Mobilovervåkingen

Metoderapport til SKUP-prisen 2014

Per Anders Johansen

Andreas Bakke Foss

Fredrik Hager-Thoresen

Aftenposten

Tittel på prosjektet:
Mobilovervåkingen

Hvor og når publisert:
Aftenposten fra fredag 12. desember 2014 til torsdag 8. januar 2015. Arbeidet fortsetter i 2015.

Redaksjon og redaksjonsadresse/tlf:
Aftenposten
Akersgata 55
Postboks 1, 0051 Oslo
Telefon: 02286

Journalistenes adresse og telefonnummer:

Per Anders Johansen, mobil 975 40 345, per.anders.johansen@aftenposten.no
Andreas Bakke Foss, mobil 977 66 389, andreas.bakke.foss@aftenposten.no
Fredrik Hager-Thoresen, mobil 951 99 877, fredrik.hager-thoresen@aftenposten.no
Postadresse: Samme som redaksjonens adresse.


Per Anders Johansen


Andreas Bakke Foss


Fredrik Hager-Thoresen

Oslo, 15. januar 2015

Innholdsfortegnelse

1 Innledning 5

2 Avslaget som startet det hele 5

3 Starten: Et lite graveprosjekt om skjulte, falske sendere 7

4 Hva er genuint nytt i saken? 7

5 Organisering av arbeidet, metodebruk, kildebruk, kildekritikk og problemer underveis 8

5.1. Hva er en IMSI-catcher og en falsk basestasjon og hvordan lete etter dem? 8

5.2. CryptoPhone-undersøkelsene 9

5.2.1. Hva er en CryptoPhone? 10

5.2.2. Målingene starter 10

5.2.3. Å forstå tysk krypto-teknologi 11

5.2.4. De første dataanalysene 12

5.2.5. Bygging av stordatabasen 13

5.2.6. Laget forsterkes og arbeidet intensiveres 14

5.2.7. Oppsummering av de 56.000 CryptoPhone-målingene og 57 måleruter 14

5.3 Jakten på feilkilder 15

5.3.1. Kildemøter med vasking av data 16

5.4. Neste steg: Falcon-undersøkelsene 19

5.4.1. Indikasjoner, ja. Men ikke noen bevis 19

5.4.2. Nye hjelpere 19

5.4.3. Kildekritikk av sikkerhetsselskapene 20

5.4.4. Et veivalg: Gå videre eller nøye oss med det vi har? 20

5.4.5 Slik fungerte kontraetterretningsutstyret Falcon II 21

5.4.6. «Target One, Target Two og Target Three»: Den første undersøkelsen 21

5.4.7. Resultatene og analyse fra den første målingen 22

5.4.8. Den andre Falcon II-målingen 23

5.4.9. Datatekniske utfordringer med Falcon-målingene 23

5.4.10. Med åpne Falcon-kort 24

5.5. Hvor lenge kunne vi vente? 25

5.5.1 Når skulle vi publisere? 25

5.5.2. Om å legge alle kortene på bordet 26

6 Spesielle erfaringer og konsekvenser 27

6.1 Kildene som ble etterforskere og samarbeidsklimaet som ble til press 27

6.2 Et uventet og uanmeldt besøk til Aftenposten 28

6.3 «Av hensyn til den pågående etterforskning…» 28
6.4 To nye arbeidsgrupper og en forutsetning 28
6.5 Ubesvarte spørsmål 29
6.5.1. Sikkerhet og beskyttelse 29
6.5.2. Spørsmålet som startet det hele er fortsatt ubesvart 30
6.5.3. Signalene som forsvant 30
6.6 Sakens internasjonale ringvirkninger 30
6.6.1. Satt dagsorden over hele verden 30
6.6.2. Undersøkelser i andre land 31
6.7 En foreløpig avslutning og et møte i Stortinget 31

1 Innledning

Vi har lagt telefonene i et låst skap i gangen. Persiennene på det vintermørke rommet er nede og lukket. Dataskjermen i enden av rommet fylles med tall som løper nedover i rader og kolonner. Vår operatør er nettopp ferdig med den første målingen i Oslos gater.

Det er første gang han jobber med journalister. Før vi diskuterer resultatene, gir han oss en klar advarsel:

-Dere må vite at dere åpner Pandoras eske her nå. Dere må være klar over hvilke sterke krefter som vil komme og forsøke å hindre dere fra å omtale dette. Før dere velger å publisere dette, må dere være klar over hvilken dør dere åpner når dette kommer ut, sa han.

For første gang i Norge kartla Aftenposten i fjor høst bruken av mobilovervåkingsutstyr i Oslo. Sakene vi publiserte mellom 12. desember 2014 og 7. januar 2015[1] avslørte at en rekke hemmelige, falske basestasjoner, såkalte IMSI-catchere, høyst sannsynlig var i bruk rundt flere sentrale bygg i hovedstaden.

I arbeidet brukte vi helt nye journalistiske metoder i Norge. Alle grunnlagsdata, kildearbeid, metoder og resultater ble gjort åpent tilgjengelige for alle.

Tallene som rullet over skjermen denne formiddagen i starten av desember og det omfattende materialet Aftenposten samlet inn og presenterte gjennom en serie artikler, skulle tre uker senere føre til to politietterforskninger, minst et krisemøte, nedsettelsen av to nye arbeidsgrupper og en redegjørelse fra justis- og beredskapsminister Anders Anundsen (Frp) i Stortinget.

I minst åtte europeiske land jobber journalister i skrivende stund med de samme metodene som vi tok i bruk. I Oslo er signalene fra de fleste falske basestasjonene nå skrudd av eller endret.

Både politiet og PST etterforsker hvem som kan ha stått bak mobilovervåkingen i Oslo. Teleselskapene har startet arbeidet med nye tiltak for å beskytte mobilnettet vårt mot overvåking. Justis- og beredskapsministeren har igangsatt en arbeidsgruppe som vurderer nye metoder for å monitorere om falske basestasjoner er i drift. En rekke bedrifter, offentlig institusjoner og virksomheter har iverksatt ekstra rutiner for å beskytte seg.

Aftenpostens avsløringer har gjort det vanskeligere å bedrive storstilt, skjult overvåking av mobilbrukere i Norge.

2 Avslaget som startet det hele

Ideen som startet det hele, dukket opp da Per Anders jobbet med en serie artikler om sammenbrudd i mobilnettet i Norge i fjor. Han søkte bredt i offentlig elektronisk postjournal etter brevtitler med stikkordet «mobil*». En av journalpostene som vakte interesse, hadde tittelen «retningslinjer for varsling av mobilregulerte soner» i Politidirektoratet. Hva betyr det egentlig å opprette «mobilregulerte soner»? Hva i all verden gjør du når du «mobilregulerer»? Et typisk eksempel på finurlige, forvirrende og uforståelige ord fra norske byråkrater.

[1] Les alle sakene på: http://mm.aftenposten.no/mobilspionasje

Post- og teletilsynet
Norwegian Post and Telecommunications Authority

23 MAI 2014

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Vår ref.:1402493-1 - 549
Vår dato: 22.5.2014

Deres ref.:
Deres dato:

Saksbehandler: Linda Must

Retningslinjer for varsling ved oppretting av mobilregulert sone

Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 6-2a om mobilregulert sone ble tilføyd ekomloven ved lov 14. juni 2013 nr. 54 og trådte i kraft 1. juli samme år. Mobilregulerte soner opprettes ved at den vanlige trafikken i mobilnettet blir jammet, det vil si at det blir sendt ut signaler som interfererer med og blokkerer signalene mellom mobiltelefonene og infrastrukturen i mobilnettene, og/eller det blir etablert falske basestasjoner (oppfangere) som avslører mobiltelefonens identitet og deretter tar over telefonens kontakt med tilbyders basestasjon. Dette medfører som regel bruk av frekvenser som er tildelt andre enn den som oppretter slik mobilregulert sone.

Figur 1 Et postjournal-sak til å undres over: Hva er en "mobilregulerte sone"? Dette prosjektet startet da norske myndigheter nektet å opplyse om hvor ofte de «mobilregulerer» norske mobilbrukere.

Per Anders fikk innsyn i brevet 15. september i fjor. Brevet fra Politidirektoratet handlet om at Stortinget sommeren 2013 hadde innførte nye regler i Ekom-lovens par 6.2A.[2] Politiet, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) fikk adgang til å innføre slik soner, men skulle samtidig rapportere om dette til Post- og teletilsynet (PT).

Det mest interessante kom i neste siste avsnitt i vedlegget til direktoratets brev. Der lå et brev fra Post- og teletilsynet 23. mai, der tilsynet beskriver hvordan politiet hadde fått lov til å ta i bruk «falske basestasjoner» og «oppfangere»:

> «*I tiden som er gått etter at bestemmelsen trådte i kraft har ikke PT registrert at Politiet eller NSM har varslet myndigheten om at mobilregulert sone er opprettet, og PT har derfor funnet det hensiktsmessig å utarbeide retningslinjer for slik varsling*».

Noen enkle Google-søk på «mobilregulerte soner» ga flere interessante treff. Blant dem en svensk utredning fra 2010 om «Særskilda spaningsmetoder». Svenskene kalte utstyret for «imsi-catcher». Spørsmålet om «mobilregulerte soner» dukket også opp i enkelte artikler på Digi.no og Teknisk Ukeblad. De var også flere artikler tilbake til 2007 da det første forslaget om å endre Ekomloven ble lagt frem. Men da endringene i Ekom-loven til slutt faktisk ble vedtatt av Stortinget rett før sommeren 2013, etter syv år med forarbeider i Samferdselsdepartementet, fikk dette nesten ingen omtale.

Dagen etter innsynet i brevet sendte Aftenposten en begjæring etter paragraf 9 i offentlighetsloven til Post- og teletilsynet og rett til å kreve innsyn i en sammenstilling fra databaser. Vi ba om å få opplyst hvor ofte tilsynet hadde fått meldinger om at «mobilregulerte soner» var innført i Norge.

Avslaget kom raskt. Tilsynet mente dette var informasjon som måtte være hemmelig «*fordi innsyn ville motvirke offentlig kontroll- eller reguleringstiltak eller andre pålegg eller forbud, eller føre til*

[2] Se vedlegg 5. Brev fra POD om «Retningslinjer for varsling ved oppretting av mobilregulert sone», samt vedlagt brev fra Post- og teletilsynet datert 23. mai 2014.

fare for at de ikke kan gjennomføres[3]». Tilsynet la også til at vi ikke kunne få innsyn fordi «*innsyn ville lette gjennomføring av straffbare handlinger*[4]». Aftenposten klaget, men avslaget blir opprettholdt. Klagen ble anket til Samferdselsdepartementet, som sto fast ved avslaget.

Norske myndigheter ville ikke fortelle oss hvor ofte de selv brukte IMSI-catchere eller falske basestasjoner. Ifølge avslaget ville det bli enklere å begå kriminalitet hvis Aftenpostens lesere fikk vite hvor ofte politiet, PST og NSM «mobilregulerte». Vi var uenige i denne vurderingen.

Det er lett og fristende å legge saken til side når dørene blir stengt. Denne gangen fungerte det motsatt. Avslaget ga motivasjon til at vi selv ville forsøke å finne ut om slikt mobilovervåkingsutstyr var i bruk i Norge. Men hvordan skulle vi klare å avdekke dette når alle dører var lukket?

3 Starten: Et lite graveprosjekt om skjulte, falske sendere

I starten av oktober i fjor sendte Per Anders en epost til Tone Tveøy Strøm-Gundersen, avdelingsleder i nyhetsredaksjonen, der han beskrev «et lite graveprosjekt» om «de skjulte falske senderne som overvåker din mobil».

Målet og bakgrunnen ble beskrevet slik:

> «Mål: *Avsløre om det finnes falske basestasjoner i Oslo, som brukes til å overvåke deg uten at du vet noe som helst».*
>
> *Bakgrunn: Norske myndigheter – og privatpersoner, kriminelle, selskaper og fremmed etterretning – kan med relativt enkle virkemidler sette opp en basestasjon hvor som helst, og fange opp alle mobiltelefonene som beveger seg i området».*

En av metodene han i utgangspunktet ville teste ut, var den tyske krypterte mobiltelefonen CryptoPhone, som ifølge flere amerikanske presseoppslag kunne brukes til å oppdage falske basestasjoner. [5]

Det skulle vise seg å ende som det største og mest omfattende journalistiske graveprosjektet som trolig har vært gjort noe sted i verden om bruken av falske basestasjoner.

4 Hva er genuint nytt i saken?

Vi lister her opp hva som er genuint nytt i det sakene dokumenterer, og hvilke nye metodegrep vi brukte:

1) Sakene og kartleggingen avslørte at hemmelige, falske basestasjoner, såkalte IMSI-catchere, med svært høy sannsynlig er i bruk rundt flere sentrale bygninger i hovedstaden som Stortinget, Slottet, kontorene til statsministeren og forsvarsministeren i Kvadraturen, Norges Bank, Regjeringens representasjonsbolig, Parkveien og en rekke ambassader.

[3] Paragraf 24. første ledd
[4] Paragraf 24 tredje ledd.
[5] En av de første artiklene vi googlet oss frem til da vi søkte på «IMSI-catcher», var i Popular Science 27. august http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls. Senere skrev også Washington Post om dette, og flere andre amerikanske nettsteder. http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html

2) Vi dokumenterte også at det med svært høy sannsynlighet sto overvåkingsutstyr på Aker brygge og Tjuvholmen. Utstyret gjør det mulig å spionere på næringsdrivende, advokater og andre som forvalter forretningshemmeligheter og milliarder av kroner.

3) Vi har brukt metoder, research og verktøy som aldri før er brukt av journalister i Norge. Hverken politiet, Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet eller noen forskningsmiljøer har noensinne gjort en like omfattende kartlegging av faren for mobilovervåking. Vi kjenner heller ikke til at dette er gjort i samme målestokk noe annet sted i verden.

4) Med høy presisjon kunne vi anslå hvor de falske basestasjonene opererte, hvilke områder de dekket og hva slags signaler de sendte ut for å lokke til seg mobiltelefoner. Funnene ble oversendt på forhånd til en rekke aktører.

5) Aftenpostens artikler dokumenterte at norske myndigheter og teleselskapene kan gjøre langt mer for å beskytte mobilbrukere mot ulovlig overvåking enn de tidligere har gjort.

6) Dette var første gang den tyskproduserte CryptoPhone 500 ble for brukt i Europa til omfattende journalistisk research, selv om den tidligere var benyttet i USA i august og september. Vi gikk imidlertid langt mer systematisk til verks enn i USA, hvor undersøkelsene i stor grad basert seg på produsentens og enkeltkundenes egne målinger. Mens amerikanske medier målte et par dager, valgte vi å gjøre omlag 50.000 målinger spredt over 57 forskjellige måleturer i halv annen måned, som dekket 100 kilometer med veier i Oslo-området. Det er i seg selv den største og grundigste undersøkelsen som er gjort med denne telefonen.

7) Vi valgte å gå et stort steg videre, og tok i bruk avansert kontraetterretningsutstyr (Falcon II+)[6] som en del av et journalistisk prosjekt. Vi samarbeidet med tidligere etterretningsfolk i private sikkerhetsselskaper for å sjekke funnene langt grundigere.

8) Vi publiserte alle våre rådata, slik at hvem som helst kan undersøke og ettergå hva vi gjorde.

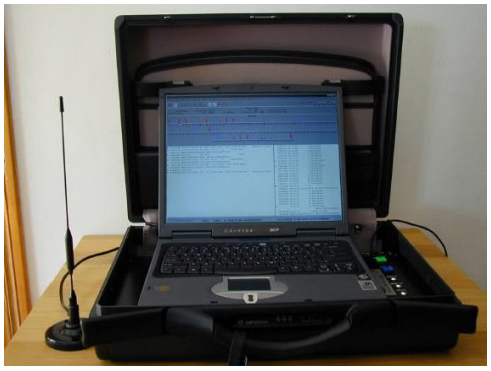
5 Organisering av arbeidet, metodebruk, kildebruk, kildekritikk og problemer underveis

Myndighetene ville ikke fortelle oss hvor ofte de brukte falske basestasjoner. De stengte dørene. Men kunne vi som journalister selv forsøke å finne aktivitet fra falske basestasjoner i Oslo? Kunne vi til og med forsøke å finne ut hvor de var i bruk? Og hvor mange?

5.1. Hva er en IMSI-catcher og en falsk basestasjon og hvordan lete etter dem?

En IMSI-catcher er en falsk basestasjon, som later som om den er en del av det lovlige regulære mobilnettet. Det er overvåkingsutstyr som har vært i brukt i ca. 15 år. Snowden-dokumentene viste at bruken er svært omfattende over hele verden. For 5-6 år siden var det dyrt å anskaffe slikt utstyr. I dag kan du kjøpe brukbare IMSI-catchere for ca. 10.000 kroner.

[6] Se vedlegg 7 for teknisk beskrivelse av Falcon II+



Figur 2 Et eksempel på hvordan en IMSI-catcher ser ut, i form av en laptop med en antenne.

Basestasjonene later som om den er ekte ved å kopiere data fra en annen ekte basestasjon, og sender ut radiosignaler som lokker til seg mobilene i området. Når en mobil kobles til en falsk basestasjon/IMSI-catcher, er det mulig å hente ut data som kan brukes til å identifisere brukeren av mobilen og hvor han eller hun befinner seg.

Det finnes svært mange ulike typer falske basestasjoner og IMSI-catchere. Avhengig av hva slags IMSI-catcher du har, kan du avlytte samtaler, eller kartlegge hvor personer befinner seg og hvem de møter. Det er også mulig å legge inn spionprogrammer på mobilen, slik at mobilens mikrofon slås på og kan brukes til romavlytting. En falsk basestasjon kan også brukes til å jamme nettet og stoppe mobiltrafikken. IMSI-catcheren er liten, mobil og kan skjules i et vindu, en bil eller jakke. Den kan se ut som en helt vanlig datamaskin, en radio eller en liten stang. Den kan slås av og gjemmes vekk raskt og enkelt.

Den store ulempen med slikt overvåkingsutstyr, er at det lager mye støy på radiofrekvensene. De falske basestasjonene sender ut sterke og uvanlige signaler for å gjøre seg attraktiv. Det er disse signalene som gjør det mulig å avsløre dem – og oppdage i hvilke områder de befinner seg. Men for å finne dem, må du første lete. Og du må ha utstyr, kunnskap og vilje til å gjøre det.

5.2. CryptoPhone-undersøkelsene

Dagen etter at vi ba om innsyn i hvor ofte norske myndigheter brukte slikt utstyr, skrev avisen Washington Post[7] om hvordan flere falske basestasjoner i den amerikanske hovedstaden ble avslørt ved hjelp av en spesialbygget kryptert telefon. Per Anders kontaktet ESD America, produsenten av CryptoPhone i USA, og sa at vi var interessert i å undersøke om det er aktive IMSI-catchere også i Oslo. Vi ble sendt videre til Bjørn Rupp, direktør i det tyske selskapet GMSK i Berlin, som lager den avanserte mobiltelefonen CryptoPhone 500 og vi ba om et eksemplar for undersøkelser i Norge[8].

Selskapet henviste til deres norske selger og leverandør, Multisys[9]. De var positive og 9. oktober i fjor hadde Aftenposten, som de første i Norge, kryptofonen med spesialbygget software i hendene i Akersgata 55. Selskapene så selvfølgelig en mulighet til å få omtale. Vi så muligheten til å prøve ut nye metoder og teste teknologien.

[7] En av de første artiklene vi googlet oss frem til da vi søkte på «IMSI-catcher», sto i Popular Science 27. august http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls. Senere skrev også Washington Post om dette, og flere andre amerikanske nettsteder og TV-stasjoner prøvde ut mobilen. http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html

[8] http://www.cryptophone.de/

[9] http://www.multisys.no/

5.2.1. Hva er en CryptoPhone?

CryptoPhone er en mobil som gjør det mulig å kommunisere kryptert og svært sikkert. Mobilen er en ombygget Samsung Galaxy SIII tømt for all programvare, som deretter er erstattet med svært avlyttingssikker software. Dette er en av flere sikre, krypterte mobiler på markedet, som har fått økt oppmerksomhet etter Snowden-avsløringen.

Det som imidlertid gjorde telefonen mest interessant for oss, var en av mobilens programvarer, det såkalte «Baseband Firewall»-programmet. Dette er utviklet med forskningsstøtte fra tyske myndigheter for å beskytte mot overvåking, avlytting og tapping av mobilkommunikasjon[10].

Programvaren prøver å oppdage sikkerhetstrusler mot mobilen ved å analysere hva som skjer på de to operativsystemene i mobilen: Det åpne operativsystemet til mobilen som utfører oppgaver hver gang du som gjør noe med mobilen (for eksempel IOS på Apple) og det «skjulte» operativsystemet til mobilens basebånd.

Selv om vi alle bruker mobilen hele tiden, er få klar at mobilen også har en basebånd-prosessor. Basebåndet sørger for at mobilen hele tiden har kontakt med nettet, og utveksler data noen få sekunder med basestasjoner i nærheten for å velge den beste.

Dersom operativsystemet til basebåndet og operativsystemet til mobilen oppfører seg unormalt i kontakten med basestasjoner rundt seg, kan Baseband Firewall varsle om dette. Når for eksempel operativsystemet til basebåndet på mobilen er i aktivitet, uten at mobilen er i bruk på noen som helst måte, er dette avvik som oppdages.

Figur 3 GSMKs CryptoPhone i bruk utenfor Slottet. Foto: Andreas Bakke Foss

Jo flere indikasjoner og avvik, jo høyere varselnivå. Basewall Firewall reagerer også hvis mobilnettverkets kryptering blir slått av, eller om mobilen din blir flyttet fra 3G/4G til 2G – noe som kan være tegn på at du blir avlyttet. Den reagerer også hvis mobilen kommuniserer på basebåndet og sender ut større mengder data, uten at mobilen er i bruk.

GSMK har en kildekode som er åpent tilgjengelig, slik at uavhengige kilder kan granske om krypteringen har svakheter eller bakdører. Dessuten er det mulig å hente ut datalogger fra mobilens program.

5.2.2. Målingene starter

Per Anders begynte å gå, sykle og kjøre rundt i Oslo med telefonen, samtidig som han hadde aktiv GPS-sporing på sin egen telefon.[11] På den første turnusfrie dagen tok kan den første av flere heldags bilturer for å få dekket et større område av Oslo. Deretter ble måleturene gjort på sykkel eller til fots.

Det første utslaget på brannmurprogrammet til den tyske mobilen kom ved Ramstadsletta på Drammensveien. En rød strek spratt opp på mobilen, og meldingen «Very high suspicion» dukket opp. På veien inn til Oslo ga mobilen utslag tre steder ved Lysaker, Skøyen og Aker Brygge. Inne i

[10] http://www.mobileeurope.co.uk/Press-Wire/german-government-calls-in-gsmk-cryptophone-to-ward-off-cyber-attacks

[11] Vi brukte app'en MyPath, først og fremst fordi det var lett å eksportere dataene i ulike filtyper. Det finnes mange andre tilsvarende programmer også.

sentrum blinket mobilen flere ganger ved Utenriksdepartementet, Karl Johans Gate og i Akersgata. Det skulle bli mange flere. Etter hver tur sendte Per Anders GPS-dataene til sin epost.

Da Popular Science, Washington Post og andre amerikanske medier skrev om sine resultater, hadde de bare brukt to-tre dager på målinger. Vi hadde ambisjoner om å gå langt grundigere til verks. Tanken var i utgangspunktet å måle tre-fire uker. Dessuten var planen å bytte sim-kort underveis, slik at vi fikk gjort målinger med abonnement fra både Telenor og Netcom.

Etter hver femte tur ble loggene eksportert fra kryptofonen og konvertert til Excel. Deretter ble avvikene sortert ut og lagt i et eget arbeidsdokument. Avvik merket både «high suspicion» og «very high suspicion» ble samlet og notater knyttet til observasjoner fra målingene ble lagt inn. Det kunne være opplysninger om området, hvilke virksomheter som var i nærheten og om det ble observert noe uvanlig, eksempelvis stor biltrafikk eller politibiler.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Dato og tid	Type mobi	Operatør	Signal	Weight	Weight 2	Finnes noe	Sted	Beskrivelse	Speed	Latitude	Longitude
53	28.10.14 15:20	3G-nett	Netcom		Signalstyrke: 24	Vekt: 1.00	0	Møllergata	Utenfor Møllergata 19	0,97	59.915078	10.747962
54	29.10.14 10:49	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 15	Vekt: 1.10	0	Briskebyveien	Utenfor Vinmonopolet	2,92	59.920702	10.717141
55	29.10.14 10:53	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 19	Vekt: 1.10	0	Parkveien	Ved Fritt Ord/Israels ar	4,8	59.919746	10.727046
56	04.11.14 12:19	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 16	Vekt: 1.10	0	Majorstuveien	Ved krysset Kirkeveien	4,95	59.928213	10.715268
57	04.11.14 12:28	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 16	Vekt: 1.10	0	Fridtjof Nansens vei	Ved Oslo Rådhus	5,15	59.91265	10.732927
58	04.11.14 12:30	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 19	Vekt: 1.10	0	Rådhusgata	Ved Kafe Skansen	2,66	59.910421	10.738142
59	04.11.14 12:40	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 23	Vekt: 1.10	0	Akershusstranda	Mellom Statsministere	10,9	59.905246	10.744208
60	04.11.14 12:44	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 24	Vekt: 1.10	0	Grev Wedels plass/Langkai	Ved havnelageret	4,64	59.906908	10.745816
61	04.11.14 12:54	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 18	Vekt: 1.10	0	Dronningens gate	Utenfor Norges Bank	3,87	59.908242	10.744233
62	04.11.14 12:54	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 24	Vekt: 1.10	0	Revierstredet	Mellom Norges Bank o	3,26	59.908194	10.743482
63	04.11.14 13:02	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 17	Vekt: 1.10	0	Skippergata	Kvartalet Prinsens gate	4,883002	59.910942	10.748014
64	04.11.14 13:05	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 26	Vekt: 1.10	0	Biskop Gunnerus gate	Ved krysset Fred Olsen	2,92	59.912159	10.750901
65	05.11.14 16:34	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 20	Vekt: 1.10	0	Apotekergata	Utenfor VG/Aftenpost	0	59.915056	10.743292
66	06.11.14 08:55	3G-nett	Netcom	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 20	Vekt: 1.10	0	Myntgata	Utenfor Forsvarsdepar	6	59.908332	10.740887
67	07.11.14 08:55	3G-nett	Telenor	Data: Ukjent aktivitet i 4 sekunder	Signalstyrke: 25	Vekt: 1.40	0	Karl Johans gate	Ved Nationalteateret s	0	59.915021	10.734563
68	07.11.14 11:19	3G-nett	Telenor		Signalstyrke: 25	Vekt: 1.00	0	Akersgata	Utenfor VG/Aftenpost	0	59.914848	10.743346
69	08.11.14 15:50	3G-nett	Telenor	Data: Ukjent aktivitet i 3 sekunder	Signalstyrke: 17	Vekt: 1.30	0	Fillipstad	Avkjøring E18 mot Ake	18,700001	59.909787	10.717706
70	08.11.14 18:19	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund	Signalstyrke: 30	Vekt: 1.10	0	Akersgata	Krysset Akersgt/Lille Gi	3,38	59.91373	10.742475
71	08.11.14 18:57	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 29	Vekt: 1.10	0	Lille Grensen	Lille Grensen/Karl Joha	1,565146	59.91367	10.740821
72	08.11.14 23:28	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 25	Vekt: 1.10	0	Møllergata	Ved Møllergata 19	5,72	59.915378	10.748441
73	08.11.14 23:28	3G-nett	Telenor	Data: aktivitet i 5 sekunder.	Signalstyrke: 21	Vekt: 1.50	0	Møllergata	Ved Møllergata 19	2,79	59.915112	10.74807
74	08.11.14 23:36	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 20	Vekt: 1.10	0	Munkedamsveien	Utenfor Thon Hotel Vik	13,21	59.911168	10.725226
75	09.11.14 15:33	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 18	Vekt: 1.10	0	Ramstadsletta	E18 retning Oslo	23,030001	59.896936	10.565159
76	09.11.14 15:45	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 20	Vekt: 1.00	0	Parkveien	Mellom Colbjørnsens g	13,47	59.916888	10.722863
77	09.11.14 15:59	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 24	Vekt: 1.10	0	Akersgata	Gangvei mellom regjer	1,42	59.916204	10.745415
78	10.11.14 00:39	3G-nett	Telenor	Data: Ukjent aktivitet i ett sekund.	Signalstyrke: 23	Vekt: 1.10	0	Grubbegata	Like ved Hammersborg	6,46	59.917678	10.747351

Figur 4 Slik så loggene ut etter å ha blitt konvertert fra CryptoPhone-loggen til Excel etter de første ukene med måleturene.

Allerede etter tre-fire målinger ble det klart at mobilen ga veldig mange utslag. Når mobilen viste rødt gang på gang, fremsto det som åpenbart at artiklene i USA var basert på altfor korte og overfladiske undersøkelser: Her kunne det være mange falske avvik, ikke minst fordi mobilen ga mange utslag ved tunneler og broer.

13. oktober fikk den norske leverandøren av kryptofonen, Multisys, flere tekniske spørsmål fra oss.[12] Det grunnleggende spørsmålet var om det var feilkilder eller alternative forklaringer som kunne forklare avvikene. Samtidig stilte vi en rekke spørsmål knyttet til rådataene for å kunne forstå absolutt alt som foregikk, hvordan programvaren fungerte og var bygget opp, og hva som egentlig lå til grunn for de ulike «svært mistenkelige» avvikene.

Eposten illustrerer en av de største utfordringene i dette prosjektet: I tillegg til å grave og lete etter mulige falske basestasjoner, brukte vi mest tid på å lære oss og forstå teknologi, programvare, mobiler, basestasjoner, tekniske beskrivelser og problemstillinger som var svært kompliserte. Multisys var imøtekommende og åpne, men spørsmålene vi stilte viste seg fort å være så kompliserte at de måtte videresendes til produsenten og teknikerne til GSMK i Berlin. Det gikk lang tid å få svar og purringer måtte til.

[12] Vedlegg 12. Epost med spørsmål datert 13. oktober.

Først 28. oktober fikk Per Anders en telefonsamtale med dr. Bjørn Rupp, direktør i det tyske selskapet hvor han svarte muntlig på de mange spørsmålene vi hadde. GSMK tilbød seg også å gjøre en egen, selvstendig analyse av loggene våre når vi var ferdig, noe vi sa ja takk til.

Samtalen ga noen svar, men var langt fra nok. Samtidig ble det klart at spørsmålene vi stilte, kom inn på det som kunne berøre selskapets forretningshemmeligheter. GSMK hadde forsket flere år og brukt store ressurser på å utvikle Baseband Firewall, og dette var en viktig del av forretningsideen. Vi måtte begynne å kommunisere kryptert med GSMK, og Per Anders utvekslet pgp-nøkkel med Rupp.

Først senere i prosessen forsto vi at mange av spørsmålene vi stilte, gikk rett inn tekniske spørsmål som GSMK jobbet med. Vi hadde oppdaget problemstillinger som faktisk nå fører til at en av de seks «reglene» i Baseband Firewalls programvare trolig blir justert i neste versjon.[13]

Samtidig viste GSMK en stor grad av åpenhet, særlig når de forsto at vi var villig til å bruke tid og ressurser på å komme til bunns i dette.

5.2.4. De første dataanalysene

Nyhetsutvikler Fredrik ble tidlig med i prosjektet for å organisere det enorme datamaterialet som kom inn fra hver tur. Allerede i midten av oktober var han og Per Anders i gang med en database der alle måledata og GPS-lokasjoner først ble lagt inn i et arbeidsdokument og deretter koblet til kartdata for Oslo.

Første versjon av det interaktive kartet var kun ment for bruk i research-fasen og ble laget etter de første rundene med CryptoPhone i Oslos gater. Dette var svært nyttig for å kunne planlegge nye måleturer. Kartene gjorde det lettere å se mønstre i avvikene og avgjøre hvor vi burde undersøke nærmere. Loggdata fra mobilen, samt posisjonsdata fra GPS-applikasjonen ble fortløpende vasket[14] og samkjørt i en relasjonsdatabase. De ble deretter eksportert til geoJSON-format, for visuelt å kunne fremstilles i et interaktivt kart.

Applikasjonen ble kodet i Javascript og Leaflet med kartgrunnlag fra OpenStreetMap/CartoDB. Dette resulterte i et Oslo-kart hvor vi kunne markere alarmoppføringer med ulike fargekoder som representerte ulik grad av signifikans fra «veldig høy» til «ingen». Kartet ga en pekepinn på hvor utslagene hadde vært, og hvor alvorlig programvaren i kryptofonen vurderte dem å være.

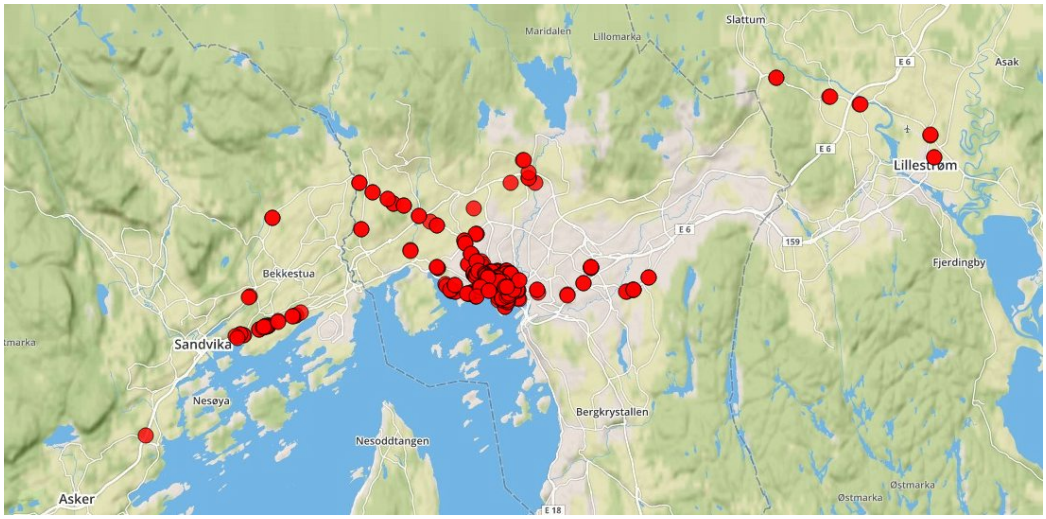
Det vil sprenge rammen for denne metodeoppgaven å nevne alle de ulike journalistiske ideene som kom opp mens vi målte, men her er noen:

- I Parkveien, Kvadraturen og ved Karl Johan/Stortinget fikk vi systematisk utslag. Hva slags utstyr kunne være utplassert her som førte til disse utslagene?
- Noen av de sterkeste utslagene fikk vi da Per Anders målte i område rundt Oslo Freedom Forum 20-21. oktober. Her var noen av verdens fremste menneskerettighetsaktivister samlet. Kunne ha vært overvåket?
- Ved flere innfartsårer var det mange utslag – foregikk det en form for systematisk overvåking av mobiltrafikk ved Lyssaker, Skøyen og Aker Brygge?

[13] Se vedlegg 6 «GSMK Baseband Firewall Technical Briefing», side 4.

[14] Med vasking menes eksempelvis å splitte opp kolonner som "går over i hverandre", eller konvertere tidskoder til et identisk og sammenlignbart format. Til dette formålet ble det brukt verktøy som csvkit, SQL, og/eller "regular expressions" i teksteditoren Sublime Text 3.

- Hvorfor forsvant de fleste signalene om kvelden? Og hvorfor var det så mange flere avvik på torsdager og fredager – og mindre i begynnelsen av uken?
- Og hvorfor lyste mobilen som et juletre da vi kjørte gjennom Møllergata sent en lørdagskveld?



Figur 5 Oversiktsbilde etter de første to ukene med CryptoPhone-målinger før vi startet kildekritikken for å fjerne «false positives».

Vi fikk etter hvert så mange avvikspunkter og oppføringer at det ble hensiktsmessig å sortere resultatene kronologisk. De påfølgende versjonene av kartet lot seg derfor filtrere på dag. De viste når på døgnet kryptofonen hadde vært i bruk, samt mer utfyllende metadata om punktene om man klikket seg videre. Dermed ble det mulig å identifisere områder med ulikt mønster av alarmtidspunkter hvis man hadde vært på samme område flere ganger.

«De svært mistenkelige» avvikene ble også gjennomgått manuelt for å filtrere ut feilkilder og svakheter i måleområdene. Utsnitt fra disse kartene og det vaskede datasettet ble videre brukt som dokumentasjon da vi senere skulle innhente uavhengige vurderinger eksternt.

5.2.5. Bygging av stordatabasen

Samtidig som målingene pågikk og vi brukte den første versjonen av dataene, jobbet Fredrik med å finne en måte å samle alle loggdata i en stor database. Dette tok mye tid, men viste seg å være svært verdifullt.

En fordel var at vi da kunne gjøre raskere sammenligninger og kalkuleringer på tid, sted eller andre målingsparametere. Det gjorde det også lettere å organisere og legge til nye rader fortløpende, noe som var nødvendig i et prosjekt av dette formatet. Nye data kunne fortløpende legges inn, enten det kom som journalistisk redigerte Excel-dokumenter, rådata fra kryptofonens basebånd-logg eller koordinater fra mobilens GPS-applikasjon.

Med databasen kunne vi eksempelvis hente ut alle tilfeller av alarmer høyere enn ”lav” for et bestemt område i et bestemt tidsrom og kombinere disse med andre referansekilder. Det ble utviklet rutiner for å eksportere utdrag fra slike spørringer direkte til interaktivt kart, slik at man raskt kunne sjekke opp enkeltområder, eller konkrete celler i mobilnettet.

```
group by Lat, Lng
ORDER BY id */

SELECT gps.id, gps.dato, Sted, Beskrivelse, vh_filtered.Latitude, vh_filtered.Longitude, vh_filtered.Weight FROM gps LEFT JOIN
 vh_filtered ON vh_filtered.`Latitude` = gps.lat AND vh_filtered.`Longitude` = gps.lon WHERE Sted IS NOT NULL
```

Query Favorites ▾ Query History ▾ Run Current

id	dato	Sted	Beskrivelse	Latitude	Longitude	Weight
4063	2014-10-11 14:20:26	Ramstadsletta	E18 retning Drammen	59.898305	10.572513	Signalstyrke fra ukjent basest…
4066	2014-10-11 14:20:30	Ramstadsletta	E18 retning Drammen	59.898062	10.570787	Signalstyrke fra ukjent basest…
4067	2014-10-11 14:20:31	Ramstadsletta	E18 retning Drammen	59.898104	10.570413	Vekt: 1.00
4735	2014-10-15 08:37:11	Ramstadsletta	E-18 retning Oslo	59.898007	10.570028	Vekt: 1.00
13294	2014-10-15 14:40:04	Operagaten	Utenfor Operaen	59.908019	10.753915	Signalstyrke fra ukjent basest…
13295	2014-10-15 14:40:05	Operagaten	Utenfor Operaen	59.908064	10.753737	Vekt: 1.00
22736	2014-11-04 12:40:48	Akershusstranda	Mellom Statsministerens kontor og…	59.905246	10.744208	Signalstyrke fra ukjent basest…
22819	2014-11-04 12:44:46	Grev Wedels plass/Langkaia	Ved havnelageret	59.906908	10.745816	Signalstyrke fra ukjent basest…
25557	2014-11-07 11:11:00	Grev Wedels plass	Ved Forsvarsdepartementet	59.907627	10.741909	Signalstyrke fra ukjent basest…
25558	2014-11-07 11:11:06	Grev Wedels plass	Ved Forsvarsdepartementet	59.907686	10.742371	Vekt: 1.00
27483	2014-11-08 23:46:08	Ramstadsletta	E18 retning Drammen	59.894773	10.551237	Vekt: 1.00
27609	2014-11-09 15:32:59	Ramstadsletta	E18 retning Oslo	59.894961	10.554327	Signalstyrke fra ukjent basest…
27610	2014-11-09 15:33:00	Ramstadsletta	E18 retning Oslo	59.894917	10.554073	Vekt: 1.00
27636	2014-11-09 15:33:35	Ramstadsletta	E18 retning Oslo	59.896936	10.565159	Signalstyrke fra ukjent basest…
27637	2014-11-09 15:33:36	Ramstadsletta	E18 retning Oslo	59.896987	10.565476	Vekt: 1.00
28532	2014-11-10 00:44:31	Skippergata	Ved Forsvarets logistikkorganisasjon	59.907715	10.745678	Signalstyrke fra ukjent basest…
28533	2014-11-10 00:44:32	Skippergata	Ved Forsvarets logistikkorganisasjon	59.907618	10.745564	Vekt: 1.00
30267	2014-11-12 01:47:53	Høvik	Rett etter Ramstadsletta E18 retni…	59.895156	10.551531	Signalstyrke fra ukjent basest…
30470	2014-11-12 17:27:00	Strand	E18 retning Oslo	59.902076	10.592242	Vekt: 1.00
31697	2014-11-13 01:52:32	Strand	E18 retning Drammen ved avkjøring…	59.903013	10.595385	Vekt: 1.00
32020	2014-11-13 11:14:14	Ramstadsletta	E18 retning Drammen	59.897688	10.568503	Signalstyrke fra ukjent basest…
32021	2014-11-13 11:14:15	Ramstadsletta	E18 retning Drammen	59.897741	10.568824	Vekt: 1.00
34618	2014-11-13 13:07:03	Holmen	E18 ved Holmenkrysset	59.858249	10.483136	Vekt: 1.00
35835	2014-11-14 01:59:25	Strand	E18 retning Drammen	59.901664	10.590137	Signalstyrke fra ukjent basest…
35836	2014-11-14 01:59:26	Strand	E18 retning Drammen	59.901594	10.589736	Vekt: 1.00

No errors; 260 rows affected, taking 1,49 s

Figur 6 Slik så databasen med dataene fra CryptoPhone ut i starten av november i fjor.

I tillegg ble det enklere å se etter mulige feil i rådataene, og finne ut om det var noe som ikke stemte. Arbeidet med å utvikle stordatabasen fungerte rett og slett som et ekstra kvalitetsledd.

5.2.6. Laget forsterkes og arbeidet intensiveres

Per Anders og Andreas jobber begge i nyhetsavdelingen og hadde flere ganger tidligere jobbet tett og godt sammen i lange graveprosjekter for Aftenposten, blant annet i halvannet år etter 22. juli-terroren. Begge hadde diskutert ideen underveis mens Per Anders gjorde CryptoPhone-målinger og 17. november ble Andreas med for fullt. For alle tre pågikk arbeidet fortsatt innimellom turnus- og helgevakter.

Etter over seks uker med målinger var det tid for å oppsummere funnene og forberede neste trinn. Kart, foreløpige resultater, funn, journalistiske ideer, oppfølgingsmuligheter og en prosjektskisse ble presentert i et møte med reportasjeleder Christine Engh, avdelingsleder Tone Tveøy Strøm-Gundersen og redaksjonssjef Peter Markovski 17. november. De var veldig positive og vi ble enige om å bruke både tid og ressurser videre. Arbeidet ble intensivert og vi startet med å legge planer for hvordan sakene, data og kart kunne presenteres digitalt. Videojournalist Sandra Mørkestøl ble også med.

Arbeidet pågikk i denne perioden på fulltid og mye mer enn det. Gruppen, som var ledet av reportasjeleder Christine Engh, besto nå av Per Anders, Fredrik, Andreas og Sandra. Her fra og ut ble dagene svært lange og doble. Per Anders og Andreas hadde alene over 250 overtidstimer fra 20. november til 20. desember.

5.2.7. Oppsummering av de 56.000 CryptoPhone-målingene og 57 måleruter

Fra 10. oktober til 21. november i fjor gjorde vi over 56.000 målinger på 57 forskjellige måleturer som dekker 100 kilometer med veier i Oslo-området, hvor ruten ble logget med lokasjonsdata.

Loggdata fra kryptofonen ble sammen med posisjonsdata fra en GPS-sporer fortløpende ryddet og vasket og lagt inn i databasen Fredrik og Per Anders hadde laget. Samsvarende tidspunkter for GPS-

og CryptoPhone-oppføringer indikerte hvor og når hver alarm stammet fra, og kunne dermed kobles sammen for videre analyser. Ved å ha dataene i relasjonsdatabaser ble det mulig å analysere og filtrere målingene basert på tid, styrke, nettverk, celle-ID eller andre relevante faktorer.

Til sammen utgjorde dette 56.000 logger fra målinger, mens GPS-koordinatene utgjorde 46 726 registreringer.

Loggene inneholdt også opplysninger om målingstidspunkt, nettverk (Telenor/Netcom), hvor opplysningene kom fra (basebåndets operativsystem eller mobilens operativsystem), type avvik/hendelse, årsak og signalstyrke.

Ved registreringer av det mobilen definerte som «svært mistenkelige» avvik ble det lagt inn manuelt opplysninger om hvor målingene fant sted, for eksempel opplysninger om hva som ble observert i området, hva som foregikk og kort informasjon dersom journalisten så noe spesielt i nærheten da man gjorde målingen.

De utvalgte alarmposisjonene ble filtrert ut, og lagt inn i et interaktivt kart som ble benyttet i research-fasen. Kartet gjorde det mulig å følge ruten dag for dag, og visuelt fremstille hvor de relevante alarmutslagene av ulik betydning befant seg i tid og rom.

Figur 7 Enkeltmålinger fra CryptoPhone vist på kart.

5.3 Jakten på feilkilder

Vi sto med 470 hendelser fra kryptofonen. Det eneste vi var helt sikre på var at dette var altfor mange. Den største utfordringen nå var derfor å lete etter alle mulige feilkilder og svakheter ved målingene.

Siden vi helt fra starten hadde bestemte oss for å være helt åpne overfor alle kilder om prosjektet, teknologien, målingene, databasen og resultatene, var det viktigste for oss at vi skulle ha vurdert alle mulige alternative forklaringer. Det var også helt avgjørende å få inn innspill, motforestillinger og mulige feilkilder. Det var på tide å gå ut i verden og legge kortene på bordet.

5.3.1. Kildemøter med vasking av data

24. november begynte vi på en lang kilderunde, hvor vi presenterte hele prosjektet, telefonen, metoden, teknologien, databasen, kartene og funnene i personlige møter med Oslo politidistrikt, Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM), Post- og teletilsynet (PT), professor Josef Noll ved Universitetssenteret på Kjeller UNIK/Institutt for informatikk ved Det matematiske- naturvitenskapelige fakultet ved Universitetet i Oslo (UiO), NetCom, GSMK i Berlin (Skype/telefon) og leverandøren Multisys[15].

Vi ville også presentere prosjektet for Telenor, men de ønsket ikke å møte oss. De fikk i stedet materialet oversendt på epost.

Forutsetning fra vår side var at dette var «bakgrunnsmøter» som vi ikke skulle sitere fra. Vi ønsket at alle skulle kunne snakke fritt uten frykt, og stille de spørsmålene eller gi alle de innspillene de kunne komme på. Avtalen var at vi i ettertid skulle komme tilbake skriftlig med spørsmål for «on record»-kommentarer.

Flere av kildene ønsket på forhånd å få oversendt en skriftlig redegjørelse med bakgrunn om prosjektet, metode, teknisk beskrivelse av telefonen og et Excel-ark med målinger, koordinater, stedsangivelse og beskrivelse. Det sa vi ja til. GSMK svarte med å gi oss sin helt fersk «technical briefing» laget rett før møtet med oss.

Bakgrunnssamtalene var nyttige, og vi er takknemlige for alle som var villig til å stille opp.

På grunnlag av «kildeuken» og alle innspillene vi fikk, gjorde vi flere store korrigeringer av databasen. Vi fjernet alle enkeltmålinger hvor det kunne være alternative forklaringer på det som CryptoPhone definerte som «svært mistenkelige» hendelser:

1) **Måling i tunneler, bomringer og broer:**
   118 av 470 hendelser ble fjernet fordi våre observasjoner og GPS-målinger viste at de er gjort i tunneler, broer eller ved bomringer. Både Vegvesenet, GSMK og professor Noll var enig i at tunneler, broer eller bomringer kunne tenkes å gjøre utslag.

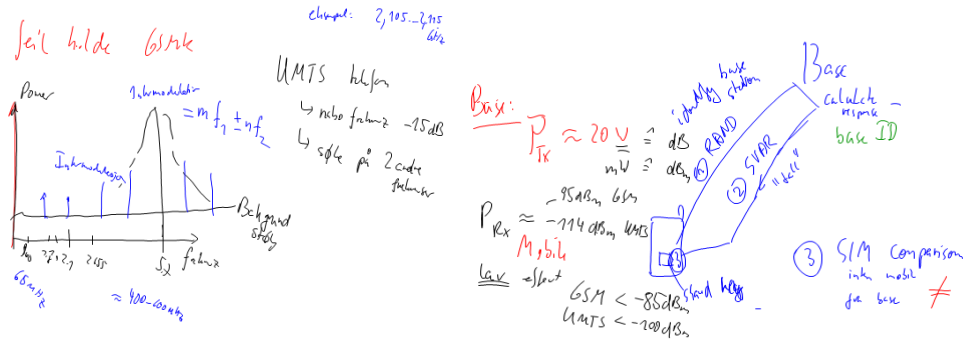
2) **Alternative forklaringer til forsinket aktivitet på basebåndet:**
   Et av avvikene som CryptoPhonen reagerte på, var hendelser hvor aktiviteten på basebåndet fortsatte mye lenger enn aktiviteten på mobilens applikasjonsprosessor/operativsystem.
   I svaret vi fikk fra GSMK med en tekniske beskrivelse av BaseBand Firewall kom frem i fotnote 3 på s. 4[16] at GSMK vurderte å fjerne eller «modifisere» denne regelen i fremtidige versjoner fordi *"this rule has shown to cause a relatively high number of false positive events in the real world".* Selv om det kunne gå lenge før denne regelen ble endret eller modifisert i Baseband Firewall, kunne dette være en viktig feilkilde. Vi bestemte oss derfor for å fjerne 158 av 470 enkeltmålinger i vårt materiale fordi de baserte seg på denne «regelen», som GSMK vurderer å fjerne den fra neste generasjon CryptoPhone.

[15] Se tidslinje i vedlegg 2 og kildeliste i vedlegg 3.
[16] Se vedlegg 7. 6 for teknisk beskrivelse fra GSMK

3) Korrigering for lav signalstyrke:

Et sentralt spørsmål som kom opp gjennom kildemøtene, var om radiostøy fra ulike kilder og dårlige dekningsforhold kunne tenkes å gi utslag dersom signalstyrken var lav. Hva som kan regnes for å være lav signalstyrke varierer avhengig om det er GMS, UMTS eller LTE nettverk. Signalstyrken i CryptoPhone-målingene er angitt i ASU (Arbitrary Strength Unit).

Per Anders tok med alle resultatene til professor Noll ved UNIK på Kjeller for å diskutere hvor vi burde sette grensen for å være helt sikre på at vi utelukket slike «false positives». Noll var meget imøtekommende, og anslo «lav» styrke som 10 eller mindre, noe som tilsvarer en signalstyrke på minst -93dBm ved GSM-nettet og -106 ved UMTS-nett (dBm= 2 x ASU – 113). Noll hjalp til med å gjøre ulike beregninger, og Noll anslo at vi ville være på sikre siden hvis vi satt grensen mellom 10 og 13. Da vil det være svært vanskelig å si at generell støy fra ulike alternative kilder kunne forklare den unormale aktiviteten på basebåndet. Vi fjernet derfor 71 enkeltmålinger i materialet hvor signalstyrken fra basestasjonene til mobilen var 14 ASU eller lavere.



Figur 8: Notater fra hurtigkurs hos professor Joseph Noll ved Unik 28. november, hvor Per Anders fikk råd om hvordan utelukke feilkilder i målingene knyttet til radiostøy.

4) Kan repeatere gi utslag?

Administrerende direktør dr. Bjørn Rupp i GSMK opplyste at de aldri har registrert at repeatere eller enkle jammere gir utslag. Vi hadde imidlertid ikke prøvd ut mobilen selv mot en ulovlig repeater. Lovlig repeater-utstyr har ikke gitt utslag.

5) Småceller?

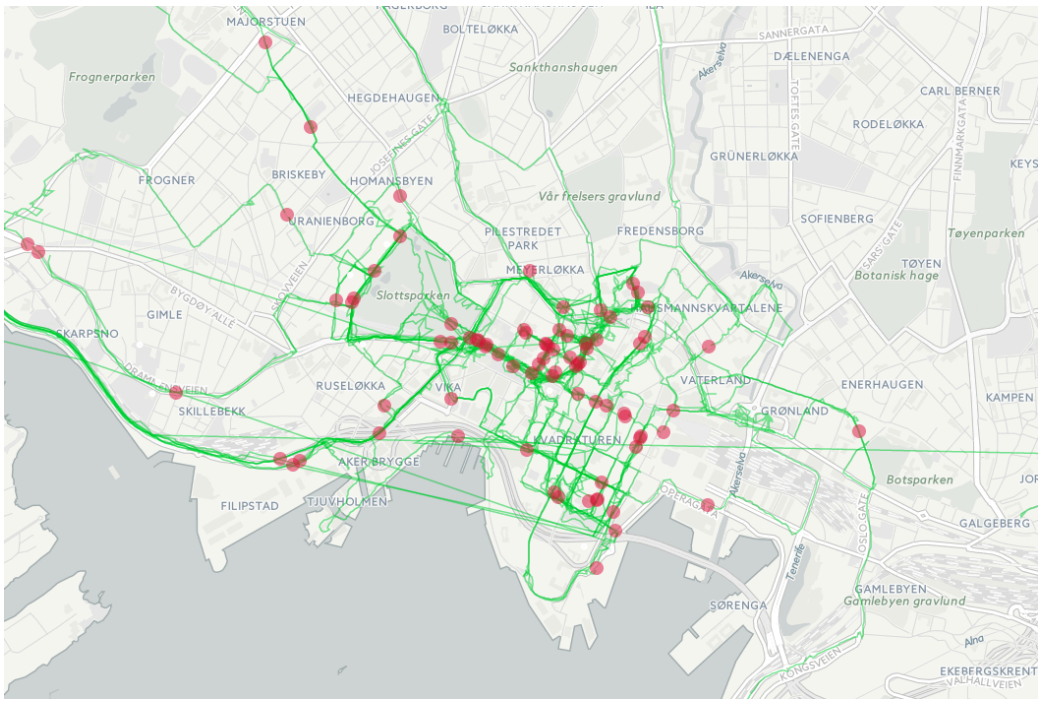
Netcom spurte om telefonen kunne gi utslag ved småceller, det vil si innendørs basestasjoner som er bygget ut flere steder. Vi testet mobilen hos selskapet CloudBerry som har slikt utstyr. Vi fikk ingen falske meldinger ved deres småceller som ikke er en del av de eksisterende mobilnettet.

Vi prøvde også å skifte simkort til et utenlandsk simkort uten å få noen utslag mot småcellen. Telefonen ble også testet mot en helt ny basestasjon hos Netcom uten at den ga utslag.

6) **Radiostøy fra spesielt utstyr?**
Innendørs kunne det tenkes at visse typer utstyr (mikroovner eller store plasmaskjermer) ga utslag. Vi fikk enkelte utslag da vi passerer tett ved Aftenpostens TV-studio, mens sending pågår. Vi fjernet derfor målinger gjort innendørs.

7) **Problemer i nettverkene?**
NetCom eller Telenor bekreftet flere ganger at de ikke hadde indikasjoner på at det hadde vært feilkonfigureringer i nettene i de områdene vi målte med kryptofonen i denne perioden.

Etter feilkildevasking sto vi med 122 enkeltmålinger fra 87 ulike hendelser i perioden 10. oktober til 21. november 2014 som CryptoPhonen mener «svært mistenkelig hendelser». I tre områder var antall hendelser høyest: Rundt Stortinget, Parkveien og Kvadraturen. Vi hadde også registrert mange avvik på Aker brygge, i Sørkedalsveien ved Garden, Skøyen, Lysaker – og flere andre enkeltsteder. Dette var hendelser vi ikke klarte å finne noen alternative forklaringer til.



Figur 7 Kartet viser det kryptofonen mente var "svært mistenkelige" hendelser" i Oslo sentrum som vi ikke hadde noen naturlige forklaringer på.

Den vanligste årsaken til at GSMKs CryptoPhone definerte dette som «svært mistenkelige» hendelser, er at programvaren som skal beskytte mobilen, oppdager dataaktivitet på basebåndet uten at mobilens applikasjonsprosessor er i bruk. Det vil si at basebåndet kan sende og motta data selv om mobilen er i dvale.

GSMK understreket sterkt at «svært mistenkelige hendelser» ikke betyr at vi hadde funnet falske basestasjoner eller avdekket et angrep eller et overvåkingsforsøk fra en IMSI-catcher, men opplyste at «et høyt antall av disse hendelsene under normale nettverksforhold kan være en sterk indikasjon på at noe er galt».

5.4. Neste steg: Falcon-undersøkelsene

5.4.1. Indikasjoner, ja. Men ikke noen bevis

27. november var en av de mørkeste dagene for oss gjennom hele prosjektet. Jo mer vi målte med kryptofonen, jo flere ubesvarte spørsmål ble vi sittende igjen med. Vi hadde svært mange indikasjoner for at falske basestasjoner var i bruk i Oslo, men ikke noen bevis.

Med unntak av Post- og teletilsynet, var det ingen av kildene som ga uttrykk for at de ønsket å undersøke dette nærmere. Tilsynet hadde imidlertid ikke utstyr til å kunne finne falske basestasjoner. De offisielle kommentarene vi hentet inn skriftlig, gikk stort sett på at alle syntes dette var interessant og at det ikke kunne utelukkes at dette var tegn på mobilovervåking.

Vi var dessuten litt oppgitt over GSMK, selv om tyskerne hadde vært meget åpne og vennlige. Det tekniske svaret vi omsider fikk 28. november på grunnlag av alle våre spørsmål, viste at det hadde vært riktig å gå kritisk til verks for å luke ut «false positives». GSMK hadde selv kommet til at en av de seks «reglene» som utløste ulike mistenkelige avvik på mobilen, trolig måtte endres.

Skulle vi publisere noe utelukkende på det vi allerede hadde gjort, måtte vi ta mange forbehold. Måten mobilen var brukt av journalister i USA, var altfor kategorisk etter vår vurdering.

Men samtidig hadde vi gjort vi en annen, viktig oppdagelse i møte ansikt med ansikt med teleselskaper, politiet, PST, NSM, tilsynsmyndigheter og forskere:

Ved å lytte til spørsmålene og kommentarene vi fikk underveis, forsto vi at hverken teleselskapene, politiet, PST eller NSM hadde gjort noen tilsvarende kartlegging som dette i så store geografiske områder.

5.4.2. Nye hjelpere

I slutten av november møtte Per Anders daglig leder Jahn-Helge Flesvik i sikkerhetsselskapet Aeger Group. Det var et av de siste i en lange rekke møter hvor vi hadde presenterte våre resultater for å få innspill.

Aeger er et selskap som brukes av blant annet Norsk Journalistforbund og Aftenposten for intern sikkerhetsopplæring av journalister som skal ut i konfliktområder. De hadde hørt om prosjektet vårt via Roar Langen i Multisys, og var positive til å se materialet og gi sine vurderinger.

Flesvik, som selv har flere år bak seg i Etterretningstjenesten, svarte som de fleste andre at han ikke var overrasket dersom det foregikk mobilovervåking i Oslo.

Vi spurte om han kjente til noen andre måter å måle dette på – og om han kunne bidra Aftenposten:

-Jeg skal undersøke, var svaret.

Sent på kvelden samme dagen ringte Flesvik tilbake og svarte at Aeger Group kunne bistå, sammen med det norske, tsjekkiske og britiske sikkerhetsselskapet CEPIA Technologies. Selskapet ledes av nordmannen Kyrre Sletsjøe, som også hadde lang erfaring fra norsk etterretningstjeneste og har bistått myndigheter i flere andre land med tilsvarende utstyr og undersøkelser. CEPIA hadde tilgang til personell med svært avansert utstyr beregnet på å avsløre industrispionasje og drive kontraetterretning.

5.4.3. Kildekritikk av sikkerhetsselskapene

Før vi kunne innlede et samarbeid, var det helt avgjørende å undersøke sikkerhetsselskapene nærmere. Vi gjorde umiddelbart en sjekk på både Flesvik og Sletsjøe og selskapene de ledet mot alle tilgjengelige registre og åpne kilder vi har, for eksempel sosiale medier, LinkedIn, Google, Facebook, Atekst, ulike offentlige registre m.m. Vi gjorde også en sjekk av underleverandøren/operatøren som CEPIA ville benytte.

Vi ba samtidig om referanser i form av saker eller kunder de hadde jobbet med. Dette er et spørsmål som er enklere sagt enn gjort i sikkerhetsbransjen, hvor alle kunder per definisjon ønsker fullstendig diskresjon. Vi fikk likevel informasjon om en stor kjent «høyprofil-sak», som omfattet granskningen av en internasjonalt kjent terroraksjon.

Her var det mulig for oss å gå inn og kontrollsjekke opplysningene, og få bekreftet at denne granskningen bidro til å avsløre bakmennene ved hjelp av mobildata. Selskapet hadde også vært innleid som sakkyndigekspert i flere større rettssaker i et stort europeisk land.

Aeger Group var ansvarlig for oppdraget, og ble derfor gjenstand for en ekstra grundig sjekk. Her var det også lettest å gjøre en grundig jobb, ikke minst fordi Flesvik hadde jobbet for Aftenposten før. Aeger hadde også en medarbeider som tidligere har hatt en meget høy posisjon i etterretningstjenesten. Selv om selskapet ikke var stort og bare hadde vært i drift noen få år, var det vår vurdering at Flesvik var en meget troverdig kilde. Han fikk også gode skussmål av de som hadde vært på kurs med ham.

Både Flesvik og Sletsjøe hadde erfaring fra den norske etterretningstjenesten. Selv om de ikke ønsket å si noe om hva de gjorde der, var det mulig for oss å sjekke ut med andre kilder om dette stemte og hva de hadde gjort tidligere. Sletsjøe fikk usedvanlige gode referanser, og var et kjent navn for flere helt uavhengige kilder vi hadde hatt kontakt med. Etter vår vurdering er han trolig blant de fremst i Norge når det gjelder dette området.

Vi vet ikke hva Sletsjøe og Flesvik gjorde i etterretningstjenesten. Men det er ingen tvil om at Etterretningstjenesten det desidert fremst og største fagmiljøet i Norge når det gjelder signal- og kommunikasjonsetterretning.

I utlandet bruker etterretningstjenesten tilsvarende utstyr regelmessig. «IMSI-catchere» og «imsi-catcher-catchere» er ikke et uvanlig verktøy når etterretningstjenesten forsvarer norske interesser i utlandet.

5.4.4. Et veivalg: Gå videre eller nøye oss med det vi har?

Fredag 28. november måtte vi ta et valg: Skulle vi investere i å gjøre helt nye og grundigere undersøkelser?

Kostnadene var ikke ubetydelige og vi hadde ingen garanti for at det ville føre oss noe videre. Tvert i mot risikerte vi at absolutt alt vi hadde gjort, kunne være bortkastet. Resultatet fra målingene md CryptoPhone ville miste mye av sin verdi dersom vi ikke fant noe i den neste runden. Motargumentet var at en måling ikke kostet mer enn det vi bruker på en normal politisk meningsmåling.[17] Og at spørsmålene vi prøvde å besvare, var så viktige at det var verdt å satse videre.

[17] Kostnadene for de tre undersøkelsene beløper seg til ca 120.000 kroner.

Etter et kort internt møte med avdelingsledelsen og redaktørene fikk vi ja til å bruke penger til å leie inn bistand fra disse to sikkerhetsselskapene for å gjøre ytterligere undersøkelser basert på målingene vi allerede hadde i databasene.

5.4.5 Slik fungerte kontraetterretningsutstyret Falcon II

Både før, under og etter målingene ba vi om – og fikk – en grundig innføring i hva kontraetterretningsutstyret faktisk målte. Det var en forutsetning fra vår side for å kunne bruke resultatene. Falcon II, som ble brukt i målingene for Aftenposten, er en hardware-enhet som kan skanne flere mobilnettverk ved hjelp av flere mobiltelefoner på samme tid. Utstyret brukes til kontraetterretning i en rekke andre land i Europa, Midtøsten og USA.

Under målingene ble det om lag hvert fjerde sekund hentet ut data fra mobilnettverkene til Telenor, Netcom og Network Norway. Sim-kort ble anskaffet av Per Anders og Andreas, slik at telefonnumrene som ble brukt i undersøkelsen skulle tilhøre oss.

Enkelt forklart sammenlignes dataene med offentlige opplysninger om de lovlige mobilnettene, for eksempel plassering på ekte basestasjoner, celleID, lister over nabotjenester, signalstyrke og en rekke andre parametere.

Utstyret fungert slik at det ga ulike typer alarmer (lav, middels og høy) dersom det ble registrerte signaler på mobilnett fra falske basestasjoner som med høy sannsynlighet utfører ulike overvåkingsaktiviteter[18]. Dette er et produkt som er til salgs hovedsakelig for statlige aktører, og vi er ikke kjent med at det noen gang er brukt i et journalistisk prosjekt. Fra nyttår er det innført visse eksportrestriksjoner på denne typen utstyr utenfor EU.

Vi forsikret oss også om at det var lovlig å bruke utstyret.

5.4.6. «Target One, Target Two og Target Three»: Den første undersøkelsen

Den første dagen i desember hadde Per Anders og Andreas møte med Flesvik for å planlegge nærmere i detalj hvordan undersøkelsene de neste dagene skulle foregå. Basert på kartet over Oslo sentrum med de 122 «mistenkelige» avvikene, definerte vi på forhånd sammen med Aeger og CEPIA Technologies tre områder vi skulle prioritere: Parkveien, Stortinget og Kvadraturen. Dette var de viktigste stedene og hadde av størst politisk betydning. Vi forsto at våre samarbeidspartnere hadde militær bakgrunn da de foretrakk å kalle dette for «Target One, Target Two og Target Three».

Neste prioritet var å gjøre målinger på Fornebu, Lysaker, Aker Brygge, Barcode og ambassadekvartalet i Drammensveien.

Operatøren ble fløyet inn dagen etter, og måling nr. 1 ble utført fra 2. til 4. desember. Det var første gang han målte i Oslo. Flesvik var med på målingene, og hadde fortløpende kontakt med oss.

4. desember møttes vi på ett rom med dunkel belysing og persiennene nede et sted i Oslo. Operatøren var en person som lever under radaren. Vi har lovet ham at vi ikke røper hans identitet og arbeidsplass. Vi kan ikke gjengi hva han fortalte om sitt arbeid, tidligere oppdrag og referanser. Grunnen er at det da i praksis kan bli umulig for ham å fortsette med jobben han gjør.

I to timer fikk vi en innføring i hvordan utstyret fungerte, gjennomgikk ruten og fikk anledning til å stille alle spørsmål vi måtte ha. Vi diskuterte hvordan rådataene og tallene skulle tolkes, og hvordan

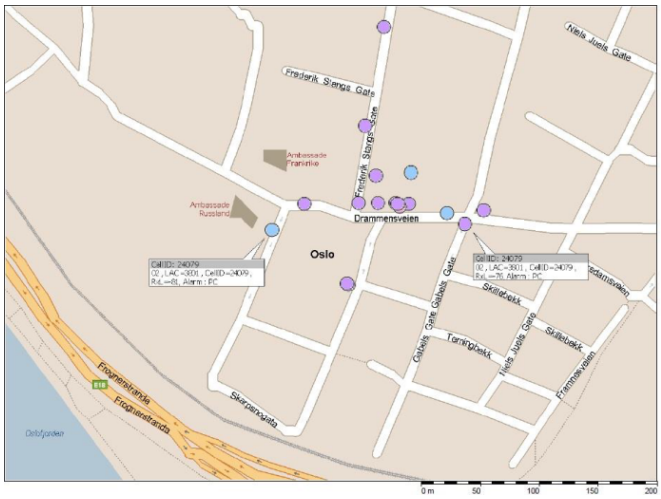
[18] Se vedlegg 7 for teknisk beskrivelse av Falcon II fra Cepia.

måleresultatene som ble vist på en storskjerm skulle forstås. Han viste oss også hvordan utstyret fanget opp data mens det gikk og tallene kom inn.

5.4.7. Resultatene og analyse fra den første målingen

- Det er absolutt ingen tvil. Vi har fanget signalene fra flere falske basestasjoner i områdene hvor vi har målt, sa operatøren. Resultatene var entydige og klare.

Det var flere grunner til at vi nå kunne være langt mer sikre:



Figur 8 Eksempel på et av kartene over målingene vi gjorde av det som høyst sannsynlig var signaler fra en falsk basestasjon ved den franske og den russiske ambassaden i Drammensveien.

1) Rådataene viste signaler til dupliserte/kopierte celler, et av de viktigste argumentene på at falske basestasjoner kan være i bruk i området.

2) På grunnlag av signalstyrken kunne vi se i hvilket område de var plassert – og sjekke dette opp mot hvor den ekte basestasjonen den hadde kopiert sto. Når en falsk basestasjon kopierer en ekte, må den stå plassert et godt stykke unna for ikke å drukne i støy. Signalene kan sammenliknes med de åpne kartene som finnes av hvor ulike basestasjoner er, for eksmepel finnsenderen.no eller opencellid.org

3) Alle basestasjoner i GSM-nettet sender ut en naboliste med inntil syv andre basestasjoner i nærheten. Alle mobiltelefoner måler kontinuerlig disse nabolistene, for til enhver tid å velge den basestasjonen som gir best mulig dekning. Mobilen velger en ny basestasjon dersom den gir sterkere dekning. Dette regnes ut fra såkalte reseleksjonsverdier, og kalles C1 og C2. Ved hjelp av Falcon II+ fikk vi også tilgang til disse verdiene, som er et ytterligere grunnlag for å dokumentere om signalene kommer fra en falsk basestasjon. De falske basestasjonene oppgir C1 og C2-verdier som villeder mobilene, og det kunne vi se med egne øyne på radiosignalene de sendte.

4) For at mobilen skal koble seg til en falsk basestasjon, må den finnes i nabolisten til ekte basestasjoner. Når den falske basestasjonen settes opp, leser den nabolisten og finner ut hvilke nabostasjoner som er mest brukt i et område. Den kopierer identiteten til den svakeste av basestasjonene i område, og gir seg ut for å være denne overfor mobiltelefoner i området.

Denne listen kunne vært mye lenger. Vi ble enige med CEPIA Technologies og Aeger Group om at vi likevel skulle legge inn et lite forbehold ved å bruke uttrykket «høy sannsynlighet» når vi omtalte funnene.

Selv om teleselskapene utelukket at det var tekniske feil i området, kunne vi ikke være sikre på at det likevel var tilfelle. Og så lenge vi ikke hadde mulighet til å gå inn i private kontorer og bygg, måtte vi ha et forbehold.

I overvåkingsbransjen er dessuten ingenting 100 prosent sikkert, selv om signaler fra falske basestasjoner er et av de sikreste sporene du kan finne.

5.4.8. Den andre Falcon II-målingen

Resultatene av den første målingen var så oppsiktsvekkende at vi umiddelbart bestemte at vi måtte forsøke å gjøre en måling til. Dessuten var det flere steder vi gjerne ville ha gjort ytterligere kartlegging for å kunne være enda mer sikre på våre funn. 5. desember fikk vi klarsignal fra redaktørene til å gjøre en ny måling fra 9. til 11. desember.

I tillegg til å gjøre flere undersøkelser der vi allerede hadde gjort funn, ønsket vi å sjekke ut om IMSI-catchere ble brukt i forbindelse med utdelingen av Nobel-prisen. Dette viste seg å være et bomskudd. De eneste radiosignalene vi oppdaget under prisutdelingen, varte i bare noen få minutter. Vår vurdering var at dette kunne være signaler fra sikkerhetsutstyr knyttet til en av bilene som leverte VIP'er, noe som er et svært vanlig og lovlig sikkerhetstiltak.

Dessuten ville vi gjerne ha utført målinger ved Barcode og Nydalen, hvor vi ikke fikk tid til å undersøke under første måling. Her hadde vi også registrert flere avvik med kryptofonen i oktober og november.

5.4.9. Datatekniske utfordringer med Falcon-målingene

For hver måling ble det utarbeidet en analyserapport med tolkninger av målingene og med kart. Rapportene, som fortløpende ble levert av CEPIA Technology, kom med analysedata og GPS-koordinater som rader i PDF-dokumenter.

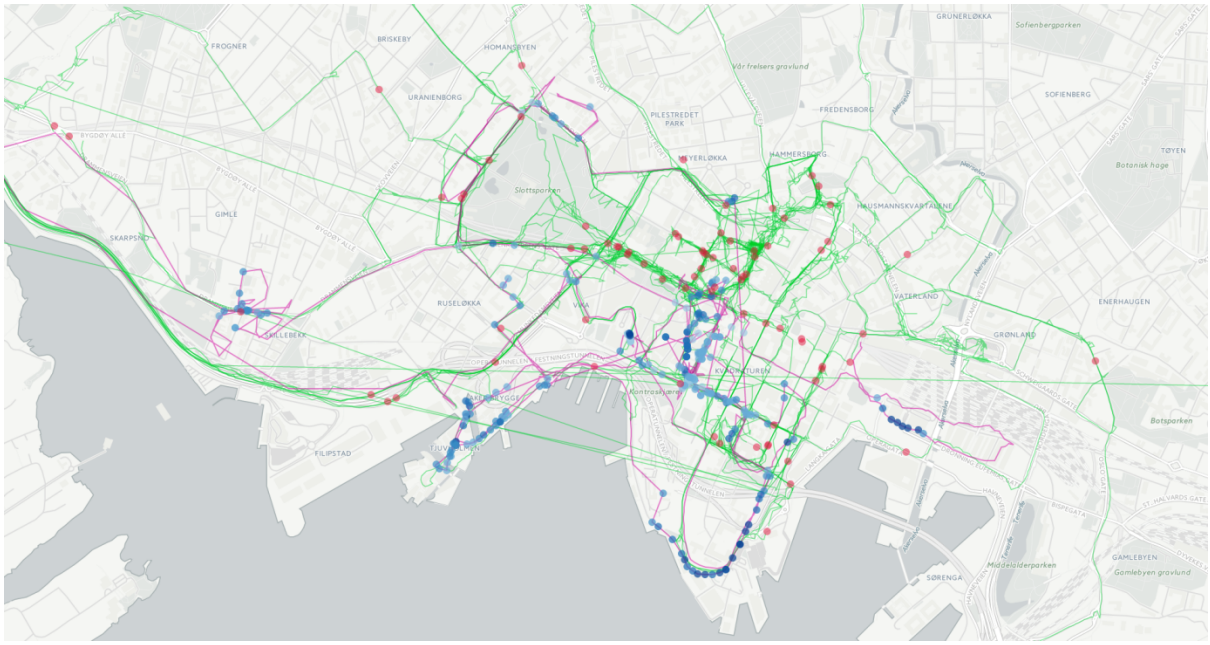
Vi konverterte dette deretter til tabulære data og ryddet og importerte de til en database. Sammen med kartutsnitt av Cepias analyserapport kunne vi dermed identifisere og plassere Cepias resultater i samme kartløsning som dataene fra CryptoPhone-kartleggingen. Vi mottok rapportene fra Cepia som loggdata i PDF-format, samt grafiske kartutsnitt som viste hvor de mente de mest signifikante alarmene befant seg med tilhørende beskrivelse.

Rapportene måtte gjennom noen oppryddingsrunder før vi kunne legge dem inn i samme struktur som CryptoPhone-dataene vi allerede hadde. Dette ble gjort ved å konvertere loggene til kommaseparerte verdier og deretter justere malplasserte kolonner. Tallmaterialet måtte også gjennom noen runder med vasking, blant annet for å vise et skjult negativt fortegn i C1, C2 og RxL-kolonnene.

Med alle Cepia-målingene i databasen kunne vi lage en egen kartløsning for visuell fremstiling av disse, for eksempel ved å fargekode alle treff på en bestemt celle-ID, eller vise relativ utslagsstørrelse på treffpunktene (signalstyrke). Dette gjorde det mulig å identifisere hvilke punkter Cepia selv hadde valgt å fremheve i sine kart, og lage vår egen visuelle fremstilling av disse i den endelige kartløsningen.

Det gjorde det også mulig for oss å kontrollsjekke materialet, og stille mer presise spørsmål når vi innhentet vurderinger fra andre kilder. Vi kunne for eksempel oppgi nøyaktig hvilke celleID'er som de falske basestasjonene så ut til å duplisere/kopiere.

Dette er viktig for å kunne dokumentere at de sterke signalene kommer fra sendere som ligger et godt stykke unna der hvor den lovlige, ekte basestasjonen står.



Figur 9 Kartutsnitt som viser hvordan vi satt CEPIAs målinger sammen med alarmene fra CryptoPhone.

5.4.10. Med åpne Falcon-kort

Materialet fra de første målingene utført 3. og 4. desember og 9. - 11. desember utgjør til sammen rundt 25.000 målinger fordelt over en rekke forskjellige måleturer. Resultatene fremgår klart av artiklene, og vi vil ikke gjenta dette her:

Vi pekte ut en rekke steder i Oslo hvor det med stor sannsynlighet var falske basestasjoner i aktivitet[19].

Kildekritikken av Falcon-undersøkelsen ble gjennomført på samme måte som for kryptofonen: Vi valgte nok engang å spille med åpne kort, selv om det økte faren for at saken kunne lekke eller komme på avveie. Kart, resultater og et sammendrag av funnene på forhånd til en rekke forskjellige, uavhengige kilder forut for publisering.

Politiets sikkerhetstjeneste fikk et sammendrag onsdag[20]. Nasjonal kommunikasjonsmyndighet fikk presentert funnene muntlig onsdag – og oversendt skriftlig torsdag. Torsdag ble funnene også oversendt til Nasjonal sikkerhetsmyndighet og Justis- og beredskapsdepartementet.

For å beskytte sikkerhetsselskapene under den siste målingen onsdag og torsdag, oppga vi ikke før fredag hvilke selskaper vi hadde jobbet med. Vi oversendte heller ikke opplysningene om målingene ved Aker brygge, Lysaker, Barcode og Nydalen, siden dette var saker vi fortsatt trengte tid til å arbeide med.

Professor Josef Noll ved UNIK ble også invitert til å gjennomgå det nye materialet, slik han hadde gjort det med CryptoPhone-målingene og kom til oss i Akersgata å lese gjennom materialet. De

[19] Les alle sakene på http://mm.aftenposten.no/mobilspionasje/
[20] Se vedlegg 10

faglige spørsmålene og kommentarene fra ham var av stor verdi for at vi skulle kunne fortolke dataene på uavhengig og fritt grunnlag, samt stille kritiske spørsmål til CEPIA og Aeger.

Telenor og Netcom fikk sammendraget av funnene fredag morgen. Dette var viktig for å kunne forsikre oss om at det ikke hadde vært feil i nettet eller andre tekniske forhold som kunne forklare utslagene som målingene viste. Selskapene kunne bekrefte at de ikke var noen slike feil i de aktuelle områdene hvor vi hadde gjort våre undersøkelser.

Figur 10 Siste møte med PST torsdag 11. desember før publisering der vi diskuterer våre funn med seniorrådgiver Siv Alsen (nr to fra venstre), Arne Christian Haugstøyl, seksjonsleder ved forebyggende avdeling og politiadvokat Signe Kathrine Aaling (ytterst til høyre).

Torsdag ettermiddag overleverte vi også materialet til Stortingets EOS-utvalg og Stortingets direktør/presidentskapet. Vi møtte på direktørens kontor og ga en kort redegjørelse. Det sentrale spørsmålet her var å få avklart om noen av målingene våre kunne skyldes internt sikkerhetsutstyr som tilhørte Stortinget. Det var det ikke.

All «on record»-kommunikasjon i denne fasen foregikk skriftlig. Det skulle ikke være noen som helst tvil om hvilke spørsmål som ble stilt, og hvilke svar som ble gitt.

5.5. Hvor lenge kunne vi vente?

5.5.1 Når skulle vi publisere?

Vi ønsket å publisere raskt etter de siste målingene. Aftenpostens vurdering var at vi ikke kunne vente for lenge med å gjøre mobilbrukere i Oslo oppmerksomme på at en rekke falske basestasjoner med høy sannsynlighet var i drift. Samtidig hadde vi nå, på flere stadier i prosessen og til stadig flere mennesker, delt vårt materiale og vært helt åpne med en rekke kilder for å få innspill og kommentarer

Vi var hele tiden klar over at radiosignalene kunne bli borte med en gang vi publiserte sakene. Det er bare å trykke på en knapp, så blir det stille. Uten signaler ville det bli svært vanskelig for myndighetene å finne ut hvem som kunne stå bak eller finne ut eksakt hvor utstyret sto. Det var

også noe av grunnen til at vi ønsket å gi dem resultatene på forhånd, så de hadde tid til å gjøre noe før vi publiserte.

Vi diskuterte i denne perioden om vi skulle gjøre ytterligere undersøkelser for å se om vi kunne få tak i en falsk basestasjon rent fysisk. Men vi kom til at det ikke var mulig, med mindre vi tok i bruk svært utradisjonelle metoder som innbrudd og falsk identitet. For å kunne gjøre dette, ville vi trenge politimyndighet og adgang til å sparke inn dører og trenge inn i private og offentlige kontorer.

Det hadde nå gått to og en halv uke siden vi hadde presentert våre første funn som tydet på at det foregikk mobilovervåking i Oslo. Ingen gjorde noe. Nå hadde vi gjort jobben. Siden sammendraget av funnene var oversendt norske myndigheter var det også en grense for hvor lenge vi kunne vente på at de gjorde noe som helst.

Redaktørene, avdelingsleder og nyhetsleder sørget samtidig for at manuskontroll, redigering og faktasjekk ble samordnet av de ulike nivåene, slik at vi ikke måtte forholde oss til svært mange forskjellige og ulike innspill i innspurten.

5.5.2. Om å legge alle kortene på bordet

Som tidligere nevnt, var det et mål fra starten av at vi på et eller annet tidspunkt skulle legge ut alle dataene. I det endelige og publiserte kartet[21] viser vi hele den sammensatte ruten der Aftenposten og Cepia gjorde målinger i hver sin fargede kartlinje.

Her kan man se kjørerute, samt filtrerte oppføringer av alarmer fra kryptofonen og/eller de alarmene Cepia mente utgjorde størst mistenkelighet etter kontrollen med Falcon II-utstyret. Alarmpunktene ble hentet ut fra en geoJSON-eksport av lokasjonsdata, mens kjøreruten ble tegnet ut som en SVG-path med visualiseringsplattformen D3.

Man kan dermed også se hvilke områder vi hadde målt uten at kryptofonen signaliserte noen betydelige alarmer. Vi gjorde det også mulig for leserne å følge vår rute gjennom et interaktivt kjørekart basert på dato/tid og GPS-koordinater (”Følg GPS-ruten”) for å kunne ettergå metoden vi har brukt og se hvilke områder vi har dekket.

Ved publisering av kartruten lot vi også leserne laste ned både ubehandlede rådata og våre strukturerte versjoner av datasettene i diverse formater. Vissheten om at alt vi gjorde på dette tidspunktet måtte tåle å bli belyst eller ettergått, var noe som lå i bakhodet vårt hele tiden.

Siden 6. januar er datapakkene lastet ned 402 ganger ekstern. Vi har på bakgrunn av dette fått flere interessante tips. Hvis bare en liten del av alle de personene som nå ser på vårt materiale går grundig inn i dette, har vi fått svært mange nyttige kilder i fremtiden. Vi har tross alt bare vært tre journalister som har jobbet fulltid med dette.

Ingen har så langt etter to uker påvist noen feil i materialet eller rådataene.

[21] http://mm.aftenposten.no/mobilspionasje/

6 Spesielle erfaringer og konsekvenser

6.1 Kildene som ble etterforskere og samarbeidsklimaet som ble til press

Da vi publiserte første sak klokken 22 fredag 12. desember i fjor spredte den seg svært raskt både i andre medier og på sosiale medier. Både justis- og beredskapsminister Anders Anundsen, statsminister Erna Solberg og PST-sjef Benedicte Bjørnland møtte pressen dagen etter. PST-sjefen uttalte at Aftenpostens undersøkelser ga grunn til bekymring og gjentok at de lenge har påpekt høy etterretningstrussel mot Norge.

Søndag 14. desember, dagen etter at justisministeren hadde sagt at «vi må gjøre det som er mulig for å finne ut hvem eller hva som står bak, og hva som er det faktiske omfanget», og etter å ha mottatt NSMs rapport om falske basestasjoner der hovedkonklusjonen var at det er sannsynlig at funnene Aftenposten hadde gjort var reelle, besluttet PST å iverksette etterforskning.

Oslo politidistrikt satte samtidig i gang etterforskning for de forhold som måtte omhandle ikke-statlige anliggender, og nedsatte et eget etterforskningsteam i saken. PST koordinerer de tekniske undersøkelsene som i skrivende stund fortsatt pågår.

De to etterforskningene som ble iverksatt endret klimaet drastisk slik vi opplevde det, spesielt i kommunikasjonen knyttet til Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og teleselskapene. Presset fra myndighetshold ble markant større og all tyngde ble brukt til det som til tider opplevdes som et svært ubehagelig press som journalist.

Der vi før hadde møtt åpenhet, interesse og et profesjonelt samarbeidsklima, var det nå en lukket, avvisende og lite vennlig tone. Fra å ha et godt samarbeid var spissene nå ute. Personer som før publisering var kilder, var nå etterforskere.

Etterforskningsledelsen dukket opp på det vi trodde var et journalistisk bakgrunnsmøte, sentrale kilder ble kalt inn til avhør og PST sendte få dager etter første sak den første begjæringen[22] til sjefredaktøren i Aftenposten der de ba om å få alle grunnlagsdata for sakene.

Det ble også gjentatte ganger gitt utrykk for at Aftenposten hadde skapt et inntrykk av at PST gjorde lite. Vi mener PST må stå for det de har sagt, og at de hadde en åpen mikrofon hos oss. PST gjorde klart før publisering at de ikke kunne løpe rundt og jage falske basestasjoner.

- For PST har det ingen hensikt å prøve å løpe rundt å finne selve utstyret, sa Arne Christian Haugstøyl, seksjonsleder ved forebyggende avdeling i Politiets sikkerhetstjeneste (PST).

Først i justisministerens redegjørelse i Stortinget, tre uker etter publisering, ble det sagt åpent at PST ved flere tilfeller i løpet av de siste årene, både i Oslo og andre steder i landet, hadde foretatt tekniske undersøkelser over lengre tidsrom for å undersøke hvorvidt falske basestasjoner er i bruk og at de disse avgrensede undersøkelsene ikke avdekket falske basestasjoner.

Hva de har målt, hvordan de har gjort det og hvor grundig dette har vært, vet vi ikke. Vi vet heller ikke hvorfor det gikk tre uker før de opplyste om dette.

[22] Les hele begjæringen i vedlegg 7.8

6.2 Et uventet og uanmeldt besøk til Aftenposten

Dagen etter at justisministeren hadde redegjort i Stortinget om mobilspionasjen kom to politietterforskere fra Oslo politidistrikt og PST på et uanmeldt besøk til Aftenpostens lokaler i Akersgata. Det var uklart hva det gjaldt. Dette var samme dag som terroraksjonen mot redaksjonslokalet til Charles Hedbo i Paris, og Andreas har tidligere mottatt trusler fra personer i det radikale islamistiske miljøet i Oslo.

Sammen med avdelingsleder møtte Andreas etterforskerne som sa de jobbet med etterforskningen av falske basestasjoner. Deres hovedbudskap var at de ville "tilby en kanal for Andreas dersom det var noe han ønsket å fortelle" utover det vi hadde levert og som hadde stått skrevet. Det opplevdes som et press.

Aftenposten har vært åpne om alt og gjort vårt råmateriale tilgjengelig. Både PST og Oslo-politiet har helt siden november har vært orientert om arbeidet og fått tilbud om de dataene de vil.

Dagen etter kom det en ny formell anmodning fra PST[23] til Aftenposten der de ba om ytterligere grunnlagsdata, samt telefonnummer og IMEI-nummer til telefonene Aftenposten brukte. De ba også om at Aftenposten fritok Kyrre Sletsjø i Cepia for generell taushetsplikt i forhold til kommunikasjonen med Aftenposten i kommende avhør.

Av hensyn til kildevernet, og behovet for å beskytte informasjon om vår egen arbeidsmetodikk, ønsket vi ikke å gi fra oss opplysninger som gjør det mulig for PST å følge kontakten med våre kilder og arbeidet med målingene fra minutt til minutt. Slike opplysninger kunne også avsløre vår operatør.

Vi kunne heller ikke gi et generelt, ubegrenset fritak for taushetsplikten til våre leverandører og kilder. Vi hadde hatt en rekke diskusjoner og samtaler med vår leverandører i sikkerhetsselskapene Aeger Group og Cepia Technologies underveis, som berørte både interne redaksjonelle spørsmål, arbeidsprosesser og vurderinger i redaksjonen. Slik vi oppfattet det, er det ikke de interne journalistiske prosessene og vurderingene i Aftenposten som er gjenstand for etterforskning.

6.3 «Av hensyn til den pågående etterforskning…»

Stemningsskifte og etterforskningen vanskeliggjorde også arbeidet med nye saker fra målingene den siste uken før jul og i romjulen. Både hos Nasjonal sikkerhetsmyndighet, Oslo-politiet, teleselskapene og hos andre kilder møtte vi standardfrasen: «*Av hensyn til den pågående etterforskning kan jeg dessverre ikke besvare dine spørsmål*». Kilder ble mer forsiktig med å uttale seg.

Etterforskningen førte til at arbeidet med å få innspill, avklaringer og motforestillinger til nye funn fra målingene vi ønsket å omtale tok mye lenger tid enn vi hadde sett for oss og var mye mer krevende enn før. Vi ønsket å gå samme runde som tidligere med alle funnene vi nå skulle omtale og jobbe like grundig opp mot feilkilder og naturlige forklaringer. Det var imidlertid ikke like lett å få hjelp til detaljspørsmål etter publisering og de fleste gjemte seg bak argumentet om etterforskning.

6.4 To nye arbeidsgrupper og en forutsetning

Som en følge av Aftenpostens avsløringer ble det ikke bare igangsatt to etterforskninger og egne undersøkelser fra myndighetene.

[23] Les begjæringen i vedlegg 7.8

Nasjonal kommunikasjonsmyndighet, som under hele prosjektet var holdt orientert om utviklingen både i personlige møter og over epost, opprettet som en følge av sakene 16. desember i fjor en arbeidsgruppe med deltakere fra Nasjonal kommunikasjonsmyndighet (Nkom), NetCom, Telenor, Tele2 og Nasjonal sikkerhetsmyndighet. Arbeidsgruppen skal se på både netteiers muligheter for å avdekke falske basestasjoner i nettene og langsiktige tiltak for å øke sikkerheten ytterligere. Gruppen ledes av Nkom og Nasjonal sikkerhetsmyndighet bidrar med faglig rådgivning.

7. januar sa justis- og beredskapsminister Anders Anundsen at Justis- og beredskapsdepartementet og Samferdselsdepartementet nedsetter en arbeidsgruppe som blant annet skal se på grensesnitt og ansvarsforhold mellom de offentlige aktørene og de private aktørene, hjemmelsgrunnlag, samt vurdere behovet for større grad av aktiv monitorering av mobilnettene. Også Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Politidirektoratet deltar i gruppen.

Anundsen gjorde det også klart at han foresetter at saken med mulige falske basestasjoner vil inngå som et viktig sakskompleks i arbeidet til utvalget som skal kartlegge samfunnets digitale sårbarheter og sa at det antagelig vil utgjøre en del av bakgrunnen for utvalgets anbefalinger da de leverer sin utredning til departementet innen utgangen av september 2015.

6.5 Ubesvarte spørsmål

6.5.1. Sikkerhet og beskyttelse

Vi vet ikke hvem som har stått bak overvåkingen og signalene fra de falske basestasjonene vi avslørte. Men uansett om det var fremmede makter, norske myndigheter, kriminelle eller private selskaper, var sikkerhet og beskyttelse et viktig og avgjørende element som preget arbeidsprosessen.

Her er var våre viktigste metoder, og avveiningene vi gjorde underveis av sikkerhetsmessige grunner:

1) Det meste av den elektroniske kontakten med sensitive kilder i denne saken skjedde med kryptert e-post (pgp-nøkkel). For en rekke kilder var dette rett og slett en forutsetning for å kommunisere.

2) Dokumenter og databaser ble fra begynnelsen av november delvis kryptert. For kryptering av word- og pdf-filer brukte vi de faste krypteringsfunksjonene som ligger i programmene.

3) Når vi skulle overlevere sensitive dokumenter og filer til hverandre, gjorde vi det på minnepinne for å unngå å sende det over nettet/epost.

4) Vi droppet å bruke åpne verktøyløsninger som ellers ville vært nyttig å bruke, for eksempel Google Docs.

5) Vi var ekstra varsomme med mailtitler på kryptert e-post, og brukte uskyldige, innholdsløse titler.

6) Under viktige møter i Aftenposten hvor vi diskuterte funn, metoder, kilder, publisering, strategi og andre sensitive ting, ble mobiltelefonene lagt igjen utenfor.

7) For å kommunisere sikkert med SMS, benyttet vi Wickr, et gratis, enkelt og rimelig sikkert verktøy.

8) Under arbeidet ventet vi med det lengste å jobbe i redaksjonens vanlige publiseringsverktøy. Først noen få dager før publisering, opprettet vi skjulte saksmapper og kurver med begrenset adgang for de ansvarlige lederne og de involverte journalistene.

9) Aftenposten innhentet også sikkerhetsråd – og gjorde en vurdering av om det var behov for beskyttelsestiltak rundt journalistene i forbindelse med publisering.

10) Dersom vi var nødt til å ha sensitive telefonsamtaler og telefonmøter, benyttet vi Skype. Så mange møter som mulig ble gjort ansikt til ansikt

6.5.2. Spørsmålet som startet det hele er fortsatt ubesvart

Den opprinnelige ideen og det første spørsmålet vi stilte til norske myndigheter, har vi ennå ikke fått svar på. Vi mener det er noe av det mest problematiske i denne saken:

Ingen vet fortsatt hvor ofte norsk politi, PST og NSM faktisk «mobilregulerer» oss.

Det vi vet er at Regjeringen ønsker å gi politiet enda videre fullmakter for å kunne bruke slikt utstyr. Mens vi arbeidet med saken, fikk vi vite at et nytt lovforslag var på trappene. Det har høringsfrist i slutten av januar.

Vår klage til Samferdelsedepartementet førte ikke frem. Siden vi i skrivende stund er lovet en statistikk i løpet av noen måneder, har vi ikke klaget til saken til Sivilombudsmannen. Spørsmålet er om den vil være fullstendig. Våre artikler har vist at politiet og PST bare har rapportert inn til Nasjonal kommunikasjonsmyndighet i svært begrenset grad.

6.5.3. Signalene som forsvant

For å undersøke hva som skjedde etter publisering, besluttet vi å få utført en ny måling 10 dager senere. Målingen ble gjort 22. desember 2014, og dataene kom i havn etter jul i fjor.

Resultatet var entydig: Det aller fleste signalene var nå vekk. Ved to steder plukket vi fortsatt opp signaler, men det var nå mye svakere. Det var ved Nydalen og Nedre Vollsgate.

Hva som ligger i disse funnene har vi per 15. januar ennå ikke funnet noe helt sikkert svar på. Både teleselskapene og PST er klare på at signalene fra Nydalen ikke stammer fra en falsk basestasjon. De knappe svarene vi har mottatt på mail fra teleselskapene, kan tyde på at de mener det finnes mange forklaringer på nettopp disse målingene, for eksempel en repeater.

Også her har den pågående etterforskningen gjort det vanskelig å få svar på de mange spørsmålene vi fortsatt har.

6.6 Sakens internasjonale ringvirkninger

6.6.1. Satt dagsorden over hele verden

Aftenpostens avsløringer og metodebruk har satt dagsorden internasjonalt. Ingen medier som vi kjenner til har gjort en så stor og omfattende undersøkelse av bruken av falske basestasjoner. Her er noen av dem:

Saken var det «The Big Story» på Ap.[24] Den ble også omtalt av Reuters[25]. International Business Times vinklet på at det var en avis som først oppdaget signalene fra overvåkingsutstyr.[26] Der Spiegel[27] og Putin-kontrollerte Russia Today[28] og Pravda[29] kastet seg også på saken. «Hvem spionerer på Israel?», spurte Israels største nettsted for nyheter da Aftenposten publiserte funnene ved landets ambassade i Oslo. [30]

6.6.2. Undersøkelser i andre land

I flere andre land har andre medier nå startet og gjennomført tilsvarende undersøkelser.

I Sverige gjennomførte både Dagens Nyheter[31] og Expressen[32] tilsvarende undersøkelser. Finnene gjorde det enda enklere. De fikk rett og slett finsk sikkerhetspolitiet til å bekrefte at de kjenner til at slikt utstyr er i bruk i Finland.[33] De som har publisert egne undersøkelser så langt, har imidlertid nøyd seg med å bruke CryptoPhone.

Så langt har ingen andre klart å få tilgang til tilsvarende kontraetterretningsutstyr som ble brukt i våre undersøkelser, selv om dette er noe vi har rådet alle til å gjøre. Journalistene vi har vært i kontakt med, sier at sikkerhetsselskapene de har kontaktet i sine hjemland er svært tilbakeholdne med å jobbe åpent.

I tillegg til dette har Aftenposten publisert vår egen tekniske beskrivelse og publisert råd om hvordan det er mulig å drive kilde- og datakritikk av CryptoPhone-dataene.

I minst åtte forskjellige europeiske land gjennomføres i skrivende stund tilsvarende undersøkelser etter mønster fra Aftenpostens mobilspionasje-serie, som vi er kjent med. Per Anders og Andreas har hatt direkte kontakt med journalistene i disse landene og gitt råd om hvordan dette kan gjøres. Av hensyn til at dette arbeidet fortsatt pågår, kan vi ikke opplyse om hvilke land dette gjelder.

6.7 En foreløpig avslutning og et møte i Stortinget

Det viktigste for oss er at våre undersøkelser og artikler har bidratt at flere tiltak nå er på gang, som vil gjøre det vanskeligere å drive mobilovervåking i Oslo i fremtiden. Vi tror at våre artikler har ført til at mobilbrukeres digitale motorveier i luften kan bli mer sikre i fremtiden, dersom politikere, myndigheter og teleselskaper gjør alvor av det de har sagt.

Da saken ble behandlet i Stortinget[34] 7. januar, formulerte politikere fra høyre til venstre seg slik:

---

[24] http://bigstory.ap.org/article/d301aea4bd304ac9ad577a81ae143e69/norway-probes-spy-equipment-found-central-oslo
[25] http://www.reuters.com/article/2014/12/15/us-norway-spying-idUSKBN0JT1GL20141215
[26] http://www.ibtimes.co.uk/newspaper-discovers-someone-listening-norwegian-politicians-phone-calls-1479385

[27] http://www.spiegel.de/netzwelt/web/norwegen-imsi-catcher-in-oslo-mit-cryptophone-entdeckt-a-1008466.html
[28] http://rt.com/news/214327-snooping-mobile-towers-norway/
[29] http://english.pravda.ru/news/world/06-01-2015/129455-russian_embassy_norway-0/#.VLUDpPl5Nyw

[30] http://www.ynetnews.com/articles/0,7340,L-4604322,00.html
[31] http://www.dn.se/nyheter/sverige/regeringskvarteren-kan-vara-avlyssnade/
[32] http://www.expressen.se/nyheter/rosenbad-misstanks-ha-blivit-avlyssnat/
[33] http://svenska.yle.fi/artikel/2014/12/19/skyddspolisen-utlandska-stater-spionerar-pa-telefontrafiken
[34] Les hele redegjørelsen her: https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2014-2015/150107/

-Jeg vil også rose Aftenposten for å ha gjort et grundig journalistisk håndtverk, som har satt denne saken og denne diskusjonen på dagsordenen, sa Aps Hadia Tajik, mens Høyres Anders B. Werp benyttet anledningen til «å berømme det journalistiske arbeidet som er utført av Aftenposten i denne saken. Gjennom grundig og kompetent håndverk har man avdekket en sak som har stor interesse for landets øverste folkevalgte forsamling».

-Jeg vil også begynne med å takke Aftenposten, takke for at vi har redaksjoner som har både kapasitet og kompetanse til å grave fram sånne saker. Det er derfor vi trenger en fri og åpen presse med såpass mange ressurser i redaksjonene at sånne jobber blir gjort, sa Venstre-leder Trine Skei Grande.

-Nå har jo sikkert selvbildet til Aftenposten vokset seg langt forbi hodet, men jeg vil likevel anerkjenne det journalistiske arbeidet som ligg bak her. Det vi har diskutert nå, kommer til å være et tilbakevendende og økende tema i den offentlige debatten i Norge og i de fleste landene i tiårene som kommer, sa SVs Bård Vegar Solhjell.

Justis- og beredskapsminister Anders Anundsen (Frp) avsluttet debatten slik:

-Spørsmålet er om ansvaret er slik det bør være, eller om det også der bør være justeringer. Derfor er det fokuset som Aftenposten har satt gjennom sine artikler, svært viktig, egentlig helt uavhengig av hva etterforskningen til slutt viser, fordi disse problemene er høyst reelle uansett. Derfor mener jeg det er veldig bra med den jobben som Aftenposten har gjort. Jeg mener det er bra tiltak som dels er iverksatt før denne artikkelserien kom, og dels iverksatt i etterkant.