunne gjøre undersøkelser av Facebooksiden i jakten på hvem som hadde opprettet den.

5.2.9 Metode 13: Søk «bak» Facebookprofil

Igjen tok jeg i bruk OSINT-verktøyet fra den tidligere FBI-agenten Michael Bazzel. Etter at jeg fant telefonnummeret til ØYSTEIN tenkte jeg at det måtte gå an å gjøre lignende undersøkelser av SELGER123s profil på Facebook. Metoden jeg brukte her har likhetstrekk med fremgangsmåten ved punkt 5.2.1, men bygger på andre opplysninger. Jeg måtte lære meg litt mer om hvordan Facebook, og Facebooks Graph Search fungerer. Sentrale begrep her er *screen name* og *user number*.

A) Hva var målet?

- Få informasjon fra «baksiden» av SELGER123s FB-konto
- Prøve å få deanonymisert en eller flere personer bak dekknavnet SELGER123

B) Hva ble funnet?

- Jeg fikk ut et navn på en person som skal ha opprettet kontoen SELGER123 på Facebook
- Jeg fant ut hvem personen er og hvor han befinner seg i den virkelige verden

Hver Facebook-konto har et såkalt *screen name*, som er en variant av navnet man velger på kontoen. *Screen name* kan ses i nettleserlenken som vises når du går inn på din profil. Min Facebook-konto heter Jonas Alsaker Vikan og jeg har *screen name* jonas.vikan. SELGER123s *screen name* var selger.123.

Hver Facebook-konto har i tillegg et *user number* som er skjult for andre. OSINT-verktøyet til Bazzel kan vise *user number* ved hjelp av tilgang på profilens *screen name*.

User number gir adgang til flere undersøkelser basert på informasjon som ligger på Facebook, så fremt brukeren ikke har foretatt en stram redigering av egne personverninnstillinger.

Dersom man søker med *screen name* for å finne *user number* til en konto, kommer det i tillegg opp andre opplysninger om profilen. Blant annet vedkommendes nasjonalitet, og det fulle navnet på profilen. Her fant jeg noe uvanlig «bak» profilen til SELGER123:

Selv om profilen var opprettet med dekknavnet SELGER123 i 2012, hadde personen bak brukt sitt virkelige navn. Det ekte navnet, her kalt PER PERSSON, var ikke blitt fjernet i etterkant. Da jeg fikk opp SELGER123s *user number*, dukket også navnet PER PERSSON opp. Det var et spor jeg kunne gå videre med.

Navnet PER PERSSON var for vanlig, så jeg kunne ikke bare søke opp kontoen. Det var for mange mulige personer med det navnet, for mange feilkilder. Jeg kunne imidlertid bruke OSINT-verktøyet til å søke etter innlegg hvor PER PERSSON var tagget. For å få til dette, måtte jeg bruke *user number* jeg fant på profilen til SELGER123.

Ved å bruke denne fremgangsmåten kunne jeg være sikker på at den PER PERSSON som var tagget, også var den riktige PER PERSSON som hadde opprettet SELGER123-profilen.

PER PERSSON opprettet SELGER123-profilen i 2012. OSINT-verktøyet bruker Facebooks egen graph Search som ble introdusert for norske brukere i 2013.

Det er fullt mulig å sperre kontoen sin for Graph Search, men det måtte gjøres etter at det ble introdusert i 2013, noe SELGER123 åpenbart ikke hadde gjort. Sikkerhetsbristen gjorde det mulig for meg å identifisere minst en av personene bak dekknavnet.

5.3 Metode 14: Metadata og bildeanalyse

Forretningsideen bak kryptomarkedene er å gi narkonettverkene en infrastruktur hvor de kan selge, og presentere forskjellige stoffer. Bilder av narkotikaen er en sentral del av hvert nettverks butikk.

A) Hva var målet?

- Lå det informasjon i bildene narkotikalangerne la ut?
- Var noen av dem egnet for publisering?

B) Hva ble funnet?

- Bildene var, som regel, fullstendig renset for informasjon
- Enkelte kunne brukes, andre viste seg å være fullstendig uegnet

C) Forholdet til andre metoder

- Analyser av bildemateriale skjedde fortløpende, og gjennom hele perioden

Under informasjonsinnsamlingsfasen (pkt. 5.1.2) utviklet jeg rutiner for å se gjennom bilder jeg lagret i et eksternt program. Jeg var på jakt etter elektroniske spor i bildefilene.

Hvis ikke et bilde «renses» kan det ligge igjen en rekke opplysninger i bildefilen. De digitale sporene kan si noe om utstyr, tid, dato for bildet og hvor kameraet befant seg da det ble tatt.

Jeg brukte en onlineløsning til å gjøre undersøkelsene i bildematerialet:

http://www.viewexifdata.com

Dessverre var min erfaring av aktørene på det mørke nettet var disiplinerte med å fjerne avslørende data. Jeg fant etter hvert ut at det florerte med sikkerhetsguider som langere og nettverk kjøpte av hverandre. Bruk av anonymiseringsverktøy og datasikkerhet var blant de mest populære.

Jeg kunne lite om slikt før prosjektet begynte, og opplevde en situasjon hvor jeg fravek fra min egen rutine om å sjekke bildedata. Det kunne fått svært kjedelige konsekvenser for sakene.

I forbindelse med jakten på SELGER123s (se pkt. 5.2.8) Facebook-profil lastet jeg ned bildene som lå publisert på FB-kontoen. Ett av bilde viste en person ikledd en Guy Fawkes-maske (kjent fra Anonymous-bevegelsen) blant en skog av cannabisplanter.

Bildet så relativt proft ut, og var blant de bedre som jeg hadde funnet fra de ulike nettverkene. Jeg tenkte umiddelbart at det måtte gå an å bruke i saken, enten som en faksimile, eller som bilde fra det som var en åpen Facebook-profil, og la det i skjermbildearkivet.

Litt senere i prosjektet fant jeg bildet i arkivet mitt igjen. Av en eller annen grunn bestemte jeg meg for å sjekke metadata, selv om jeg ikke hadde gjort det den første gangen jeg hentet det ned. I metadataene fant jeg et navn som viste seg å høre til en kvinne i Oslo.

Jeg tenkte umiddelbart at her hadde noen gjort en tabbe. Det kunne være en person som var involvert, eller en kjæreste av vedkommende som bidro med bilder. Et nytt, konkret spor å gå etter i den virkelige verden var sjelden vare i dette prosjektet.

Jeg googlet navnet, og kom rett inn på en hjemmeside. Det viste seg at kvinnen var frilansfotograf. Jeg fant det samme bildet i oversikten over arbeid hun hadde fått publisert. Bildet var tatt i forbindelse med besøk hos noen som dyrket cannabis. Det hadde ingen verdens ting med det mørke nettet og gjøre.

SELGER123 hadde rett og slett stjålet det, og brukte det til å profilere seg med. At narkotikanettverkene også begikk åndsverkstyveri var ikke like interessant for sakene mine, men heldigvis sjekket jeg metadata på nytt og oppdaget det.

Hendelsen ble et eksempel på hvor viktig det var å ha kontroll på hvor jeg hadde de ulike detaljene i saken fra.

5.4 Metode 4: Kildearbeid

Arbeidet med denne saken har hele tiden vekslet mellom det mørke nettet, og det åpne nettet.

Nordmennene som operer seg på det mørke nettet er personer som begår, har begått eller ønsker å begå narkotikakriminalitet. De ser på det mørke nettet som et fristed som de vil holde unna politi og norske myndigheter.

Journalister ble regnet som en del av «fienden» fordi personene på det mørke nettet fryktet at omtale ville skape problemer for dem – noe sakene våre for så vidt gir dem rett i.

I den virkelige verden støtte jeg på utfordringer i omgang med mer tradisjonelle kilder som politi, myndigheter og lignende:

Det skjedde flere ganger at jeg måtte forklare kildene hva det mørke nettet var, hvordan det hang sammen og fungerte. Kontakten med kildene var stort sett uproblematisk, men det jeg stusset over at de kunne så lite om det jeg spurte om. Det var tydelig at det mørke nettet ikke var særlig kjent, og heller ikke et prioritert område for norsk politi og påtalemyndighet.

5.4.1 Lukkede kilder

Jeg ønsket i størst mulig grad å belyse forholdene på det mørke nettet ved hjelp av åpne kilder og metoder.

Da problemstillingen ble endret (se pkt. 3.5) hadde jeg allerede kommet meg inn på kryptomarkedene med falsk identitet. Jeg så at jeg hadde god tilgang til informasjon. Etter hvert klarte jeg og «å misbruke» systemene på det mørke nettet til å gi meg opplysninger og tallgrunnlag for sakene.

Jeg var bekymret for hva som kunne skje dersom jeg tok direkte kontakt med personer og nettverk. Jeg fryktet at kildene ville melde fra til aktører og til kryptomarkedenes bakmenn.

Det kunne føre til at jeg ble svartelistet, eller kastet ut. Selv om jeg hadde sikret meg mot problematikken ved å operere med flere falske identiteter (se pkt. 7.1), så var det likevel en fare for at mitt nærvær ville føre til at nettverk, langere og aktører sluttet å kommunisere åpent på undergrunnsforumene. Det ville vært svært problematisk fordi undergrunnsforumene hadde vært en gullgruve av informasjon.

Ved å følge samtaler på undergrunnsforumene kunne jeg få bred oversikt over sentrale tema som norske nettverk, stoffer, priser, metoder, modus, teknologi og sikkerhet. Det var tema jeg hadde regnet med at jeg måtte rekruttere kilder til å si noe om.

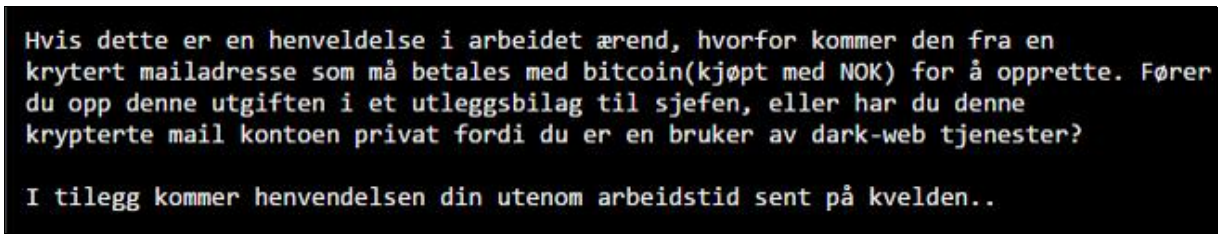
Jeg så at nettverk og langere var ivrige i å dele «hemmeligheter» med kundene. De lovte at ingen sjekket innenlandsposten i Norge, og at det derfor var trygt å bestille hos dem. De lovte i tillegg at saken kom til å bli henlagt dersom man nektet for å ha bestilt narkobrev.

Til internasjonale kunder fortalte nettverkene at Norge ikke var ansett som et narkotikaproduserende land, og at det derfor ikke var kontroll av brev sendt fra Norge til utlandet.

Dette var opplysninger jeg måtte sjekke med kilder i politi. Kunne det virkelig stemme?

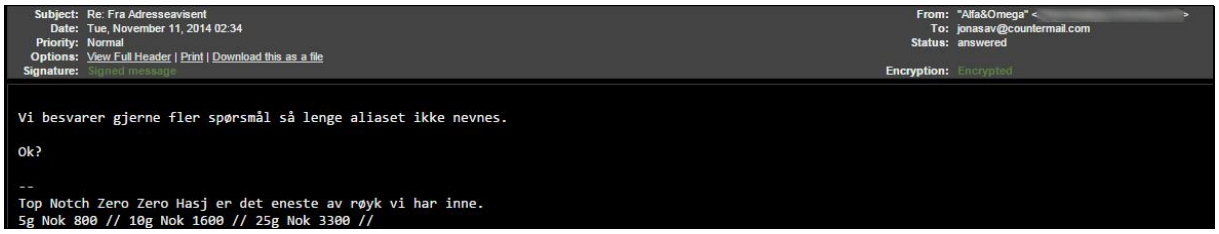
Mot slutten av arbeidet kontaktet jeg etter hvert alle nettverk og langere som jeg skulle omtale. Få av dem ønsket å si noe, og de som gjorde det var svært skeptiske (1) og forsøkte å sette begrensninger for arbeidet (2 og 3).

1)



Figur 6 Skeptisk: Nettverket FOXHOUND NORWAY var ikke spesielt interessert i å svare på spørsmål. Skjermbilde av kryptert e-postkommunikasjon i forkant av publisering 5. november.

2)



Figur 7 Forutsetninger: Nettverket ALFA&OMEGA ville ikke ha omtale. Skjermbilde av kryptert e-post 11. november 2014.

3)

Figur 8 Misfornøyd med omtale: En kilde fra det mørke nettet ønsket at jeg skulle fjerne dokumentaren «silkeveiene». Skjermbilde fra TOR Chat er tatt i etterkant av publisering 5. november 2014.

I løpet av arbeidet var jeg i kontakt med flere personer som hadde kjøpt narkotika på det mørke nettet. Kontakten skjedde både via kryptert e-post, kryptert chat, SMS og ved møter på ulike steder.

Forutsetningen for å snakke med meg, var at identiteten deres aldri skulle bli avslørt.

5.4.2 Kilder: Åpne

Etter innsamlingsfasen hadde kommet et godt stykke på vei, begynte jeg å ta kontakt med «vanlige kilder». For å svare på problemstillingen måtte jeg snakke med sentralt plasserte kilder i politiet, Kripos, påtalemyndighet, Tollvesen, Posten, forskningsmiljøet nasjonalt og internasjonalt.

A) Hva var målet?

- Finne ut hva de ulike offentlige etatene visste om det mørke nettet
- Sjekke om opplysninger som kom fra nettverkene stemte: At det ikke var kontroll av innenrikspost eller brev på vei ut av Norge
- Finne ut av om norsk politi har tilstrekkelig kompetanse til å bekjempe kriminaliteten som begås fra det mørke nettet
- Sjekke hva som skjedde med etterforskningen etter en pågripelse i Oslo våren 2014 (se pkt. 5.5.3)

B) Hva ble funnet?

- Ifølge Norsk narkotikapolitiforening hadde politiet liten eller ingen kunnskap om innenriksmarkedet vi var i ferd med å avsløre
- Det eksisterte ingen statistikk over beslaglagt innenlandspost, fordi den ikke ble kontrollert
- Statistikken over beslaglagte brev og pakker med narkotika fra utlandet viste at 87 prosent av sakene ble henlagt på landsbasis

- Ifølge Tollvesenet i Oslo var det riktig som nettverkene hevdet, at det ikke var kontroll av innenriksposten. Samtidig bekreftet Tollvesenet at mye tydet på at mye narkotika fløt gjennom innenriksposten.
- Det var i tillegg også riktig at brev som sendes ut av Norge ikke sjekkes, hvilket gjorde at nettverkene kunne reklamere med at de kunne selge narko fra Norge og sende det rundt i verden uten risiko
- Kripos var i en opprustningsfase, hvor en ny seksjon, for "internettrelatert etterforskning" var i ferd med å bli bygd opp. Kripos drev ikke aktiv etterforskning mot narkotikanettverkene på det mørke nettet

C) Forholdet til andre metoder

- Å hente inn uttalelser fra offentlige kilder pågikk parallelt med research på det mørke nettet (pkt. 5.1.2) og graving i dokumenter (se pkt. 5.5)

Norsk Narkotikapolitiforening (NNPF) var en av de første offentlige kildene som ble kontaktet fordi foreningen ofte har oversikt over trender og utfordringer som politiet står overfor. Det styrket min tro på prosjektet at de hadde liten kunnskap om narkoselgende nordmenn på det mørke nettet.

I forbindelse med spørsmål om pågripelsen av en 24-åring i Oslo våren 2014 så møtte jeg på en politiadvokat som var vanskelig å forholde seg til. Fordi kommunikasjonen ble vanskelig, ble det nødvendig for meg å få tilgang til rettsdokumenter som var unntatt offentlighet, se pkt. 5.5.3.

5.5 Dokumentgraving

Denne delen av rapporten vil redegjøre for skriftlige kilder som er brukt og hvordan tilgang til disse ble skaffet.

Jeg har brukt det jeg fant av norske, svenske og amerikanske rettskilder, enkelte forskningsartikler og bøker, nasjonale og internasjonale politirapporter i tillegg til etterforskningsdokumenter fra Sverige. Volumet på materialet var på rundt 1500 sider.

5.5.1 Metode 15: Analyse av OPERASJON LARVEN

Dokumentkilde: Länskriminalen i Skåne, Sverige
Dokumentmengde: 1200 sider

Da problemstillingen ble endret (pkt. 3.5), og jeg bestemte meg for å kartlegge det norske markedet og aktørene tenkte jeg at noen måtte ha etterforsket dem. Men jeg klarte ikke å finne noen norsk politietterforskning.

Var det ingen som hadde sett omfanget på kriminaliteten i Norge?

Det virket litt usannsynlige, men jeg begynte uansett å se mot andre land. Jeg fant etter hvert ut at politiet i Sverige hadde vært involvert i en stor etterforskning med det hemmelige navnet OPERASJON LARVEN.

I januar 2013 hadde noen etterforskere begynt å se på organisert narkotikasalg fra det mørke nettet. Jeg fant ut at flere personer ble pågrepet i 2013, og det ble etter hvert tatt ut en alvorlig tiltale mot dem.

Fra erfaringer jeg har gjort i andre kriminalsaker visste jeg at pressen i Sverige har rett til å be om å få utlevert etterforskningsdokumentene i en sak med en gang det er tatt ut tiltale.

Jeg bestemte meg for å få tak i dokumentene og rettet en formell henvendelse til riktig instans, som var länskriminalen i Skåne. Det tok litt tid, men jeg fikk tilgang i slutten av september.

Materialet besto av cirka 1200 sider og var delt inn i seks ulike .pdf-dokumenter.
Omfanget var for stort til å lese digitalt så jeg printet ut sidene og begynte å se gjennom.

A) Hva var målet?

- Jeg ville se hva politiet hadde avdekket
- Jeg ville se hvordan de hadde avslørt nettverket
- Var det mulig å lære noe av fremgangsmåtene?
- Lå det opplysninger i dokumentene om nettverkenes modus?
- Kunne jeg finne spor til Norge?

B) Hva ble funnet?

- Svenskenes pakkerutiner, kalt «stealth», ble avslørt
- Spaningsrapporter fortalte inngående om sikkerhetstiltak som hansker, masker, tape over fingerspisser, og fraværet av DNA-spor på brevene som ble postet
- Politiet hadde brukt omdømmesystemet på samme måte som meg (se pkt. 5.1.3)
- Jeg fikk navn og adresser til narkokunder i Oslo, Ålesund, Trondheim og Namsos. Disse sakene var ikke etterforsket av norsk politi

C) Forhold til andre metoder?

- Jeg sjekket opplysningene om «stealth» mot arkivet mitt (pkt. 5.1.2) og fant at de var sammenfallende med det jeg samlet inn om hvordan de norske nettverkene gikk frem

OPERASJON LARVEN hadde vært svært omfattende, opp mot tretti personer hadde deltatt. Svenskene hadde brukt mye ressurser på å spane på en mann på 30 år som var mistenkt for å være hovedmannen i nettverket SWEEXPRESS. Spaningsrapportene viste at mannen postet 25-30 brev om dagen. Politiet hadde i tillegg åpnet og undersøkt mange av narkobrevene SWEEXPRESS sendte. Brevene ble fotografert. Etterforskerne hadde i tillegg kjøpt narkotika, noe jeg ikke hadde adgang til (se pkt. 6.2).

Svensken solgte også til Norge, og i etterforskningsdokumentene fant jeg adresser og navn til kunder i flere deler av Norge. Den omfattende etterforskningen sa også mye om fremgangsmåter og modus. Jeg visste at dette ble delt etter «beste praksis»-metoden på det mørke nettet, så det var rimelig sikkert at også norske nettverk opererte på lignende måte.

Gjennomgangen av dokumentene i OPERASJON LARVEN viste i tillegg at svensk politi hadde trukket samme konklusjoner rundt omdømmesystemet som jeg hadde gjort. Etterforskerne la til grunn at hver tilbakemelding måtte være bevis for at det hadde skjedd et salg av narkotika.

Da jeg begynte på prosjektet kunne jeg ingenting om det mørke nettet eller salg av narkotika. Jeg måtte lære alt fra bunnen av, og finne egne metoder (se pkt. 5.1). Flere ganger tvilte jeg på om metodene dokumenterte det jeg mente de dokumenterte.

At politiet i Sverige hadde fått ressurser til en stor etterforskning, fått medhold til varetektsfengslinger, en tiltale og dom på bakgrunn av en lignende analyse av omdømmesystemet, bidro til å fjerne noe av tvilen jeg satt med.

I tillegg til å gå gjennom etterforskningsdokumentene intervjuet jeg. De var erfarne narkotikaetterforskere som hadde begynt med noe de kalte nettspaning. De fortalte meg at det var umulig å gjennomføre 1880 salg av narkotika på gata på samme tid som SWEEXPRESS hadde gjort det via det mørke nettet.

Kriminalitetsformen jeg var i ferd med å beskrive var tydeligvis mer effektiv og derfor langt mer lønnsom enn tradisjonelt narkotikasalg. Narkonettverkene kunne betjene flere kunder, spre mer stoff, få inn mer penger - alt på kortere tid.

Nordmennene som opererte på kryptomarkedene hadde en tilleggsfordel:

Det var ingen sjanse for at de ble oppdaget siden politiet i Norge ikke etterforsket kriminaliteten slik kollegaene i Skåne gjorde.

Svenskene fortalte at de i etterkant av OPERASJON LARVEN hadde fått besøk fra politi fra flere europeiske land som ville lære om metodene deres. De stusset over at ingen fra Norge hadde tatt kontakt.

5.5.2 Analyse av svenske rettsavgjørelser

Dokumentkilde: Helsingborgs tingsrätt og hovrätt
Dokumentmengde: 43 sider

Fra intervjuet med etterforskerne fant jeg ut at svensken bak «SWEEXPRESS» ble dømt for 1880 tilfeller av narkotikasalg i mai 2014. Hovedmannen fikk 8 år i fengsel, og anket uten at det hjalp.

Jeg kontaktet Helsingborgs tingsrätt og hovrätten og fikk utlevert rettsavgjørelsene. Jeg måtte sjekke hva retten hadde lagt vekt på. Mest spent var jeg på hvordan bevis fra omdømmesystemet ble vurdert.

A) Hva var målet?

- Å se hva som ble lagt til grunn for dommen
- Å se om analysen av omdømmesystemet holdt vann
- Å se hvordan retten vurderte kriminalitetsformen

B) Hva ble funnet?

- Analysen av omdømmesystemet ble godtatt som bevis på 1880 narkosalg
- Retten mente salg fra det mørke nettet var en straffeskjerpende fremgangsmåte

Tingsrätten i Helsingborg slo fast at en tilbakemelding via omdømmesystemet på kryptomarkedene var bevis på ett salg av narkotika. Hovrätten opprettholdt dommen.

Tvilen jeg hadde (om metodikken jeg hadde brukt) forsvant etter at jeg så to svenske rettsinstanser slå fast at tilsvarende metodebruk var sterk nok til å avsi en så streng dom.

Hovedmannens virksomhet var «omfattende og velorganisert» heter det i dommen. Fra rettspapirene gikk det frem at retten hadde reflektert rundt konsekvensene av denne nye formen for narkotikasalg. Det ble sett på som straffeskjerpende at distribusjonen fra det mørke nettet bidro til så mange salg - til så mange forskjellige kunder. At spredningen ble så stor, førte til en strengere dom.

- Det er brukt et sofistikert og effektivt system for salg ved bruk av det krypterte nettstedet Silk Road som gir mulighet for anonym betaling med bitcoins. Systemet innebærer at terskelen for å kjøpe narkotika har blitt senket *(min oversettelse)*

SWEEXPRESS var størst i Sverige i 2013. Min gjennomgang og kartlegging av de norske nettverkene viste at flere av dem hadde stått for over 1000 salg det påfølgende året.

Tre av de norske nettverkene var på samme nivå som hovedmannen bak SWEEXPRESS fikk en 8 år lang fengselsstraff for.

5.5.3 Metode 16: Dokumenter unntatt offentlighet

Dokumentkilde: Oslo Tingrett
Dokumentmengde: 4 sider

Selv om det ikke hadde vært noen norsk etterforskning av det organiserte narkotikasalget, fikk jeg tips fra en kilde om at en person knyttet til et norsk nettverk, hadde blitt pågrepet ved en tilfeldighet våren 2014.

A) Hva var målet?

- Finne ut om tipset stemte
- Finne ut hva som skjedde med saken
- Skaffe tilgang til eventuelle rettsdokumentene

B) Hva ble funnet?

- En 24-åring ble pågrepet, og fengslet i Oslo før han ble løslatt etter noen uker
- Han ble tatt med et narkobrev ved en falsk postkasse han hadde satt opp
- Hjemme hos mannen ble det funnet flere typer narko og brev til flere steder i Norge
- Mannen ble karakterisert som «sentral i et nettverk», men likevel var det kun en person siktet og lite tydet på videre etterforskning av saken og nettverket

C) Forhold til andre metoder?

- Det var nødvendig å få ut dokumentene fordi politijuristen på saken viste seg som en (i mine øyne) unødvendig vanskelig kilde

Den største utfordring var at jeg ikke hadde noen opplysninger som kunne identifisere saken. Det ble et forsøkt på å finne nåla i høystakken:

Jeg tok utgangspunkt i at det var mest sannsynlig at det hadde skjedd i en stor by, og begynte med Oslo. Fra presseområdet på domstol.no fant jeg ut at det hadde vært 1130 fengslinger i Oslo tingrett våren 2014.

En svakhet ved pressetjenestene på domstol.no er at det er opp til den enkelte rettsinstans å beskrive hvilke forhold saken gjelder. 1130 fengslinger var for mange til å gå gjennom en og en, og jeg bestemte meg for å begynne med førstegangsfengslingene.

Det var 465 førstegangsfengslinger og jeg skummet gjennom på utkikk etter en narkotikasak. Noen timer senere fikk jeg treff: En 24-åring ble fengslet 16. april.

Det var imidlertid et problem: Kjennelsen var i sin helhet unntatt offentlighet med hjemmel i Domstolovens § 130, første ledd. Politiet fryktet at bevis skulle bli forspilt hvis saken ble omtalt i pressen.

Da jeg jobbet med dette i slutten av august var det månedsvis siden fengslingen av mannen. Jeg kunne ikke se at mannen hadde blitt refengslet så jeg gikk ut fra at han var løslatt, noe jeg fikk bekreftet av politijuristen på saken som ellers ikke ville si stort. Problemene med å få politiet til å uttale seg gjorde at jeg måtte skaffe tilgang til rettsdokumentene.

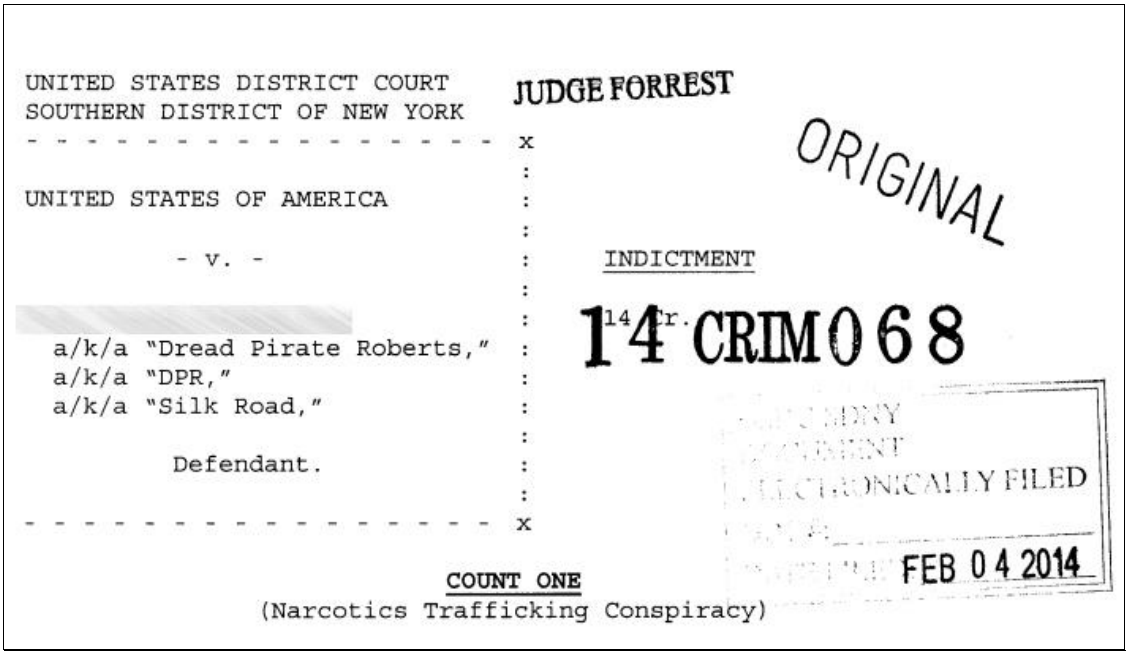
Jeg skrev en begjæring til Oslo tingrett hvor jeg argumenterte med at det ikke kunne foreligge bevisforspillelse i saken når påtalemyndigheten ikke hadde bedt retten om å refengsle 24-åringen etter utløpet av den første varetektsperioden. 24-åringen sto dermed fritt til å fjerne bevis som ikke var sikret av politiet, eller til å prate med andre involverte eller pressen.

Dette var en fremgangsmåte jeg hadde brukt med hell i Trondheim tingrett flere ganger tidligere. Jeg hadde god tro på at jeg skulle få medhold.

Etter å ha behandlet begjæringen i et par dager, sa en dommer seg enig og opphevet forbudet mot offentlig gjengivelse av opplysningene i kjennelsen. Jeg kunne referere fra dokumentene.

5.5.4 Metode 17: Siktelser Silk Road 1 og 2

Dokumentkilde: Det amerikanske justisdepartementet
Dokumentmengde: 48 sider



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JUDGE FORREST

ORIGINAL

UNITED STATES OF AMERICA

- v. -

INDICTMENT

14 Cr. CRIM 068

a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

ELECTRONICALLY FILED

FEB 04 2014

COUNT ONE

(Narcotics Trafficking Conspiracy)

Figur 9 Rettsdokumentene mot den antatte bakmannen fra Silk Road 1 ble hentet fra det amerikanske justisdepartementet.

I oktober 2013 ble en amerikaner pågrepet i et bibliotek i San Francisco, mistenkt for å stå bak det opprinnelige kryptomarkedet kjent som Slik Road. I løpet av tiden etter pågripelsen ble siktelsen mot ham frigjort av det amerikanske justisdepartementet.

Jeg hentet inn disse dokumentene.

A) Hva var målet?

- Var det mulig å se noe om hvor stor handelen på kryptomarkedet var?

B) Hva ble funnet?

- FBI mente å kunne bevise at omsetningen lå på over en milliard kroner (7,6 milliarder norske) i løpet av 2013.

Det var åpenbart at størrelsen på narkotikatrafikken på det mørke nettet var enorm.

Det var også rimelig å anta at den hadde økt i løpet av året som gikk fra beslagleggelsen av Silk Road 1 i oktober 2013 og til prosjektet mitt begynte i august 2014. Siktelsen mot amerikaneren ga i tillegg opplysninger om hvordan siden var kodet, hvilke funksjoner den hadde og hvordan de skulle skape tillit i markedet (se pkt. 5.1.3).

I kjølvannet av pågripelsen av bakmannen, ble flere selgere pågrepet i USA. Jeg brukte også siktelser mot disse selgerne. Siktelsene ga meg informasjon om metodebruk og modus på det mørke nettet, opplysninger som jeg visste at de norske nettverkene også hadde tilgang på.

Etter at vi publiserte de første sakene våre 5. november 2014, slo politi fra 16 land til mot flere kryptomarked. Etterfølgeren til Silk Road, kjent som Silk Road 2, ble beslaglagt og en ny bakmann, som var i 20-årene, ble pågrepet.

Siktelsen mot ham ble frigitt av justisdepartementet. På samme måte som tidligere, hentet jeg inn dokumentene som beskrev hans aktivitet. Dokumentene ga meg nye opplysninger om hvordan systemene ble endret for å svare på den første FBI-aksjonen i 2013 og ble lagt til grunn i flere oppfølgingssaker.

5.5.5 Metode 18: Politidokumenter

Dokumentkilder: Politidirektoratet, Kripos, Europol, påtalemyndigheten i Nederland
Dokumentmengde: 250 sider

I løpet av august og september klarte jeg ikke å finne en ekspert på narkotikasalget fra det mørke nettet i norsk politi. Jeg gikk derfor til det fremste kunnskapssenteret i norsk politi, Kripos, for å få informasjon og eventuelt finne kilder.

Jeg lette i tillegg bredere, kontaktet det europeiske politisamarbeidet Europol og, etter hvert, den nederlandske påtalemyndigheten. Til slutt satt jeg på rapporter om kriminalitetsutvikling og kriminalitetstrender fra etatene.

Det var nok til å danne seg et inntrykk av hvordan de spissede politienhetene så på problemstillingen.

A) Hva var målet?

- Finne ut hva Kripos visste om narkotrafikken
- Se hva Europol mente om handelen på kryptomarkedene
- Finne ut det lå noen føringer for hvordan politiet skulle håndtere dette, både nasjonalt og internasjonalt

B) Hva ble funnet?

- Kripos' strategirapport som løper til og med året 2015, sa fint lite om narkotika fra det mørke nettet. I en annen rapport ble det vist til en flere år gammel Europol-rapport
- Europol skjenket temaet 2 linjer i en 79 sider lang rapport som beskriver kriminalitetstrender for 2014
- Den nederlandske påtalemyndigheten gikk i spissen for et prosjekt som skulle ramme kunder, selgere og bakmenn på kryptomarkedene. Prosjektet hadde fått EU-midler, men budsjettet var svært lavt
- European Cybercrime Centre slo fast at kryptomarkedene utgjorde en trygg havn for kriminelle

C) Forholdet til andre metoder

- Jeg jobbet med å skaffe, og gjennomgå rapportene i september og begynnelsen av oktober. Innholdet, eller fraværet av innhold, ble vurdert opp mot resultater fra informasjonsinnhentingsfasen i forbindelse med skriving av dokumentaren «silkeveiene»

KRIPOS skal være Norges spydspiss mot grov og organisert kriminalitet. I rapportene «Den organiserte kriminaliteten i Norge: Trender og utfordringer 2013-2014» og «Kripos' strategi 2011-2015», sto det svært lite om det mørke nettet. Det var ingenting som tydet på at etaten hadde mye kunnskap om kryptomarkedene, norske aktører, omfanget på det norske narkotikasalget og modusen som langere og selgere opererte med.

Ettersom Norges dyktigste politietat viste til gamle Europol-dokumenter måtte det være her kunnskapen var samlet. Jeg fikk tak i en helt fersk rapport som het «Europeisk narkotikarapport: Trender og utvikling 2014». Europol fattet seg i korthet:

- Utfordringene øker ved at anonyme nettverk – såkalte "darknets" – i stadig større grad brukes til salg av narkotika til langere og brukere

Via en internasjonal nettside som skriver om det mørke nettet fant jeg ut at det forelå en slags europeisk slagplan for å ramme kryptomarkedene. Jeg fikk tak i dokumenter hvor den nederlandske påtalemyndigheten beskrev «PROJECT ITOM». Prosjektet skulle bygge opp et europeisk kompetansenettverk bestående av politi i EU-land som hadde kunnskap om kjøp og salg av ulovlige varer på det mørke nettet. Jeg kontaktet nederlandsk påtalemyndighet og fant ut at prosjektet hadde et budsjett som var urealistisk lavt budsjett. Jeg bestemte meg likevel for å omtale «PROJECT ITOM» i en oppfølgingssak.

I oktober 2013, omtrent samtidig som FBI beslagla det første kryptomarkedet, etablerte Europol underetaten European Cybercrime Centre. Da jeg var i ferd med å sluttføre arbeidet med prosjektet i oktober 2014, slapp ECC en gedigen rapport kalt «The internet organised crime threat assessment 2014». Der var kryptomarkedene hyppig omtalt, og ble utpekt som en trygg havn for kriminelle.

Alle disse skriftlige politikildene forsterket en hypotese jeg delte med de norske nettverkene på det mørke nettet:

Norsk politi kan lite, og gjør enda mindre med det organiserte narkotikasalget som gjør alle typer stoff tilgjengelig for personer i alle aldre, på store og små steder i Norge.

Dessverre viste det seg også at norsk politi gjorde like lite for å få tilgang til det som eksisterte av kunnskap blant internasjonale kolleger.

5.5.6 Internasjonal forskning

Dokumentkilder: «Drugs on the dark net» (Martin), «Not an Ebay for Drugs» (Decary-Hetu og Aldrige)
Dokumentmengde: 116 sider

Forskning på narkotikatrafikken fra det mørke nettet er i startgropa. Jeg kontaktet Statens Institutt for Rusmiddelforskning (SIRUS), men der fikk jeg opplyst at ingen nordmenn hadde begått forskning på området.

Jeg måtte igjen løfte blikket, og se til utlandet. Der kom jeg over noen få forskningsprosjekt.

A) Hva var målet?

- Visste forskere noe om hvem som handlet narkotika på det mørke nettet?
- Hadde noen dokumentert omfanget?
- Ble det sagt noe om denne nye formen for narkotikakriminalitet?

B) Hva ble funnet?

- Forskere så omdømmesystemet som sentralt i kryptomarkedene
- De mente kryptomarkedene utgjorde en «fundamental endring i internasjonal narkotikatrafikk»
- Forskere dokumenterte at organiserte kriminelle dominerte på kryptomarkedene

C) Forholdet til andre metoder

- Gjennomgangen av Martins forskning rundt omdømmesystemet skjedde etter min egen innsamling av data (5.1.2) og analyse av systemet (5.1.3)

Rundt oppstarten på prosjektet mitt ga forskeren James Martin ut en bok om narkohandelen. Jeg kjøpte tilgang til boka «Drugs on the Dark Net: How Cryptomarkets are transforming the global trade in illicit drugs», og leste den. James Martin har doktorgrad i politivitenskap og etterretning ved et universitet i Australia.

Martins bok baserte seg på tall han hadde samlet på det opprinnelige kryptomarkedet SILK ROAD i 2013. Tallene var allerede utdaterte, men Martin slo fast at de teknologiske virkemidlene som narkotikalangerne bruker, vil endre salget av illegale stoffer.

Den nyeste forskningen jeg fant, ble publisert av forskerne Judith Aldrige og David Decary-Hetu i mai 2014. Forskerne, som var knyttet til universitetene i Manchester og Montreal, så i likhet med Martin på kryptomarkedene som et slags paradigmeskifte i handelen med narkotika.

Samtidig hadde forskerne en annen og oppsiktsvekkende analyse av brukermønstre:

Deres data pekte på at mye av handelen skjedde i større kvantum, noe de mente underbygget at det dreide seg om organiserte kriminelle som handlet med og fra organiserte kriminelle.

Det var oppsiktsvekkende fordi rådende beskrivelse av kryptomarkedene var at de var narkotikatorg for enkeltbrukere, ikke en formidlingssentral for grupper og nettverk slik Aldrige og Decary-Hetu kunne dokumentere.

At organiserte grupper handlet store mengder narkotika fra hverandre ved hjelp av disse sidene, og senere distribuerte stoffene lokalt, var urovekkende.

5.6 Metode 19: Spaning

Fra analysen av OPERASJON LARVEN (pkt. 5.5.1), og fra informasjonsinnsamlingsfasen, hadde jeg opplysninger om flere brukere av det mørke nettet. Noen av personene holdt til i Midt-Norge.

Vi ønsket å prate med dem, og skaffe bildedokumentasjon av postmodus. Spesielt var vi ute etter å finne falske postkasser som fungerte som mottakerledd for narkotika bestilt på det mørke nettet (se pkt. 5.5.3 om Oslo-saken).

A) Hva var målet?

- Finne adressene og personene bak adressen
- Undersøke om noen av dem brukte falske navn og falske postkasser
- Skaffe bildemateriale

B) Hva ble funnet?

- Vi fant flere personer, flere steder i Midt-Norge
- Vi dokumenterte flere adresser hvor vi visste at det var bestilt narkotika, etter å ha holdt øye med stedet
- Vi kom i kontakt med flere av personene som hadde bestilt narkotika
- Vi fant ut at flere brukte falske navn, og fant minst en postkasse som ikke hørte til personer registrert på adressen
- Vi fant ut at en av kundene fra det mørke nettet hadde omkommet som følge av en overdose

C) Forholdet til andre metoder

- Denne metoden var den siste vi tok i bruk før prosjektet ble publisert

Etter at fotograf Ole Martin ble koblet på saken spanet vi ved flere anledninger på adresser vi fant i etterforskningsdokumentene fra OPERASJON LARVEN. Årsaken til at denne metoden ble brukt sist, var at vi fryktet at personene skulle fortelle andre på det mørke nettet at de var blitt kontaktet av journalister som hadde lokalisert dem i den virkelige verden. Vi fryktet det ville påvirke tilgangen vår til informasjon.

Selv om spesielt Jonas begynte å få god oversikt over hvordan nordmennene brukte det mørke nettet følte vi fortsatt at det var viktig å lære mer.

Spaningen førte til at vi dokumenterte postbokser og postkasser flere steder. I tillegg møtte vi kunder som ble fotografert. Dessverre ble ikke alle bildene publisert (se mer i pkt. 6.4 om bildebruk).

6. Pressetiske vurderinger

Det mørke nettet er et spesielt fenomen, men ikke et område hvor presseetikken ikke gjelder. Det er foretatt flere presseetiske vurderinger i forbindelse med sakene. Tema har vært personer under 18 år, kjøp av narkotika, samtidig imøtegåelse og bildebruk. Jeg har brukt falsk identitet for å samle opplysninger. Dette er redegjort for i punkt 7.1.

6.1 Personer under 18 år

I Adresseavisen kontakter vi foreldre først dersom vi ønsker å intervjue personer under 18 år. Det ble en utfordring i denne saken, i forbindelse med deanonymisering av BRUKER123 som jeg fant ut var 16 år gamle ØYSTEIN (se pkt. 5.2.1).

Det var langt fra sikkert at BRUKER123s foreldre kjente til at han brukte det mørke nettet, eller at han bestilte narkotika derfra. Jeg ble enig med reportasjeledelsen om at det var best å ta kontakt med BRUKER123 direkte, uten å gå gjennom foreldrene. Hensynet som var avgjørende her, var kildevernet.

En forutsetning for at ØYSTEIN skulle snakke med oss var at han ble anonymisert. Det gikk vi med på, fordi vi vurderte at han satt på en viktig historie som illustrerte problemet som oppstår når ungdommer kan sitte på gutterommet og ha tilgang på alle mulige typer narkotika.

6.2 Kjøp av narkotika

Kjøp av narkotika ble vurdert som metode i denne saken. Målet var å skaffe bildedokumentasjon fra innpakkingen av narkotikaen, og forsøke å spore forsendelsene.

Redaksjonsledelsen var imidlertid av den oppfatningen om at vi ikke skulle gjennomføre kjøp av narkotika siden det ville stride mot norsk lov. Jeg måtte finne andre metoder.

6.3 Samtidig imøtegåelse

I dagene før publisering ga jeg meg til kjenne til nettverkene og langerne jeg kom til å omtale. Selv om det dreide seg om personer som skjulte seg bak dekknavn var det rimelig å opprettholde retten til samtidig imøtegåelse.

Ingen av dem jeg kontaktet ønsket å uttale seg i noen særlig grad. Enkelte ønsket imidlertid identifikasjonspapirer fra meg (se pkt. 10.4 om trusler) noe de fikk tilgang på.

6.4 Bildebruk

I forbindelse med spaning (se pkt. 5.6) tok vi bilder av postkasser og postbokser på flere adresser. Bildene ble ikke brukt i sakene fordi vi ikke kunne være hundre prosent sikre på at personene bak postkassene var de samme som vi satt på opplysninger om. Det var blant annet vanlig å bruke falske navn på postkasser. Derfor vurderte redaksjonsledelsen at det ikke var riktig å publisere bildene i sakene.

Det ble trykket bilder av 16 år gamle ØYSTEIN, men bildene ble anonymisert av hensyn til gutten. Vi bestemte at bildene og saken om ØYSTEIN kun skulle gå i papirutgaven, slik at de ikke var søkbare på nett. Igjen var årsaken til kildevern. Etter å ha lært mye om miljøet på det mørke nettet, visste jeg at svært mange var datakyndige. Dox var en vanlig måte å henge ut personer på: Private opplysninger ble lekket og publisert slik at personen som ble rammet kunne bli utsatt for identitetstyveri, hjemsendelse av narkotika og lignende. Jeg var veldig oppsatt på at det ikke skulle skje med ØYSTEIN.

Vi anonymiserte også de svenske etterforskerne fra Skåne etter et ønske fra deres arbeidsgiver i Sverige. Selv om de uttalte seg med fullt navn, arbeider de videre som spanere i tungt kriminelle miljø. Det ville vært skadelig for deres videre arbeid dersom det lå bilder av dem på nettet.

7. Spesielle erfaringer

Bare det å jobbe med fenomenet det mørke nettet var en spesiell erfaring. Alt som foregikk her var totalt ukjent for meg før jeg begynte på prosjektet. Arbeidet var en læringsprosess hvor det meste var nytt.

Samtidig kunne jeg ved noen anledninger nyte godt av tidligere erfaringer (se pkt. 5.1.4 om krypteringsnøkler og pkt. 5.5.3 om oppheving av referatforbud) og kurs (se pkt. 5.2.7 om OSINT-søk og pkt. 7.2 om Operations Security) jeg hadde deltatt på.

I tillegg til begrep som OSINT, måtte forstå hva Operations Security (OPSEC) betød for brukerne. Jeg måtte også forholde meg til OPSEC i forbindelse med å sikre min egen tilgang til informasjon og datainnsamling. Jeg kunne imidlertid nyte godt av den samme opplæringen som tusenvis av andre brukere hadde tilgang til.

Miljøet på det mørke nettet, både det norske og det internasjonale, består av personer som mener at narkotika i all hovedsak er greit og at det er opp til hver enkelt hva de vil putte i kroppen sin. De er de i sterk opposisjon til ruspolitikk og juridiske systemer som de mener undertrykker dem.

Derfor var ingen stor overraskelse for meg at det kom en rekke sterke, og svært negative tilbakemeldinger og trusler i etterkant av publiseringen av prosjektet.

7.1 Metode 3: Falsk identitet

Jeg har i denne saken operert med flere falske identiteter fordi jeg vurderte at det å identifisere seg som journalist ville føre til at tilgangen til kilder og informasjon ville forsvinne. Identitetene ble opprettet tidlig i prosjektet og parallelt slik at jeg kunne infiltrere flere kryptomarkeder og undergrunnsforum. Hvis en identitet ble avslørt, hadde jeg flere profiler jeg kunne bruke.

A) Hva var målet?

- Få adgang til kryptomarkedene
- Finne mest mulig informasjon om kryptomarked, undergrunnsforum, norske aktører og deres salgstall, modus, varelager og priser.
- Opprette kontakt med kilder

B) Hva ble funnet?

- Jeg fikk invitasjon til kryptomarkedet AGORA
- Se punkt 5.1.1 til og med 5.4.2.

C) Forholdet til andre metoder

- Jeg brukte de falske profilene mine til research gjennom hele perioden, og etter publisering. De var en forutsetning for at datagraving (pkt. 5.1) og kildearbeid (pkt. 5.4) kunne skje på det mørke nettet

Kryptomarkedet Agora krevde invitasjon på tidspunktet da jeg begynte mine undersøkelser. Invitasjonen fikk jeg tak i på et undergrunnsforum hvor jeg opererte under dekknavn.

Identitetene, eller dekknavnene, ble satt opp ved hjelp av en spesiell type e-post (se pkt. 7.2), og de skulle ikke kunne lede tilbake til meg som journalist eller privatperson. Jeg har operert med dekknavn i flere faser av prosjektet.

Vær Varsom-plakaten sier følgende om denne typen metode:

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

Forutsetningen for at jeg skulle klare å samle inn informasjon fra det mørke nettet, var at brukerne av kryptomarkedene oppfattet meg som «en av dem», og at jeg ikke skilte meg vesentlig ut.

Jeg mener at funnene i denne saken forsvarer bruken av falsk identitet – og er ikke i tvil om at forholdene som er avdekket er av vesentlig samfunnsmessig betydning. Opplysningene ville ikke kunnet bli fremskaffet ved annen metodebruk.

7.2 Operasjonssikkerhet

Begrepet OPSEC er sentralt for brukerne på det mørke nettet. Alle ønsker å være anonyme, og at det mørke nettet forblir mørkt og ukjent. OPSEC betyr for Operations Security (operasjonssikkerhet).

Begrepet er hentet fra etterretningssjargong og viser til grepene en person må ta for å kunne operere fritt uten fare for pågripelse, eller for å få sin virkelige identitet avslørt.

Jeg hadde ikke gjort meg noen tanker om dette da jeg begynte på prosjektet. Det endret seg fort. OPSEC var et begrep jeg skjønte at jeg måtte ta på alvor da problemstillingen ble endret (se pkt. 3.5).

Vanligvis ville det være et problem å følge narkotikasalget digitalt, fordi bakmenn kunne sitte på teknologi til å lese av IP-adressen min. Men siden dette var det mørke nettet, hvor TOR var en forutsetning, så var jeg like usynlig som alle andre. Dermed kunne jeg jobbe fra redaksjonslokalene i Trondheim uten å være redd for at jeg skulle bli deanonymisert og kastet ut fra kryptomarkedene.

Jeg måtte imidlertid gjøre noen tilleggsgrep:

- Jeg brukte en rekke falske profiler med dekknavn som var bygget på falsk identitet, for å få tilgang til kryptomarkeder, undergrunnsforum og kilder. Det var avgjørende at profilene ikke knyttes til meg som person, eller til rollen min som journalist. En utfordring med å få opprettet identitetene var at det ble krevd e-postverifisering. Jeg måtte unngå at e-postadressen kunne spores tilbake til meg som journalist. Derfor brukte jeg e-posttjenesten «Yopmail» som lar brukerne finne på midlertidige e-postadresser.
- Jeg opererte samtidig med flere krypterte e-postadresser som jeg brukte til å kommunisere med kilder. Countermail går for å være en av de sikreste på markedet, noe som bidro til at kildene kunne ha tillit til at jeg tok anonymitet på alvor. Jeg brukte min personlige countermailadresse til å hente inn tilsvar fra narkotikanettverk og langere, mens jeg hadde andre countermailadresser som jeg brukte til kildekontakt.
- Til de mest paranoide kildene brukte jeg programmet TOR-chat. TOR-chat er en tjeneste som kjører i bakgrunnen mens brukeren er logget inn på TOR. Det skal sørge for at man er hundre prosent anonym. Brukerne oppretter egne profiler, men de er uten forståelige navn og fremstår som skjult bak tilfeldig utvalgte bokstaver og tall
- I forbindelse med research så har jeg snakket med dataeksperter. De er ikke sitert i sakene, men jeg fikk råd om at jeg måtte ta grep med min egen datasikkerhet hvis jeg skulle gå etter aktører på det mørke nettet. De advarte mot hacking. Jeg var primært bekymret for materialet jeg hadde samlet inn, og sørget for at jeg aldri tok med materiale utenfor redaksjonslokalene i Trondheim
- Som et kildevernsgrep sørget jeg for at stedstjenester alltid var skrudd av på mobiltelefonen da jeg skulle møte aktuelle personer i den virkelige verden

«Yopmail» var et system som var ukjent for meg før jeg deltok på SKUP-konferansen i 2013 hvor jeg plukket det opp i forbindelse med et foredrag med sikkerhetsekspert Tor Andre Breivikås. «Yopmail» er gratis, krever ingen registrering og lagrer meldinger i åtte dager.

TOR-chat var helt nytt for meg. Jeg oppfattet at det var relativt populært og lastet det ned. Det viste seg å være like enkelt å bruke som TOR, og bidro til at jeg kunne ivareta min egen anonymitet så vel som kildenes.

Jeg har i flere år hatt en countermail-adresse, etter arbeid med en annen kriminalsak. Erfaringene jeg hadde gjort meg med slike tjenester gjorde at jeg kunne bruke tjenesten metodisk i arbeidet (pkt. 5.1.4), og ikke bare til å sjekke e-post.

7.3 Misbruk av systemer

Da arbeidet begynte, hadde jeg aldri sett for meg at det skulle være så mye infrastruktur og så mange systemer i virksomhet. Aktiviteten på kryptomarkedene på det mørke nettet er svært avansert, og veldig organisert.

Narkotikahandelen på det mørke nettet har eksistert internasjonalt siden 2011, og genererer mange milliarder i årlig omsetning. Sammenholdt med kunnskapsdeling (som er en del av både den åpne, og den mørke internettkulturen) fikk systemer og infrastruktur vokse frem. Disse hadde blitt spisset i løpet av de tre årene.

Det norske miljøet nøt også godt av delingskulturen. Nordmennene kunne rett og slett se hva de internasjonale aktørene tok seg til og kopiere atferd og metoder fra dem.

For meg som jobbet alene krevde det mye kunnskap før jeg var i stand til å identifisere de ulike systemene og se hvilke formål de tjente. Jeg brukte mye tid på å lese meg opp, se gjennom forumtråder og lese guider.

Da jeg omsider satt med en del kunnskap, var det mulig å «misbruke» systemene på kryptomarkedene til å lage journalistikk om det som foregikk i skjul for norske myndigheter. Systemene (se pkt. 5.1.3 om omdømme, og pkt. 5.1.4 om krypteringsnøkler) satte meg i tillegg i stand til å måle omfanget på narkotikasalget, og tallfeste det.

At det eksisterte system som brukes til å spore kriminelle handlinger var vanskelig å forstå. At systemene ble gjort tilgjengelige av det samme kriminelle miljøet som brukte dem, var enda vanskeligere å skjønne.

Etter hvert gikk det opp for meg at systemene var en av årsakene til at narkohandelen hadde vokst til en milliardbutikk med titusenvis av brukere: Systemene skapte den tillitten som er nødvendig for at folk skal handle med hverandre. Tilliten var avgjørende i en skyggeverden hvor identiteten til brukerne var skjult av TOR.

Da arbeidet begynte måtte jeg finne lenker til sidene jeg skulle undersøke (se pkt). I løpet av prosjektet har jeg kommet over verktøy som gjør at framtidig journalistisk arbeid på det mørke nettet vil være langt lettere.

Det eksisterer nå en søkemotor som heter «Grams». «Grams» gjør det enklere å navigere. Direktelenke til søkemotoren finnes her (krever TOR-browser):

http://grams7enufi7jmdl.onion/

7.4 Norsk impotens

Vi publiserte funnene våre 5. november. Ett døgn senere gikk politi fra 16 land til aksjon mot flere av kryptomarkedene vi hadde kartlagt i sakene. Tre av de viktigste ble beslaglagt av FBI og EUROPOL som ledet aksjonen.

Med i dragsuget gikk selgerkontoene til de norske nettverkene, samt forumet nordmennene brukte til å kommunisere, utveksle sikkerhetstips og til å lære opp nye brukere og kunder. Det er snakk om store mengder data, bevis på den omfattende kriminelle aktiviteten som er beskrevet i sakene.

I Haag ligger tusenvis av dokumenter, omdømmesystemet og meldinger til og fra norske narkotikanettverk: Et koldtbord av informasjon og bevis på den omfattende narkotikakriminaliteten som blir begått av norske, profesjonelle aktører.

Materialet leveres ut til norsk politi etter forespørsel fra Kripos. Da jeg kontaktet Kripos i forbindelse med artikkelserien fikk jeg opplyst at «internasjonalt samarbeid var svært viktig for å avsløre kriminalitet på nettet».

Men selv om justisministeren sier at narkotikasalg fra det mørke nettet er uakseptabelt, og Kripos selv hevder at internasjonalt samarbeid er svært viktig, har etaten så langt ikke bedt om å få materialet utlevert. Under følger Kripos' egen definisjon av organisert kriminalitet.

> Dersom seks av punktene nedenfor foreligger, deriblant 1, 3, 5 og 11, definerer Europol kriminaliteten som organisert:
>
> 1. **samarbeid mellom flere enn to personer**
> 2. hver med egne tildelte oppgaver
> 3. **over lang eller ubegrenset tidsperiode**
> 4. gjennom bruk av en form for disiplin og kontroll
> 5. **mistanke om gjennomførte alvorlige kriminelle handlinger**
> 6. virksomhet på internasjonalt nivå
> 7. bruk av vold eller annen form for trussel
> 8. bruk av kommersielle eller forretningsmessige strukturer
> 9. deltakelse i hvitvasking
> 10. utøve innflytelse på politikk, media, offentlig forvaltning, rettsmyndigheter eller økonomi
> 11. **styrt av målsetting om vinning og/eller makt**

Avsløringene i våre saker viser at aktiviteten med rette kan betegnes som organisert, og derfor svært samfunnskadelig. Men mens norsk politi har stått og sett på, har de norske nettverkene gjort flere hundre narkohandler også i etterkant av sakene i Adresseavisen og den internasjonale politiaksjonen.

I Sverige har Kripos' motsats, Rikskriminalen, vært involvert i flere etterforskninger mot narkosalg på det mørke nettet. I Finland har politiet deltatt i de internasjonale aksjonene.

Narkoflyten, og Kripos' impotens vil bli gjenstand for oppfølgingssaker gjennom januar og februar 2015.

7.5 Trusler og reaksjoner

Som journalist har jeg hatt som prinsipp at jeg skal være tilgjengelig i åpne registre som telefonkatalogen. Dette har jeg opprettholdt selv om jeg tidligere har arbeidet med alvorlige kriminalsaker og mottatt trusler og sjikane.

Rundt en måned før publisering av «silkeveiene» innså jeg at funnene ville føre til sterke reaksjoner fra et kriminelt miljø som fremsto som organisert. Jeg valgte derfor å få fjernet telefonnummer og adresse.

Da de første sakene ble publisert slo de ned som en bombe i miljøet på det mørke nettet. Selv om det er et nasjonalt miljø og Adresseavisen er en regionavis så hadde brukerne tilgang på sakene umiddelbart, både digitalt og i papirform.

Kritisk journalistikk ble ikke særlig godt mottatt.

Det ble laget en diskusjonstråd på et hemmelig, norsk forum hvor den mest aktive diskusjonen handler om våre saker. Der uttaler nettverkene seg også, og uttalelsene bærer preg av at de ble rasende over at modus og salgstall ble offentliggjort.

«Denne artikkelen setter oss i fare, så ja nå er han i fare!!»

«Fokuser heller sinnet deres på den som faktisk er fienden her, avisa, journalisten og politiet.»

«Når dere leser de håper jeg litt flere forstår hva slags følelser vi har mtp Jonas...»

Summen av innholdet i disse innleggene, gjorde at Adresseavisen valgte å anmelde dem som trusler. En anmeldelse ble levert til Sør-Trøndelag politidistrikt i desember. Per 14. januar 2015 har det ikke kommet noen tilbakemelding fra politiet om hvor etterforskningen står. Jeg forventer imidlertid at det ender i henleggelse.

I forbindelse med at jeg innhentet tilsvar i forkant av publisering, ba det ene nettverket kjent som FOXHOUND NORWAY om å få tilsendt et bilde av mitt pressekort. Det var en forutsetning for å svare, oppga de. Da de fikk et bilde av pressekortet, viste det seg at nettverket ikke hadde til hensikt å komme med et tilsvar.

I den samme diskusjonen om sakene i Adresseavisen skriver de:

«Jeg spurte journalisten om ID slik at vi har identiteten hans for.. la oss kalle det senere bruk..Han trodde det bare var for å avkrefte at han var politi, nå har vi både bilde og navn på han.»

Fra kilder på det mørke nettet har det blitt antydet at det er bestilt narkotika i Jonas' navn og sendt til hans hjemmeadresse. Stoff skal ha blitt bestilt fra utenlandske selgere, slik at pakken skal bli stoppet av Tollvesenet og journalisten kalt inn til politiavhør.

Samtidig hadde flere norske brukere gravd på nettet for å finne opplysninger om Jonas. På det hemmelige, norske forumet som nordmennene samlet seg på i etterkant av publisering og

FBIs aksjoner i november, ble det publisert en lenke til et intervju gjort med Jonas i 2005. En annen bruker har oppfordret andre til *«å grave opp noe dritt»* om meg fra ti år tilbake i tid.

Jeg har hatt mulighet til å følge innleggene, og skal ikke legge skjul på at det ikke har vært hyggelig. Det har imidlertid aldri vært aktuelt å la innleggene påvirke det videre arbeidet, eller ytterligere omtale av nettverk eller enkeltselgere. I løpet av 2015 vil det bli publisert flere saker om dette miljøet og aktørene.

8. Etterspill

Både i for- og etterkant av publisering, har det vært utfordrende å få kommentarer fra norske politi- og justismyndigheter. Det har forsterket inntrykket mitt om at det mørke nettet overhodet ikke er på radaren til etatene.

Politimester Nils Kristian Moe ved Sør-Trøndelag politidistrikt er ansvarlig for etterforskningen av Europas største dopingsak, Operasjon Gilde, hvor teknologi ble brukt til å skjule spor. Moe reagerte på følgende måte på avsløringene om at nordmenn hadde fått stå for minst 5500 narkohandler, uten innblanding fra politiet

- Hvis problemet er i nærheten av det Adresseavisen skriver om, så har dere tatt tak i en svært alvorlig og omfattende kriminalitet som er, og som har vært, forholdsvis ubehandlet. Gitt dette så bør alle tiltak som kan være mulige vurderes, også eventuelle lovendringer som kan gi oss mulighet til å etterforske sakene på en bedre og enklere måte

8.1 Statsråder rykker ut

Noen uker etter publiseringen av «silkeveiene» annonserte justisminister Anders Anundsen og samferdselsminister Ketil Solvik-Olsen at et nytt kontrollregime for innenlandsposten skulle innføres umiddelbart.

- Vi har fulgt sakene med interesse. Omfanget er bekymringsfullt. Det har ikke fått den oppmerksomhet og prioritet som det bør ha
(Samferdselsminister Ketil Solvik-Olsen)

- Det er en helt uakseptabel situasjon. Denne typen forsendelser må og skal stoppes. Vi ønsker å nå både selgere og kjøpere
(Justisminister Anders Anundsen)

Samferdselsminister Solvik-Olsen karakteriserte Adresseavisens avsløringer som «et stort problem» mens justisministeren slo fast at narkosalget som «en stor utfordring for samfunnet».

Det var bakteppet for at statsrådene fikk Postens samtykke til at politiets narkotikahunder skal ha adgang til å gjennomføre regelmessig søk i innenlandsposten. Utgangspunktet for den nye ordningen er Østlandsterminalen hvor 60 prosent av norsk post håndteres daglig.

Samtidig sa konsernsjef i Posten Dag Mejdell at Posten stiller seg bak et forslag om lovendring i etterkant av sakene våre. Lovendringen skal gi politiet adgang til å åpne brev uten en rettslig kjennelse og lette etterforskningen av slik narkotikakriminalitet.

Justisministeren lovte at politiet skal gå etter nettverkene på det mørke nettet i 2015:

- Skal man pågripe de som står bak distribusjon og omsetning så må man følge linjene fra kundene og bakover. Det skal prioriteres av politiet

8.2 PODs omverdenanalyse

Rundt en måned etter sakene ble jeg kontaktet av en politianalytiker fra Rogaland politidistrikt.

Analytikeren arbeidet med materiale som leveres til Politidirektoratets omverdenanalyse for 2015. Omverdenanalysen er et dokument som POD sender ut til landets politidistrikter som skal ta for seg trender og utfordringer innenfor ulike kriminalitetsområder.

«Omverdenanalysen skal være ett av bakgrunnsdokumentene som POD bruker til sin flerårige virksomhetsplan, men den skal også ligge til grunn når politidistrikter og særorgan skriver egne strategiske analyser.»

Analytikeren var opptatt av funnene og modus som ble beskrevet i Adresseavisens saker, og ville inkludere det i den neste omverdenanalysen. Politidirektoratets omverdenanalyse utgis i april 2015.

Trondheim, 14. januar 2015

Jonas Alsaker Vikan

Ole Martin Wold

9. Publiseringsliste

5.11: Adressa Pluss «silkeveiene» (Hovedsak)

6.11: Adresseavisen s. 1 og s. 8, 9, 10 og 11

6.11: Adressa.no - Kryptomarkeder er en trygg havn for kriminelle

6.11: Adressa.no Internasjonal storaksjon mot det skjulte narkotikasalget

7.11: Adresseavisen s. 1 og s. 2 og 3

7.11: Adressa.no Stengte svensk narkomarked

8. 11: Adresseavisen s. 8

10.11: Adresseavisen s. 10

11.11: Adressa.no Her eksploderer antallet anonyme norske nettbrukere

11.11: Adresseavisen s. 1 og 2, 3 og 4

14. 11: Adresseavisen s. 2 og 3

15.11: Adressa.no Narkonettverk gir opp

15.11: Adresseavisen s. 10, 11 og 12

1.12: Adressa.no Norske nettverk fortsetter å spy ut narkotika

3.12: Adressa.no – Et stort problem

3.12: Adressa.no – Svært alvorlig og omfattende kriminalitet

3.12: Adressa.no – En stor utfordring for samfunnet

4.12: Adresseavisen s. 7

20.12: Adressa.no Fikk årevis i fengsel for skjult narkosalg

2015

05.01: **«Mesterhjerne» kan få 30 år i fengsel**

14.01: **Er dette internetts Pablo Escobar?**

10. Vedlegg

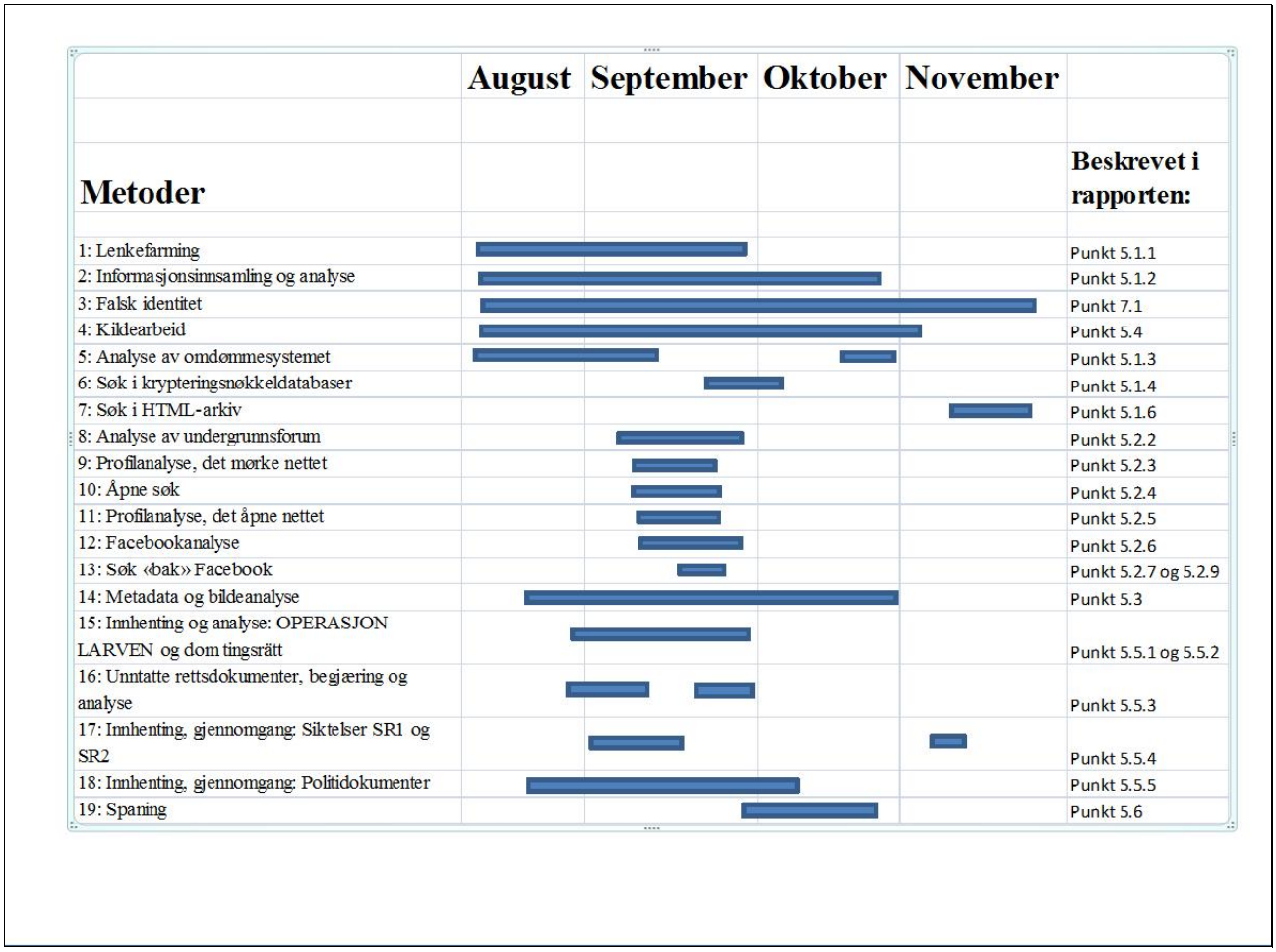
10.1 Hjelpemidler

Undersøkelsene på det mørke nettet krevde at jeg måtte lære meg flere program og tekniske hjelpemidler. De fleste var helt nye for meg.

Under er en oversikt med kobling mot hvilke metoder de ble brukt i forbindelse med.

1) TOR (se punkt 5.1.1 til og med 5.2.3)
2) Yopmail (se punkt 5.1.2 og 7.1)
3) Excel (se punkt 5.1.2)
4) Countermail (se punkt 5.1.4 og 5.4)
5) OSINT-søk (se punkt 5.2.6, 5.2.7 og 5.2.9)
6) Steam (se punkt 5.2.4)
7) Exif viewer (se punkt 5.1.2 og 5.3)
8) TOR Chat (se punkt 5.4)
9) Sublime text (se punkt 5.1.6)

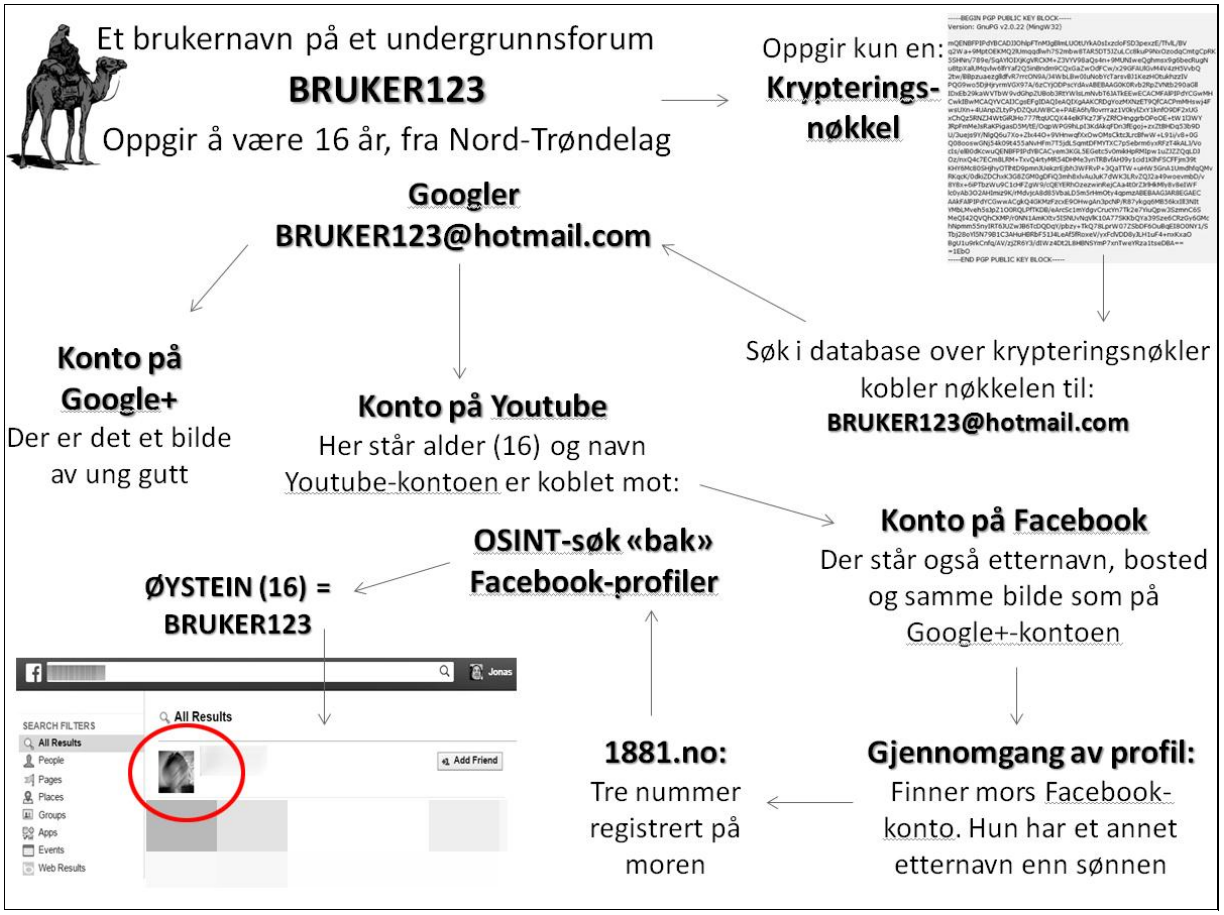
10.2 Metodeoversikt



Figur 10 De ulike metodene som ble brukt i saken, og cirka når de ble brukt i løpet av arbeidsperioden.

10.3 OSINT-kart

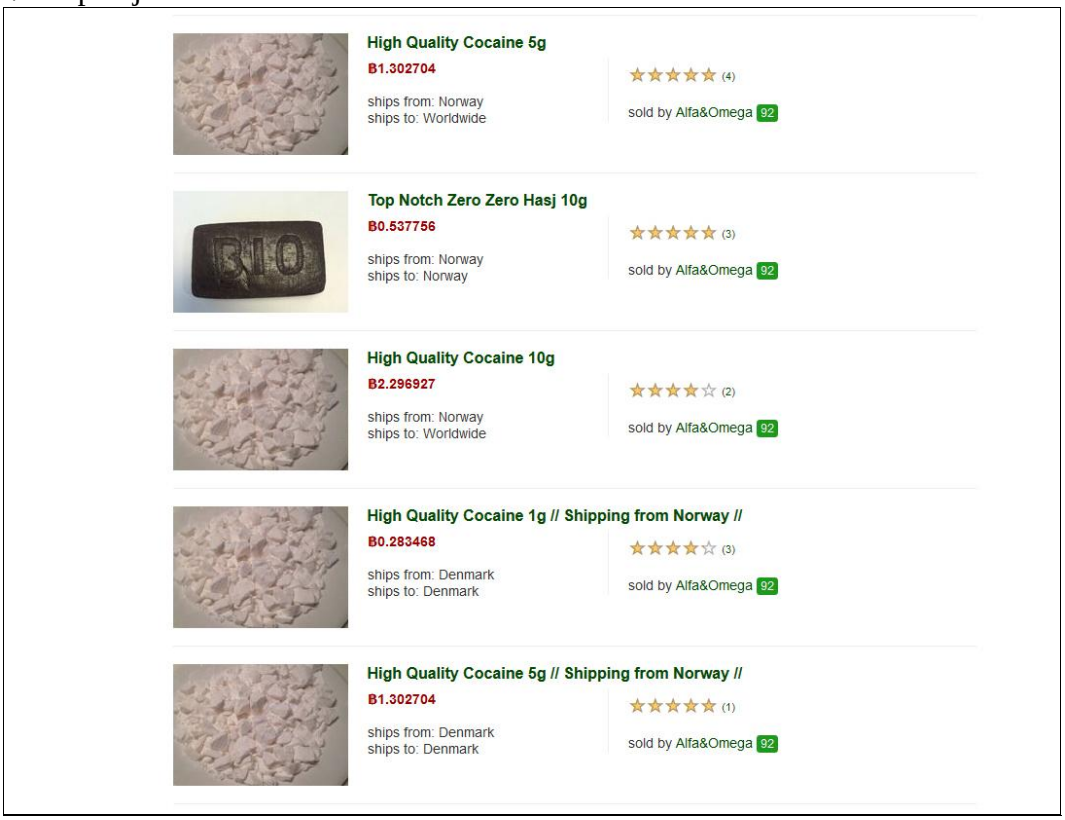
Fremgangsmåten fra BRUKER123s profil på det mørke nettet til å lokalisere ham i den virkelige verden, via profiler han brukte på det åpne nettet (se punkt 5.2.2 – 5.2.7).



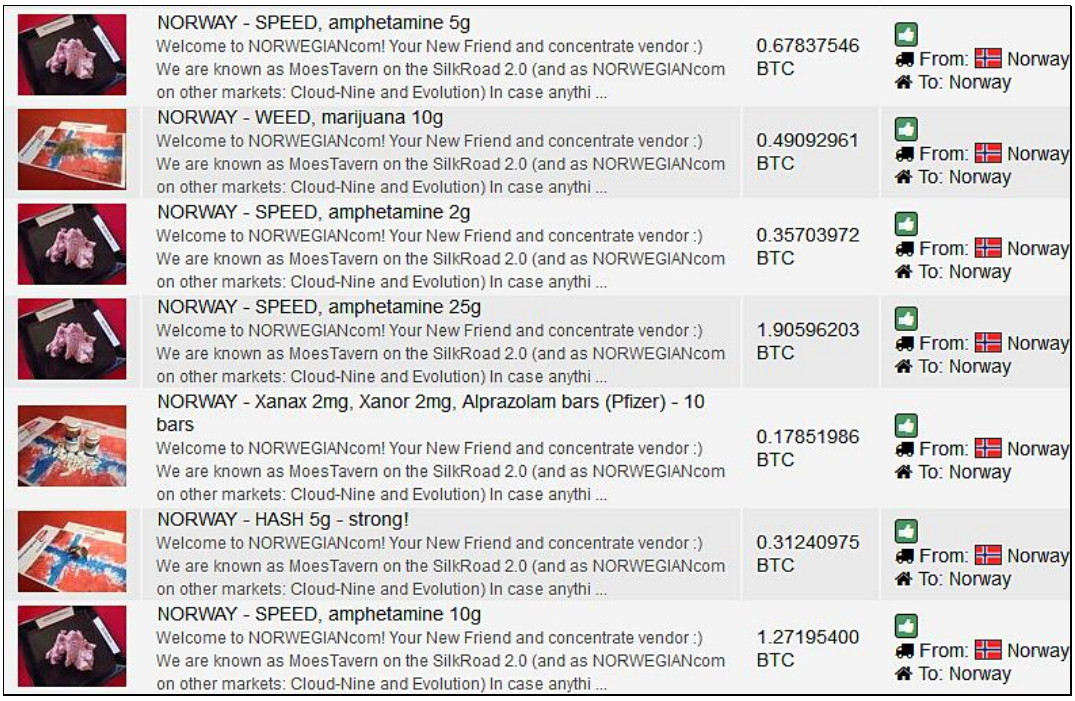
Figur 11 Visualisering av fremgangsmåte for deanonymisering av BRUKER123 på det mørke nettet.

10.3 Prislister

Dette er eksempler på varebeholdningen og prislistene til to norske nettverk som ble undersøkt i prosjektet.



Figur 12 Deler av vareutvalget til det norske nettverket ALFA&OMEGAs høsten 2014. Skjermbilde tatt på Silk Road 2



Figur 13 Deler av vareutvalg og prisliste til det norske nettverket NORWEGIANcom høsten 2014. Skjermbilde tatt på Agora

10.4 Trusler / sjikane

I etterkant av publisering var flere av nettverkene rasende på materialet i sakene.

1)

Her skriver et av de mest aktive norske nettverkene, FOXHOUND NORWAY, at jeg er i fare på grunn av innholdet i «silkeveiene».


Re: Artikkel om norsk aktivitet på deepweb

by FoxHoundNorway » 09 Nov 2014, 19:54

Jeg spurte journalisten om ID slik at vi har identiteten hans for.. la oss kalle det senere bruk..Han trodde det bare var for å avkrefte at han var politi, nå har vi bilde og navn på han. Denne artikkelen setter oss i fare, så ja nå er han i fare!!

Fokuser heller sinnet deres på den som faktisk er fienden her, avisa, journalisten og politiet.

Vi er å finne på Evolution Market nå.

Hilsen
FHN

2)

En måned etter publisering diskuterer norske brukere av et hemmelig forum om «Operasjon Narkospam» skal igangsettes ved at det bestilles narkotika som sendes til myndighetspersoner og journalisten.


Re: Artikkel om norsk aktivitet på deepweb

by Freedomwillreign » 04 Dec 2014, 18:12

> freerida wrote:
> Spam postkassen til Anundsen, Solvik-Olsen, polititopper, politikere osv. med f.eks. noe muggen hasj, hundene markerer og makteliten sitter plutselig med et lite forklaringsproblem. Med litt flaks blir de sendt i fengsel, der får de muligheten til å gjenopprette bakkekontakten slik at de ser galskapen i den såkalte "krigen mot narkotika".

Haha god ide jeg donerer gjerne btc til det formålet jeg. Burde iaff prøve å få organisert noe så det blir sendt til privat adressen til alle på stortinget, og flere av disse "kjære" maktpersonene våre. Kanskje vår kjære Journalistvenn i Adressa burde på et brev også. Operasjon Narkospam synes jeg faktisk høres ut som en veldig god ide faktisk.

You cannot restrain or tame an idea with idle threats Once it has crept into the mind The mouth will not keep it in silence We will protest Because you cannot tell a concept to not raise it's fist in anger You cannot censor that which only exists intheory

10.5 Spaningsobjekt

Figur 14 Noen av stedene som vi holdt oppsikt med for å finne personer som hadde handlet på det mørke nettet.

10.6 Publiserte artikler

Hovedfunnene ble publisert i den digitale dokumentaren «silkeveiene» onsdag 5. november klokken 18.37. Tekstlengden var på 19 sider, cirka 40 000 tegn. Dokumentaren er vedlagt som en pdf-versjon av nettpubliseringen, men jeg anbefaler at den leses digitalt ved **å følge denne lenken**

Den digitale versjonen har noen spesielle funksjoner som ikke lar seg vise på pdf.

En kortversjon av dokumentaren ble publisert i Adresseavisen torsdag 6. november. Her ble også historien om 16-åringen som handlet narkotika på det mørke nettet fortalt. I løpet av den neste måneden gikk de fleste oppfølgingssakene i papirutgaven. Sakene (i ett pdf-dokument) er på 20 avissider.

De kan lastes ned **ved å følge denne lenken**