



Metoderapport til SKUP 2013

Marte Ramuz Eriksen og Osman Kibar
Dagens Næringsliv

En umulig oppgave?

Hvordan man kan:

Uten konkrete tips, uten kilder i felten, uten kjennskap til markedene begynne å nøste opp hvordan et av verdens største teleselskaper, med Telenor på eiersiden, har forsterket og beriket noen av verdens verste regimer ved å inngå hemmelige avtaler med håndlangere til noen av verdens mest brutale regimer og hjelpe dem til å avlytte demokratiforkjempere Alt dette for å berike selskapets aksjonærer – en russisk oligark og den norske stat?

Når:

- kildene er milevis unna
- store selskaper med store informasjonsavdelinger holder potte tett
- desinformasjon er systematisert
- all informasjon om overvåkningsmetodene er taushetsbelagt
- sakens hovedpersoner er i samfunnets øverste sjikt av mektige, rike og privilegerte i ukjente land
- alle som kan gi informasjon om hva som egentlig skjer, risikerer å bli forfulgt og trakassert av myndighetene
- det man skriver, sender og sier for å få informasjon om hva som skjer kan være overvåket
- hovedpersonene er hemmelige bakmenn som skjuler seg i skatteparadiser
- og nesten alle nettsøkene ender opp i sider på tadsjikisk, kirgisisk, kasakhstansk eller usbekisk.

Men likevel fastslå at:

Mobilselskapet Vimpelcom har bidratt til autoritære regimers overvåkning og forfølgelse av demokrati- og menneskerettighetsforkjempere. Storeier Telenor har gitt grønt lys til hemmelige avtaler med diktatorenes innerste sirkel.

Alle disse har vært kilder:

- En intetanende hestepasser
- En søkkrik diktatordatter
- En etterretningssjef på rømmen
- En dame med 35 telefoner
- En drapstruet mann som skal omfordele 84 millioner dollar
- En håndfull av Vimpelcoms 20 millioner mobilkunder i sentral-Asia
- Sporene etter en internasjonalt etterlyst mobiltopp
- En av verdens rikeste menn
- En modig kvinne som er blitt fratatt indre organer
- Advokater som ikke får tak i klientene sine
- En politimann som vil fryse to milliarder kroner
- Eiere som har gått under jorden
- Ambassader som roser landet sitt
- Informasjonsavdelingen til flere av verdens største mobilselskaper (og mange flere)

Samt:

- Registersøk i skatteparadiser – med resultat!
- Kredittilsynsrapporter, salgsprospekter for store banker, søksmålspapirer fra flere land
- Gamle avisartikler, tidligere årsrapporter, utskrifter av telefonsamtaler med investorer
- Nedlagte nettsider som ikke lenger finnes
- Lovtekster fra fire land
- Tiltalebeslutninger på russisk
- Lisensutlysninger
- Selskapsstrukturer som aldri har vært offentliggjort
- Byggetillatelser
- Internasjonale selskapsdatabaser
- Bilder fra motenettsteder
- Departementskunngjøringer fra Kasakhstan, Kirgisistan og Usbekistan
- Twitter-meldinger
- Mobilreklamekampanjer
- Beslaglagte e-poster
- Svenske kontoopprettelsesdokumenter
- Aksjonærbrev
- En avhandling om konspirasjonsteorier i sentral-Asia
- Et kasakhisk sjekkenettsted

Informasjon

Tittel på prosjektet	Farlige forbindelser
Journalister	Marte Ramuz Eriksen, mob. 952 21 425, mre@dn.no Osman Kibar, mob. 932 56 013, osman.kibar@dn.no
Publisert	Oktober til desember 2012.
Redaksjon	Dagens Næringsliv Postboks 1182 Sentrum 0107 Oslo Sentralbord: 22 00 10 00

Hva er nytt

DN har for første gang fortalt historien om det delvis Telenor-eide teleselskapet Vimpelcoms suksessrike ekspansjon til Sentral-Asia. Vimpelcom har gitt sin storeier Telenor 40 milliarder kroner samlet i urealisert gevinst. Den norske toppsjefen i selskapet, Jo Lunder, har lang fartstid fra norsk næringsliv. Telenor-sjef Jon Fredrik Baksaas sitter i styret.

DNs artikkelserie viser at suksessen har hatt en høy pris:

Vimpelcom har systematisk inngått hemmelige partnerskap med forretningsfolk med meget nær tilknytning til myndighetspersoner i Kasakhstan, Usbekistan, Tadsjikistan og Kirgisistan. Blant dem er rådgiveren til Kasakhstans mangeårige president, svogeren til Tadsjikistans mangeårige president og personer med nær tilknytning til Usbekistans presidentfamilie. Dette har skjedd med Telenors fulle velsignelse.

Vimpelcom har også forpliktet seg til å gi myndighetene overvåkingstilgang gjennom en bakdør til mobilnettet. Denne bakdøren blir brukt til å overvåke, forfølge og kneble opposisjonelle, regimekritikere, journalister og menneskerettighetsforkjempere.

Dette har tidligere aldri vært omtalt i norske eller utenlandske medier.

Arbeidet

I dette sakskomplekset er det to sentrale selskaper. Innledningsvis følger en kort beskrivelse.

Vimpelcom

- Internasjonalt teleselskap med 212 millioner abonnenter i 18 land.
- Verdssettes til rundt 18 milliarder dollar (rundt 100 milliarder kroner) på børsen i New York.
- Toppsjef er norske Jo Lunder, som har lang fartstid fra Telenor-systemet.
- Telenor har vært aksjonær i Vimpelcom siden 1998.
- Storeire er norske Telenor (37,5 %) og den russiske oligarken Mikhail Fridmans Altimio (52,7 %).
- I 2004 besluttet styret i Vimpelcom at selskapet skulle vokse ut av hjemmemarkedet Russland. Første stopp var Kasakhstan (2005), deretter kom Tadsjikistan (2005), Armenia, Georgia og Usbekistan (alle i 2006) og Kirgisistan (2008).
- Samme år startet en åpen maktkamp mellom de to storeierne Telenor og Altimio. Denne maktkampen har dominert nyhetsdekningen av Vimpelcom det siste tiåret.

Telenor

- Andre største aksjonær i Vimpelcom.
- Internasjonalt teleselskap med 150 millioner abonnenter i 11 land.
- Verdssettes til rundt 180 milliarder kroner på Oslo Børs.
- Toppsjef er norske Jon Fredrik Baksaas.
- Den norske staten, ved Nærings- og Handelsdepartementet, er største eier med 54 prosent. Folketrygdfondet har nesten fem prosent.
- I 1998 gikk Telenor inn i det konkurstruede russiske mobilselskapet Vimpelcom. Har siden sittet med en stor aksjepost og en rekke styremedlemmer i selskapet. Dagens Telenor-representanter i Vimpelcom-styret er konsernsjef Jon Fredrik Baksaas, konserndirektør Kjell Morten Johnsen og Russland-sjef Ole Bjørn Sjulstad.
- Siden 2004 har Telenor utkjempet en åpen maktkamp med den andre storeieren i Vimpelcom, Altimio.

Når og hvordan kom arbeidet i gang, hva var ideen som startet det hele?

I april 2012 sendte SVTs Uppdrag Granskning en dokumentar om det svenske teleselskapet TeliaSoneras operasjoner i en rekke tidligere Sovjet-stater. Dokumentaren viste hvordan teleselskapene i disse landene må gi myndighetene en bakdør til mobilnettet. Adgangen til befolkningens kommunikasjon brukes av sikkerhetstjenestene til å overvåke og kontrollere regimekritikere.

Det hadde fått så godt som ingen oppmerksomhet i Norge, men Telenor-eide Vimpelcom hadde også spesialisert seg på å drive mobilvirksomhet i de tidligere Sovjet-republikkene – om enn i andre stater enn svenskene: Hadde Vimpelcom forpliktet seg til å gi samme overvåkingstilgang som TeliaSonera?

Den første henvendelsen vår gikk til Telenor: "Dette må Vimpelcom redegjøre for", var beskjeden. Neste henvendelse gikk til Vimpelcom: "Vimpelcom følger lojalt regelverket i landene de opererer i. Kontakt de respektive land for en redegjørelse for lovverket", svarte selskapet.

Der stoppet det.

Det var året etter den arabiske våren, da internetts og mobilteknologiens frigjørende egenskaper var hyllet og feiret verden over. Men den nye teknologien og de revolusjonsliknende begivenhetene i arabiske land hadde også en annen side. I frykt for politiske omveltninger valgte mange av verdens autoritære regimer å stramme til overvåkningen av kommunikasjonen via sosiale medier, mobiltelefoni og internett – for å prøve å forhindre sosiale opprør og dempe eventuell kritikk. Teleselskapene bidro.

Et statlig eid norsk selskap, Telenor, hadde i all stillhet vært med på å erobre en viktig markedsposisjon i noen av verdens mest autoritære regimer gjennom eierskapet i Vimpelcom. Kunne det være at Vimpelcom også hadde forpliktet seg til å gi sikkerhetstjenestene tilgang til befolkningens kommunikasjon gjennom hemmelige bakdører i mobilnettet – med Telenors fulle velsignelse? Hvordan kunne vi eventuelt dokumentere dette?

Dette var land vi aldri tidligere hadde skrevet om, og hvor vi heller ikke hadde en eneste kilde fra før. Hvor skulle vi begynne? Informasjonen var ikke bare vanskelig tilgjengelig. Den var også bevisst hemmeligholdt – både fra selskapenes side og myndighetenes.

Marte Ramuz Eriksen er journalist i Dagens Næringslivs finansredaksjon. Hun følger telebransjen spesielt. Osman Kibar er journalist i Dagens Næringslivs lørdagsredaksjon og har skrevet flere saker om nyere overvåkingsteknologi. De to ble fristilt fra annen feature- og nyhetsjobbing for å fordype seg i materien. Research-fasen varte i to måneder, med mye kvelds- og helgearbeid. Vi startet undersøkelsene ultimo august, første artikkel ble publisert ultimo oktober.

Problemstillingen

Utgangspunktet for prosjektet var å sjekke om også Vimpelcom hadde forpliktet seg til å gi myndighetene en bakdør til mobilnettet.

Vimpelcom har operasjoner i 18 land. Ettersom verken Telenor eller Vimpelcom ville bidra til å opplyse om regelverket, måtte vi researche hvert enkelt land.

Vi innså raskt at disse landene også har utfordringer knyttet til korrupsjon og nepotisme. Antydninger i lokale medier om at Vimpelcoms partnere satt i sentrale myndighetsposisjoner, vekket vår interesse. Vi utvidet researchen til også å undersøke hvem som var Vimpelcoms lokale partnere.

Tidlig i prosjektet lagde vi en hypotese vi mente var dristig:

Delvis Telenor-eide Vimpelcom har systematisk inngått forretningsmessig og politisk samarbeid med noen av verdens verste diktatorer.

Betingelse: å gi myndighetene overvåkingstilgang og å dele selskapene med diktatorenes innerste sirkel.

Vi var innstilt på at denne hypotesen måtte justeres etter hvert som vi fant ut mer, men dette ble ikke nødvendig.

På bar bakke

Vi startet i praksis på scratch, basert på en idé og noen hypoteser. Det ble et spesielt utfordrende prosjekt av flere grunner:

- Det var snakk om hemmelige selskapsavtaler inngått av store teleaktører, med fremmede lands myndigheter som ikke har noen tradisjon for åpenhet.
- Vi måtte følge selskapsstrukturer som strakte seg over en lang rekke land, i flere verdensdeler og gjennom kjeder av skatteparadiser. Hver gang eierskapene strakk seg over en ny landegrense, var vi nødt til å identifisere selskapsregistre og rapporteringsregler.
- Vi hadde ingen kunnskap om markedssituasjonen i de respektive landene på mobilområdet. Informasjonen om lokale aktører, deres selskapsstrukturer og eierposisjoner er ikke like lett tilgjengelig i Tadsjikistan som i Norge.
- Vi hadde ingen informasjon eller tilgang til sentralasiatiske lands jurisdiksjon innen telekomsektoren og de lovmessige forpliktelsene til teleselskapene i Kasakhstan, Usbekistan, Tadsjikistan, Kirgisistan. Vi kjente heller ikke til deres juridiske terminologi for overvåkning.
- Vi måtte skaffe oss kunnskap om mobilteknologisk infrastruktur, oppdatert kunnskap om teknologiske muligheter for overvåkning, oversikt over hva som finnes på markedet og innblikk i selve operasjonen av systemer for avlytting og overvåkning.

- Kunnskap om de politiske forholdene i sentralasiatiske land, situasjonen for opposisjonelle, menneskerettigheter sett fra primærkilders ståsted, hadde vi heller ikke på forhånd.
- Vi måtte identifisere opposisjonelle med høy troverdighet og omfattende erfaring med problemstillingene en halv jordomdreining unna. Finne dem, kontakte dem og få dem til eventuelt å stille til intervju uten å utsette dem for fare.
- Vi måtte researche, navigere i og forstå tung informasjon på mange språk – flere av dem utenfor allfarvei, som kasakhisk, usbekisk, tadsjikisk og kirgisisk – foruten engelsk, russisk, fransk og tyrkisk.

Slik gikk vi frem

Vi sto overfor et formidabelt arbeid. Vimpelcom har mobilvirksomhet i 18 land langt unna. Arbeidet ble gjennomført i flere faser. Vi vil redegjøre for hver enkelt fase.

FASE 1: OVERBLIKK OG AVGRENSNING

Overblikk

Hva vi gjorde: Vimpelcom har mobilvirksomhet i 18 land, i all hovedsak langt fra Norge. For å skaffe oss et oversiktsbilde av Vimpelcoms operasjoner strukturerte vi undersøkelsene etter følgende kriterier:

- Hva er de demokratiske forholdene i landet?
- Hvilken lovgivning finnes for avlytting? Hvor utbredt er det, og finnes det tegn på at avlytting er politisk motivert?
- Hva er Vimpelcoms markedsposisjon, hvem er partnere, og hvordan kom selskapet seg inn på markedet?

Fremgangsmåte: Vi konsulterte rapporter og rådgivere fra menneskerettighetsorganisasjoner og frivillige organisasjoner som Den norske Helsingforskomiteen, Freedom House, Amnesty International og Human Rights Watch for å skaffe oss et bilde av situasjonen. Vi gjorde også søk i mediearkiver og konsulterte Vimpelcoms egenpresentasjoner. Vi opprettet egne ringpermer der vi plasserte relevant informasjon kategorisert etter land og tema. De mest interessante funnene ble samlet med relevante lenker i et eget Word-dokument, hvor den mest interessante informasjonen fremgikk i komprimert form. På denne måten fikk vi bedre oversikt og kunne lettere spore informasjon og research, også da mengden ble overveldende stor. Dokumentet fulgte oss hele veien. Vi gjorde omfattende søk i Wikileaks "Cablegate"-arkiv med lekkede dokumenter fra amerikanske ambassader, gjennom nett-tjenester som Cablesearch.org. Her var det mye interessant informasjon å hente. Vi kontaktet også aksjeanalytikere.

Hva vi fant: Vi fant alt fra mer eller mindre velfungerende demokratier til autoritære diktaturer. Avlyttingslovgivningen var i stor grad lik, men bruken av tilgangen varierte sterkt.

Vi fant at Vimpelcom som hovedregel hadde kommet seg inn i markedene ved å kjøpe hele eller deler av eksisterende mobiloperatører. Det var i varierende grad inngått partnerskap med lokale investorer.

Avgrensning

Hva vi gjorde: Vi satt med grunnlagsdokumentasjon på 18 land. Nå måtte vi systematisere. Hvilke land ville vi gjøre grundigere undersøkelser på? Vi gikk etter de punktene som vi pekte ut i orienteringsfasen, og peilet oss inn på land som oppfylte følgende kriterier:

- Demokratiseringsprosessen er ikke kommet langt
- Avlytting er utbredt og trolig brukt politisk
- Vimpelcom har en vesentlig markedsposisjon og eierandel.

Hva vi fant: Eliminasjonsprosessen ga oss til slutt en liste på fire land: Kasakhstan, Kirgisistan, Tadsjikistan og Usbekistan. Vi hadde skaffet oss basiskunnskaper om landene og markedene. Nå kunne vi gjøre grundigere undersøkelser.

FASE 2: DYPDYKK

Undersøkelsene fortsatte å følge stort sett de samme sporene som i den innledende fasen. Da vi skulle dykke videre ned i dette, fulgte vi tre spor: Overvåkingen, regimene og businessen. Vi vil gå gjennom arbeidet punkt for punkt, og sortert etter tematiske underkategorier.

Spor 1: Overvåkingen

Kartlegging av selskaper og land som hadde vært i søkelyset for avlytting

Hva vi gjorde: Vi kartla problemstillingene som hadde vært oppe knyttet til avlytting og overvåkning av mobilbrukere i andre land.

Fremgangsmåte: Vi gjennomgikk norske og internasjonale avisarkiver samt nyere faglitteratur om avlyttingsteknologi som var tilgjengelig fra tidligere research og fortløpende kontakt med kilder.

Hva vi fant: Den amerikanske telekjempen AT&T hadde gitt myndighetene hemmelig adgang til nettverket sitt. Lignende saker var rullet opp i en rekke europeiske land, deriblant Italia og Hellas og involverte store mobilselskaper. I Sverige var mobilselskapet TeliaSonera i søkelyset på grunn av avlyttingsbruk i den samme regionen som vi valgte å fokusere på, nemlig Sentral-Asia. Våre fokusland var ikke de samme som i TeliaSonera-saken med ett unntak: Usbekistan.

Hva vi brukte det til: Det ga oss innblikk i de tekniske mulighetene for overvåkning, rekkevidden og mulighetene for misbruk. Kartleggingen ble en sentral byggestein i det videre arbeidet, som gjorde det mulig å gjenkjenne overvåkning.

Kartlegging av infrastrukturen som muliggjør nasjonal overvåking

Hva vi gjorde: Målet var å få oversikt over situasjonen og teknologien og hvordan avlyttingssystemer kan implementeres hos en mobiloperatør. Hvem har tilgang, hvordan får de tilgangen, hva slags utstyr blir brukt og hvordan fungerer det i praksis?

For å få svar på dette gjennomgikk vi tekniske manualer for bruk og tilgang til bakdører i telenettet. Flere store leverandører av avlyttingsteknologi har produsert omfattende kataloglitteratur om produktene sine. Der beskrives løsningene i detalj. Flere av disse katalogene hadde vi enten fremskaffet selv eller konsultert online gjennom Wikileaks.

Vi ervervet kunnskap om oppbyggingen av infrastrukturen for moderne telefonsentraler gjennom faglitteratur og kildesamtaler, samt kunnskap om teknologi som fasiliteterer informasjonsinnsamling og overføring av samtale- og trafikkdata til politi- og sikkerhetsmyndigheter.

Hva vi fant: Hva som skal til for å bruke bakdøren, og hvem som sitter på nøkkelen, varierer fra land til land.

Hva vi brukte det til: Researchen ga oss en grunnleggende forståelse av hvordan systemene for overvåking virker i praksis, hvem som kan ha og få tilgang. Samt hvordan teleselskapene i praksis gjennomfører det, når de forplikter seg til å gi myndighetene tilgang til kommunikasjonen i et land. Ettersom den reelle praksisen kan kamufleres gjennom komplisert fagterminologi, var det viktig å få en eksakt forståelse av kapasiteten og tjenestene.

Kartlegging av det juridiske grunnlaget for mobildrift og avlytting

Hva vi gjorde: Gjennom kildesamtaler fikk vi indikasjoner på at de fleste tidligere Sovjet-republikkene hadde lovgivning som lignet på den russiske lovgivningen for overvåking av kommunikasjon, også kalt SORM. Regelverket ble så vidt omtalt i Vimpelcoms årsrapporter. De gikk imidlertid ikke i detalj på samme måte om de andre landene selskapet opererer i. Vi måtte dermed likevel identifisere hvert enkelt lands telekomlovgivning – i henholdsvis Kasakhstan, Usbekistan, Kirgisistan og Tadsjikistan.

Fremgangsmåte: Her gjaldt det å finne lovtekstene som regulerer politiets og sikkerhetstjenestenes tilgang til telenettet, prosedyrene for uthenting av samtaleinformasjon og -data. Dette gjorde vi gjennom å finne de originale lovtekstene der de var tilgjengelige via nettsøk, for eksempel via departementer. Når tekstene ikke var tilgjengelige elektronisk, baserte vi oss på akademiske forskningsrapporter som refererer til de aktuelle lovene gjennom åpne nettsøk. Vi gikk for eksempel i gang med åpne nettsøk med riktig juridisk terminologi på de lokale språkene, snevret inn søkene til nasjonale ressurser og oppsøkte de statlige departementer via nett. Vi tok også kontakt med departementene.

Hva vi fant: Vi lyktes i stor grad å skaffe oss oversikt over lovtekstene og forskriftene som viser hva teleselskapene er pålagt å gjøre når de blir tildelt lisenser og frekvenser i de aktuelle landene.

Å finne dette forutsatte søk av tekniske termer på fremmede språk og alfabeter på nettet og maskinelle grovoversettelser underveis i researchen.

Vi fant ut at de fleste land har en form for lovgivning som gir myndighetene en bakdør inn i telenettet. Denne bakdøren, som på fagspråket kalles kommunikasjonskontroll, på engelsk "lawful

interception”, gir sikkerhetstjenester og politi mulighet til å gå inn i selve ryggraden av nettet og hente ut samtale- og trafikkdata.

Hva vi brukte det til: Dette gjorde at vi allerede hadde informasjonen på plass og kunne stille mer spesifikke spørsmål til teleselskapene, som gjerne besvarte disse spørsmålene i generelle termer.

Blant de interessante funnene ved gjennomgåelsen av disse tekstene var også informasjonen om at teleselskapene var pålagt å hemmeligholde avlyttingsprosedyrene.

Informasjonen ble også nyttig i kontakten med case-personene som var utsatt for overvåkingen.

Søk etter skriftlig dokumentasjon på politisk bruk av avlytting

Hva vi gjorde: Skriftlig dokumentasjon av telefonavlyttingen var også et viktig element. Vi ville dokumentere hvordan informasjon hentet ut av mobilnettene blir brukt i domstolene. Dette førte oss til en provins som befinner seg langt unna hovedstaden i Kasakhstan – og til en rettssak mot streikende gruvearbeidere.

Etter å ha kartlagt flere land gjennom samtaler med NGOer og lesning av rapporter, fattet vi interesse for en rettssak i den kasakhiske byen Zhanaozen. Den pågikk mens vi arbeidet med saken og hadde sterke innslag av avlytting i bevis materialet. Human Rights Watch hadde skrevet en egen rapport om saken og vi hadde to kilder som fulgte rettssaken tett som observatører. I tillegg lyktes vi i å finne tiltalene på nett.

Hva vi fant: I den lille provinsbyen Zhanaozen hadde en gruppe gruvearbeidere brutalt blitt meid ned av politiet etter måneder med fredelige protester. I kjølvannet av streiken var sentrale fagforeningsmedlemmer og støttespillere tiltalt for å ha oppfordret til sosial hat og uro. Tiltalene etter Zhanaozen-streiken var på rundt 1000 sider.

En sentral del av tiltalene var informasjon basert på telefonavlytting uten rettslige kjennelser - og også fra tiden før streiken brøt ut. Vi gikk gjennom samtlige tiltaler både ved hjelp av Google translate og ved hjelp av en norsk-russisk tolk.

Hva vi brukte det til: Gjennom rettssaken i Zhanaozen fikk vi håndfast dokumentasjon på flere ting:

- a. Et skriftlig bevis på at myndighetene benyttet seg av detaljert telefoninformasjon – telefonsamtaler, tekstmeldinger, informasjon fra basestasjoner og trafikkdata fra selskapene.
- b. Dokumentasjon på at avlyttingsinformasjonen som var fremskaffet ved hjelp av delvis Telenor-eide Vimpelcom ble brukt i politiske rettssaker, for å rettsforfølge og fengsle regimekritikere og opposisjonelle.
- c. Vi fikk også tilgang til et kildeunivers som ga oss mer informasjon og kunnskap om hva som hadde skjedd og hvordan avlytting var en del av hverdagen for regimekritikere.

Kartlegging av avlyttingen - bruk og omfang

Hva vi gjorde: Den tekniske muligheten for tilgang til kommunikasjonen gir både myndigheter og andre aktører muligheter – både til lovlig bruk med basis i rettslige kjennelser og ulovlig bruk/misbruk. Vi måtte derfor undersøke omfanget av både den lovlige/formelle og den ulovlige/uformelle avlyttingen. Samtidig måtte vi finne ut av om avlyttingen på noe vis begrenset muligheten for å drive regimekritikk i landene. Vi visste at avlyttingsmateriale ble brukt i rettsaker, fra forrige punkt. Vi måtte nå også snakke med folk. Vi tok kontakt med internasjonale observatører, opposisjonelle, journalister, bloggere, menneskerettighetsarbeidere – alle kunne fortelle at de var blitt gjenstand for avlytting uten rettslig kjennelse. I tillegg oppdaget vi at det flere lekkede telefonsamtaler på nett, som ifølge kildene ble brukt som pressmiddel enkelte steder.

Hva var hensikten: De fleste land har lover som gjør det mulig å overvåke personer og miljøer som mistenkes for kriminalitet og terrorisme. Dersom teleselskapene var delaktige i en mer uformell/ulovlig avlytting som gikk på bekostning av menneskerettighetsaktivister og demokratiforkjempere, ble problemstillingen både viktigere og mer omstridt.

Hva vi fant: Researchen vår og kildesamtalene våre viste nå at selv om kommunikasjonskontrollen er lovregulert, så blir den brukt og misbrukt av myndighetene i land med demokratisk underskudd. Flere av våre kilder hadde opplevd å bli avlyttet uten at det fantes noen rettslig kjennelse.

Hva vi brukte det til: Dette ble en av grunnpillarene i saken vår og en av de viktigste tematiske aksene som senere ble diskutert, debattert og fikk politisk oppmerksomhet i Norge.

Kartlegging av kommunikasjonsmuligheter

Når myndighetene har en stor overvåkningskapasitet og følger kommunikasjonen til kildeuniverset, er det svært viktig å kjenne til styrker og svakheter ved ulike kommunikasjonskanaler.

Når all kommunikasjonsinfrastruktur er eller kan være overvåket, er hensyn som kommunikasjonens integritet – at personen vi kommuniserer med er personen den utgir seg for å være - og kommunikasjonens konfidensialitet - at den ikke fanges opp av utenforstående - også noe å tenke på.

Hva var hensikten: Å ha høy bevissthet rundt risikofaktorer i kommunikasjonen og researchen. Dette forutsetter inngående kjennskap til hvordan internett fungerer: En epost som sendes, forsvinner aldri. Den hopper mellom ulike servere før den når frem. Det er mulig å fange opp kommunikasjonen på alle disse punktene underveis. Derfor er kryptering fra ende til ende en fordel. Den sikrer at kommunikasjonen er uleselig frem til den når motparten, men det er ikke nødvendigvis løsningen. For mange myndigheter besitter teknologi som gjør det mulig å fange opp kommunikasjonen likevel. Dessuten kan mottakeren i andre enden være ”kompromittert” i utgangspunktet, dersom for eksempel tastaturet til en kilde er overvåket. Da er ikke kryptering like nyttig. Det er nyttig å vite at Gmail inntil nylig har vært tryggere å bruke for enkelte enn for eksempel Hotmail på grunn av innloggingsløsninger og kryptering ved innlogging. Men dette er – som alle andre sikkerhetsvurderinger - kontekst- og caseavhengig.

Hva vi fant: Det var nødvendig å vise den ytterste aktsomhet fordi det var vanskelig å vite på hvilket nivå avlyttingen og overvåkingen kunne foregå. Vi fant sterke indikasjoner på at det var omfattende og i flere ledd.

Hva vi brukte det til: Kunnskapen gjennomsyret hele vårt arbeid. Vi prøvde å bevisstgjøre kildene på svakhetene i teknologien, var forsiktige med å sende e-post og valgte å benytte oss av kryptert kommunikasjon, samt ansikt-til-ansikt møter med kildene. Av kildebeskyttelseshensyn ønsker vi ikke å spesifisere disse metodene nærmere.

Spør 2: Regimene

Kartlegging av maktpersonenes innflytelse og forretningsvirksomhet i fire land

Hva vi gjorde: Vi skaffet oss en oversikt over hvem som sitter i posisjon i disse landene, hvordan makten er fordelt, hvilke sektorer myndighetspersonene hadde interesser i, samt selve mønsteret for å få og drive business generelt i landet. Målet var å få et så bredt bilde av regimesituasjonen som mulig.

Fremgangsmåte: Vi leste en stor mengde rapporter (Amnesty, Crisis Group, Freedom House, Human Rights Watch, Helsingfors-komiteen m.fl), nasjonale databaser (UDs landsider, CIA Factbook), internasjonale avisartikler, akademiske avhandlinger, vi konsulterte land- og områdeeksperter og leste mange rapporter fra Wikileaks Cablegate-base. Vi leste også utlegningene og fremstillingene som de aktuelle landene gjorde av seg selv online.

Hva var funnene: Et gjennomgående trekk ved flere sentralasiatiske land er at maktpersoner antas å ha store interesser i sektorene som representerer de nasjonale verdiene. Telesektoren er intet unntak. Problemet er at dette systematisk er forsøkt holdt skjult og vanskelig dokumenterbart.

Hva brukte vi det til: Vi brukte funnene i problematiseringen som ett av sakens sentrale elementer. Vi lyktes i å etablere at personer i makthavernes innerste sirkel hadde eierinteresser i delvis Telenor-eide Vimpelcoms lokale selskaper. Dette er stikk i strid med praksisen for moderne corporate governance og interessant å vurdere ut fra en korrupsjonsvinkel.

Kartlegging av regimekritikere i fire land

Hva vi gjorde: Vi måtte identifisere personer og miljøer med høy troverdighet som har erfaring med avlytting i forbindelse med sin virksomhet.

Fremgangsmåte: Gjennom de ideelle, frivillige organisasjonene fikk vi hjelp til å identifisere personer som kunne fremstå som gode vitner på forholdene i landene.

Gjennom en FN-sesjon i Genève, der forholdene i Kasakhstan ble belyst, fikk vi inngående innsikt i forholdene i landet – samt kontakt med flere regimekritikere

En viktig kilde – og intervjuobjekt – var belønnet med tunge menneskerettighetspriser fra flere menneskerettighetsorganisasjoner. Dette forsterket inntrykket av kildens troverdighet.

Hva var hensikten: Dette anså vi som en svært viktig del av jobben. De personlige erfaringene til de som er blitt utsatt for overvåkning var en avgjørende del av historien, fortellingen og troverdigheten i fremstillingen av problemstillingene.

Hva var funnene: Vi lyktes i å komme i kontakt med og møte en håndfull profilerte menneskerettighetsforkjempere, dissidenter og de politiske opposisjonelle i Kasakhstan og Usbekistan.

Vi fant også ut at det eksisterer myndighetsskapte, falske NGO-er, som har som eneste formål å skape støy og ta oppmerksomheten bort fra de reelle forholdene.

Hva brukte vi det til: Noen av disse personene ble caser i sakene våre. Historiene deres ga sakskomplekset et ansikt.

Spor 3: Businessen og partner-puslespillet

Kartlegging av rammebetingelsene for mobilsektoren i hvert enkelt land

Hva vi gjorde: Teleselskapene besto av tidligere statseide selskaper og strukturer som er blitt privatisert. Vi skaffet oversikt over tidligere og nåværende strukturer og hvem som hadde kjøpt og solgt verdifulle selskaper og lisenser i markeder som var i sterk vekst.

Fremgangsmåte: I Vimpelcoms årsrapporter til børsen i New York (20F-rapporter), identifiserer selskapet de største konkurrentene i hvert enkelt land. Vi søkte oss til hjemmesidene til hver enkelt konkurrent på bakgrunn av dette. En lang rekke av disse er børsnoterte selskaper, som russiske MTS og svenske TeliaSonera, som også er pålagt å gi investorer detaljert informasjon. Via hjemmesidene og børsene i de respektive landene, hentet vi ut detaljerte årsrapporter, som vi leste nøye. Flere rapporterte om tvister relatert til tidligere og nåværende eiere. I slike tilfeller søkte vi oss til de konkrete rettskildene i jurisdiksjonene det var snakk om. I disse rettsdokumentene kom det frem sterke anklager om selskapsraiding og korrupsjon mot maktapparatet og enkeltpersoner.

Hva var hensikten: Hensikten var å kartlegge konkurrentene samt se etter/finne forbindelseslinjer og eierinteresser i og rundt makthavernes innerste sirkel.

Hva var funnene: Å sette seg inn i eierskapshistorikken til de ulike selskapene var nyttig, ettersom vi gjorde flere interessante funn i krysningspunktet makthavere/forretningsinteresser.

Hva vi brukte det til: Dette ble en av de sentrale tematiske pilarene i saken.

Kartlegging av Vimpelcoms partnere og forretningsforbindelser

Hva ville finne: Hvem er, eller har vært, Vimpelcoms lokale partnere? Hvilke avtaler er inngått? Hvem kjøpte Vimpelcom mobilselskapene av?

Hva vi gjorde: Vi søkte oss til primærkildene: Vimpelcoms årsrapporter, rapporter til amerikanske børsmyndigheter, kvartalsrapporter, ordrette transkriberinger av investorpresentasjoner og pressemeldinger gjennom ti år. Da dette var en meget omfattende del av arbeidet, vil vi redegjøre for dette i detalj i neste kapittel.

Hva vi fant: At lokale partnere ikke var identifisert i offisiell, tilgjengelig informasjon. At Vimpelcom hadde inngått avtaler om å holde partnerne hemmelige. At samtlige eierforhold endte i skatteparadiser, og gjerne i flere skatteparadiser etter hverandre.

Hva vi måtte gjøre videre: Søke en rekke alternative kilder og sette sammen puslespillet selv.

PARTNER-PUSLESPILLET

Hvordan kom Vimpelcom seg inn i de respektive markedene? Hva var forhistorien? Hvem var partnerne? Hva var avtalene? Når selskapet selv ikke rapporterte informasjon eller ville gi om disse forholdene, måtte vi nøste selv.

Steg 1: De store puslespillbitene

Vi håpet å sette sammen et puslespill med store biter. Vi sjekket følgende sentrale kilder:

Rapporter til amerikanske børsmyndigheter.

Vimpelcom er børsnotert i New York, og derfor forpliktet til å rapportere til børsmyndigheten US. Securities and Exchange Commission (SEC). Informasjonen gjøres tilgjengelig gjennom søketjenesten Edgar. I den årlige 20F-rapporten, som er på mellom 200 og 300 sider, rapporterer selskapet detaljert om eierskap og regulatoriske forhold i landene de opererer i. Her finnes informasjon som er langt mer detaljert enn den ordinære årsrapporten. Vi gikk gjennom samtlige 20F-rapporter siden 2004.

Kvartals- og investorpresentasjoner

Som børsnotert selskap plikter Vimpelcom å gjøre store deler av informasjonen tilgjengelig for investorer og analytikere. Via selskapets hjemmeside, samt rapporteringer til SEC, fant vi frem til samtlige kvartalsrapporter og investorpresentasjoner siden 2004. I tillegg til den tradisjonelle rapporteringen, lager nyhetstjenesten Bloomberg et ordrett referat fra telefonkonferanser som holdes med investorer hvert kvartal. Vi gikk også gjennom disse kvartal for kvartal.

Lokale myndigheter

Vi klarte ikke å identifisere tilgjengelige registre for innhenting av selskapsinformasjon i de landene vi undersøkte. Vi henvendte oss til departementer med ansvar for mobilsektoren, både per telefon og e-post. Våre henvendelser ble ikke besvart.

Kilder i og rundt de berørte selskapene

Skriftlige kilder: Vi søkte Vimpelcom og de berørte selskapenes offisielle egenpresentasjon, i form av pressemeldinger og egenpresentasjoner.

Muntlige kilder: Vi identifiserte sentrale personer i og rundt selskapene, både på administrasjon og styrenivå gjennom tidene. Vi kontaktet analytikere, finansielle rådgivere og investorer.

Av hensyn til kildevernet ønsker vi ikke å gå i detalj om informasjon vi eventuelt fikk av disse.

Børsen

Børsnoterte selskaper av Vimpelcoms kaliber følges av en stor mengde finansanalytikere. De lever av å selge grundige analyser av selskapsforhold. Vi gikk gjennom tilgjengelige analyser i perioden både for Vimpelcom og storeier Telenor. Disse analysene fant vi blant annet gjennom Reuters investordatabase Reuters Knowledge og betalingstjenesten til analyse- og nyhetsbyrået Bloomberg.

Ryktebørsen

Vi identifiserte de viktigste avisene lokalt og regionalt. Vi oppdaget at det fantes få uavhengige medier. De få som fantes, har liten tradisjon for gransking av selskapsforhold, og baserer seg i stor grad på muntlige og anonyme kilder.

På nettet, i diskusjonfora, blogger og sosiale nettsteder florerer informasjon og rykter om sakskomplekset. Selv om det ikke kan tjene som dokumentasjon, kan slike diskusjoner gi en interessant pekepinn for videre research.

Rettskilder

I jakten på forhistorien til Vimpelcoms selskaper og konkurrentenes selskaper fant vi flere tilfeller av konflikter rundt tidligere eierskap.

En sentral rettskilde ble Verdensbankens voldgiftstribunal International Centre for Settlement of Investments Disputes. Hele rettsprosessen legges ut på tribunalets hjemmeside. Vi fant informasjon om ankesaker og videre prosesser gjennom å henvende oss direkte til tribunalet.

Dun&Bradstreets GRS-database

Denne betalingsbasen inneholder informasjon om selskaper fra en lang rekke land. Vi søkte her på samtlige involverte selskaper, men fant lite informasjon her om skatteparadisene og våre fokusland.

Skatteparadiser

Skatteparadiser er kjent for sin manglende transparens og muligheten til å kamuflere eierskapet. De spilte en sentral rolle i dette sakskomplekset. Vi erfarte at det var mulig å hente frem viktig informasjon, også fra ellers vanskelig tilgjengelige skatteparadiser som Gibraltar, Kypros og British Virgin Islands. Også her finnes det offentlige registre, som er mulige å kontakte.

Mot en avgift på under 100 norske kroner kan man få ut tilgjengelig, registrert informasjon elektronisk. Det er viktig å være klar over at ikke all informasjon som leveres inn fysisk, blir registrert elektronisk (se nedenfor).

Vi fant mye, men ingen konklusjon

Årsrapportene ga ingen eksakt informasjon om partnerforholdene. Lokale myndigheter besvarte ikke henvendelser. Mange muntlige kilder ønsket ikke å snakke, selv ikke under løfte om anonymitet. Vi måtte legge et puslespill med langt mindre biter enn vi trodde på forhånd.

Steg 2: De små puslespillbitene

For hvert land måtte vi legge et nytt puslespill. Vi gjør her rede for hvert land enkeltvis.

Kasakhstan/Kirgisistan

Dette hadde vi: Fra Vimpelcoms 20F-rapporter visste vi at Vimpelcoms lokale partner i Kasakhstan og Kirgisistan var et selskap registrert på Kypros. Rykter og nettskriverier tydet på at det var presidentrådgiveren Bulat Utemuratov, men dette var aldri dokumentert. Vimpelcom hadde gjort avtaler om å holde medinvestoren hemmelig.

Dette ville vi vite: Om det var presidentrådgiveren – eller andre sentrale maktpersoner – som var forretningspartnerne.

Dette fant vi: Vimpelcoms partner i Kasakhstan og Kirgisistan er Bulat Utemuratov – en av Kasakhstans presidents mest betrodde personer og landets spesialutsending til Kirgisistan.

Metode: Kartlegge selskapsstrukturer i Vimpelcom-sfæren, tidligere og nåværende eier samt presidentrådgiverens forretningsimperium.

Verktøy/Mannen

- Pressemeldinger fra Vimpelcom der partneren blir identifisert som "storeier i ATF Bank".
- Bankprospekter identifiserte ham som bankens største enkelteier. Her fantes også detaljert informasjon om hvem som hadde tillitsverv i banken.
- Informasjon fra andre virksomheter, deriblant en pressemelding om den samme rådgiverens hotellkjøp i Moskva og Wien, inneholdt informasjon om øvrig virksomhet. En melding fra hans advokatforbindelse identifiserte ham som storeier i et lokalt fond.
- Selskapshjemmesider: Hjemmesidene til Bulat Utemuratovs fond Verny Capital inneholdt informasjon om tidligere avtaler og bragder – deriblant en meget lukrativ mobilinvestering.
- Memoarene til en avgått etterretningssjef: Han var presidentens svigersønn og uoffisiell kronprins. Nå var han i unåde, i eksil og bitter. Vi klarte å finne et eksemplar av hans famøse selvbiografi på Nobel-instituttet. I denne boken fant vi informasjon om en rekke personer i den sentrale makteliten i Kasakhstan.

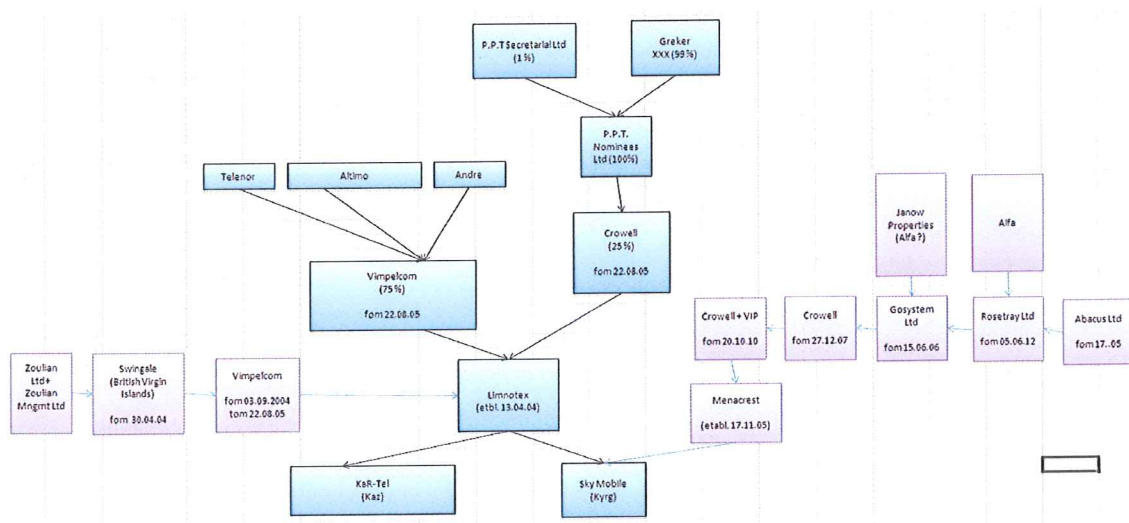
Andre verktøy

- Selskapsregisteret på Kypros

Om partneren: Til tross for sekrethese-ryktet er det mulig å søke elektronisk i det kypriotiske selskapsregisteret. Mot en avgift på en snau hundrelapp kan man hente ut informasjon om blant annet nåværende og tidligere styremedlemmer, adresser, eierskap og låneavtaler. Eierskapet til det kypriotiske selskapet som er Vimpelcoms partner, var skjult bak lag på lag med skallselskaper. Vi bestilte informasjon om samtlige. Da den registrerte informasjonen ikke ga noe entydig svar, kontaktet vi administratoren av selskapene, som ikke ville gi ytterligere informasjon. Da vi hadde kjennskap til at den elektroniske informasjon ikke var fullstendig, lot vi en lokal researcher gå til arkivene å gå gjennom informasjonen manuelt.

Om Vimpelcoms egne selskaper: Også Vimpelcoms eierskap til mobilselskapene i Kasakhstan og Kirgisistan er plassert på Kypros. Informasjon om registrerte styremedlemmer i det kypriotiske selskapsregisteret var avgjørende: Her fant vi både presidentrådgiverens sønn og hans mangeårige betrodde medarbeider både i banken ATF og fondet Verny.

- Rettskilder: Gjennom Vimpelcoms 20F-rapporteringer, samt medierapporter, fant vi at eierskapet til Vimpelcoms kasakhstanske mobilselskap Kar-Tel var omstridt og behandlet i Verdensbankens voldgiftstribunal. Dette ga oss viktig bakgrunnsinformasjon om salgsprosessen.
- Eierskapet til det kirgisiske mobilselskapet var omstridt og under rettsbehandling i Isle of Man. Denne kompliserte saken ga oss nyttig informasjon om tidligere eiere.
- Informasjon fra tidligere eiere: Både russiske Alfa Group og russiske MTS har hevdet eierskap til Vimpelcoms kirgisiske mobilselskap. I deres selskapsrapporteringer fant vi både informasjon om verdsettelse som ikke var tilgjengelig andre steder, samt transaksjonshistorikk.
- Systematisering: Informasjon om nåværende eiere (blå) og tidligere eiere (rosa) ble plottet inn i et selskapskart for å systematisere informasjonen.



- Wikileaks-rapporter: De mange lekkede ambassaderapportene fra Wikileaks ga et interessant innblikk i forhold som ellers ikke var omtalt på samme måte andre steder: Bak kulissene-beskrivelser av maktapparatet og forretningspraksisen i de sentralasiatiske landene som ble en svært nyttig tilleggskilde med tips og detaljer som var nyttig å ha med seg.
- Deltakelse på FN-sesjon i Genève om forholdene i Kasakhstan: Situasjonen for menneskerettighetene i Kasakhstan ble drøftet i FNs hovedkvarter da vi var der for å møte flere sentrale kilder. Det ga oss interessant tilleggsinformasjon og innblikk i hvordan myndighetsopprettede frivillige organisasjoner brukes for å desinformere eller forkludre den offentlige debatten i slike fora.

Tadsjikistan

Dette hadde vi: I en pressemelding fra Vimpelcom da det kjøpte 60 prosent av selskapet, ble det nevnt at en av de gjenværende eierne er eier og styreleder i Orienbank. Den lokale ryktebørsen mente presidentens svoger og landets mektigste mann, Hasan Asadullozoda, var både selger og fortsatt storeier. Vimpelcom meldte at det var begrenset av konfidensialitetsklausuler, og derfor ikke kunne navngi verken selgere eller medinvestorer i Tadsjikistan.

Dette ville vi vite: Var det Asadullozoda – eller andre sentrale maktpersoner – som var partner i Tadsjikistan. Det sentrale ble å finne ut hvem som var styreformann da Vimpelcom sendte ut sin pressemelding.

Dette fant vi: Vimpelcoms partner var svogeren til landets mangeårige president – og landets mektigste mann. Vimpelcom slo av all kommunikasjon i et større område på myndighetenes ordre.

Metode: Kartlegge transaksjonshistorikk for Vimpelcom i Tadsjikistan, strukturer i næringslivet i Tadsjikistan og presidentens innflytelse.

Verktøy

- Pressemeldinger og årsrapporter fra Vimpelcom viste hvordan Vimpelcom gradvis hadde økt eierandelen i det tadsjikiske selskapet. Hvem som solgte, og hvem som sto igjen som medinvestorer, kom ikke frem.
- I Orienbanks årsrapporter og egenpresentasjoner på engelsk, russisk og tadsjikisk fremsto Asadullozoda som styreformann, men rapportene for de årene vi var interessert i, lå ikke ute.
- Gjennom historiske nettsøk kan man hente historiske øyeblikksbilder av en lang rekke websider. Her fant vi frem både selskapspresentasjoner og årsrapporter fra perioden vi var ute etter. Asadullozoda var styreformann også da avtalen med Vimpelcom ble inngått.
- Moteblogger og skrytebilder: Vi visste at Tadsjikistans mangeårige president hadde vært gift med Asadullozodas søster. Men var de fortsatt gift? Tadsjikistans førstefrue viste seg sjelden å opptre offentlig. En arabisk moteblogg ble nyttig. Slakt av førstedamens antrekk i forbindelse med et statsbesøk i 2007 fikk bekreftet at Asadullozoda var presidentens svoger ved avtaletidspunktet. Dette supplerte vi med omfattende bildesøk, tråling av statsbesøksdekning i medier og research rundt førstedamer i tidligere Sovjetrepublikker:



Somebody's stylist is getting beheaded today...

This photo was on the front page of all our local newspapers this morning. The woman on the left is the very popular and highly respected second wife of our Emir (also very popular and highly respected). The woman on the right is the First Lady of Tajikistan.

<http://road-to-rubda.blogspot.no/2007/08/wrong-day-to-wear-mumu.html>

- Konspirasjonsforskning: Var Asadullozoda fortsatt i live? Ryktebørsen i Tadsjikistan hadde gått bananas da han forsvant fra offentlighetens. Stemte ryktene om at presidentens sønn og Asadullozodas nevø hadde skutt ham i misunnelse over hans makt og formue? Og hadde Asadullozoda ukjente tvillingbror tatt hans plass? En forsker ved universitetet i Exeter

punkterte ryktene. Vi gikk ut fra at Asadullozoda neppe var drept av sin nevø og dermed fortsatt var i live.

- Banken selv: Gjentatte henvendelser over flere uker til banken, både via telefon og e-post, på norsk og russisk, ble tatt imot, men ikke besvart.

Usbekistan

Dette hadde vi: Vimpelcoms årsrapporter beskrev en lokal partner som hadde vært medinvestor i det usbekiske selskapet i en kort periode, med solid og garantert gevinst. Gevinsten var sikret gjennom en lukrativ opsjon til å selge tilbake aksjene til Vimpelcom til en på forhånd avtalt pris. Partneren var ikke navngitt.

Dette ville vi vite: Hvem var denne partneren som hadde fått en så gunstig avtale?

Hva fant vi: Et lite selskap i et skatteparadis, eid av en kvinne i 20-årene ble garantert en gevinst på mer enn 200 millioner kroner da Vimpelcom etablerte seg i Usbekistan. Partneren etterforskes nå for hvitvasking i Sveits og Sverige, og kobles av svensk politi til datteren til Usbekistans president.

Metode: Kartlegge Vimpelcoms eierskapshistorikk i Usbekistan. Identifisere partneren.

Verktøy

- Selskapsregisteret på British Virgin Islands (BVI): Den usbekiske partneren var blitt medeier i det usbekiske mobilselskapet gjennom et felleseid selskap på BVI. Dette regnskapsregisteret har ikke elektronisk søkbare registre. Vi leide en representant til å oppsøke det lokale registeret og hente ut relevante opplysninger. Her fantes ingen informasjon om partneren.
- Kilder: Personer med inngående kjennskap til sakskomplekset ga oss detaljerte beskrivelser av hendelsesforløp. Dette ga ingen dokumentasjonsverdi, men fungerte som en viktig pekepinn for videre research.
- Tips: En sentral kilde med kjennskap til Usbekistan tipset oss om at Vimpelcoms lokale partner var et selskap ved navn "Takilant".
- Dybdesøk: Navnet "Takilant" var ikke å finne i Vimpelcoms fyldige årsrapporter til SEC, eller i andre tilgjengelige selskapspresentasjoner. Ved å søke i Vimpelcoms rapporter på både russisk og engelsk fant vi det likevel ett eneste sted: I Vimpelcoms årsrapport på russisk for 2007. Informasjonen ble dobbeltsjekket ved hjelp av en norsk-russisk oversetter.
- Selskapsregisteret på Gibraltar: I Dun & Bradstreets GRS-database fant vi at Takilant er hjemmehørende på Gibraltar. Ved å kontakte selskapsregisteret på Gibraltar fikk vi stiftelsespapirer, informasjon om styremedlemmer og årsrapporter for en tiårsperiode mot en gebyr på noen hundrelapper. I disse papirene fantes ingen dokumentasjon på partnerskapet med Vimpelcom. En ung kvinne ved navn Gayane Avakyan var kontaktperson.
- Dun & Bradstreets GRS-database: Hvilke andre forretningsinteresser hadde Avakyan? Et rollesøk i GRS-databasen viste at hun hadde verv i et britisk selskap.
- Det britiske selskapsregisteret: Gjennom det britiske selskapsregisteret fikk vi årsrapporter, og informasjon om personer i sentrale tillitsverv i det britiske selskapet Avakyan hadde verv i. I årsrapportene kunne vi lese at Avakyan var den endelige eieren av det britiske selskapet gjennom Takilant. Dermed kunne vi utlede at Avakyan var den endelige formelle eieren av Takilant.
- Sveitsiske og svenske medier: Det viste seg at Avakyan var i søkelyset både hos sveitsisk og svensk politi, med mistanker om korrupsjon og hvitvasking samt mulige koblinger tildatteren til Usbekistans president gjennom mange år. Også TeliaSonera hadde inngått partnerskap med Takilant. Svenske medier hadde gransket Avakyans relasjoner særlig til TeliaSonera, med SVTs Uppdrag Granskning i spissen. Dette ga oss verdifull informasjon, men ettersom

mye var basert på anonyme kilder, måtte vi verifisere dette på egenhånd. Vi klarte ikke å finne hold for alle påstander.

- Politikilder: Både sveitsisk og svensk politi bidro til å opplyse om sine respektive saker.
- Svenske rettsdokumenter: Svensk politis etterforskning av Takilants forretningsrelasjoner til TeliaSonera resulterte også i arrestbegjæringer. Ved å henvende oss til rettsinstansene som behandlet arrestbegjæringene, fikk vi tilgang på påtalemyndighetens bevismateriale. Her fant vi blant annet kontoopplysninger som knyttet Vimpelcom direkte til beslaglagte konti og viktig bakgrunnsinformasjon.
- Wikileaks-lekkasjer: Ga oss antydninger om den usbekiske presidentdatterens sterke interesse for telekomsektoren. Ingen dokumentasjonsverdi i seg selv, men viktige pekepinn for videre research.
- Hennes eksellense: Vi kontaktet Usbekistans FN-ambassade med en rekke konkrete spørsmål om presidentdatteren Gulnara Karimova, fra svensk og sveitsisk politi, fra avisartikler og Wikileaks-kilder. Det eneste spørsmålet som ble besvart var: Er Gulnara Karimova den egentlige eieren av Takilant.



UZ/UN/12-303

The Permanent Mission of the Republic of Uzbekistan to the United Nations Office at Geneva and other International Organisations presents its compliments to Dagens Næringsliv (DN), and in reply to the e-mail of Ms. Marte Ramuz Eriksen, journalist of DN, dated 6 November 2012, has the honour to inform on following.

H.E. Ambassador Gulnara Karimova, Permanent Representative of Uzbekistan to the UN Office and other International Organizations in Geneva, has no connections with commercial activity and contacts of Takilant.

The Permanent Mission of the Republic of Uzbekistan avails itself of this opportunity to renew to Dagens Næringsliv the assurances of its highest consideration.

Geneva, 8 November 2012



Attn.: Ms. Marte Ramuz Eriksen

Dagens Næringsliv
Postboks 1182
Sentrum 0107
OSLO

Brev til DN.

- Sosiale medier: Gulnara Karimova er meget aktiv på Twitter og Facebook. I hennes Twitter-meldinger omhandles stort sett hennes parallele karrierer som artist, designer og moteikon. I Twitter-korrespondansen fremkom hennes private epost-adresse. Henvendelser til denne er ikke besvart.
- Vimpelcom: Idet DN var iferd med å publisere informasjon om Vimpelcoms usbekiske partner, sprakk saken noen dager før i svenske og internasjonale medier. Vimpelcom kom dermed med en uttalelse knyttet til den usbekiske partneren. Her ble DN's researchfunn om

partneren bekreftet. Selskapet ville imidlertid ikke identifisere Takilants datterselskap, som Vimpelcom hadde kjøpt en viktig mobillisens av.

- Usbekiske myndigheter: Usbekistans telekomdepartementets hjemmesider er en materie i bevegelse. Informasjon fjernes og legges til, og kamufleres også for historiske nettsøk. Henvendelser per telefon og epost med forespørsel om regelverk og praksis knyttet til lisenskrav og –tildelinger samt teleselskapenes forpliktelser ble ikke besvart.

Utfordringer og erfaringer

Overvåkning og ny teknologi

For å kunne skrive disse sakene har vi vært nødt til å sette oss inn i forutsetningene for å kunne kommunisere i et helt nytt teknologisk landskap preget av omfattende overvåkning. Aldri før i verdenshistorien har graden og rekkevidden av overvåkning, den teknologiske anvendelsen og tilgjengeligheten, samt bruken av avlyttingsmateriale vært mulig i samme skala som i dag. Mange flere kan avlyttes på en enklere måte, billigere og mulighetene til å gjennomgå avlyttingsmaterialet er også perfektjonert.

Den teknologiske kunnskapen vi skaffet oss, gjorde det vanskeligere for selskapene å snakke seg rundt problematikken.

Dokumentasjon av overvåkning

Vi lyktes i å få tak i respekterte menneskerettighetsforkjemperne i flere av landene vi så nærmere på. Men også de muntlige fortellingene og vitnesbyrdene har sin begrensning. Først da vi klarte å fremskaffe dokumentasjonen som viser at et stort antall mennesker ikke har kunnet kommunisere fritt i lengre tid, kunne vi slå fast og dokumentere sakskomplekset på et helt annet nivå.

Ved at avlyttingsmaterialet ble brukt i to store politiske rettssaker, dokumenterte myndighetene i Kasakhstan også hva de selv har gjort. Rettsdokumentene ble en svært vesentlig informasjonskilde og dokumentasjon på hvordan overvåkningen foregår i praksis.

Regimekritikere, menneskerettighetsforkjempere og politiske opposisjonelle blir trakassert, dømt og fengslet av autoritære regimer og diktaturer på grunn av de nye teknologiske mulighetene til å overvåke befolkningen. I autoritære regimer benyttes disse teknologiske nyvinningene for å samle informasjon, for i neste omgang å forfølge mennesker på en mye enklere og farligere måte enn tidligere. Dette er altså et helt nytt trekk ved samfunnsutviklingen. Når Vimpelcom tjener penger på mobilvirksomhet i disse landene, gir dette profitt også for den norske stat, gjennom eierskapet i Telenor.

Kildebeskyttelse

Vi bestemte oss for at menneskene som opplevde overvåkning på nært hold var en avgjørende del av sakskomplekset – og måtte bli det i de ferdige sakene. De var de beste vitnene på hvordan slik overvåkning kunne slå ut i praksis og fungere undertrykkende. At overvåkning også brukes politisk, gjør det ekstra interessant at partnerne til Telenor-eide Vimpelcom i disse landene nettopp er en del av maktpersonenes indre sirkel.

Personer som er utsatt for overvåking og forfølgelse er i utgangspunktet utsatt for fare. Det var derfor litt mer komplisert enn vanlig å opprette kontakt, få tillit og opprettholde kontakt med personer. Vi måtte ha kjennskap til overvåkningsinfrastrukturen, vite om dens rekkevidde og muligheter og ta dette i betraktning når vi hadde kontakt: Hvordan håndteres lovverket? Når påberoper myndighetene seg retten til å hente ut samtaleinformasjon og trafikkdata? Foreligger

rettslige kjennelser før avlyttingen gjennomføres? Blir bakdøren til telenettet misbrukt for å kneble opposisjonen?

For å få svar på disse spørsmålene, ville vi snakke med regimekritikere, opposisjonelle og menneskerettighetsforkjempere. Men raskt dukket det opp nye spørsmål.

Vil det å la seg intervju om dette skape problemer for de involverte? Ville kun en henvendelse fra oss skape problemer for dem? Det ble sentralt for oss at vi ikke uforvarende skulle øke risikoen ytterligere for dem vi ønsket å snakke med. Derfor sendte vi generelle henvendelser først, og lot dem bestemme gjennom hvilken kanal de ønsket å kommunisere med oss på.

Selv kilder som ønsket å stå frem med navn ville ikke la seg intervju på vanlig mobiltelefon. Mange ønsket å benytte krypterte kommunikasjonstjenester over internett. Ettersom også disse er mulige å overvåke og fange opp, på tross av krypteringen, var man forsiktig også her.

Vi vurderte det dit hen at vi ikke ville kunne være i stand til å gi våre kilder god nok beskyttelse om vi som utenlandske journalister reiste inn i landet og hadde møter med personer som i utgangspunktet kunne antas å være i myndighetenes søkelys. Mulighetene for identifisering av kildene med tilhørende represalier gjorde at vi bestemte oss for å intervju de som allerede var i sikkerhet, i eksil. Vår vurdering etter å ha snakket med eksperter og berørte, var at dette var en riktig beslutning.

I samtaler med oss beskrev disse hvordan de kommuniserte med hverandre for å unngå overvåking. De ønsket ikke at dette ble omtalt i DN i frykt for at metodene skulle oppdages.

Frivillige organisasjoner vi kontaktet, pekte i retning av at regimekritikere med stor sannsynlighet er under oppsyn av sikkerhetstjenestene. Det fremgikk også av skriftlige rapporter. Dette ble også bekreftet da vi tok kontakt med sentrale regimekritikere i landene.

Vi måtte også vite om Vimpelcom-abonnentene spesielt kunne bli utsatt for overvåking. Vi ønsket å få denne informasjonen ubedt. Vi stilte aldri et direkte spørsmål om overvåkingsofrene ble avlyttet som Vimpelcom-kunder. De fortalte oss det selv, uoppfordret, og uten at vi hadde gitt dem informasjon om at Vimpelcom er et delvis norsk-eid selskap.

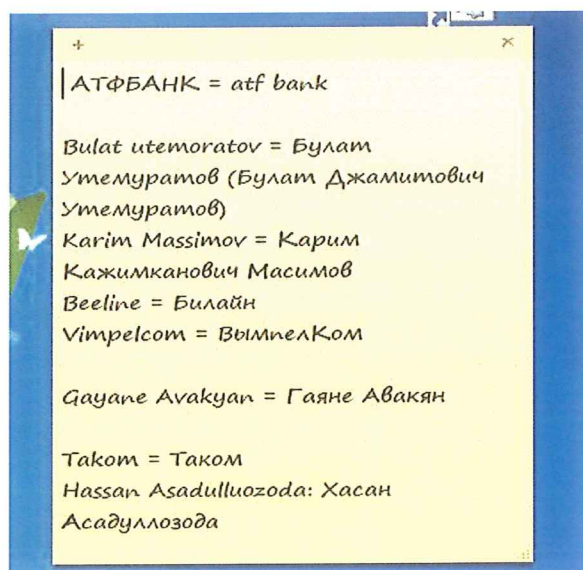
Språket

Vi måtte forholde oss til tilgjengelig informasjon på russisk, usbekisk, kasakhstansk, kirgisk, tadsjikisk, tyrkisk, engelsk og fransk. Fordi det var vanskelig å finne muntlige kilder var vi i stor grad nødt til å basere oss på skriftlige kilder.

Den største utfordringen lå i at transkriberingen fra det kyrilliske til det latinske alfabetet kan variere kraftig. For eksempel omtales Usbekistans presidentdatter med fornavnene Gulnora, Gulnara og Goulnara. Etternavnet til Tadsjikistans presidents svoger er transkribert til latinsk på så vidt forskjellige måter som Asadullozoda, Sadullaev, Saduloev og Sadullayev. Lignende eksempler var mange, også på selskapsnavn.

Vi fant det derfor formålstjenlig å gjøre søk også med kyrillisk stavemåte. Nettleseren Google Chrome ble et nyttig verktøy, ettersom den har en funksjon som oversetter sider til engelsk/norsk automatisk. I tillegg til å identifisere de ulike transkriberingsformene på person- og selskapsnavn, ble

også identifisering av den korrekte stavemåten på kyrillisk en sentral del av researchen. Vi brukte Microsofts notatfunksjon for å holde oversikt på de kyrilliske stavemåtene:



(skjermdump)

Oversettertjenesten Google Translate ble også et nyttig verktøy for å få en indikasjon på opplysninger.

Ved enkelte tilfeller, for eksempel for å kvalitetssjekke sentral informasjon og sikre høy presisjon, brukte vi også en norsk-russisk oversetter.

Systematisk hemmelighold og manglende transparens

Norge er en særstilling når det kommer til åpenhet rundt selskapsforhold. Landene vi hadde valgt å konsentrere oss om, er på den helt andre enden av skalaen. Mye av researchen vår resulterte i erkjennelsen om at informasjonen enten ikke var å finne eller at den var bevisst forsøkt skjult. I researchen møtte vi på flere sentrale hindringer:

- Landene vi researchet er lite transparente. De har ikke tradisjon for åpenhet. De mangler tjenester som gir oversikt over selskapsforhold. Offentlige nettsider er kompliserte å navigere i. Henvendelser til myndigheter både via telefon og e-post ble ikke besvart.
- Avtalene Vimpelcom har inngått er designet for å hemmeligholdes. Eierstrukturer går lag-på-lag og ender i skatteparadiser.
- Lokale medier er i liten grad uavhengige. De har liten tradisjon for å granske selskapsforhold. Saker som omhandler maktpersoners eierforhold er ikke dokumentert, eller basert på rykter.
- Muntlige kilder frykter overvåking og sanksjoner, og er redde for å snakke.

Samtidig imøtegåelse

Å komme i kontakt med personer som ville bli omtalt og tilby dem muligheten til å komme med samtidig imøtegåelse viste seg å være en av de mest tidkrevende elementene ved researchen. I

tillegg til vanlige internettsøk brukte vi også sosiale nettjenester som Facebook og LinkedIn for å identifisere mulige kontaktpunkter.

For å få en sentral kilde i tale, kontaktet vi for eksempel banken han tidligere var storeier i, hoteller han har kjøpt seg opp i og fondet som tilknyttet ham. Hans partner gjennom mange år ble kontaktet via Facebook. En annen kilde ble forsøkt nådd gjennom den franske treneren av sønnens rasehest. Flere ambassader benyttet seg av anledningen til samtidig imøtegåelse.

Vimpelcoms norske toppsjef Jo Lunder stilte til et halvtime langt intervju med DN om sakskomplekset. Han har siden avslått alle forespørsler om oppfølgingsintervjuer gjennom informasjonsavdelingen. Vimpelcoms informasjonssjef har håndtert alle senere henvendelser.

Telenor-sjef Jon Fredrik Baksaas stilte til et timelangt intervju med DN om sakskomplekset. Telenors informasjonsavdeling har håndtert senere henvendelser og oppfølgingsspørsmål.

Regelverket

Hvert av landene i sentral-Asia har egne, omfattende regelverk for hvordan myndigheter, sikkerhetstjenester, politi og påtalemyndigheter kan innhente og iverksette avlytting, innhenting av samtaleinformasjon og trafikkdata. Prosedyrene for dette er beskrevet i detalj i de lokale lovgivningene, men omtales selvfølgelig ikke som "overvåkning" som er motstandernes betegnelse på myndighetspålagt kommunikasjonskontroll.

For å finne ut av regelverket måtte vi gjennomgå de til dels omfattende lovtekstene til de respektive land – og i første omgang oversette det gjennom Google Translate, finne de rette lovparagrafene som fastslår forpliktelsene teleselskaper er pålagt angående overvåkning.

Den russiske lovgivningen SORM utgjorde utgangspunktet for flere av de andre tidligere Sovjetrepublikkene og var dermed et utgangspunkt for både forståelse av – og søk etter relevant terminologi på området.

Et kompleks kompleks

De to store skandinaviske teleoperatørene valgte ulike strategier da de skulle erobre de jomfruelige markedene i det tidligere Sovjetunionen. TeliaSonera gikk direkte inn. Telenor valgte en indirekte metode, gjennom Vimpelcom.

Ved å satse gjennom en partner ville Telenor redusere sin økonomiske risiko, har toppledelsen uttalt. Samtidig ble det bygget en kompleks selskapsstruktur over en rekke jurisdiksjoner som er vanskelig å trenge gjennom: Vimpelcom er registrert på Bermuda, børsnotert i New York, har hovedkontor i Nederland og opprinnelse i Russland. Telenor har spilt en sentral og viktig rolle i Vimpelcom de siste 15 årene, og den urealiserte gevinsten på investeringen nærmer seg 40 milliarder kroner. Telenor-sjefen og to sentrale Telenor-topper sitter i styret i selskapet. Likevel holder Telenor Vimpelcom på en armlengdes avstand. Konsernsjefen og informasjonsavdelingen viser til Vimpelcom selv for alle detaljspørsmål.

Ved å gå inn i de tidligere Sovjet-republikkene med en partner, kunne Telenor også redusere eget ansvar. Der svenske medier og svensk påtalemyndighet kunne granske et svensk selskap med svensk

ledelse etter svenske lover, fremstår Vimpelcom-saken langt mer kompleks. Når selskapsstrukturen, organiseringen og ansvaret strekkes over en rekke land og flere kontinenter blir det vanskelig å identifisere hvem som har det egentlige ansvaret. For journalister, politikere og andre meningsbærende blir det nesten en uoverkommelig bøyg: Hvilket land skal etterforske et slikt selskap? Hvilke politikere skal be om at det granskes? Hvem har det egentlige ansvaret? Hvor langt ned i den endeløse rekken av eierselskaper må det gå før norske eierskaps- og styringsprinsipper opphører?

Vimpelcoms gjentatte respons på våre henvendelser var at selskapet lojalt følger lover og regler i landene de opererer i. Vår gjentatte vurdering av dette var at lovlighet i seg selv ikke er en god rettesnor når man skal vurdere diktaturer og autoritære regimer, ei heller om man skal gjøre journalistikk på et område. Et autoritært regimes vurdering av korrupsjon og brudd på menneskerettigheter kan ofte avvike fra vurderinger etter vestlige standarder.

DN har til tross for disse utfordringene avdekket hvordan Vimpelcom, med statseide Telenors fulle støtte, har skaffet seg et fotfeste i noen av verdens verste regimer. Verken norsk eller internasjonal presse har tidligere presentert systematikken i Vimpelcoms partnerskap og myndighetskontakt.

Presentasjon og etterspill

Etter to måneders research satt vi med en enorm samling materiale. I prinsippet hadde vi gjort research for minst fire dokumentarer: én om hvert land. Arbeidet med å strukturere og disponere stoffet tok tid. Vi måtte også ta hensyn til at landene vi ville omtale er ukjente for de fleste av våre lesere.

Vi landet på en modell der problemstillingen ble presentert i én omfattende feature i DN's lørdagsutgave der Vimpelcoms satsinger i telemarkedet i Kasakhstan ble det sentrale. Det resterende materialet og oppfølgere ble presentert på nyhetsplass. I den senere oppfølgingen hadde vi også en artikkel med samme tematikk om Vimpelcoms eierskap til et mobilselskap i Robert Mugabes Zimbabwe. Senere ble også en påbegynt etterforskning av svensk politi sentralt i oppfølgingsarbeidet. I perioden oktober-desember ble det publisert 20 saker på nyhetsplass. Totalt har vi fylt mer enn 60 avissider med stoff. Dekningen av etterspillet og etterforskningen i Sverige pågår fortsatt.

Som følge av vår artikkelserie har Telenors styreleder bedt om en redegjørelse, etikkomiteen i Telenor-styret startet et eget arbeid, og næringsminister Trond Giske har bedt Telenors styreleder og konsernsjef om redegjørelser.

Proessen med å avdekke eierforholdene, pengestrømmene og de menneskerettighetsmessige konsekvensene er ennå ikke avsluttet. Politiet og myndighetene i flere land etterforsker og gransker i skrivende stund sakskomplekset: De har en vanskelig oppgave foran seg når de skal skaffe seg den fulle oversikten over hemmeligholdte partnerne, pengestrømmene og de menneskerettighetsmessige konsekvensene omtalt i noen av disse sakene.

Oslo, 14. januar 2013

Marte Ramuz Eriksen

Osman Kibar

Vedlegg 1: Publiseringsliste

Samtlige artikler er publisert i Dagens Næringslivs papiravis (se vedlegg).

Dato	Tittel	Beskrivelse/ingress
20.10.12	Farlige forbindelser	Feature-artikkel om overvåking av opposisjonelle og Vimpelcoms hemmelige avtaler i Kasakhstan.
23.10.12	Vil avlytte alle statsråder	Myndighetene i Kirgisistan går inn for at samtlige statsråder i landet skal avlyttes. Teleselskapene er en viktig bidragsyter til avlyttingen. Delvis Telenor-eide Vimpelcom har 2,4 millioner abonnenter i Kirgisistan.
03.11.12	Garanterte gevinst på 200 mill.	Med full støtte fra storeier Telenor, inngikk Vimpelcom en avtale som garanterte en lokal partner i Usbekistan 200 millioner kroner i gevinst. Partneren etterforskes nå for hvitvasking i Sveits og Sverige, og kobles av svenske myndigheter med datteren til Usbekistans diktator
06.11.12	Et av de verste diktaturene i verden	Telenor er via Vimpelcom tungt inne i et av verdens verste diktaturer. Ø Det er få samfunn i verden som er mer gjennomautoritære, sier Jan Egeland i Human Rights Watch.
06.11.12	Varslet Økokrim om Telenor-selskap	Korrupsjonsjegere i svenske Riksenheten mot korrupsjon har varslet Økokrim om Telenor-eide Vimpelcoms partner i Usbekistan. Partneren, som har solgt mobillisenser til Vimpelcom og TeliaSonera, har hverken erfaring eller finansiell styrke, mener svensk politi.
07.11.12	Krever svar fra Baksaas - Teleselskaper har blod på hendene	Styreleder i Telenor, Svein Aaser ber konsernsjef Jon Fredrik Baksaas redegjøre for den omstridte investeringen i diktaturstaten Usbekistan. - Når teleselskapene samarbeider med et diktatur, er de like skyldige som regimet, sier Mutabar Tadjibaeva (50), Usbekistans mest kjente menneskerettighetsforkjemper. Før hun måtte flykte fra hjemlandet, ble hun avlyttet som kunde hos Telenor-eide Vimpelcom.
08.11.12	Vi ville ikke bære risikoen alene	Telenor vurderte å gå direkte inn i diktaturstatene i Sentral-Asia, men overlot jobben til Vimpelcom. Det forteller tidligere Telenor-sjef Tormod Hermansen.
10.11.12	Avviser mobilforbindelse	Usbekistans presidentdatter Gulnora Karimova avviser å være en del av en gigantisk hvitvaskingssak i Sveits og Sverige.
12.11.12	Kjøpte selskap av diktatorens svoger Hjalp myndighetene - stengte hele nettet	Telenor-eide Vimpelcom fikk innpass i den lutfattige eks-sovjetstaten Tadsjikistan ved å kjøpe et mobilselskap av presidentens svoger I sommer beordret Tadsjikistan stenging av nettsider som BBC og Youtube. Omtrent samtidig slo Telenor-eide Vimpelcoms selskap av all kommunikasjon i et større område på myndighetenes ordre.

14.11.12	Krever kontroll av tekno-våpen	Europaparlamentet krever strengere eksportkontroll av "digitale våpen". Ny teknologi som kan brukes til å bryte menneskerettigheter, skal kontrolleres på samme måte som våpeneksport.
15.11.12	Vill vekst i Usbekistan	På få måneder har Telenor-eide Vimpelcom fått mer enn to millioner nye kunder i diktaturet Usbekistan. Det knallharde diktaturet Usbekistan er blitt en gullgrube for delvis Telenor-eide Vimpelcom.
20.11.12	"Alt" er hemmelig	Delvis Telenor-eide Vimpelcom hemmeligholder en lang rekke av sine avtalepartnere i korrupte land. Vimpelcom vil ikke oppgi navnet på selskapet i Usbekistan som det overførte rundt 145 millioner kroner til.
21.11.12	Krever svar fra Telenor	Næringsminister Trond Giske har bedt Telenor-sjef Jon Fredrik Baksaas redegjøre for selskapets samfunnsansvar i forbindelse med Vimpelcom-satsingene i Sentral-Asia.
22.11.12	Jobbes intensivt	Næringsminister Trond Giske har bedt om en redegjørelse fra Telenor om selskapets engasjementer i Sentral-Asia. Ø Jeg har nulltoleranse for korrupsjon, sier Giske.
26.11.12	Nest størst i Zimbabwe	Telenor-eide Vimpelcom selger mobiltjenester i diktaturet Zimbabwe. Teleselskapet er forpliktet til å gi landets overvåkningstjeneste full tilgang til kundenes telefonsamtaler.
01.12.12	Tar detaljene på kammerset	Telenor gir ingen opplysninger om Vimpelcoms hemmelige partnere i en skriftlig orientering til næringsminister Trond Giske. Detaljene skal drøftes i et møte med ministeren.
10.12.12	Forvirring om mobillisenser	Svensk politi mener Vimpelcom ble fratatt lisenser og frekvenser i Usbekistan, og at TeliaSonera kjøpte disse av et korrupsjonsmistenkt selskap. Feil, mener Vimpelcom.
13.12.12	Teletopper etterforskes	Bestiktelser: To høyt plasserte sjefer i TeliaSonera etterforskes for å stå bak bestiktelser i forbindelse med det svenske teleselskapets etablering i Usbekistan.
15.12.12	Borte vekk og etterlyst av Interpol	Telenor-eide Vimpelcom forhandlet med usbekeren Bekhzod Akhmedov da selskapet skulle etablere seg i Usbekistan. Han er nøkkelperson i hvitvaskings- og korrupsjonssaker som rulles opp i to land. Akhmedov er forsvunnet og etterlyst av Interpol.
18.12.12	Tror kvinnen bare er et mellomledd	Gayane Avakyan leder selskapet som solgte mobillisens til delvis Telenor-eide Vimpelcom i Usbekistan. Advokaten til den 29 år gamle kvinnen fra motebransjen tror klienten er et mellomledd som skjuler selskapets egentlige eier.
19.12.12	Vil ha svar fra Vimpelcom	Næringsminister Trond Giske legger press på Telenor-deleide Vimpelcom for mer åpenhet om investeringene i Usbekistan. Åpenhet kan få en slutt på spekulasjonene, mener han.
22.12.12	Vil offentliggjøre hemmelige partnere	Telenor presser på for at Vimpelcom skal offentliggjøre hemmeligholdte avtalepartnere.

Vedlegg 2: Liste over sentrale kilder

Selskapsregistre

- Companies House Gibraltar <http://www.companieshouse.gi>
- Companies House (UK) <http://companieshouse.gov.uk/>
- Department of Registrar of Companies and Official Receiver (Kypros) <https://efiling.drcor.mcit.gov.cy/>
- U.S. Securities and Exchange Commission (SEC <http://www.sec.gov/edgar.shtml>)
- Dun & Bradstreet Global Reference Solution (abonnement) <https://solutions.dnb.com/grs/>
- www.Companydocuments.com

Hjemmesider/selskapsinformasjon

- Vimpelcom (Vimpelcom.com, beeline.ru og lokale nettsider)
- Telenor
- Alfa Group/Altimo
- Orienbank
- ATF Bank
- Verny Capital
- TeliaSonera
- MTS

Andre nettressurser

- Facebook
- LinkedIn
- CIA Factbook <https://www.cia.gov/library/publications/the-world-factbook/>
- International Centre for Settlement of Investment Disputes <https://icsid.worldbank.org/ICSID/Index.jsp>
- Wayback Machine <http://archive.org/web/web.php>
- UD's landsider

Frivillige organisasjoner

- Human Rights Watch
- Freedom House
- Amnesty International
- Den norske Helsingforskomite
- Open Dialogue Foundation
- Transparency International