Globalisering på norsk: Vipps-indere på overtid og en tastefeil på Mongstad

Metode-rapport til SKUP 2017 fra NRK Nyheter

Line Tomter line.tomter@nrk.no og Anne Cecilie Remen anne.cecilie.remen@nrk.no

Innholdsfortegnelse

1.0 Bakteppet:

IT-arbeidere i India kan med et tastetrykk stoppe arbeidet på norske oljeinstallasjoner. Det handler om globalisering, fri flyt av tjenester og direktører som vil spare penger. Sentrale norske bedrifter har gitt fra seg IT-ryggraden i virksomheten. Asiatiske gjestearbeidere som aldri har hørt om regulering av arbeidstid overtar jobbene til høyt utdannede nordmenn.

Det er et mantra, budskapet om at alle tjener på globalisering og friere flyt av tjenester.
I fjor vinter ble det tydelig at mange berørte parter er uenige. Flere som har tapt på globalisering utfordret etablerte sannheter ved å stille spørsmål ved om fri flyt av arbeidskraft tjener andre enn store selskaper. Ut over 2015 økte oppslutningen om Brexit og Trump. Hendelsene skapte sjokkbølger i toppen av samfunnssjiktet.

I norske bedrifter har mange blitt stemplet som uvitende og til og med som rasister når de har stilt spørsmål ved utflagging av IT til Asia. Også NRK har blitt beskyld for stigmatisering og for å komme med negative skildringer av indiske arbeidstakere.
Da vi startet vår artikkelserie om utflagging av IT, møtte vi motbør fra miljøer i norsk næringsliv, de ønsket seg ikke saker om negative konsekvenser av outsourcing. En sentral aktør i norsk IT-bransje skrev i fjor til oss i en e-post: "Jeg mener dere verken forstår dette eller anlegger et bredt perspektiv" Tonen var nedlatende og belærende.

Konsekvenser av globalisering

Prosjekt Globalisering tok oss ut på en reise som ga oss kilder og kontakter langt utover landets grenser. Til sammen snakket vi med mennesker fra ni ulike nasjonaliteter. Kildetilfanget var omfattende. Det var indiske IT-ingeniører, norske sivilingeniører, konsulenter fra ulike land, mellomledere i norske bedrifter, bedriftsledere, plattformsjefer, oljearbeidere, oppsagte medarbeidere som var skjøvet ut av billige indere, sikkerhetseksperter, forskere, myndighetspersoner. Saken viste at landegrenser på mange måter er visket ut. Samtidig var dette første året vi for alvor opplevde at kilder var skeptiske til å kommunisere digitalt, de ville ikke legge igjen elektroniske spor. Selv telefonsamtalene måtte gjøres ved hjelp av kryptertingsapplikasjoner.

Idé og arbeidshypotese tok form: Store norske selskaper som Telenor, DNB og Statoil kutter ansatte for å spare penger og hyrer inn indiske IT-arbeidere på korttidskontrakter. Globalisering av arbeidslivet presser norsk IT-konsulenter ut av de store norske selskapene til fordel for arbeidstakere i lavkostland.
Outsourcingen skjer til land som India, Sri Lanka og Kina. Land hvor korrupsjonen er utbredt, hvor arbeidstakere ikke har rettigheter som i vestlige land. Det trigget vårt engasjement at omfanget av outsourcingen har gått under radaren uten offentlig debatt.

Organisering av arbeidet

Vi kjørte saken i tospann og jobbet tett sammen fra første dag. Kildearbeidet ble fordelt, og etterhvert som vi fikk nye kontakter, drev vi kildepleie på hver vår kant. Når kilder ville møte oss dro vi begge avgårde, uansett hvor sent det var på kvelden eller om kilden befant seg i en annen del av landet. Sakene var krevende og vanskelig dokumenterbare, mens selskapene vi ettergikk er mektige og klare til å sable oss ned ved første anledning.

I arbeidet med saken gikk vi back-to-basic i journalistisk forstand, slik man jobbet før digitaliseringens tidsalder. Vi møtte folk ansikt til ansikt og hadde hemmelige møter i parkeringshus og parker i ulike deler av landet. Mange av kildene ønsket ikke under noen omstendigheter å bli sett med journalister fra NRK. Flere turte ikke sende dokumenter med e-post, og insisterte på fysisk overlevering av dokumenter slik at ingen elektroniske spor ble etterlatt.

Når mektige IT-aktører er under lupen, øker oppmerksomheten om digital sårbarhet. Nesten alle kildene var engstelige, de krypterte meldinger og samtaler eller de insisterte på fysiske møter.
Også reporterne ble mer oppmerksomme på hvor IT-giganter har ressurser til, ble vi mer forsiktige med hva vi sa over telefon også til hverandre og ingen hemmeligheter ble delt uten kryptering. For etter hvert som arbeidet skred frem ble det også tydelig for oss hvor mye av IKT-infrastrukturen i Norge som kontrolleres av amerikanske og indiske selskaper og som driftes utenfor landets grenser.

Idéen utvikler seg

Et indisk outsourcingselskap dukker opp i Porsgrunn sammen med Bjørn Richard Johansen, tidligere partner i First House. Det er november 2015 og NRKs reporter Line Tomter ble nysgjerrig på hva inderne bedrev i Norge.
Noen telefoner til tillitsvalgte og større fagforeninger i Telenor, førte ikke frem, da NRK gjorde det første forsøket på å dykke i saken desember 2015. Samtidig var det tydelig at omfanget av outsourcing i norsk næringsliv var større enn reporteren først hadde sett for seg. Indias største IT-selskaper var alle på plass i Norge og i sterk vekst.

En samtale med en bekjent i februar satte fart i tanken på å gjøre noe journalistisk på de indiske IT-gigantene. En kar i omgangskretsen uttrykte bekymring.
"En hel generasjon norske IT-utviklere er i ferd med å gå tapt", sa reporterens bekjente. Konsulenten kjente flere godt voksne menn som lærte opp billige asiatiske IT-arbeidere, som skulle ta over deres arbeidsoppgaver. Han mente alle norske kunder etterspurte billige asiatiske arbeidere, det skapte en viss iver at de kunne få minst fem asiatere til prisen av en nordmenn.

I løpet av vinteren hadde en annen kollega snappet opp interessant informasjon. På hyttetur med skivenner diskuterte reporter Anne Cecilie Remen globaliseringen av arbeidslivet. En advokat som hadde jobbet for et større multinasjonalt selskap fortalte at Telenor stadig fikk nye puljer med indere til landet. Etter at de hadde vært her i tre måneder ble de byttet ut med nye.

Etter et morgenmøte startet samarbeidet mellom reporterne. Prosjekt Globalisering var i gang. Vi bestemte oss for å bruke noen dager til å sjekke ut om hypotesen om at store norske kunnskapsbedrifter bedriver sosial dumping. Begge reporterne var overbevist om det fantes historier verdt å fortelle om bruken av indiske arbeidstakere og IT-selskaper.

IT-nomadene overtar norske jobber

Vi tok kontakt med Telenor og spurte om hvor mange utenlandske indiske medarbeidere som jobbet der, hvor lenge de var ansatt og til hvilken lønn. Svarene var omtrentlige, de kunne ikke gi tydelig svar på omfanget. Det trigget vår nysgjerrighet. Det var også tydelig at fagforeningene fortsatt var lite engasjerte i forholdene til utenlandske kolleger. Forventninger fra desk om å produsere gjorde at vi lagde saker til nett og radio; " Slik overtar indiske IT-arbeidere norske jobber." Telenor åpnet dørene og lot oss få tilgang til et par mellomledere fra den indiske underleverandøren. De første sakene fortalte om indere som jobber for Telenor, om jobbpendling og et liv som IT-nomader, inderne i 30-40 årene som hadde jobbet i 20 ulike land.

Telenors ledelse avviste sosial dumping. Bruk av indisk IT-kompetanse handlet om at det ikke fantes riktig kompetanse i Norge. Det var en uttalelse som provoserte og som bidro til nye tips.

Vi fikk på samme tid anslag på at 30 milliarder kroner sendes ut av landet i forbindelse med utflagging av IT.

Telenor-artikkelen og den neste: "Frykter at ondsinnede utnytter It-nomader" førte til at vi fikk en uvanlig stor mengde tips fra it-folk, mellomledere og sjefer i IT-selskaper. Tipsene gikk ut på det samme. Det foregikk en utstrakt outsourcing av IT-jobber til asiatiske selskaper og norske IT-ansatte mistet jobbene sine. Noen av e-postene hadde skjulte avsendere, men budskapet var tydelig. Mange var bekymret.

Her er et eksempel på mail.

"Nordmenn kastes ut i arbeidsledighet og erstattes av, som dere sier indere og østeuropeere. Disse jobber for helt andre betingelser. Men ikke la dere lure av fagre ord om kompetanse, dette gjøres for å redusere kostnader. Det som skjer i IT-bransjen nå, er det samme som skjedde med norske sjøfolk.Se på en halvstatlig bedrift som DnB, med ca 20 milliarder i overskudd. DnB har sparket hundrevis av norske IT-folk på dør og erstattet disse med indere, for å spare "kanskje" 200 millioner i året? For meg fremstår dette som kynisk kapitalisme av verste sort."

Denne tipseren og flere andre nevnte DNB. Vi visste at storbanken hadde flagget ut noe av IT-virksomheten, men vi visste ikke noe om omfanget. Vi var blitt nysgjerrig på sikkerhetsaspektet etter et møte med Nasjonal sikkhetsmyndighet. De første e-postene fra indere dukket også opp, vi skjønte at arbeidskulturen i de indiske selskapene var veldig annerledes enn hva norske arbeidstakere er vant til.

Påstander om sosial dumping i DNB

En dag fikk vi et tips fra en IT-konsulent som hadde jobbet med Vipps-prosjektet. Han fortalte at det i DNBs lokaler ble drevet rovdrift på indere og at de fikk ikke overtidsbetalt.

"Dette omhandler indere, som jobber mellom 14 og 16 timer om dagen - 7 dager i uka. Og dette skjer inne i DNB's hovedkontor på Dronning Eufemia's Gate 30 i Oslo. I Øst bygging på 5 etasje (5Ø) sitter Vipps utviklingsteamet fra TCS, som DNB har hyret inn til å skape og vedlikeholde Vipps prosjektet. Jeg har en log over versjons-styrings-systemet, subversion, som bl.a. viser arbeidstider, men jeg har ikke ID-kort logs fra dørene, så man kan se nøyaktig når de kom og gikk."

Dette var et av flere tips om at det ikke var DNB, men den indiske underleverandøren som sto bak suksessen Vipps og at utlendingene jobbet under andre forhold enn de norske. Fordi kilden var anonym nølte vi først, men da også El og IT-forbundet engasjerte seg og meldte saken til Arbeidstilsynet ble det enklere. Da Arbeidstilsynet ville undersøke sosial dumping for VIPPS-arbeiderne, hadde vi grunnlag for å presentere påstandene.

Vi fikk også kontakt med flere andre kilder med tilknytning til DNB, de bekreftet tipserens påstander. DNB informasjonsdirektør avviste overfor NRK sosial dumping, lange arbeidsdager og at indere ble sendt hjem hvis de klaget. Direktøren sa først at inderne var her bare i korte perioder, så hjemsending før tiden var ikke relevant. Det resulterte i saken, Arbeidstilsynet gransker VIPPS-prosjektet. Samme dag fikk vi de første e-poster fra indiske IT-arbeidere som bekreftet innholdet i saken. Noen dager senere dukket det opp påstander om fryktkultur og hundsing av indiske IT-arbeidere. Snøballen rullet.

2.0 Metode og jakten på informasjon:

Spaning som metode

Vi fikk tips om at DNBs mange asiatiske IT-arbeidere satt isolert fra resten av de bank-ansatte, men at de ofte sto på gaten utenfor hovedkontoret i Bjørvika og røyket. Vi dro ned til Bjørvika og plasserte oss utenfor lokalene midt på dagen. Vi ble overveldet over å oppdage at det sto flere titalls indere, i all hovedsak menn, utenfor. Vi la merke til at de fleste hadde adgangskort på brystet som så annerledes ut enn det de DNB-ansatte gikk med.

Vi tok kontakt med indere som sto utenfor DNB. De bekreftet at de jobbet for banken, men ville ikke la seg intervjue. Hvis de snakket med media, ville de miste jobben. Vi var utenfor banken flere ganger og hver gang vi var der, var det grupper av indere utenfor.

Vi trålet gatene på Skillebekk og Frogner hvor vi hadde fått tips om at det var hybelhus for indere. Vi spurte folk på gaten om de visste om slike hybelhus, vi tittet etter navn på ringeklokker.

Vi dro opp til lokalene til selskapet TCS og lette etter lokalene til HCL i Bjørvika. Vi dro ut til Fornebu. Etter hvert så vi indere overalt. . Spaningen førte til at vi forsto at omfanget av asiatiske IT-arbeidere i Oslo-området var enormt.

Plassert utenfor DNBs lokaler på cafe tok vi bilder av flokkene av indere for å dokumentere omfanget. Vi spurte ikke om tillatelse til det, og vi valgte ikke å bruke bildene selv om de var tatt på et offentlig område.

Anonyme kilder som metode

Bruken av anonyme kilder var helt avgjørende for sakene. Noen av sakene var utelukkende basert på påstander fra anonyme kilder. Men når 30 personer uttalte det samme, følte vi oss trygge på å publisere påstandene, men selvsagt hentet vi først inn tilsvar fra de berørte selskaper.

Det var flere runder internt med ledere om bruken av påstander basert på anonyme kilder, da flere av påstandene var skadelige for omdømmet til selskapene vi omtalte.

Å få informasjon fra folk på innsiden var avgjørende. Alle tipserne og kilder vi kontaktet hadde mye å tape på å stå frem. For indiske IT-arbeidere kan det bety et liv i rennesteinen dersom de svartlistes av et stort IT-selskap. Også norske ansatte var redde for jobbmuligheter dersom det ble kjent at de snakket med NRK. Selv om kildene hadde mye å tape, var det mange som så viktigheten av å belyse sakene.

IT-arbeidere i norske virksomheter og flere mellomledere i store, norske bedrifter, som uttrykte frustrasjon, fortalte om stadig nye arbeidsoppgaver som forsvinner ut av landet. Vi var overrasket over flere av e-postene, de fortalte om frustrasjon vi aldri hadde sett uttrykt i det offentlige rom. Det nedslående var at ingen ville stå frem med kritikk og frustrasjon, det var likevel konkret nok til å gå videre. Og det motiverte oss til å dykke dypere.

Etter de første sakene manglet det ikke på reaksjoner fra IT-arbeidere i norske bedrifter. VI begynte å få henvendelser fra indiske IT-arbeidere. Vi tok systematisk kontakt med alle som sendte oss reaksjoner på sakene våre. Etter hvert fikk vi også dokumenter som var relevante for saken.

Snart dukket det opp opplysninger om VIPPS-arbeiderne. Det var vanskelig for oss å påstå dette uten dokumentasjon.

VI fikk etter hvert møte en kilde som ga oss datalogger som viste når folk hadde vært logget på VIPPS-prosjektet. Kilden ønsket kun å være anonym. Det var først da fagforbundet El og IT ble informerte av kilden og sendte saken videre til Arbeidstilsynet, at vi følte oss trygge nok på å kjøre en egen sak på de grove påstandene. Verken i DNB eller Telenor virket det som om de fleste fagforeningene engasjerte seg. De indiske it-arbeiderne var ikke organiserte, holdningen til fagforeningene var at disse er ikke medlemmer hos oss, og vi kan derfor ikke engasjere oss i deres arbeids og lønnsforhold.

I løpet av arbeidet fikk vi kilder blant indere i Norge, i andre vestlige land og i India. Noen tok direkte kontakt med oss etter å ha lest artikler (et par ble oversatt til engelske/indiske nettsteder), vi fikk tips om indiske kilder av norske kilder. Ved hver ny kontakt fikk vi gjerne minst en ny. Noen møtte vi på cafe, andre snakket vi med på telefon, på mail eller meldte. Vi møtte ikke bare indiske IT-arbeidere, vi hadde også kontakt med indiske mellomledere. Mange ønsket å bidra med informasjon for å bedre arbeidsforholdene i Norge, men ingen ønsket å stå fram.

Innhenting av informasjon fra offentlige registre og myndigheter som metode:

Vi tok kontakt med UDI, Skatteetaten og AA-registeret, Utenriksdepartementet, SSB , Arbeidstilsynet og utenlandske ambassader for å få informasjon om hvor mange utenlandske IT-arbeidere som jobbet i Norge. Vi fikk tall som viste at reisende med forretingsvisa fra land som Kina, Sri Lanka og India hadde økt dramatisk de siste årene. Men det var ikke mulig å få oversikt over hvor mange IT-arbeidere som var i Norge. Kontakt med ambassader bekreftet at det var en sterk vekst i antall IT-arbeidere som reiste til Norge, men ingen hadde konkrete tall. Skatteetaten og SSB hadde heller ikke oversikt over hvor mange It-arbeidere som betalte skatt til Norge. Vi var i kontakt med forskningsmiljøer, men fant ingen forskning på omfanget av outsourcing i norske virksomheter, og hvordan dette påvirket arbeidslivet, lønninger og arbeidsplasser. "Det er umulig å få penger til å forske på outsourcing", sukket en kilde med interesse for temaet.

Vi hadde møter og utallige telefonsamtaler med UDI for å få innsyn i hvor mange IT-arbeidere som jobbet i Norge på kortidskontrakter under tre måneder, under seks måneder og over et år. Men vi fikk ikke tall som kunne hjelpe.

Mangelen på oversikt hos myndigheter og mangelen på engasjement hos politikere og forskningsmiljøet for konsekvenser av outsourcing på arbeidslivet var en utfordring.

Kartleggingen viste at mange av de store indiske selskapene som HCL, Tata Consultency Services og Tech Mahindra hadde etablert seg i Norge siste årene. En sjekk i regnskapstallene viste at omsetningen deres hadde økt kraftig siste år. Vi ble derfor overrasket over at tallene for antall ansatte ikke var i samsvar med inntektene. Dette bekreftet teorien om at de utenlandske IT-arbeiderne var her på korttidskontrakter og at flesteparten etter opplæring jobber fra India.

Vi ba om innsyn i flere rapporter fra Arbeidstilsynet, men oppdaget at de i liten grad hadde gjort tilsyn blant utenlandske IT-foretak. Tilsynene hadde gått mer på HMS og fysiske arbeidsforhold enn på lønn og jobbbetingelser. Vi undersøkte med TCS og med Arbeidstilsynet om TCS hadde søkt om å få dispensasjon for sine ansatte om utvidet overtid, men fikk bekreftet at de ikke hadde søkt om det.

Innhenting av dokumentasjon arbeidsforhold

En ung mann ønsket å møte oss. Vi hadde fått tips om at vedkommende hadde varslet sin tidligere arbeidsgiver, Norgesgruppen, om hundsing av indiske IT-arbeidere etter at dagligvaregiganten outsourcet IT-infrastrukturen til indiske TCS. Vi tok en lunsj med kilden, som i detalj fortalte om alle han kontaktet for å varsle om hundsing av indiske kolleger og hvordan norsk lov etter hans oppfatning systematisk ble brutt av det indiske outsurcingselskapet. Ingen hadde engasjert seg etter hans varsling, hverken Norgesgruppen, Arbeidstilsynet,verneombud, fagforening eller politikere, fortalte varsleren. Et en kort tenkepause stilte han opp til intervju, men valgte å være anonymisert. Saken fokuserte på at indiske IT-arbeidere som jobber for dagligvaregiganten hundses og lever i en fryktkultur. I et brev til ledelsen i Norgesgruppen hadde han året før skrevet:

"Disse kollegene ønsker ikke at det varsles om lovbruddene som finner sted. De frykter for jobben og livsgrunnlaget sitt. Det er derfor vanskelig for meg å skrive dette brevet, men det ville vært enda vanskeligere å fortsette uten å si ifra. Jeg gjør dette helt på eget initiativ og uten innblanding eller viten hos noen i Norgesgruppen eller TCS."

Nye e-poster dukket opp, så snart saken var ute. Indiske IT-arbeidere uttrykte takknemlighet over at vi satte fokus på deres arbeidsforhold. Ingen avkreftet innholdet i saken.

Kort tid etter tok ledelsen i TCS Norway kontakt, de ønsket nå å stille opp i media og fortalte at de opplevde mye av kritikken mot dem som urettferdige.

Ved at kildene stolte på oss fikk vi etter hvert overlevert dokumentasjon av privat karakter. Vi mottok kopier av lønnsslipper, vi fikk arbeidsavtaler, sluttavtaler, vi fikk tilgang til e-poster og vi fikk kopier av brev som varslere hadde sendt ledere. Alt dette mottok vi under løfte av å ikke bruke det som faksimile, ikke gjengi navn, ordlyd eller tall direkte. Det viktige var at dokumentene viste at indiske IT-arbeidere fikk vesentlig lavere lønn enn sine norske kolleger, de ble trukket i lønn for bolig, for telefon, de fikk ikke overtid. Vi fikk historier om fryktkultur som de jobbet under. Fryktkultur er vanskelig å dokumentere, men vi snakket med en rekke norske IT-ansatte som jobbet med eller hadde nylig jobbet med indiske IT-arbeidere i Norge, og fikk det entydig samme bilde.

De indiske IT-arbeiderne jobbet lange dager og de måtte være tilgjengelige 24/7. Vi snakket med indere som var sendt hjem fra Norge og erstattet med nye indere etter at de hadde klaget på arbeidsmengde og på lønnsbetingelser i Norge.

Vi fikk innblikk i at det fantes to system for timeføring. En for de norske ansatte og en for de indiske eller utenlandske ansatte. Vi mottok skjermdump av timesystem som viste at det var teknisk umulig å føre inn mer enn 8 timer arbeid per dag for indiske arbeidstakere i Norge. I kildemøter med ikke-asiatiske ansatte for TCS fikk vi se skjemaer som viste hvor lenge en rekke TCS-ansatte i Vipps-prosjekter var innlogget på jobb. Vi fikk ikke med oss loggene, for kilden var redd for at de kunne spores tilbake til ham, men vi fikk ta bilder av deler av loggene og brukte informasjonen i reportasjene.

Gjengangeren hos mange av de indiske IT-arbeiderne vi snakket med var:"We are afraid."

Gjennom å søke innsyn i dokumenter hos Arbeidstilsynet fikk vi etter hvert navn på mange titalls indere som jobbet i Norge. Vi søkte på disse navnene i folkeregisteret og i skattelistene for å finne ut hvor lenge de var her og om de hadde permanent opphold. Bare et fåtall var registrert som arbeidstakere og skattet til Norge. Vi sporet opp en rekke indiske IT-arbeidere og hadde bakgrunnssamtaler med dem.

Interne varsler-brev på ulovlige arbeidsforhold var viktige kilder. Her er deler av et brev som ble sendt flere ledere og verneombud i Norgesgruppen.

"Det finner sted flere og gjentatte brudd på arbeidsmiljøloven både på Kalbakken og i Nydalen hvor TCS nå har flyttet. Disse lovbruddene gjelder kun TCS-ansatte fra India. Vi som er overflyttet fra NG Data til TCS er ikke utsatt for lovbruddene, men det er selvfølgelig en belastning å være maktesløse vitner til slike lovbrudd.

Jeg har blitt fortalt av flere indiske kolleger er at de har fått beskjed om at hvis de forsøker å stille krav vil de bli sendt hjem til India for så å bli sagt opp. De ønsker derfor ikke å stå frem. Om de vil bekrefte påstandene jeg nå fremlegger er også usikkert."

Men arbeidet med å skaffe oss skriftlig dokumentasjon og flere kilder fortsatte. Vi fikk navn på flere nåværende og tidligere ansatte i TCS i Norge. Noen av disse befant seg i India etter å ha blitt sendt hjem. Vi kommuniserte med dem gjennom kryptert mail og krypterte meldingstjenester som Signal og Telegram fordi de var livende redde for represalier. Alle bekreftet informasjonen som vår kilde hadde fortalt. De jobbet døgnet rundt, de fikk en fastlønn som lå på rundt 20.000-25.000 i måneden, de ble trukket 5000-8000 kr i bolig. De var ikke vant til på få verken overtid, ferielønn eller ferie i India, og trodde det skulle være slik når de kom til Norge. Til forskjell fra i DNB og i Telenor satt de i samme lokaler som de norske ansatte og ble gjort oppmerksomme på forskjellene i lønnsnivå og arbeidstid. De indiske IT-arbeiderne fortalte at om de klaget på lønn eller arbeidsforhold, eller nektet å komme på jobb i fritid eller om natten, ble de sendt hjem til India

Vi snakket med verneombud og tok kontakt med Norgesgruppen og TCS. Ledelsen i Norgesgruppen hadde nok fryktet at vi tok kontakt etter Vipps-historien, og vi opplevde at de var forberedt. Vi hadde et flere timer langt møte med 4 ledere i Norgesgruppen. Vi la frem den informasjonen vi hadde fått, de sa de var sjokkerte, men samtidig visste vi at de hadde fått samme informasjon året før og lite eller ingenting var blitt gjort for å hjelpe inderne til å få bedre arbeidsdager. Vi intervjuet Tatas talsmann i Norge, en nordisk PR-sjef som satt i Finland. Han avviste alle påstander og fremhevet at TCS fulgte norske lover og regler.

Etter at vi sendte manus til gjennomlesning opplevde vi at Norgesgruppen ba om å få god tid til å lese og gi kommentarer. Vi forsto snart at det var fordi de ønsket å ta brodden av saken med å samtidig kunne fortelle at de satte i gang en granskning hvor de hyret på med advokater og revisorer.

https://www.nrk.no/norge/xl/hevder-indiske-it-arbeidere-jobber-i-en-fryktkultur-hos-dagligvaregiganten-1.13010035

Jakten på Statoil- dokumentasjon

Etter sakene om Vipps og fryktkultur i TCS fikk vi flere tips om at vi burde se nærmere på outsourcingen i Statoil. Tipsene kom i hovedsak på mail og var fra folk som jobbet i Statoil , som hadde jobbet i Statoil eller som jobbet hos Statoils underleverandører. Tipsene dreide seg om at Statoil hadde hatt utfordringer med outsourcingen, uten at det var mer konkret. Vi forsto at det ville bli utfordrende å grave i dette, særlig fordi vi manglet gode kilder i Statoil og i oljebransjen. For hvor skulle vi begynne uten gode kilder?

Vi la tipset til side en periode. Men i forbindelse med et kildemøte om sikkerhet og sårbarheter knyttet til outsourcing ble Statoil nevnt. For første gang hørte vi om en hendelse på Mongstad. Også i andre samtaler fra et andre miljøer hørte vi Statoil og Mongstad bli nevnt, og vi bestemte oss for å finne ut mer.

Statoil har mengder med tillitsvalgte og verneombud og vi startet med å ringe dem alle. Vi fordelte de ulike mellom oss. Men vi måtte konstatere at vi fikk lite napp . Vi tok også kontakt med tillitsvalgte og verneombud på Mongstad for å høre om det hadde vært hendelser der slik tipsene gikk ut på. Ingen av de vi snakket med bekreftet at det hadde vært problemer på Mongstad, men flere fortalte at outsourcingen førte til mange praktiske utfordringer og forsinkelser. Vi opplevde at det er stor lojalitet hos Statoil-ansatte og at de var redde for å skade selskapets rennomme, de ville ikke at sårbarheten skulle komme frem i offentligheten. Utfordringen med å få napp på tipset om Mongstad avdekket også hvordan Statoilansatte ønsket å beskytte norske arbeidsplasser.

Hver gang vi snakket med noen i selskapet, spurte vi etter navn på andre som kunne vite noe. Slik utvidet vi kildenettverket gradvis i løpet av et par-tre uker. Men slik forsto vi også at rykter om at vi holdt på med noe spredde seg i selskapet. Det ble en vanskelig balanse; å ikke fortelle for mange om hva vi visste samtidig som vi gravde etter mer detaljer og info. Vi fanget også opp at Stavanger Aftenblad ble tipset om at vi gravde rundt tema IT-sikkerhet.

Vi tok kontakt med Petroleumstilsynet for å høre om de hadde fått rapporter fra Statoil om en hendelse på Mongstad og om andre hendelser knyttet til outsourcing og sikkerhet. Det hadde de ikke. Vi møtte Petroleumstilsynet i Stavanger, vi søkte om innsyn i en rekke dokumenter og brev hos tilsynet og lette etter IKT-hendelser uten å finne mye konkret.

En dag snakket vi med en kilde som kjente Statoil fra innsiden som bekreftet at det hadde vært en alvorlig hendelse knyttet til Mongstad, men at den var blitt dysset ned. Vedkommende ville ikke si mer, men vi avtalte å snakke sammen igjen neste dag. Neste gang fikk vi vite at hendelsen skjedde i mai 2014. Samtidig fikk vi vite at det fantes noe som

het "synergirapport" om hendelsen. Kilden oppfordret oss til å finne folk som kunne hjelpe oss å lete etter synergirapporten. "Alt står der," sa kilden.

Det lages rundt 30.000 synergirapporter i året i Statoil om små og store hendelser og ulykker. Rapportene ligger tilgjengelig for Statoil-ansatte, men det er ikke et system som gjør det enkelt å søke informasjon. Vi tok kontakt med Statoil og spurte om det fantes en rapport på Mongstad fra mai 2014. Informasjonsavdelingen uttalte at rapporten var unntatt offentlighet. Igjen tok vi kontakt med Petroleumstilsynet og spurte om de kjente til en alvorlig hendelse på Mongstad i mai 2014, men vi fikk ikke bekreftet noe mer av dem. Vi fikk Statoil- kilder til å lete i synergirapport-systemet, men kilder fant ingen alvorlige hendelser fra Mongstad. Synergirapportene er ikke lett å søke i for folk som er uten teknisk kompetanse. Dessuten er det sporbart for ledelsen om noen har vært inne i rapportene. De vi snakket med sa de trengte dato og klokkeslett. Etter kontakt med ulike Statoilkilder fikk vi datoen for IKT- hendelsen på Mongstad. Vi formidlet datoen til en person som hadde vært ansatt i Statoil, og som fortsatt hadde kontakt med tidligere kolleger. En morgen dukket rapporten opp i en e-post, og det føltes det som et gjennombrudd. Her kunne vi lese svart på hvitt hva som hadde skjedd og hva Statoils egne mente om hendelsen. En tastefeil i India førte til at blandingen av olje og lasting på Mongstad stoppet opp. En indisk IT-ansatt var innenfor brannmuren uten godkjenning av Statoil og tok ned produksjonen. Vi kontaktet eksperter på infrastruktur og data for å prøve å forstå hvordan det var mulig. Vi snakket med PST, forsvaret, forsvarsforskere, it-eksperter og nasjonale sikkerhetsmyndighet. Vi viste noen av kildene synergirapporten, men fikk da kommentarer fra folk som jobbet med IKT-sikkerhet at en slik hendelse ikke nødvendigvis var så alvorlig, men fant vi 20-30 av samme karakter da kunne man snakke om et sikkerhetsproblem knyttet til outsourcing. Etter enda noen dager fikk vi mer dokumentasjon på flere IKT- hendelser i Statoil. Vi leste mengder av interne dokumenter og fant beskrevet mange IKT-uhell, i blant i bisetninger og andre ganger mer utførlig. Vi fikk overlevert flere rapporter om IKT-sikkerhet og referater fra ledermøter og seminarer. Vi dro til Stavanger og møtte Statoil-ansatte som viste oss rapporter og dokumenter som avslørte stor intern misnøye med IKT-sikkerhet etter outsourcingen. Vi fikk se presentasjoner som avdekket at ledelsen i Statoil lenge hadde vært klar over at mange IKT-hendelser kunne være en trussel. Det fremgikk av informasjonen at svært mange indisk ansatte IT-arbeidere hadde hatt mastertilgang til hele Statoils IT-system, til samtlige av Statoils produksjonsanlegg, plattformer og landanlegg. Vi lette i interne dokumenter som vi hadde fått tilgang i og leste om hvordan fageksperter uttrykte stor bekymring for sikkerhetsrisikoen knyttet til dette.

Over 100 ansatte hos Statoils indiske underleverandør HCL hadde slik mastertilgang, fikk vi etter hvert bekreftet av flere uavhengige kilder. Vi fikk informasjon om IT-arbeidere som på den andre siden av jorden tok ned brannmurer på anlegg uten å informere de lokalt ansatte eller ledelsen. Ved flere tilfeller glemte de å sette opp brannmurer igjen, slik at flere

produksjonsanlegg faktisk i timer og ved flere anledninger flere dager (ofte over helger) var helt ubeskyttet og uten brannmurer mot den ytre verden. Det var bare flaks som gjorde at ingen av disse situasjonene endte fatalt og resulterte i et fiendtlig digitalt angrep.

Vi snakket med kilder i Luftfartstilsynet og hos Meteorologisk institutt for å forstå hvor alvorlig det var for plattformer og helikopter når feil i India førte til at værdata falt ut. Etter hvert satt vi med innblikk i rundt 30 hendelser som direkte kunne knyttes til problemer knyttet til outsourcingen av IT .

Å beskytte kildene

Vi bestemte oss for å konfrontere Statoil og ba om intervjuavtale. Statoils informasjonssjef ville ha spørsmålene på forhånd. Statoil ville også vite hvilke konkrete rapporter vi hadde fått innsyn i. Det ville vi ikke gi selskapet, fordi vi var redde at det kunne spores tilbake til kildene våre. Vi leste mange typer rapporter og de bar alle forskjellige sifre, koder og navn. Dersom ledelsen kunne finne ut hvem som hadde tatt ut rapportene av systemet og formidlet til oss, kunne de avsløres.

Statoil ble provosert over at vi ikke ville gi den informasjonen til dem og spilte på at vi ikke la frem alle premissene for intervjuet (jfr Vær varsom-plakaten). Vi sendte spørsmål avgårde til selskapet og fikk beskjed om at selskapet trengte tid på å svare, og vi fikk avtale om intervju først etter 8 dager. Mongstad-hendelsen var omtalt i mange ulike interne rapporter med stor detaljgrad. Vi bestemte oss for å dra dit. Det var krevende, for intervjuobjektene trakk seg og lokal ledelse på Mongstad ville ikke stille til intervju, og vi fikk ikke lov til å filme. Men etter hvert fikk vi snakket med flere lokalt ansatte og tillitsvalgte som i intervju uttalte at outsourcingen skapte praktiske og sikkerhetsmessige utfordringer , både mht språk og at de indiske IT-ansatte flere ganger hadde tatt ned brannmurer og glemt å sette den opp igjen. De bekreftet også hendelsen hvor produksjonen ble tatt ned fra India. På Mongstad fikk vi tips om at Stavanger Aftenblad var på sporet av den ene hendelsen vi i flere uker hadde hatt kunnskap om. Vi bestemte oss for å fremskynde publiseringen med noen dager og ba om å få telefon-intervju med Statoil samme kveld, i stedet for neste morgen slik vi opprinnelig hadde planlagt. Vi følte det hastet og vi fryktet at Statoil selv ville sende ut en pressemelding for å ta brodden av vår sak.

https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013

I denne rapporten har vi måttet være vage når det gjelder å beskrive hvordan vi tak i en god del informasjon, nettopp for å beskytte kildene og ikke avsløre identiteten.

Jaktet informasjon på Dark Web som metode

Vi hadde hørt at mye sensitiv informasjon strømmer ut fra India etter hvert som stadig flere selskaper har plassert drift av datasystemene sine til indiske selskaper. Vi ville finne ut om det var etterspørsel etter informasjon om Statoil på det mørke nettet. Først måtte vi lære oss hvordan vi kom inn på "dark web ", men forsto raskt at vi ville slite med å finne ut hvor vi skulle lete. Det mørke nettet er ikke bare svart, det virker for utrente ugjennomtrengelig. Vi leide derfor en frilanser for å lete for oss. Han skulle jobbe etter journalistiske prinsipper. Han skulle lete, ikke etterspørre informasjon. Vi fant ut at det var stor etterspørsel etter Statoil i lukkede fora, men kunne ikke konkludere med at informasjon om Statoil eller andre norske selskaper strømmer ut fra India. Under arbeidet med Statoil ble spørsmål rundt sikkerhet stadig mer sentralt. På Dark Web var det ikke minst stor etterspørsel etter informasjon om styring- og kontrollsystemene til oljeplattformer. Våre kilder hadde uttrykt bekymring, nettopp over at mange av Statoils kontrollsystemer er gamle og utdaterte. Flere mente det var en ekstra risiko at brannmurer og servere knyttet til de gamle systemene ble oppgradert og jobbet på fra India.

https://www.nrk.no/norge/kriminelle-pa-dark-web-jakter-statoil-informasjon-1.13198354

Metode- jakten på informasjon om styringssystemer og brannmurer

Tidlig i prosessen fikk vi innspill fra kilder i ulike miljøer at mange av Statoils kontroll- og styringssystemer er gammeldagse og ikke tilpasset den nye digitale verden. Vi leste oss opp på Scada og de gamle styringssystemene i forskningsrapporter både nasjonalt og internasjonalt, og vi snakket med en rekke IT-eksperter og folk som var tilknyttet industrien.

Da vi sjekket dette med interne Statoil-kilder viste det seg at dette stemte: Svært mange av Statoils produksjonsanlegg har gammeldagse IT-systemer. De gammeldagse styringssystemene i kombinasjon med den omfattende outsourcingen til India og Statoils dårlige kontroll med indernes tilgang, ble av interne eksperter sett på som en stor sikkerhetsrisiko. Informasjon om helhetsbildet av problemstillingen ble holdt tilbake i organisasjonen, men flere hundre Statoil-ansatte var likevel klar over dette. Det var kjent i store deler av ledelsen på ulike nivåer og det var kjent blant IT-eksperter, men altså i liten grad blant de ansatte som jobbet i dette risikobildet til daglig.

Vi møtte IT-ansatte og IT-eksperter utenfor Statoil, forskere, ansatte i PST, forsvaret og sikkhetsmyndigheter for å forstå trusselbildet og hvordan brannmurer og styringsystemer som Scada fungerte. Vi snakket med IT-folk på plattformer, tekniske sjefer, plattformsjefer, alle under fullt kildevern. Gamle plattformer med IT-system laget før internetts tid og ikke skapt for å knyttes sammen i et nettverk med andre plattformer og med IT-systemer på land, er en utfordring Statoil ikke liker å snakke om. Datasystemene var et lappeteppe hvor man hadde oppgradert og modernisert deler av systemene, men aldri alt. Kilder fortalte oss at det fantes bare en eneste brannmur på mange av plattformene. Vi hoppet der vi satt. En

eneste brannmut. Den eneste andre beskyttelsen mot omverden var det organisatoriske,- tilgang til passord. Det ville være nok med en illojal indisk It-arbeider for å kunne slå ut hele eller deler av norsk oljeproduksjon.

Vi var målløse og gira. Målløse fordi situasjonen var mye verre enn våre første antagelser. Gira fordi vi forsto at vi var på sporet av en fantastisk historie.

Nå måtte vi finne ut omfanget av svakhetene. Hvor mange plattformer var dårlig sikret?

Å fritte ut Statoil-ansatte for hvilke plattformer og anlegg som hadde en brannmur og hvilke som var sikrere var en utfordring. Folk ønsket ikke at dette skulle komme ut. Mediedekning av svakheten i IKT-sikkerhet ble av mange kilder sett på som en risikofaktor.

Men etter hvert fikk vi navn på noen plattformer med høy sikkerhet og på plattformer med lav sikkerhet og bare en eneste brannmur. Noen dager så det ut som vi ville få et åpent intervju med en sentral IT-leder som var villig til å fortelle om den dårlige sikkerheten. Motivasjonen for vedkommende for å stille opp var at mediedekningen ville føre til at selskapet investerte de nødvendige milliarder i å oppgradere sikkerhetssystemene. På mange plattformer ville det bety nedstenging en lang periode, fikk vi opplyst. Spørsmål meldte seg etterhvert; skulle vi publisere navnene på plattformene og dermed blottstille hvor utsatte tusenvis av Statoil-ansatte på plattformene var for en fiendtlig handling? Et mulig terrorangrep på norsk sokkel ville ikke bare føre til store menneskelige tap og økonomiske konsekvenser, det ville også være en omfattende miljø-katastrofe.

Hensyn til nasjonal sikkerhet

Først fikk vi grønt lys internt av redaktører for å fortelle hva vi visste om brannmurer og mangel på IT-sikkerhet på plattformer og landanlegg. Vi hadde gode kilder som vi stolte på, vi var sikre på at historien de fortalte stemte. Flesteparten av Statoils gamle pengemaskiner av noen plattformer hadde bare en eneste brannmur. Sikkerhetseksperter vi snakket med kalte det en kalkulert risiko å knytte disse plattformene til internett. De tekniske systemene var ikke bygget for å kommunisere med andre system, men å virke i et lukket system. Notatbøkene våre forteller om jakten på navn på plattformer. Vi visste at oljebransjen og norske oljeselskaper daglig er utsatt for cyberangrep. Vi visste at informasjon om Statoil ligger til salgs på "dark web". Skulle vi publisere navnene?

Da vi satt der med disse konkrete plattformene tok vi noen runder med oss selv og med redaktører. Vi ville ikke publisere navnene av respekt for de ansatte, for de enorme konsekvensene en slik blottstilling kunne føre til.

> https://www.nrk.no/norge/oljeplattformer-med-bare-en-brannmur_-ansatte-frykter-hackerangrep-1.13208019

Samtaler via krypterte forbindelser

Særlig indiske IT-arbeidere var opptatt av å skjule alle elektroniske spor. Som ansatte i store teknologiselskaper visste de utmerket at ukryptert e-post i praksis er like lite sikkert som et postkort. Apper som Signal og Telegram ble flittig brukt i kildepleien. Når det begynte å bli snakk om dokumenter det var strengt forbudt å gi fra seg eller la utenforstående lese, ønsket ikke kildene å sende dette elektronisk, selv ikke når vi foreslo kryptert epost. Vi måtte derfor ut på et par reiser for å få tak i og for å få kikket på dokumentasjon til sakene våre. Noen kilder lot oss få lese dokumenter å ta noen bilder, men ønsket ikke gi fra seg dokumentene fysisk. Det var også kilder som benyttet seg av mellommenn, slik at det ikke dokumenter kunne spores direkte til person som var opprinnelig kilde.

3.0 Kildene – de gode hjelperne

Mange av tipsene vi fikk var konkrete og gode. Problemet var at få ville stå frem. IT-arbeidere var redde for jobbe sine, eller de var redde for å ramme kolleger, eller redde for å ikke få flere oppdrag for de store selskapene. Viktig å få folk til å stole på oss, og at de fikk trygghet på at vi beskyttet dem som kilder. Flesteparten av kildene i disse sakene var helt nye. Vi hadde over uker og måneder gjentatte samtaler, møter, telefoner og meldinger med over hundre kilder. Slik sett brukte vi disse møtene til å skaffe oss brokker av informasjon som til slutt skapte et helhetlig bilde. I og med at de første sakene om Vipps og TCS og Norgesgruppen i stor grad baserte seg på kilder som ikke ville stå frem med fullt navn og la seg identifisere , var vi opptatt av å få bekreftet informasjonen fra flest mulig kilder, fra kilder som var uavhengige av hverandre. Vi brukte også tid på å få bekreftet at kildene var den de utgav seg for og at de jobbet eller hadde jobbet for de indiske selskapene.

Vi hadde også bakgrunnssamtaler med forskere, Arbeidstilsynet, sikkerhetseksperter ansatt i det offentlige og folk i Forsvaret for å få best mulig oversikt over problemstillingene, men uten å referere fra møtene.

Vi opplevde at snøballen rullet. Når kildene forsto at vi brukte anonyme kilder i reportasjene og beskyttet deres identitet, ble flere trygge på å ta kontakt med oss. Kildeomfanget vårt ble etter hvert stort.

Muntlige: Mange titalls IT-arbeidere, norske, indiske, flere andre land, tidligere IT-arbeidere, IT-ledere, direktører for IT-bedrifter, tillitsvalgte, forskere, byråkrater, ansatte i sikkerhetsmyndighet, Luftfartstilsynet, forsvarsfolk, vaktmester, sikkerhetsvakter, kontoransatte, plattformsjefer, Statoil-ansatte, tidligere Statoil-ansatte, ansatte i andre oljeselskaper enn Statoil, ansatte på plattformer og oljerigger, russiske IT-eksperter, hackere.

Skriftlige: Ansettelsesavtaler, lønnslipper, interne mailutvekslinger, varslerbrev, datalogger, forskningsrapporter, offentlige rapporter, NOU, dokumentasjon som viste hvordan Scada-system og brannmurer som Statoil har virker, Statoils interne synergirapporter, Statoils

interne dybdestudier, interne brev, referat fra ledermøter, informasjon om salg av informasjon på "The dark web". Tilsynsrapporter fra Petroleumstilsyn og fra Arbeidstilsyn.

4.0 Intervju med selskapenes talsmenn

I disse sakene har vi hatt med å gjøre noen av de største selskapene i Norge og India. DNB og Statoil, Norgesgruppen og Telenor. TCS og HCL i India.

Utfordringene handlet mye om trenering, vi fikk ikke svar på spørsmålene våre på flere dager, vi opplevde at de brukte Vær varsom-plakaten aktivt for å hindre eller å utsette publisering av saker. Det er tungt å jobbe mot de store selskapene som omfattende pr-apparat rundt seg og som vet å utnytte alle. Ved et par anledninger opplevde vi at både Statoil og DNB og Norgesgruppen ville ha et døgn og opp til en uke for frist på tilsvar. Vi opplevde at selskap brukte tiden til å sette i gang tiltak for å ta brodden av våre saker.

I DNB ble vi nektet å få bilder fra områder hvor de indiske it-arbeiderne jobbet. I stedet ble vi vist til en sofa i resepsjonen. Vi ba om å få intervjue It-arbeiderne, men fikk ikke tillatelse til det. Heller ikke i Statoil fikk vi komme inn og ta bilder der hvor it-ansatte jobber. Vi ba om å få reise ut på en plattform for å gjøre opptak , men fikk til svar at det ville de ikke gi oss tillatelse til.

Vi spurte også om å få komme inn og filme på Mongstad. Vi fikk beskjed om at det ikke lot seg gjøre og at det var for kort varsel å spørre om det med noen timers varsel eller dagen etter.

I Telenor fikk vi komme inn i en etasje hvor utenlandske IT-arbeidere jobbet, men vi fikk ikke lov til å snakke med noen eller ta bilder. De vi fikk intervjue var ledere og mellomledere i TCS og i Telenor.

Norgesgruppen. Her fikk vi møte ledelsen av selskapet. Først fikk vi tillatelse til å filme og gjøre opptak i lokalene hvor inderne satt. Men selskapet ombestemte seg.

5.0 Fordelen med å være to

I NRK jobber man oftest ikke i tospann. Vi jobber i turnus og det er ikke lett å finne dager og vakter hvor det er sammenfallende arbeidstid.

Det er mange fordeler å være to. Vi utfyller hverandre og vi oppmuntrer hverandre . Hvis den ene har en dårlig dag, drar den andre kollegaen opp. Vi har alltid en sparringspartner. To tenker bedre enn en. Vi har ulike kilder. Men en annen fordel ved å være to er at vi sammen blir sterkere. Vi utfordret noen av landets største og mest innflytelsesrike selskaper og noen av Indias mektigste selskaper. Det er lettere å la seg overvelde av taushet, trenering og trusler om advokatbruk når man jobber alene. Det gir også mer styrke, selvtillit å være to i selve intervjusituasjonen. Vi opplevde også at kilder ga oss tilbakemelding på at de opplevde oss som et energisk og engasjert team som de syntes det var spennende å forholde seg til. Alt dette ga oss et trøkk vi ikke hadde fått alene. Mye av informasjonen vi fikk var teknisk, og

vi opplevde at vi ble "belønnet" av kildene våre når de oppfattet at vi forsto det tekniske og at de stolte på at vi forvaltet informasjonen vi fikk godt.

6.0 Utfordringene

Mangelen på interesse hos sentrale aktører var den første bøygen.

Omkvedet hos den politiske eliten og hos bedriftsledere, om at globalisering utelukkende er et gode for samfunnet, gjorde det vanskelig å engasjere politikere. Både denne Regjeringen og den forgående har tilrettelagt for at internasjonale IT-giganter med indisk arbeidskraft skal operere i Norge.

Sentrale tillitsvalgte i fagforeningene var defensive, mange så seg lite tjent med å kritisere ledelsens beslutninger.

Elitene har etablert en sannhet om at utflagging av IT utelukkende er et gode for samfunnet og at det tjener oss alle.

Når vi stilte spørsmål om mulige negative konsekvenser ble vi karakteriserte som bakstreverske, teknologifiendtlige og kunnskapsløse

Saken var politisk død, ingen partier brydde seg om strømmen av sentrale IT-oppgaver og penger som forsvant utover grensene.

Det var vanskelig å dokumentere påstander om fryktkultur, og det var utfordrende å få tak i interne dokumenter fra landets viktigste bedrifter. Vi måtte belage oss på anonyme kilder og dokumenter skaffet av folk på innsiden av selskapene.

7.0 Erfaringer, funn og konsekvenser

Fra dag en hadde vi flere hypoteser og gikk bredt ut da vi startet innsamling av informasjon. Flere av hypotesene er ikke bekreftet eller avkreftet, og vi samler fremdeles inn informasjon. Sakskomplekset fremstår som endeløst. Og det er nettopp en av de viktigste erfaringene, at hver sak førte til kontakt med nye kilder, som igjen satte oss på nye vinklinger.

Først var vi opptatt av endringer i arbeidslivet, på å finne ut om det finnes sosial dumping i IT-bransjen. Og hvor virksomhetenes behov for å kutte kostnader har ført til en trend med at høyt utdannede mister jobben til utenlandsk arbeidskraft. Helt uten debatt har politikerne skreddersydd regelverket for denne praksisen. Det er svært enkelt å hente inn asiatisk IT-arbeidskraft, både til korte og lengre opphold.

Etterhvert ble vi opptatt av sårbarhet og sikkerhet, da vi skjønte at det er en relevant problemstilling hos flere sikkerhetsmyndigheter.

Aldri tidligere har vi benyttet så mange anonyme kilder, det er utfordrende å konfrontere landets største og mektigste selskaper med beskyldninger som i stor grad baserer seg på skjulte kilder og påstander.

Vi oppdaget etter hvert at det er tilnærmet fri flyt av IT-nomader i landets viktigste bedrifter. Et forsøk på å skaffe oversikt over omfanget av sentrale IT-oppgaver som er flagget ut av landet og importen av arbeidskraft som er i Norge midlertidig førte til nye funn.

Vi klarte å finne frem til flere eksempler der feil gjort i India påvirker viktige norske olje og gassinstallasjoner og lot oss overraske over manglende oppfølging fra myndighetenes side. I oljesektoren er det sjeldent at IKT-sikkerheten sjekkes ut av myndighetene.

IT-nomadenes påvirkning på det norske samfunnet var et tema få har vist interesse for. Heller ikke internasjonalt er det fortalt noe særlig om konsekvenser for arbeidstakeres rettigheter og sikkerhetsmessige utfordringer av utflagging av IT-virksomhet. Sakene våre viste at globalisering også har konsekvenser for høyt utdannede nordmenns jobber og for sikkerheten ved anlegg og virksomheter som er avgjørende for landets økonomi.
Våre undersøkelser viste at fakta og informasjonen om utenlandske IT-arbeidere i Norge og konsekvensen av outsourcing er særs mangelfull, men etter møter med myndighetspersoner som jobber eller har jobbet med sikkerhet, skjønte vi at mange ansatte hos myndighetene stiller spørsmål, både ved sikkerheten og risikoen når arbeidere sitter i Asia og utfører viktige driftsoppgaver mot oljeanlegg og sentral infrastruktur.

Viktige funn

I Norge har myndighetene latt selskaper som Statoil, DNB og Telenor fått lov til å ta IT-beslutninger uten å involvere myndighetene. Så langt vi vet har bedriftene i liten tatt kontakt med relevante myndigheter for å få innspill på sikkerhet. Alle beslutninger har vært drevet av hva direktørene tror er best for bunnlinja. I samtaler med myndighetspersoner skjønte vi at lover og regler gjør at de fleste bedriftene har full frihet til å flytte IT-infrastruktur og oppgaver ut av landet. Vi fant også ut at de såkalte kompetansemiljøene i Statoil hadde lite de skulle sagt da Statoil-ledelsen tillot at IT-arbeidere som sitter i India, uten sikkerhetsklarering, har full tilgang til det aller helligste i norsk oljevirksomhet. Underveis ble vi nærmest litt skremt når vi fikk innsikt i hvor sårbare infrastrukturen vår er, og hvor enkelt det vil være for indiske arbeidere å skru av viktige samfunnsfunksjoner fra et lite kontor i Bangalore.

Andre funn vi gjorde

- Helt ulike regler og lønn for norske og indiske arbeidstakere
- Norske oppdragsgivere forventer at inderne er tilgjengelige døgnet rundt
  Fastpris gjør det umulig å utføre hele oppdraget med norske lønninger
- At tilsyn med IKT i oljevirksomheten er mangelfull. Statoil og andre oljeselskaper passer på egen IKT-sikkerhet
- Flere av de gamle plattformene er dårlig sikret, lappeteppe av gamle datasystemer

- Det er lite eller ingen bakgrunnssjekk på eksterne og utenlandske konsulenter som jobber for store norske virksomheter med sensitiv informasjon
- Det er ikke mulig for norske myndigheter å gi sikkerhetsklarering til indiske statsborgere. Likevel jobber de med sensitiv informasjon for store norske virksomheter i næringslivet og det offentlige.
- Norske sikkerhetsmyndigheter har ikke noe samarbeid med tilsvarende sikkhetsmyndigheter i India.
- At ikke alle indiske IT-arbeidere er erfarne. Det er stor utskifting av indiske arbeidere og med de konsekvenser det får for lojalitet. Virksomhetene drives med autoritær lederstil og fryktkultur er utbredt, ifølge ansatte.
- Sårbarhet knyttet til personvern, mange utenlandske arbeidstakere plassert i India har tilgang til store mengder informasjon om norske pasienter, kunder og klienter.
- Utflagging til land som India øker sårbarheten knyttet til viktig norsk infrastruktur, ifølge kilder hos myndighetene som jobber med sikkerhet
- Hendelser som truer IKT- sikkerheten blir aldri omtalt utenfor lukkede møterom.
- Globalisering har konsekvenser for norske høyt utdannede IT-konsulenter

Konsekvenser

* Samme dag som vi hadde reportasjene om "En tastefeil stoppet Statoil" ble selskapets ledelse hasteinnkalt til et møte med Petroleumstilsynet hvor tema var IKT-hendelsene som NRK hadde omtalt.

* Mange av Statoils egne IT-folk, jurister og informasjonsfolk jobbet dag og natt hele helgen etter NRKs første reportasje for å kartlegge omfanget av IT-ulykker og uheldige hendelser.

* Uken etter bestemte Petroleumstilsynet seg for å gjennomføre det første rene IKT-tilsynet av Statoil noensinne. Frem til nå har IKT vært en del av de ordinære sikringstilsynene, og Petroleumstilsynet har ikke tidligere gransket hvordan outsourcingen til et selskap på den andre siden av kloden har påvirket ikt-sikkerheten . Dette tilsynet pågår i skrivende stund. Da de innledet tilsynet sa Petroleumstilsynet at de skulle gå inn i de 29 hendelsene som NRK hadde omtalt. Ingen av disse hendelsene var klassifisert som kritiske av Statoils ledelse, og var derfor heller ikke rapportert inn til Petroleumstilsynet. På dette tidspunktet hadde antall IKT- hendelser som NRK hadde fått informasjon om økt til 35. Det er uvisst om Petroleumstilsynet har disse siste med i undersøkelsene, og det later til at vi sitter på mer informasjon enn myndighetene

* Statoil satte få dager etter ned et internt utvalg for å gjennomgå IT-sikkerheten i selskapet. I første omgang skulle bare ledelser og fagpersoner sitte i utvalget. Men etter at NRK fortalte at selskapet ikke inviterte de ansatte og tillitsvalgte med i utvalget, kom de likevel med.

* Etter halvannen måneders arbeid konkluderte rett før jul. Statoil må ta tilbake oppgaver som var outsourcet til HCL. De indiske IT-arbeiderne på den andre siden av jorden skal ikke lenger jobbe med å oppgradere og vedlikeholde brannmurene på plattformene og landanleggene. De har ikke lenger mastertilgang og passord til alle Statoils anlegg. Dette er et stort prestisjenederlag for den indiske IT-giganten HCL.

* Statoil må bruke ressurser til å lære opp ansatte til å foreta arbeidet med brannmurene. Siden dette arbeidet de siste fire-fem årene er satt ut av huset er mye av denne kompetansen gått tapt. Statoil betaler dobbelt opp for å gjøre denne jobben selv.

* Utvalget jobber med ulike tiltak for å bedre IT-sikkerheten og kommer med flere nye retningslinjer i løpet av første halvår 2017. Dette er tiltak som handler om teknologi, styrke brannmurer, organisatorisk i Statoil, nye regler og retningslinjer, og rene kontraktmessige forhold.

* Fra kilder i Statoil har vi fått opplysninger om at ledelsen jakter etter hvem som lekker informasjon til NRK og ansatte må skrive under på nye avtaler som pålegger dem taushet. NRKs reportasjer har ført til at frustrasjonene om outsourcingen er kommet tydeligere opp i dagen blant de ansatte.

* HCL og Statoil skal i løpet av våren 2017 reforhandle ny avtale. Vi vet at avdekkingen av mangler ved IKT-sikkerheten vil påvirke forhandlingene.

* Arbeidstilsynet iverksatte granskning av TCS. Arbeidstilsynet gjorde et forsøk på et tilsyn hos TCS kunde Norgesgruppen sommeren 2015, men la det bort. Etter NRKs reportasjer om lange arbeidsdager uten overtid i Vipps – prosjektet og om fryktkultur blant it-arbeidere om jobbet for Norgesgruppen gjennomførte Arbeidstilsynet en omfattende granskning. Selv kaller de det en revisjon som er mye mer omfattende enn et tilsyn. Det ble satt på jurister, tolker, flere inspektører i tillegg til en leder. Arbeidstilsynet intervjuet over 50 personer i TCS , men også ledelse og ansatte i DNB.

* Arbeidstilsynet fant flere lovbrudd. TCS betalte ikke eller svært lite overtid, ansatte jobbet for lange dager, de jobbet i perioder uten hviledager, det fantes ikke et skikkelig system for registrering av overtid, det fantes ikke verneombud, ingen ansatte var fagorganiserte.

* Arbeidstilsynet pålegger TCS å betale overtid og få et system for å registrere overtid. Selskapet har fått pålegg om å få en verneombudsordning knyttet til alle underleverandører og til det norske hovedkontoret. De pålegges også å ha egne koordinerende HMS-forum med klynger av kundene sine. TCS har bedt om å få utsatt fristen til å gjennomføre tiltakene til mars/april 2017.

* Arbeidstilsynet påla TCS å etterbetale overtid til ansatte.

* Arbeidstilsynet fremhever at heretter må alle som kjøper tjenester av TCS innordne seg påleggene, og bidra til at ansatte får overtidsbetalt, får tilstrekkelig med fritid og at det er ordninger for verneombud og for fagorganisering.

* Tata har innrømmet at de ansatte i Norge ikke har god nok HMS-kompetanse og innsikt i norske lover og regler. Tata har etter mediedekning uttalt at de vil kurse gi ledere og personalmedarbeidere i regler for norsk arbeidsliv og gi dem et kompetanseløft mht til HMS.

* Norgesgruppen har gjennomført egen revisjon og hyret inn advokater og revisorer for å gå gjennom arbeidsforholdene til TCS-ansatte som jobber for Norgesgruppen.

* DNB har vært i India på inspeksjon av kontrakten og arbeidsforholdene til de indiske it-arbeiderne. DNB har hatt møter og oppfølging av avtalen med TCS.

* Mediedekningen har fått kommersielle konsekvenser for TCS. Vi vet at blant annet Nortura etter våre saker ba TCS om en bekreftelse om at norsk arbeidsmiljølov ble fulgt og at deres ansatte ville beholde jobben i TCS i Trondheim. En slik garanti kunne ikke TCS gi, og oppdraget gikk til et annet selskap. Etter det NRK erfarer har flere indiske IT-selskaper blitt valgt bort i frykt for dårlig PR.

8.0 Avslutning:

I det det stille har norske kompetansebedrifter kvittet seg med kritisk IT-infrastruktur og IT-ansatte. På få år har utenlandske outsourcingsselskaper vunnet fotfeste i Norge og fått stadig flere kontrakter. I året da globaliseringsskeptikerne for alvor ble synlige, klarte disse sakene å vise konsekvensene av utflagging av IT til India. Gjennom våre saker ble ledelsen i viktige norske selskaper ansvarliggjort for beslutninger tatt til IT. Vi lyktes med å sannsynliggjøre at sosial dumping skjer i store norske kunnskapsbedrifter. Og for første gang ble sikkerhetsrisikoen ved utflaggingen grundig problematisert. I store norske selskaper har staten som eier aldri stilt spørsmål ved utflaggingen. Det er aldri stilt spørsmål ved konsekvens for sikkerheten når det meste av IKT infrastruktur driftes fra India, et land norske sikkerhetsmyndigheter ikke har noe kontakt med. Og hva skjer med IT-infrastrukturen skulle det bli urolige tider i verden, i all den tid det skal driftes fra andre siden av kloden. At over hundre indiske IT-arbeidere har hatt full tilgang til å stenge ned eller sabotere norske oljeanlegg fra India, var en godt bevart hemmelighet i Statoil. Det mye som tyder på at føljetongen om utflagging av IT fortsetter. Mens vi skriver denne rapporten har det dukket opp flere tips.

Temaside nrk.no for utflagging av IT:

https://www.nrk.no/emne/utflagging-av-it-arbeidsplasser-1.12941470

Første sak: 28.04.2016

Slik overtar utenlandske IT-selskap norske jobber

https://radio.nrk.no/serie/dagsnytt/NPUB12008416/28-04-2016#t=45s

https://www.nrk.no/norge/slik-overtar-utenlandske-it-selskap-norske-jobber-1.12918438

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50008116/28-04-2016#t=28m2s

29.04.2016

Frykter at ondsinnede utnytter IT-nomader

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50008216/29-04-2016

https://www.nrk.no/norge/fri-flyt-av-informasjon-kan-utnyttes-av-ondsinnede-1.12920235

09.05

Tapte mye på IT-utvikling i India

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50008716/09-05-2016

https://www.nrk.no/norge/tapte-mye-pa-it-utvikling-i-india-1.12930103

13.05.2016

- Direktørene hører for mye på JA-mennesker

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50009116/13-05-2016

https://www.nrk.no/norge/outsourcing_-sjefene-omgir-seg-med-ja-mennesker-1.12937632

18.05

- Utflagging av IT har gått for langt

https://www.nrk.no/norge/ap-vil-flagge-hjem-it-arbeidsplasser-1.12946940

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50009216/18-05-2016

15.06.2016

Arbeidstilsynet gransker Vipps-prosjektet i DNB:

https://www.nrk.no/norge/xl/arbeidstilsynet-gransker-vipps-prosjektet-1.12983488

https://radio.nrk.no/serie/dagsnytt/NPUB10011816/15-06-2016#t=46s

Skjønner ikke at bedriftene tør:

https://www.nrk.no/norge/_-skjonner-ikke-at-bedriftene-tor-1.12921501

16.06.2016

Ingen oversikt over omfanget av utenlandske IT-arbeidere

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50011316/16-06-2016#t=33m36s

https://www.nrk.no/norge/ingen-oversikt-over-utenlandske-it-arbeidere-1.12999275

17.06.2016

Tillitsvalgte i DNB om inderne – glade for gransking:

https://radio.nrk.no/serie/dagsnytt/NPUB10012016/17-06-2016#t=48s

https://radio.nrk.no/serie/dagsnytt/NPUB11012116/17-06-2016#t=1m42s

https://www.nrk.no/norge/dnb-ansatte-er-glade-for-vipps-gransking-1.13000803

28.06.2016

En varsler forteller: - IT-ansatte i Norge blir hundset og lever i frykt

https://www.nrk.no/norge/xl/hevder-indiske-it-arbeidere-jobber-i-en-fryktkultur-hos-dagligvaregiganten-1.13010035

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50012116/28-06-2016#t=1m23s

https://radio.nrk.no/serie/dagsnytt/NPUB12012716/28-06-2016#t=43s

29.06.2016

Arbeidstilsynet lover indiske IT-arbeidere anonymitet

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50012216/29-06-2016#t=9m31s

https://www.nrk.no/norge/arbeidstilsynet-garanterer-vipps-arbeidere-full-anonymitet-1.13018782

14.07.2016

IT-selskap avviser fryktkultur

https://www.nrk.no/norge/indisk-it-selskap-avviser-fryktkultur-og-sosial-dumping-1.13036916

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50013316/14-07-2016

19.08.2016

Fant lovbrudd i Vipps-arbeidet

https://www.nrk.no/norge/arbeidstilsynet-fant-lovbrudd-hos-vipps-arbeiderne-i-dnb-1.13092693

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50015916/19-08-2016

Hadde aldri skjedd dersom DNB brukte egne ansatte:

https://www.nrk.no/norge/_-hadde-aldri-skjedd-dersom-dnb-brukte-egne-ansatte-1.13097316

02.09.2016

Flagger ut sykehusenes datasystem til amerikanerne

https://www.nrk.no/norge/flagger-ut-sykehusenes-datasystem-til-amerikanere-1.13114047

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50016916/02-09-2016

Skandale om helseminister tillater utflagging

https://www.nrk.no/norge/ber-helseminister-stoppe-it-utflagging-1.13117346

12.09.2016

Bøndenes selskapet Nortura velger indisk

https://www.nrk.no/norge/frykter-tap-av-omdomme-til-landbruket-nar-nortura-flagger-ut-1.13102676

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50017516/12-09-2016

16.09.2016

Norgesgruppen frikjenner indisk selskap

https://www.nrk.no/norge/norgesgruppen-frikjenner-indisk-it-selskap-1.13137322

28.10.2016

Tastefeilen som stoppet Statoil

https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50020916/28-10-2016

Statoil kalt inn på teppet

https://www.nrk.no/norge/statoil-kalt-inn-pa-teppet-av-petroleumstilsynet-1.13199612

https://tv.nrk.no/serie/dagsnytt-atten-tv/nnfa56102816/28-10-2016

Datasikkerhet på norske oljeplattformer

https://tv.nrk.no/serie/dagsrevyen/nnfa19102816/28-10-2016#t=1m35s

-Sjokkerende at de ikke griper fatt i dette

https://www.nrk.no/norge/_-det-er-sjokkerende-at-de-ikke-griper-fatt-i-dette-1.13200557

31.10.2016

Statoil gransker egen sikkerhet:

https://www.nrk.no/norge/statoil-gransker-egen-sikkerhet-1.13203883

02.11.2016

Myndighetene sjekker aldri IT-sikkerhet i Statoil

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50021216/02-11-2016#t=1h2m25s

https://www.nrk.no/norge/it-sikkerheten-til-statoil-er-aldri-gransket-1.13205885

04.11.2015

Ansatte på oljeplattformer frykter hackerangrep

https://www.nrk.no/norge/oljeplattformer-med-bare-en-brannmur_-ansatte-frykter-hackerangrep-1.13208019

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50021416/04-11-2016

Russisk sikkerhetsekspert: - Datasystemer på gamle oljeplattformer bør skiftes

https://www.nrk.no/norge/russisk-sikkerhetsekspert_-_-vi-advarer-mot-gamle-datasystemer-pa-oljeplattformer-1.13209712

Statoil-ansatte føler vond usikkerhet

https://www.nrk.no/norge/statoil-ansatte-foler-vond-usikkerhet-1.13211209

13.11.2016

Kriminelle på nett jakter Statoil-informasjon

https://www.nrk.no/norge/kriminelle-pa-dark-web-jakter-statoil-informasjon-1.13198354

https://tv.nrk.no/serie/dagsrevyen/NNFA19111116/11-11-2016

21.12.2016

Indiske IT-arbeidere mister datatilganger på Statoils anlegg

https://www.nrk.no/norge/indiske-it-arbeidere-mister-tilganger-pa-statoils-oljeplattformer-1.13282643

https://radio.nrk.no/serie/dagsnytt/NPUB96036216/21-12-2016#t=35s

22.12.2016

Statoilansatte jubler over at IT-jobber flagges tilbake fra India

https://www.nrk.no/norge/statoil-ansatte-jubler-over-it-julegave-1.13287187

https://radio.nrk.no/serie/nyhetsmorgen/NPUB50024816/22-12-2016

23.12.2016

IT-selskap ba om unntak fra loven

https://radio.nrk.no/serie/dagsnytt/NPUB12025516/23-12-2016#t=2m46s

https://www.nrk.no/norge/it-selskap-onsket-unntak-fra-norsk-arbeidsmiljolov-1.13261942

Varslerbrev til ledelsen i Norgesgruppen Data
https://fido.nrk.no/26bea6f855e4056fef3b398f42b390c43c99f6e4f291bbe5551a5f06b2fc5572/tilespen.pdf

Lenker til dokumenter lest for bakgrunn:

Samhandling for sikkerhet, Traavik-utvalget:
https://www.regjeringen.no/no/aktuelt/sikkerhetsutvalget-overrekkelse-av-nou-2016-19-samhandling-for-sikkerhet/id2515491/

Digital sårbarhet - sikkert samfunn, Lysne I
https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

Digitalt grenseforsvar, Lysne II
https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf

Uavhengighet av sikkerhetssystemer
http://www.psa.no/getfile.php/PDF/Uavhengighet-sikkerhetssystemer%20endelig_rapport.pdf

Varslerbrev til ledelsen i Norgesgruppen Data
https://fido.nrk.no/26bea6f855e4056fef3b398f42b390c43c99f6e4f291bbe5551a5f06b2fc5572/tilespen.pdf

Helhetlig IKT-risikobilde 2015
https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf

Helhetlig IKT-risikobilde 2016
https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2016_web_enkel.pdf

Risiko- og sårbarhetsanalyse fra Finanstilsynet
http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2015/ROS_analyse_2014.pdf
http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2016/Risiko_og_s%c3%a5rbarhetsanalysen_2015.pdf

IKT-systemenes betydning for strukturendringer
http://www.thema.no/wp-content/uploads/2016/03/THEMA_R-2015-36_IKTsystemenes_betydning_for_strukturendringer-1.pdf

Rapport, Outsourcing to India
http://www.sintef.no/en/latest-news/bad-business-outsourcing-to-india/

http://www.sintef.no/publikasjoner/publikasjon/?pubid=CRIStin+1194994

Lenker til dokumenter lest for bakgrunn:

Samhandling for sikkerhet, Traavik-utvalget:
https://www.regjeringen.no/no/aktuelt/sikkerhetsutvalget-overrekkelse-av-nou-2016-19-samhandling-for-sikkerhet/id2515491/

Digital sårbarhet - sikkert samfunn, Lysne I
https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

Digitalt grenseforsvar, Lysne II
https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf

Uavhengighet av sikkerhetssystemer
http://www.psa.no/getfile.php/PDF/Uavhengighet-sikkerhetssystemer%20endelig_rapport.pdf

Helhetlig IKT-risikobilde 2015
https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf

Helhetlig IKT-risikobilde 2016
https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2016_web_enkel.pdf

Risiko- og sårbarhetsanalyse fra Finanstilsynet
http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2015/ROS_analyse_2014.pdf
http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2016/Risiko_og_s%c3%a5rbarhetsanalysen_2015.pdf

IKT-systemenes betydning for strukturendringer
http://www.thema.no/wp-content/uploads/2016/03/THEMA_R-2015-36_IKTsystemenes_betydning_for_strukturendringer-1.pdf

Rapport, Outsourcing to India
http://www.sintef.no/en/latest-news/bad-business-outsourcing-to-india/
http://www.sintef.no/publikasjoner/publikasjon/?pubid=CRIStin+1194994

Nations Ranked on Their Vulnerability to Cyberattacks
https://obj.umiacs.umd.edu/news_release_pdfs/FDD-writeup.pdf

https://obj.umiacs.umd.edu/news_release_pdfs/GCVR-Feb-2016.pdf