Grenseløs

Jakten på de som oppsøker overgrepsbilder skjult av avansert teknologi på det mørke nettet er grenseløs. Det kan også politiets etterforskningsmetoder være.

Skup 2018

Jonas Alsaker Vikan, 928 28 316, jonas.vikan@adresseavisen.no
Pål Solberg, 986 20 134, paal.solberg@adresseavisen.no
Simen Granviken, 920 88 101, simen.granviken

Adresseavisen

Sammendrag:

Et snodig sitat fra en etterforsker førte til oppstarten på et prosjekt hvor Adresseavisen i januar 2017 avdekket at menn over hele Norge var avslørt etter hacking fra amerikanske FBI – uten at norske domstoler, mennenes forsvarere eller lokalt politi som etterforsket dem visste om dette. Saken vokste utover året til å dokumentere at dette hadde skjedd på samme måte med 43 nordmenn.

Mennene hadde besøkt en side for overgrepsbilder som FBI styrte i dypeste hemmelighet fra sine lokaler i Virginia, USA. De visste ikke at da de tok seg inn, ble pcene deres infiserte med et lite program av FBI. Dette samlet inn informasjon om datamaskinene der de sto – også i Norge. Programmet fjernet den ugjennomtrengelige teknologiske kamuflasjen Tor-nettlesern gir og avslørte IP-adressene til brukerne. IP-adressene ble sendt til Kripos som hentet ut identiteten til mennene og opprettet straffesaker mot dem i Norge. IP-bevisene var det eneste grunnlaget som gjorde at domstoler tillot ransakinger og pågripelser over hele landet.

Alt dette skjedde uten at noen i rettsystemet kjente til følgende problem med beviset før Adresseavisen brakte informasjonen i en dokumentar 09.01.2017:

- FBIs metode kalles dataavlesing. I Norge var ikke dette lov da det skjedde
- Utenlandske politimyndigheter har ikke adgang til å foreta ransakelser på norsk jord
- Kripos fortalte ingen om hvordan IP-adressene, det eneste som knyttet en virkelig identitet til den kamuflerte datatrafikken, ble skaffet av amerikansk politi
- Måten Kripos forklarte at bevisene var hentet, er ikke teknologisk mulig, ifølge to eksperter på krypteringsteknologi

Og slik havnet sakene i rettssystemet uten at domstolene, mennenes forsvarere, eller lokalt politi visste at de opererte med bevis innhentet i strid med norsk lov fra politi som på tidspunktet satt ved spakene på verdens verste overgrepsbildenettsted.

I den første saken presenterte vi funn av sju tilfeller i tre fylker. Komplekset vokste utover 2017 og omfattet etter hvert 43 nordmenn. Mer enn 15 har fått en rettskraftig dom, fortsatt uten at hackingen har vært kjent for eller behandlet av rettsystemet.

Flere av de domfelte nordmennene er psykisk syke, ifølge avgjørelsene. Andre gikk gjennom hele rettsprosessen uten forsvarer. Se fullstendig publiseringsliste i punkt 4 på slutten av denne rapporten.

Innhold

1. Oppstart, hypotese og mål

1.1 Inngang til saken

Høsten 2016 sto jeg (Jonas) med begge beina oppe i et annet graveprosjekt. I en pause kom jeg over en sak Pål hadde skrevet som en del av vanlige krim-dekning i Trondheim:

> FBI-tips førte til dom mot trondheimslærer (13.10.2016)

To ting slo meg. Saken handlet om en politiaksjon på det mørke nettet, som jeg hadde erfaring med fra andre prosjekt. Og dette sitatet fra en av etterforskerne på saken:

> - FBI hadde overvåkning av diverse overgrepsbildesider på det mørke nettet, og logget IP-adressene til de som koblet seg til. Det var der de fant IP-adressen til den siktede, forklarer etterforsker ved Trøndelag politidistrikt.

Logget IP?

Slik jeg kjente det mørke nettet var hele poenget at nettleseren Tor kamuflerer IP-adressen til brukerne slik at den ikke er synlig og kan leses av, eller logges. Var polititjenestemannen feilsitert? Pål kunne fortelle at etterforskeren hadde fått en sitatsjekk som han godkjente.

Her hadde politiet i Trondheim tydeligvis fått logget IP-adressen til læreren. Det så ut som et enormt gjennombrudd siden etterforskning av personer som skjuler seg på det mørke nettet er svært vanskelig. I 2015 var det nær umulig. Dette var en kjempegod nyhetssak. Jeg måtte finne ut hvordan politiet hadde løst det.

1.2 Hypotese og mål

Gladsaken om en revolusjonerende ny etterforskningsmetode falt umiddelbart sammen.

Ekspertene på Tor-teknologien jeg ringte til avkreftet at det var noen kjent måte å logge IP-adressene, slik politet hadde sagt. Det var nettopp dette teknologien skulle hindre.

I enkelte tilfeller de kjente til fra utlandet, hadde IP-adresser imidlertid blitt skaffet ved hacking. Jeg hadde fulgt debatten om overvåkning, digitalt grenseforsvar og nye politimetoder og visste at hacking, eller dataavlesing som politiet kaller det, ikke var lov i Norge på tidspunktet hvor læreren hadde blitt avslørt. Dette, og kildesamtalene gjorde at jeg umiddelbart fortalte Pål om følgende hypotese:

> *Politiets forklaring skulle vært teknisk umulig. Kunne det være det slik at de opererte med avgjørende bevis som de ikke visste hvordan var skaffet? Visste noen hva som hadde skjedd her? Var noe lovstridig eller problematisk?*

Pål var skeptisk, dette var usannsynlig. I Norge er fremleggelse av bevis regulert slik at siktede, forsvarer og eventuelle domstoler skal kunne drive kontradiksjon. Å kjenne til og utfordre bevisene og bakgrunnen for en sak staten fører mot enkeltpersoner er grunnleggende i en rettsstat.

Søk viste at både Bergens Tidene og VG hadde skrevet om det som var kjent som «PLAYPEN-saken». BT fortalte at noen bergensere var tatt som følge av FBI-innsats, og i en sak fra VG+ skrev avisen at den hadde vært inne på PLAYPEN på tidspunktet fra politiet drev siden, som en del av VGs fortjenestefulle dekning av overgrepsbildeproblematikk. Ingen av artiklene gikk inn i problematikken med metodene, og eller eventuelle konsekvenser det hadde for de norske sakene - slik vi ønsket å gjøre.

Før vi begynte å se nærmere på sakene fra PLAYPEN-aksjonen noterte vi oss noen mål:

Mål 1:
Stemte hypotesen? Kunne det være flere tilsvarende saker? Hvor mange?

Mål 2:
Fikk aktørene i rettsvesenet opplyst at nordmennende var identifisert gjennom utenlandsk hacking? Hva ble aktørene fortalt? Var noen allerede dømt?

Mål 3:
Hva hadde egentlig Kripos visst da anmeldelsene ble sendt ut?

2. Arbeidet med saken

Sjekking av hypotesen begynte i slutten av oktober 2016, og arbeidet fortsatte på heltid frem til den første saken i januar. Deretter fulgte vanlig oppfølging før det ble en ny, intensiv periode mellom august og oktober for å få dokumentert hele omfanget, og antall dommer.

Sakene har oppstått i skjæringspunktet mellom en relativt ny teknologi, avanserte politimetoder, et grusomt kriminalitetsområde, amerikansk rett og norsk juss. For å avklare faktum måtte det gjøres undersøkelser i USA, og så handlet mye om tid- og ressurskrevende jobbing mot norsk politi, påtalemyndighet, forsvarere, domstoler for å dokumentere hva som hadde skjedd i Norge. I det videre går vi gjennom dette arbeidet så kronologisk som mulig – fordi saken utviklet seg underveis.

2.1 Mål 1

2.1.1 Innsyn i rettsdokumenter USA

Jeg hadde lest om PLAYPEN i amerikanske medier, som en del av generell research på teknologiske og juridiske problemstillinger. Nå måtte dette komplekset undersøkes skikkelig.

A) Hva var målet?

For å se om dette var noe å gå videre med, måtte et klart faktum etableres fra den amerikanske delen av saken. Jeg brukte amerikanske medier, teknologinettsider og hentet ut offentlige rettsdokumenter fra ulike instanser på kryss og tvers av USA ved hjelp av referanser fra nettsøk. Så lenge slike dokumenter ikke er «under seal», er de som regel tilgjengelig på åpne nettsteder som ikke krever registrering, var erfaringen fra dette arbeidet.

Jeg fikk hjelp til research av journalisten Joseph Cox som hadde skrevet mye om PLAYPEN. Hjelp fikk jeg også av advokater i nonprofit-organisasjonen Electronic Frontier Foundation, som arbeider for å ivareta borgerrettigheter i det digitale rom.

B) Hva ble funnet?

Rettsdokumentene viste at dette hadde skjedd fra høsten 2014 og til 04.03.2015:

- FBI hadde funnet identiteten til opphavsmannen bak PLAYPEN i begynnelsen av 2015 og pågrep ham
- Så flyttet FBI PLAYPEN-serveren til sine egne lokaler. Deretter driftet det føderale politiet overgrepsbildenettstedet i to uker fra 21.02.2015-04.03.2015
- En ransakingsbegjæring til en dommer i Eastern District of Virginia viser at det ble overført et lite dataprogram fra FBI til de som logget seg inn på en del av PLAYPEN.
- Programmet tok seg i hemmelighet inn på maskinene ved å utnytte et ikke-offentlig kjent sikkerhetshull i Tor-nettleseren.
- Programmet leste av lokal informasjon på brukernes datautstyr, og sendte informasjonen ukryptert tilbake til FBI
- Slik manipulerte FBI maskinene til å avgi IP-adressene som kunne brukes til å identifisere mennene
- Over 1000 maskiner ble hacket over hele verden, inkludert i Norge

C) Videre undersøkelser og forhold til andre metoder

Etter 04.03.2015 sendte FBI de norske IP-adressene de skaffet på denne måten til Europol. Kripos fikk dem i løpet av 21 dager. Dette fordi norske lover krever at tjenestetilbyderne sletter informasjon om IP-adressene etter tre uker.

Kunnskap om perioden hvor hackingen foregikk fikk betydning da saken vokste (se 2.2.6) og vi måtte lete i norske dommer etter folk som dette hadde skjedd med. Datospennet gjorde at vi kunne identifisere dommer som antakelig stammet fra PLAYPEN-komplekset selv der navnet på overgrepsbildenettstedet ikke var oppgitt.

2.1.2 Juridisk research

Klargjøring av faktum fra USA avgjorde hvilke nye spørsmål vi måtte finne svar på: De gikk inn i amerikansk føderal straffeprosess og noe som heter Rule 41 (b), den internasjonale Folkeretten samt norsk lovverk rundt datainnbrudd, bevisavskjæring og tema som fri bevisføring og bevisfremleggelse i norsk rett.

For å kunne vurdere om dette var en sak eller ikke, var det hensiktsmessig å bryte ned de mange teknologiske og juridiske elementene og søke svar i litteratur og hos jusseksperter.

A) Hva var målet?

Avklare flere juridiske spørsmål fra USA og Norge:

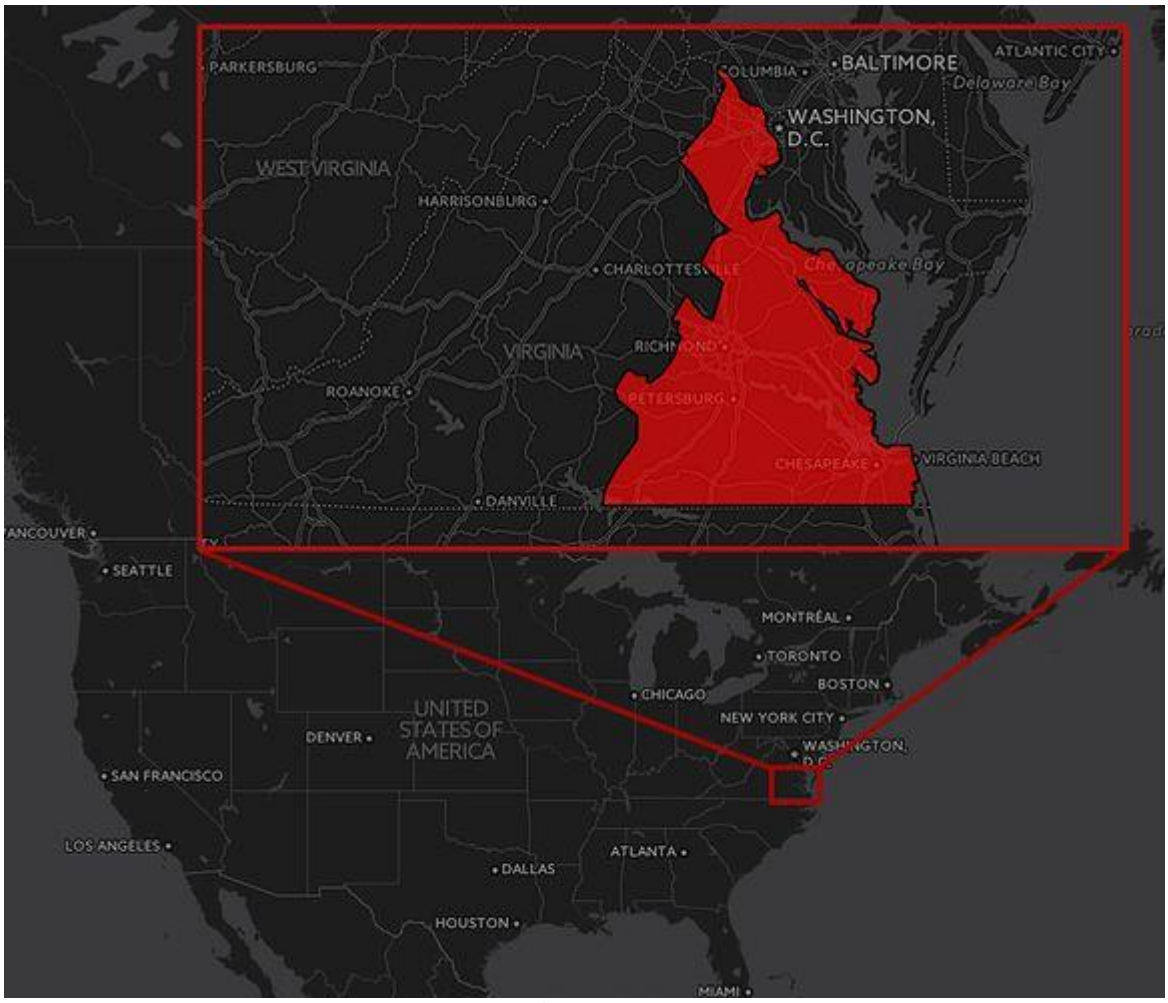
I. Kunne politiet virkelig styre et overgrepsbildenettsted fra egne lokaler?
II. Kunne politiet hacke i USA?

III. Skjedde hackingen i USA med en gyldig ransakingskjennelse?
IV. Var ransakingskjennelsen gyldig i Norge?
V. Var det lovlig for FBI å hacke maskiner som står i Norge?
VI. Kunne norsk politi hacke nordmenn i Norge?
VII. Var det FBI foretok seg jevngodt med det som på norsk ble kalt «dataavlesing»
VIII. Var det FBI gjorde på de norske maskinene straffbart, etter norsk lov?

B) Hva ble funnet?

De juridiske undersøkelsene ga følgende funn av betydning for arbeidet:

I. Dette var noe FBI fikk kritikk for, men det lot til at det var akseptert i USA. I Norge hadde det aldri kunne bli aktuelt, verken da eller nå.
II. Amerikansk politi har adgang til å bruke hacking som metode, også i februar / mars 2015 da PLAYPEN skjedde.
III. Ransakingskjennelsen ble utstedt av en dommer i Eastern District of Virginia. Da hackingen skjedde regulerte den såkalte Rule 41 (b) hvorvidt domstolen kan tillate inngrep utenfor eget nedslagsfelt. Ifølge den åpne jussdatabasen Legal Information Institute ved universitetet Cornell, begrenser Rule 41 (b) slike kjennelser til kun å gjelde innenfor jurisdisksjons-området. Dette bildet viser jurisdiksjonsområdet:



1 Det rødmerkede feltet viser jurisdiksjonsområdet til Eastern District of Virgina i en del av en av de 50 delstatene i USA.

IV. Ransakingskjennelsen fra Eastern District of Virgina var ikke gyldig i Norge.

V. FBI kan ikke hacke maskiner på norsk jord, det bryter med et prinsippet i Folkeretten som sier at politi i et land ikke kan gjøre etterforskningskritt på et annet lands territorie uten samtykke.

VI. Hacking, kalt dataavelesing når politiet gjør det, var ikke en lovlig politimetode i Norge i februar / mars 2015.

VII. Dataavlesing som metode(r) ble beskrevet i lovforslaget som Stortinget vedtok sommeren 2016. Beskrivelsene har mange likhetstrekk ved det FBI gjorde:

> (...) er metoden definert som «avlesing av opplysninger i et ikke offentlig tilgjengelig informasjonssystem ved hjelp av programmer eller annet utstyr».
>
> (...) Plasseringen av programvare kan blant annet gjennomføres ved å modifisere filer som lastes ned av informasjonssystemets bruker (...)
>
> (...) gjeldende ip-adresser for nettverksenhetene
>
> (..) ved å hente den ut fra internett ved å utnytte såkalte «bakdører» i programvaren

Videre, i straffelovens paragraf 216 heter det:

> Retten kan ved kjennelse gi politiet tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem (...)

Hvis Tor-nettleserens formål er å kamuflere brukerens reelle IP-adresse, er det logisk at IP-adressen anses å være «ikke offentlig tilgjengelige opplysninger».

VIII. Slik definerte norsk politi datainnbrudd på egne sider i 2014:

> «Med datainnbrudd menes det å trenge seg inn i datasystemer for å skaffe seg tilgang til beskyttet informasjon. Innbruddet kan straffes når man har skaffet seg tilgang til dataene / programutrustningen. En slik handling er straffbar selv om man ikke har gjort seg kjent med informasjonen. Man kan skaffe seg uberettiget tilgang på mange forskjellige måter, for eksempel ved å misbruke passord eller utnytte sikkerhetshull.»

Siden poenget med Tor-browseren er å beskytte identiteten og IP-adressen til brukeren, lot beskrivelsene av FBIs teknikk til at det kunne se ut som de hadde gjort seg skyldig i datainnbrudd i Norge.

2.2 Mål 2

2.2.1 Innsyn uten innsyn - runde 1

Etter å ha brakt på det rene at metodebruken etter all sannsynlighet var kontroversiell eller ulovlig i Norge, måtte vi finne ut hva norsk politi fortalte siktede, domstolen og forsvarerne om IP-bevisene. Var dette noe man politiet visste om?

Her var det eneste vi hadde å gå etter saken om læreren, som Pål hadde laget. Der fikk vi opplyst at IP-adressen kom fra en anmeldelse sendt ut av Kripos, og at lokalt politi ikke visste mer enn det. Vi fikk senere opplyst fra en førstestatsadvokat at det var vanlig *å ikke* gjøre egne undersøkelser av anmeldelser fra Kripos.

En anmeldelse er et straffesaksdokument som ikke er offentlig i Norge. Innsyn som journalitisk metode og verktøy var uaktuelt.

A) Hva var målet?

Kun anmeldelsene fra Kripos kunne vise hva de fortalte om hvordan IP-adressen var skaffet. Vi måtte finne ut hva som sto.

B) Hva ble funnet

Politiet avgjør selv om de vil la media se en anmeldelse. Noen ganger funker dumme spørsmål. Det gjorde det ikke i dette tilfellet, og vi fikk ikke se anmeldelsen.

Vi skaffet etter hvert tilgang ved å kontakte personer som var siktet. Slik hadde Kripos forklart hvordan amerikanerne avslørte nordmennene:

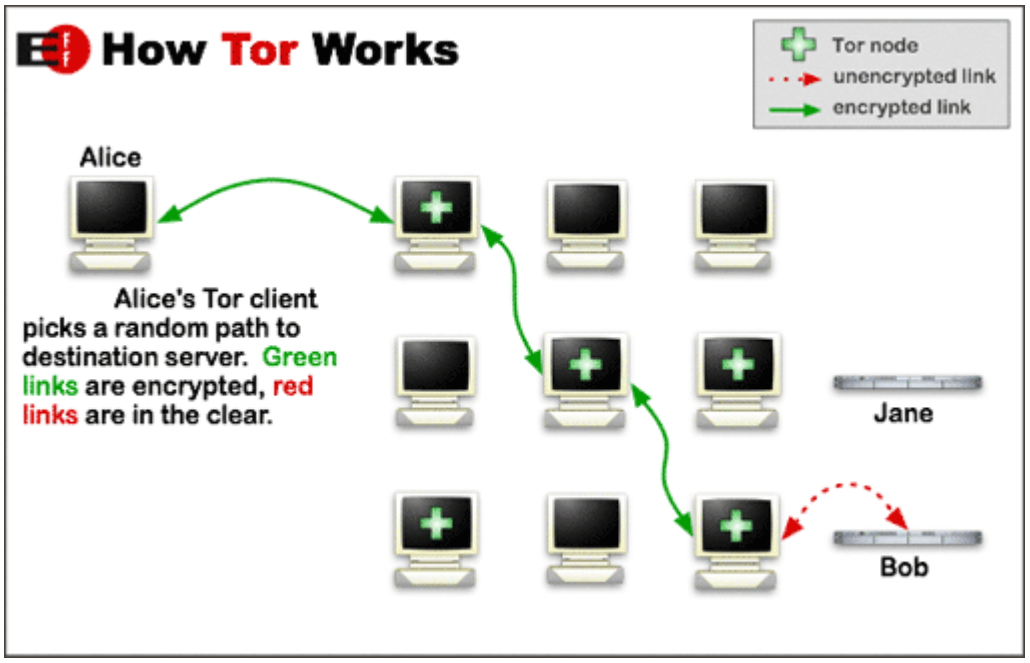
> «I forbindelse med aksjonen ble det logget en norsk IP-adresse: *XXXXXXXX* Det ble i denne forsendelsen ikke oppgitt hva brukeren av den angitte IP-adressen hadde foretatt seg på de ulike sidene. 09.06.15 mottok Kripos informasjon fra Europol som inneholdt hva brukeren av IP-adresse *XXXXXXXX* gjort på nettsiden.»

Den første setningen var det eneste som skulle forklare lokalt politi, forsvarere og domstoler at siktedes pc hadde blitt hacket mens utstyret sto i hus og kontor i Norge. Videre var IP-adressen det eneste beviset som knyttet personen til kriminalitet.

C) Videre undersøkelser 1

Teksten i anmeldelsen var akkurat slik etterforskeren i Trøndelag hadde formulert seg. Jeg kontaktet eksperter på krypteringsteknologi og Tor-nettleseren igjen for å få undersøkt om setningen stemte opp mot det faktum vi hadde avklart fra USA.

Ifølge ekspertene vil en server kunne se hvilke IP-adresser som kontakter den over vanlig nett. På det mørke nettet ser serveren kun IP-adresser fra tilfeldig valgte maskiner i Tor-systemet:



2 Denne forklaringen viser hvordan en Tor-nettleser kamuflerer brukerens ekte IP-adresse: Datatrafikken sendes gjennom tilfeldig valgte maskiner før trafikken når målet.

IP-adressen serveren vil se, er altså en tilfeldig maskin på et vilkårlig sted i verden, og *ikke* IP-adressen til personen man jakter på. Begge ekspertene avviste at det politiet fortalte i anmeldelsen, var teknologisk mulig.

D) Videre undersøkelser 2

Læreren i Trondheim hadde blitt ransaket av politiet. For å få gjøre dette må politiet be en domstol om lov. Da må man legge frem bevis som dokumenterer skjellig grunn til mistanke mot personen. Alt dette skjer i en hemmelig prosess, uten innsyn. Vi fikk bekreftet at ransakingen i lærersaken og de to andre sakene i Trøndelag, skjedde som følge av at politiet la frem anmeldelsen fra Kripos.

Ingen la frem for dommeren at det eneste grunnlaget stammet fra FBIs lovstridige hacking. Fordi politiet ikke visste det selv, var det ingen i rommet som kunne fortelle retten det.

2.2.2 Antall og omfang

Hypotesen min så ut til å stemme. Men hvor mange norske saker var det?

A) Hva var målet?

På dette tidspunktet, i slutten av november 2016, hadde vi funnet tre i Trøndelag som alle hadde samme tekst som utgangspunkt. Hvis det var tre bare i Midt-Norge, måtte det være flere rundt om i landet.

B) Hva ble funnet?

Frem til den første dokumentaren i januar 2017 fikk jeg to ganger beskjed fra Kripos om at de ikke ville kommentere eventuelle norske deler av PLAYPEN-saken, eller opplyse om det norske omfanget. Jeg så ingen andre utveier enn at vi måtte gjennomføre en grovjobb:

- Samtlige politidistrikt ble kontaktet med spørsmål om de hadde saker knyttet til PLAYPEN, eller OPERATION PACIFIER (et annet navn på komplekset).
- Søk ble gjort i Retriever etter avisomtaler av norske saker som stammet fra opplysninger fra FBI, eller som omhandlet det mørke nettet.
- Domstoladministrasjonen ble kontaktet for å få hjelp. Jeg gikk gjennom alle saker i Oslo tingrett som omhandlet overgrepsbilder i 2016 (ingen treff)

Politidistriktene var i varierende grad villige til å svare. Gjennomgangen førte til at vi fikk identifisert ytterligere tre saker i Bergen og en i Hedmark. Det totale antallet så ut til å være sju. Disse sakene ga også svar på om mennenes forsvarere og domstoler ble orientert om metodebruken, slik de skal bli.

Ingen av dem hadde fått opplysninger om FBIs hacking før jeg ringte dem. Forsvarerne hadde vanskelig for å tro det jeg fortalte, i likhet med politiet i Trondheim. Det tok mye tid å forklare faktum, også fordi det er en komplisert materie. For forsvarerne gikk vantro over i irritasjon:

> - Jeg har aldri vært borti en sak hvor bevis er innhentet ulovlig, sa advokat Torfinn Svanem
>
> - Myndighetenes bruk av ulovlig ervervede bevis er i seg selv ille. Dersom det i tillegg tildekkes og tåkelegges på hvilken måte beviset er ervervet, og ved dette avskjærer mulighetene for nærmere etterprøving og domstollkontroll, er det undergraving av rettssikkerheten, sa advokat Jostein Alvheim

Vi bestemte at vi hadde nok til å publisere den første saken, for så å jobbe videre.

2.2.3 Uavklarte mål

Noe den første saken ikke lykkes i å besvare var i hvor mange norske saker det var. Siden rettssikkerhet ble trukket frem som et sentralt moment ved dette, var det viktig å finne hele omfanget.

Et dokument fra Europol, funnet av Motherboards journalist, hadde tidligere avslørt at det var 34 danske borgere som ble pågrepet som følge av FBIs hacking. Vi syntes sju saker i Norge hørtes for lite ut.

Vi visste heller ikke om noen hadde blitt dømt, uten at hackingen ble gjort kjent i retten. Vi fikk ikke svar på hva Kripos visste eller ikke visste om hackingen da anmeldelsene ble sendt ut og fikk ikke intervjue noen der. Mens oppfølging av dokumentaren pågikk, jobbet vi for å finne ut av disse problemstillingene.

2.2.4 Saken vokser

I juli, over et halvt år etter at jeg begynte med saken fikk jeg på tredje eller fjerde forsøk svar fra Kripos på hvor mange norske anmeldelser de hadde opprettet i PLAYPEN-saken. Kripos hadde sendt 43 anmeldelser til lokale politidistrikt.

Jeg måtte få avklart at anmeldelsene var like, og at grunnlaget var det samme i hver av disse. Da jeg ba Kripos om å få spesifisert at det gjaldt IP-adresser og med «logging» som forklaring, fikk jeg dette til svar:

> «Det er distriktene som eier sakene og som må ta stilling til spørsmål om innholdet i hver enkelt anmeldelse. For mer info om selve operasjonen henviser vi til Europol»

For å få bekreftet at samtlige saker var like, og følgelig problematisk, måtte jeg altså kontakte politidistriktene om hver enkelt sak - igjen.

2.2.5 Innsyn uten innsyn - runde 2

Det eneste jeg hadde fått var en oversikt som viste fordelingen av saker på politidistrikt. Den tydeliggjorde at svarene jeg hadde fått i runde 1 ikke stemte. De fleste distrikt hadde flere saker enn de hadde oppgitt da jeg ringte første gang.

Siden det var fortsatt snakk om anmeldelser, så kunne ikke innsynsforespørsler fungere. For å få ut informasjonen måtte jeg først kontakte distriktenes kommunikasjonsavdeling og identifisere sakene med de samme nøkkelordene. Siden jeg hadde antallet var det litt enklere enn første runde, men fortsatt arbeidskrevende og det pågikk fra august og i et par måneder.

Jeg gikk ut i permisjon fra Adresseavisen 1. august, men bestemte meg for å bruke kvelder og ledig tid på å gjøre ferdig oppfølgingen. Jeg visste, eller hadde i hvert fall en svært sterk mistanke, om at anmeldelsene var like. Det gjorde at jeg kunne lage spørsmål som avkreftet eller bekreftet det jeg hadde behov for å vite:

- Hva var grunnlaget for mistanken mot siktede?
- Hvordan er grunnlaget beskrevet?

For å holde oversikt over hvem som svarte, på hva og hvor mange purringer til rekken med informasjonsmedarbeidere, så brukte jeg Excel med fargekoder for å indikere status.

4	Agder	1	NEI	Ja	kommunikasjon.agder@politiet.no			8.08	Purret 31.08	Purret 30.09
5	Finnmark	1	NEI	Ja	kommunikasjon.finnmark@politiet.no			8.08	Ring påtaleleder Morten Daae på 78 97 20 00	Ferie til 07.09
6	Innlandet	3	NEI	Ja	kommunikasjon.innlandet@politiet.no		8.08	Ja	Hjalmarsen har en, i tillegg kommer politiadvokat Ingveig Nøkleby, tlf 61 15 15 09 og en til (på Lillehammer)	Mail til Hjalmarsen og kommunikasjonsavd 31.08
7	Møre og Romsdal	3	NEI	Ja	olav.sindre.rise@politiet.no		8.08	Ja	Politiadvokat Inger Myklebust Ferstad	To dommer, og en ferdig etterforsket
8	Nordland	4	NEI	Ja	kommunikasjon.nordland@politiet.no		8.08	Ja	Purret 31.08	Svarer ikke, purr igjen 07.09
9	Oslo	6	NEI	Ja	kommunikasjon.oslo@politiet.no		8.08	Ja	3 etterforskes, 1 er avgjort i retten, 2 henlagt. Påtaleansvarlig er Lene Hammersland	Mail til Hammersland 31.08, purret 04.09
10	Sør-Vest	4	NEI		SMS sendt til kommunikasjon			Ja	Annbjørg Ingebrigtsen Erik W. Rand Lars Ole Berge 22.08 Synnøve Haugstvedt Lande	
11	Sør-Øst	5	NEI	Ja	kommunikasjon.sorost@politiet.no		8.08	Ja	Ann Iren Svane Mathiassen Søndre Buskerud 32 80 55 00, Mari Gjersøe, Vestfold, 33 34 44 00 - Tine Henriksen , Telemark, 35 90 64 00 9.08 Saken ligger hos Nordland, altså at de skal	Mathiassen svarer ikke 31.08, Gjersø svarer ikke 31.08, Henriksen borte til 01.09
12	Troms	0	Ingen sak	Ja	Post.troms@politiet.no		8.08	Ja	8.08 ha 4 saker	Ferdig
13	Trøndelag	5	NEI		Har kontroll			Har kontroll	Ferdig Vil ha spørsmål på mail til	Ferdig

3 Henvendelser og svar fra alle politidistriktene ble logget i et Exceldokument

De fleste politidistriktene og politiadvokatene forholdt seg profesjonellt, og svarte på spørsmålene. I ett tilfelle takket også en for informasjonen om hackingen. Fra andre distrikt kom det noen ganske spesielle svar, for å unngå å svare på spørsmålene knyttet til anmeldelsene og grunnlaget for dem.

Jeg supplerte med å snakke med siktedes representanter, og etter et par måneder hadde jeg fått svar i 40 av 43 saker. De tre siste hørte til i Oslo som ikke ville si noe fordi de var under etterforskning to år etter at de hadde fått opplysningene:

> Når det gjelder anmeldelser vi mottar fra Kripos, kan jeg på generelt grunnlag si at det i enkelte tilfeller vil være slik at vi har tilstrekkelig informasjon i det materialet vi mottar fra Kripos (nok info til å identifisere en mistenkt) mens det i andre tilfeller vil være slik at vi må foreta oss ytterligere etterforsking for å avklare nærmere hvem som er mistenkt i saken.

A) Hva var målet?

Få bekreftet at det nasjonale antallet hackingsaker var 43.

B) Hva ble funnet

Jeg kunne dokumentere at utgangspunktet for 40 straffesaker mot nordmenn var hackingen fra USA. I de tre siste fikk jeg kun opplyst at anmeldelsen kom fra Kripos. Jeg har lagt til grunn at de ikke skiller seg fra de andre 40 som er opprettet av Kripos på bakgrunn av IP-bevis fra FBI i samme sak og i samme avgrensede tidsperiode.

2.2.6 Innsyn i rettsdokumenter

Selv om det totale omfanget nå var dokumentert, ville vi også vite om det hadde kommet rettskraftige dommer. Det virket sannsynlig, siden det nå var 2 år siden norske myndigheter fikk opplysningene fra FBI.

A) Hva var målet?

Få tak i dokumenter som viste om noen var dømt som en direkte konsekvens av hackingen. Finne ut om påtalemyndigheten opplyste om metodebruken da de førte sakene for norske tingretter.

B) Hva ble funnet

Som følge av grovjobben i andre runde, hadde jeg fått identifisert de tilfellene som var avgjort ved dom. De var, som sakene, spredt over hele landet. Jeg kontaktet 15 tingretter på vanlig måte og fikk tilsendt dommene. Jeg fikk sjekket at de stammet fra FBI-hackingen på to måter:

- Det var opppgitt at saken hadde utspring i opplysninger fra USA i forbindelse med PLAYPEN
- Jeg kunne bruke datospennet for aksjonen til å se at nordmennene var hacket. Dette var i saker hvor det kun var oppgitt i tiltalepunktene at vedkommende hadde vært inne på en overgrepsbildeside på det mørke nettet mellom 21.02.2015 og 04.03.2015.

Metodebruken til FBI var ikke beskrevet i dommene. I en sak hadde imidlertid retten fått vite om hackingen: En forsvarer i Bergen gikk hardt ut mot metodebruken, og at den var skjult for ham som forsvarer og for klienten. Forsvareren hadde funnet ut om hackingen ved å lese vår første dokumentar fra januar. Denne saken var en av tre fra FBI-hacking som inngikk i bergenspolitiets bejublede «Dark Room»-kompleks.

2.3 Mål 3

2.3.1 Runddansen

En annen forsvarer i en av de første sju sakene, advokat Jørn Mejdell Jakobsen, forsøkte å finne ut hva som hadde skjedd. Han var ikke orientert om at klienten, en mann fra Hedmark, var hacket. Selv om flere av de andre advokatene ga uttrykk for overraskelse og eller irritasjon, var det ingen som formelt utfordret bevisene. Det hadde sammenheng med at de siktede ikke ønsket offentlighet, eller oppmerksomhet rundt det faktum at de hadde sett på overgrepsbilder. De fleste ville bare ha saken ut av verden.

Mejdell Jakobsen var den eneste forsvareren som forfulgte IP-beviset. Han krevde forklaring fra Kripos, og ba om en redegjørelse fra påtalemyndigheten. Vi hadde også spurt om dette, uten å få svar. Men når en aktør i en sak spør, skal imidlertid påtalemyndigheten svare.

A) Hva var målet?

Finne ut hva man hadde visst om metodebruken til FBI.

B) Hva ble funnet?

Advokatens spørsmål til myndighetene ble starten på en spesiell runddans:

Henvendelsen hans ble først rettet til lokal politiadvokat, så til Kripos før den kom i retur og var innom stedelig statsadvokat på Hedmark før den gikk til Det Nasjonale Statsadvokatembetet og tilbake – uten en redegjørelse advokaten var fornøyd med.

Det lot videre til at norske myndigheter ikke hadde fått informasjon om metodebruken, eller funnet grunn til å spørre amerikanerne om hvordan de hadde gått frem for å avgjøre om det kunne være problematisk i henhold til norsk lov.

C) Forholdet til andre metoder

Jeg skulle skrive en sak om at advokaten ikke fikk de svarene han var ute etter. I den forbindelse stilte jeg noen spørsmål til Kripos. Jeg inkluderte, for tredje eller fjerde gang, spørsmålet om hvor mange norske PLAYPEN-saker det var. Det var her jeg omsider fikk opplyst hva antallet var.

2.3.2 Det siste spørsmålet

Jeg hadde også forsøkt å få svar fra Kripos om hva de visste da anmeldelsene ble sendt ut, uten å lykkes. Jeg fikk ikke intervjue tjenestemannen som hadde skrevet dem, eller leder for retts- og påtaleenheten. Jeg sendte flere spørsmål på e-post, men fikk som regel kun generelle svar i retur.

Gjennomgangen av alle dommene ga imidlertid et slags svar på spørsmålet:

I den foreløpige siste, avsagt i Vesterålen tingrett, ble det lagt «avgjørende vekt» på vitnemålet til en etterforsker fra Kripos. Han skal ha oppgitt til retten at Kripos ikke visste hvordan FBI hadde fått tak i IP-adressene og at det «egentlig ikke skulle gå an» å logge dette fra personer som brukte en Tor-nettleser.

Uttalelsene ble forelagt Kripos for korrigering dersom det ikke var riktig gjengitt. Det ble ikke gjort, og Kripos svarte meg med at retten hadde fått opplyst det Kripos visste om saken.

3. Spesielle erfaringer

3.1 Motstand

Norske journalister har veldig få verktøy tilgjengelig for å ettergå politiets etterforskning. Dette preget alt arbeid med «Grenseløs»-prosjektet. Som nevnt har ikke pressen i dag adgang til å kreve innsyn i anmeldelser. Vi har heller ikke tilgang til innsyn i etterforskningsdokumenter (med noen få unntak som ikke har vært relevante her).

Erfaringen var at et journalistisk fokus som vårt, ikke ble satt særlig pris på. Det er dog ikke utelukkende urimelig: Politiet har en lang rekke legitime årsaker til å ville beskytte sine etterforskninger. I mange av tilfellene var sakene også pågående på et nivå i systemet.

Vi ble møtt med taushet fra Kripos, som ikke ville svare på noen konkrete spørsmål om saken eller opplyse om omfanget, som vi ba om gjentatte ganger, før etter over et halvt år.

Kripos ønsket kun å stille med generelle formuleringer om internasjonalt politisamarbeid og hvordan dette håndteres her. Norge legger til grunn at det som er samlet inn av internasjonale partnere, er gjort i samsvar med lokale lover, var omkvedet. Senere dukket de samme

formuleringene opp igjen fra Kripos på høsten 2017 da VG publiserte sitt arbeid rundt CHILDS PLAY.

I forbindelse med den første grovjobben for å få dokumentert det totale antallet saker viste det seg senere at vi hadde fått svært upresise svar fra politidistriktene. Det er verdt å notere seg, uten å ta stilling til hvorfor.

På et tidspunkt i denne første kartleggingsfasen ble det sendt eposter om våre henvendelser fra minst et distrikt til et annet. Ved et tilfelle fikk vi også spørsmål om vi ikke ville se eksempler på hvilke bilder som de siktede mennene hadde lastet ned. Dette takket vi nei til.

3.2 Kritikk

I forbindelse med arbeidet har vi skrevet ulovlig hacking. Dette har vi fått kritikk for, spesielt i intervjusituasjoner med politikilder og Kripos. Anføringene har vært at det ikke kan slås fast at hackingen er ulovlig, fordi den skjedde med en ransakingskjennelse utstedt av en dommer i USA.

Jurist Ingvild Bruce, som forsker på internasjonale politimetoder ved Universitet i Oslo, har også ment at selv om norsk politi ikke kunne hacke selv, så er ikke FBIs metode ulovlig fordi norsk Høyesterett har tillatt bruk av informasjon innhentet av politi i andre land med metoder som norske tjenestemenn og kvinner ikke kan bruke.

Dette er legitim kritikk som vi skal være lydhør for. Adresseavisens omtale av metodebruken som ulovlig hviler på følgende faktum:

- FBI driver et overgrepsbildenettsted, en utenkelig, ulovlig virksomhet for norsk politi
- FBI får adgang til å ransake serveren med en ransakingskjennelse utstedt av en domstol med jurisdiksjon i en avgrenset del i en av USAs femti delstater. Med denne som eneste lovhjemmel infiserer og ransake pcer over hele verden
- FBI har ingen jurisdiksjon i Norge, og kan heller ikke bruke tvangsinngrep, som dataavlesing, på norsk jord
- FBI har tatt seg inn på norske pcer i Norge ved å manipulere / bruke et ikke offentlig-kjent sikkerhetshull i programvaren uten norsk lovhjemmel
- Dataavlesing som politimetode var ikke lov i Norge, hvor det skjedde, da det skjedde

3.3 Etterspill

- Da den første dokumentaren ble publisert i januar 2017 ble den første konsekvensen at forsvarsadvokatene i de sju sakene fikk vite at klientene hadde blitt ransaket fordi FBI hadde hacket dem i strid med loven, uten at de eller domstolen som tillot ransakingen fikk vite om det. En av dem karakteriserte det som et rettsikkerhetsproblem, slik også jusseksperter gjorde.

- I Hedmark ble en tilståelse utsatt mens forsvareren krevde forklaring fra Kripos og påtalemyndigheten om hvorfor han og domstolen ikke var fortalt om bakgrunnen for beviset. Han ville også ha forklaring på hva norske myndigheter visste om FBIs metodebruk.

- I Trøndelag ble også lokalt politi gjort oppmerksom på at det problematiske utgangspunktet for sakene de hadde etterforsket og ført for retten. Førstestatsadvokat Bjørn Kristian Soknes uttalte at han var kritisk til at opplysningene om hacking ikke var blitt gjort kjent:

  - Jeg er imponert over at Adresseavisen har klart å få frem dette, men hadde det kommet en anmeldelse fra Kripos som formelt sett virket i orden, så hadde jeg lagt den til grunn selv også, sa Soknes.

  Videre instruerte førstestatsadvokaten lokalt politi i at en sak som skulle avgjøres ved tilståelse skulle til full behandling i retten, og at informasjonen om FBI-beviset nå skulle legges frem.

- Inntrøndelag tingrett trakk en sak mot en mann i Nord-Trøndelag som hadde tilstått. Saken ble senere omberammet. Også i denne saken må politiet fortelle retten om bevisene i en hovedforhandling. Alt dette skjedde fordi forsvareren problematiserte bevisene etter å ha lest Adresseavisens saker.

- Leder for forsvarergruppen i Advokatforeningen, Marius Dietrichson, ba om gransking av hvorfor Kripos ikke opplyste om hackingen. Det ble ingen granskning etter det vi kjenner til.

- Forsvareren på Hedmark var ikke fornøyd med svarene han fikk fra norske myndigheter. Han begjærte IP-beviset avskåret fra saken mot hans klient. Dette ble avvist av Glåmdal tingrett og Eidsivating lagmannsrett. Høyesterett ville ikke behandle anken.

- På Vestlandet har flere FBI-saker blitt satt i bero, i påvente av ankene på Hedmark.

- Hadia Tajik (Ap) var leder for justiskomiteen på Stortinget da den første saken ble publisert i januar 2017:

  - Dette er en kompleks sak. Full honnør til dere som har klart å nøste i den, sa Tajik (Ap) som uttalte at hun ville følge sakene:

  - Jeg vil ikke foregripe domstolens behandling her, men vi vil følge nøye med utfallet for å vurdere om det er behov for oppfølging fra lovgivers side.

  Etter at saken med det totale omfanget ble publisert forsøkte vi å få en ny kommentar fra Arbeiderpartiet, uten hell. Vi var i kontakt med Riksadvokaten allerede i januar 2017, men uten å få kommentarer til sakskomplekset.

3.3.1 CHILDS PLAY

7. oktober publiserte VG en stor sak om overgrepsbildenettstedet CHILDS PLAY, som var det mørke nettets største i 2017. Artikkelen forteller at VG avdekket at det var australsk politi som driftet CHILDS PLAY, etter samme fremgangsmåte som FBI brukte i PLAYPEN-komplekset i 2015.

CHILDS PLAY fikk imidlertid være i virksomhet (under politiets kontroll) mye lengre, i 11 måneder, selv om det ikke skal ha blitt brukt hacking for å avsløre brukere slik FBI gjorde.

Saken, som er glimrende løst, skapte mye oppmerksomhet. VGs jobb førte til at riksadvokaten innkalte Kripos, PST og andre politiorganisasjoner til et møte om «utradisjonelle etterforskningsmetoder på nett».

I innkallelsen het det at behovet for møtet var der også før CHILDS PLAY-saken sprakk:

> «I forbindelse med VGs omtale av hvordan australsk politi har operert på nettet for å avsløre seksuelle overgrep mot barn og et tidligere formidlet, sterkt ønske fra enkelte miljøer innen norsk politi om endrede retningslinjer for slik virksomhet, er det behov for et møte ved Riksadvokatembetet for å drøfte ulike problemstillinger.»

Et av punktene på agendaen var spesielt interessant med henblikk på PLAYPEN-komplekset:

> Hvordan norsk politi kan bruke informasjon som andre lands politi og samarbeidende tjenester har hentet inn med metoder som ikke er i samsvar med norsk regulering. Og hvorvidt dagens situasjon er tilfredstillende.

En konklusjon var ventet før jul. 14. desember svarte Riksadvokaten slik på vår henvendelse:

> Til info er ikke ferdige med oppfølgingen av møtet.
> Vi holder på, både med å vurdere behovet for å endre retningslinjene (for bruk av utradisjonelle etterforskingsmetoder på internett) og å vurdere behovet for å ta et initiativ overfor lovgiver.

3.4 Moralske problemstillinger

Da vi oppdaget at det hadde skjedd noe i disse sakene som flere svært rutinerte forsvarere sa de aldri hadde sett før, var det vanskelig å tenke at det ikke var dypt problematisk. Saken synliggjør de juridiske utfordringene som norsk politi og påtalemyndighet blir stilt ovenfor stadig oftere i en verden med grenseløs teknologi.

Funnene var også problematiske på et moralsk nivå. Disse 43 mennene oppsøkte bevisst overgrepsbilder av små barn. De var alle skyldige. Tanken på at journalistikken vår kunne «hjelpe» disse personene til lavere straff eller eventuelt opphevede dommer, var vond å forholde seg til.

- Ingen går i fakkeltog for disse folkene her, sa kollega Simen Granviken som i månedsvis forsøkte å få riksadvokaten i tale, eller noen politikere i Oslo til å reagere på det flere eksperter og advokater omtalte som et soleklart rettsikkerhetsproblem.

Internt i redaksjonen ble den samme problematikken luftet: «Er det ikke bare bra at politiet tar disse folkene da?» Det er synspunkt som er til å forstå.

Samtidig går mye av jobben som journalist ut på å sørge for at myndighetene forholder seg til spillereglene, og at loven er lik for alle, uansett type kriminalitet. Det var prinsipielt vanskelig

å se hvordan det skulle være greit at norske borgere ble utsatt for inngrep som ikke er lov her til lands, selv om deres er blant de verst tenkelige forbrytelsene.

Videre var det tilsvarende vanskelig å skulle se at det ikke var et problem at denne kontroversielle metodebruken ikke skulle løftes til behandling av rettssystemet – på samme måte som all annen metodebruk i alle andre saker.

Vi har forsøkt å holde tak i rettssikkerhetsproblematikken i dette sakskomplekset, og det er tydelig fra disse sakene (og fra VGs prosjekt om Childs Play) at det er behov for å definere på nytt hva man i Norge aksepterer av metoder fra samarbeidende politimyndigheter i utlandet.

Erfaringen fra PLAYPEN-sakene er at man tilsynelatende ikke sjekker informasjon fra utlandet fordi man stoler på internasjonale samarbeidspartnere. Her er det verdt å merke seg at FBI har en rik historie med kontroversiell metodebruk og skandaler knyttet til den.

Informasjon om metodebruken i PLAYPEN-sakene lå offentlig tilgjengelig på nettet allerede kort tid etter at Kripos mottok de 43 IP-adressene i 2015. Det var mulig å lese seg opp om metodebruken ved enkle google-søk, også for norske etterforskere.

Det kan være direkte farlig dersom Norge kan tillate seg å rettsforfølge borgere som er utsatt for rettighetskrenkende inngrep av andre lands politimyndigheter som ikke er tillatt her – uten at de det gjelder eller rettsstaten får vite om det.

Den internasjonale kampen mellom grenseoverskridende nettkriminalitet begått ved hjelp av avansert krypteringsteknologi og nye politimetoder sklir tilsynelatende ofte over i juridiske og etiske gråsoner. Derfor er det viktig at debatten om dette ikke bare skal foregå i lukkede fora. Fordi den handler om rettssikkerhet, likhet for loven og hva samfunnet skal akseptere, må debatten tas lengst mulig vekk fra det mørke nettet, og tåle dagens lys.

4. Publiseringsliste

09.01.2017	Tatt etter ulovlig politihacking
12.01.2017	- Veldig alvorlig
13.01.2017	Hva sier loven om FBI-hackingen?
14.01.2017	Førstestatsadvokat kritisk til håndtering av FBI-hacking
18.01.2017	- Kripos må svare på hva som har skjedd her
20.01.2017	Politikerne vurderte aldri utenlandsk dataavlesing
22.01.2017	Mener politi-hacking må granskes
12.02.2017	Utsetter tilståelse etter hacking
16.03.2017	- Uten ulovlige bevis ville saken vært avvist
19.03.2017	Statsadvokat ber politiet fortelle om FBI-hacking
21.10.2017	43 nordmenn ulovlig hacket av FBI
21.10.2017	Åpner for å la FBI hacke lovlig i Norge
23.10.2017	Domstol trakk sak etter info om FBI-hacking
02.11.2017	15 dømt etter ulovlig FBI-hacking
08.11.2017	Behov for oppdatering av retningslinjer
29.11.2017	Domstoler: Bevis fra ulovlig hacking er lovlig
28.12.2017	Høyesterett avviser hacking-anke i FBI-sak