

Foredrag i Oslo Militære Samfund mandag 7. desember 2009

Ved

Kommandør Geir Gade Sjef Forsvarets sikkerhetstjeneste (FOST)



Foto: Stig Morten Karlsen, OMS

Innledning

Jeg er glad for at OMS velger å sette den militære sikkerhetstjenesten på programmet i årets siste foredrag. Temaet er utvilsomt aktuelt. Vi som jobber med dette faget er glade for å forklare nærmere hva sikkerhetstjeneste er og hvorfor dette er viktig i militær virksomhet. Jeg vil i også forklare hva nettverksovervåkning er, og dessuten kort si litt om den situasjonen vår tjeneste nå står midt oppe i.

Jeg vil innledningsvis presisere at jeg gir uttrykk for mine egne faglige synspunkter. (Helt uavhengig av hva forsvarsledelsen eller andre måtte mene om de samme forhold.)

Det er 7. desember i dag og årsdagen for det japanske angrepet på den amerikanske stillehavsflåtens base på Pearl Harbour. Angrepet kom totalt *overraskende* på amerikanerne. Manglende beredskap på Hawaii bidro til at amerikanerne som en konsekvens var nær ved å tape sin evne til å hevde amerikanske interesser i Stillehavsområdet. Tyskerne hadde på samme måte tatt herredømme i store deler av Europa. Angrepet på Norge viser hvordan en trusselaktør med bruk av relativt beskjedne ressurser gjennom gode etterretninger om motparten og god sikkerhet rundt sine egne operasjonsplaner i løpet av svært kort tid kan sette en annen nasjon helt ut av spill. USA og Norge og en rekke andre land betalte en høy pris for manglende militære forberedelser.

Mange vil vite og noen få fremdeles huske at det i Norge etter krigen var stor enighet om at man aldri skulle tillate seg å komme i en situasjon hvor landet kunne bli utsatt for en tilsvarende hendelse igjen. Vi ser allikevel gang på gang at "lessons identified" ikke nødvendigvis blir "lessons learned".

Sikkerhetstjeneste i Forsvaret

Det hevdes ofte at det var mye lettere å drive forsvar under den kalde krigen fordi trusselen over en svært lang periode var både åpenbar og nokså forutsigbar. Arbeidet med forebyggende sikkerhet var intet unntak.

I Vesten eksisterte det en betydelig frykt for Warsawapaktens militærmakt og vilje til å benytte denne. Etterretningstrusselen fra Sovjetunionen og alliansepartnerne i "Østblokken" var godt dokumentert blant annet gjennom en rekke større spionasjesaker både i Norge og hos våre allierte. Denne settingen bidro i betydelig grad til å motivere for en god sikkerhet. Forsvaret hadde derfor et høyt fokus på sikkerhet, og forebyggende sikkerhet ble vektlagt og var en gjennomgående og grunnleggende del av tjenesten. Man hadde også inntrykk av at folk flest utenfor forsvaret hadde stor forståelse for at forsvaret drev slik virksomhet.

Det høye sikkerhetsfokus forsvant imidlertid så å si ut med badevannet i forbindelse med Warsawapaktens avvikling og avslutningen av den kalde krigen. Russland opplevde et politisk og militært sammenbrudd og ble derfor ikke lenger oppfattet som en like potent trussel. I sammenheng med oppløsningen av Warsawapakten vokste det fram en sterk tro i Vesten om at den nye verdensordenen ville fremme samarbeid og åpenhet mellom stater, heller enn mellomstatlig rivalisering og militær opprustning.

Det er med sikkerhetstjeneste som med gudstro og forsikring, man verdsetter ikke betydningen av å ha forholdene i orden før ulykken rammer.

Avslutningen av den kalde krigen førte til store endringer i Forsvaret. Fokuset på, og kunnskapen om militær sikkerhetstjeneste ble utsatt for en betydelig forvitring. Da det tidligere FO/S ble nedlagt 1. januar 2003 ble Forsvarets sikkerhetsavdeling (FSA) etablert som et lite stabselement på 13 stillinger i Forsvarets Overkommando. FSA skulle ivareta Forsvarssjefens behov og ansvar for en tilstrekkelig militær sikkerhetstjeneste.

Det tok ikke lang tid før man ble klar over at det sto dårlig til med sikkerhetsforvaltningen i Forsvaret. Eksempelvis fantes det bare 15 heltidsstillinger med ansvar for sikkerhetstjeneste. Allerede fra tidlig i 2003 erfarte vi en rekke alvorlige sikkerhetstruende hendelser. Dette bidro til stor medieoppmerksomhet med et etterfølgende fokus på sikkerhetstjeneste. Dere husker sikkert medieoverskrifter relatert til manglende kontroll på et betydelig volum graderte dokumenter i forbindelse med flyttingen fra "Huseby". Vi hadde tilsvarende saker i Brussel, i Stavanger og i Bodø. I forbindelse med en alvorlig kriminalsak fant politiet flere hundre graderte dokumenter hjemme hos en offiser. Mangelfull vakt og sikring av Forsvarets baser førte til "Jørstadmoen-saken", "Flekkerøya-saken" og "HV03-saken" hvor militære våpen kom på avveie.

I tillegg til dette var det jevnlig oppslag i mediene med utgangspunkt i lekket gradert informasjon som følge av at ansatte var uenige i omstillingstiltak.

FNs og NATOs operasjoner på Balkan hadde også vist hvordan de stridende partene i disse konfliktene klarte å skaffe seg viktige etterretninger om de fredsbevarende styrkenes engasjementsregler og hvilken informasjon de hadde om de stridende partene. Dette bidro sannsynligvis til å forlenge krigshandlingene. Dårlig operasjonssikkerhet bidro, også til at fremtredende krigsforbrytere fra disse konfliktene fremdeles er på frifot, med det dette innebærer for normalisering og forsoning mellom de tidligere stridende partene.

Manglende fokus på sikkerhet og svak sikkerhetsorganisasjon i Forsvaret førte til at general Frisvold i løpet av 2003 bestemte seg for at den militære sikkerhetstjenesten skulle styrkes. Forsvarets sikkerhetsavdeling ble derfor omgjort til en selvstendig driftsenhet utenfor Forsvarsstaben i den nye ledelsesstrukturen. En rekke sikkerhetsfunksjoner ble i tiden deretter sentralisert og lagt inn under FSA. FSJ utarbeidet en egen **detaljert** instruks for sjef FSA. Det viste seg raskt at Sikkerhetsloven av 20. mars 1998 ikke var tilstrekkelig for å ivareta de militære sikkerhetsbehovene. FSJ etablerte derfor et eget Direktiv for den militære sikkerhetstjenesten. I dette direktivet slås det fast at sikkerhetstjeneste er en del av den operative virksomheten. Det var en uttalt ambisjon fra ledelsen i Forsvaret at direktivet skulle bidra til økt fokus på sikkerhetstjeneste og etablere klare ansvarlinjer innenfor sikkerhetsforvaltningen. Direktivet slår fast at et tilstrekkelig sikkerhetsnivå er en forutsetning for gjennomføring av all virksomhet i Forsvaret. "En målrettet sikkerhetstjeneste som understøtter operasjoner, skal støtte Forsvarets operative behov i fred, krise, væpnet konflikt og krig – både nasjonalt og internasjonalt".

Det utøvende ansvaret for den forebyggende sikkerhetstjenesten delegeres fra FSJ til sjef FSA. Sjef FSA får også rollen som sikkerhetsleder i Forsvaret. Det slås fast at sikkerhetstjenesten skal være dimensjonert for å løse FSJs sikkerhetsbehov.

Utfordringer

Med utgangspunkt i det som i 2005 fremsto som en klar instruks og en klar ordre og som bidro til at sikkerhetstjenesten fikk en tydelig og uttalt ledelsesforankring, burde alt ligget vel til rette for en effektiv opprydning. Det viste seg imidlertid raskt at det for det første var en betydelig motstand hos Nasjonal Sikkerhetsmyndighet (NSM) mot etableringen av en styrket sentral militær sikkerhetstjeneste.

NSM var grunnleggende uenige i at FSJ var virksomhetsleder i Forsvaret. Ansvarlinjene i sikkerhetsloven klargjør at det er virksomhetens leder som er ansvarlig overfor tilsynsmyndigheten (NSM) for at pålegg i sikkerhetsloven er oppfylt. NSM mente at sjefer på et mye lavere nivå i Forsvaret skulle regnes som virksomhetsledere i lovens forstand, og de fikk delvis støtte av Forsvarsdepartementet i dette. Dette bidro til at det var svært utfordrende å ivareta rollen som sikkerhetsleder i Forsvaret på en effektiv måte. For det andre etablerte enkelte avdelinger med utgangspunkt i NSMs definisjon av virksomhetslederbegrepet svært tette bånd til tilsynsmyndigheten.

Eksempler på denne type forhold finner vi særlig innenfor fagområdet informasjonssikkerhet. Både FLO/IKT og sambandsavdelingen ved fellesoperativt hovedkvarter hadde hatt et vel etablert samarbeid med spesialister i det gamle FO/S. Det ble derfor slik at man i begge disse fagmiljøene videreførte dette som et samarbeid med de samme spesialistene som nå jobbet i NSM. Utfordringen for FSA var at det ikke ble gitt innsyn i hva som foregikk innenfor det samarbeidet som var mellom disse avdelingene og NSM. Dette har vært situasjonen helt frem til i dag til tross for at FSJs sikkerhetsdirektiv slo fast at FSA skulle koordinere dette arbeidet mot NSM. Dette har selvsagt bidratt til at det har vært tyngre å drive FSA og bidratt til å undergrave tjenestens rolle og myndighet.

I løpet av 2006 gjennomførte FSA en kontroll med et stort antall avdelinger i Forsvaret for å få et bilde av sikkerhetstilstanden. Resultatet var nokså nedslående; bare ca 10% av de kontrollerte avdelingene tilfredsstilte lovens minimumskrav til tross for FSJs uttalte behov for sikkerhet ut over de lovpålagte kravene.

Mange avdelinger hadde en svak sikkerhetsorganisasjon og det var gjennomgående mangel på kompetanse. Konsekvensen av dette var at mange sjefer ikke hadde tilstrekkelig oversikt over sin egen situasjon på det sikkerhetsfaglige område. Det ble derfor gitt en rekke sentrale pålegg om å få orden på sikkerhetstjenesten ute ved avdelinger og gi faget en mer sentral plass ved Forsvarets skoler.

Risikobildet i Forsvaret

Sikkerhetsrisiko er en funksjon av verdi, trussel og sårbarhet. Det nye norske innsatsforsvaret kan på mange måter beskrives som en nodestruktur som er teknologiavhengig og lite redundant. Det bidrar til at enkeltelementer blir mye viktigere enn tidligere. Konsekvensen av at et enkeltelement ødelegges eller får redusert funksjonalitet kan derfor bli svært alvorlige. Vi har med andre ord fått flere egg i færre kurver. Det etableres gjensidige avhengigheter mellom enkeltelementer som er helt avgjørende for å oppnå full militær effekt. Disse enkeltelementene må derfor verdivurderes i lys av disse gjensidige avhengighetene og deretter sikres tilstrekkelig.

En god forståelse av sikkerhetstruslene er avgjørende for å skape aksept for en effektiv og kompetent sikkerhetstjeneste. Et lands evne og vilje til å forsvare eller ivareta sine nasjonale interesser har opp gjennom historien vært gjenstand for oppmerksomhet fra andre lands etterretningstjenester. Som nevnt tidligere tok man det nærmest for gitt at denne situasjonen endret seg etter avslutningen av den kalde krigen. Det fremgår imidlertid fra ugraderte kilder at etterretningstrusselen mot Norge og NATO minst er på nivå med det den var da den kalde krigen var på sitt kaldeste.

Det er i denne sammenhengen viktig å ha i mente at etterretning og sikkerhet er to sider av samme sak. Den enes dårlige sikkerhet bidrar til den andres gode etterretninger. Potensielle trusselaktører vil alltid forsøke å finne våre sikkerhetsmessige svakheter og benytte dette til å tilegne seg informasjon som kan få negative konsekvenser for vårt Forsvars operative evne og for rikets sikkerhet.

Det er imidlertid ikke bare trusler fra fremmed etterretning som truer Forsvaret og Forsvarets operasjoner, men også terroranslag. Trusselbildet er blitt mer hybrid. Vi

ser ganske ofte at trusselaktører fra fremmede etterretningstjenester, terrororganisasjoner og kriminelle organisasjoner innenfor et gitt geografisk område samarbeider for å oppnå størst mulig effekt. Vi har sett nokså klare tilfeller av dette hos trusselaktører på Balkan og i Afghanistan. Dette er særlig tilfelle innenfor det nye området for militære operasjoner som mange allerede kjenner som cyberspace.

FD uttalte allerede i St.prp. 45 (2000-2001) at informasjonsrevolusjonen er i ferd med å forandre rammebetingelsene for krig og konflikt. Angrep på sivile og militære informasjonssystemer må antas å ville utgjøre et sentralt element i framtidens konflikter.

Ett slikt eksempel var det som skjedde i april 2007; svært nær Norges grenser. En ganske liten krig helt uten blod og bomber. Likevel var den lille, ublodige krigen skremmende interessant. Den var nemlig historiens første nettkrig. Konflikten begynte med at man i Estland fjernet en bronsestatue av en sovjetisk soldat fra Tallinn i det som i ettertid kan sies å ha vært et lite gjennomtenkt oppgjør med fortiden. Statuen var reist til minne om soldater fra den Røde Armé som falt i kampen mot nazismen. Estlands betydelige russiske minoritet likte dårlig at minnesmerket ble fjernet. Det samme gjorde Russlands myndigheter, som reagerte med kraftige protester og krav om boikott av det vesle nabolandet. Ganske snart begynte angrepene.

Anslagene mot landets elektroniske infrastruktur var kraftige, og de varte i uker. Myndighetenes nettsider ble angrepet, og banker og aviser ble satt ut av drift i en lengre periode. Flere av angrepene kunne spores til servere eid av den russiske stat, men mange av angrepene kom fra andre deler av verden. Noe ble sikkert gjennomført av russiske privatpersoner. Så hvem var egentlig angriperne i denne krigen? Hvem kunne man forsvare seg mot? Og hvordan? Det finnes en rekke andre tilsvarende eksempler som er like kjente, men som det ikke er plass til å omtale. Dette er utfordringer som vi møter daglig innenfor utøvelse av det som vi betegner som Computer network Defence (CND).

I forbindelse med at det nylig var skifte av sjef for Politiets sikkerhetstjeneste uttalte den påtroppende sjefen at Forsvarets operasjoner ute bidrar til økt risiko hjemme. Selv om etterretningstruslene vanligvis oppfattes å komme hovedsakelig fra det som på fagspråket kalles for HUMINT og SIGINT, er det også slik at det som skrives i åpne medier finner veien til trusselaktører i fjerne områder der norske militære styrker er deployert. Vi så nylig at pressen tok konsekvensen av dette i forbindelse med en kidnappingssak i Afghanistan. I forbindelse med introduksjonen av nye IVECO-stridskjøretøyer for styrkene i Afghanistan ble disse kjøretøyenes svake sider i detalj omtalt i pressen. Det samme var tilfelle med vår nye fregatt som nå er satt inn i operasjoner mot piratvirksomheten utenfor Somalia. Dette bidrar til å undergrave militær effekt og utsette personellet for en høyere risiko.

Noe av det mest alvorlige kan være en illojal medarbeider som kommer i forbindelse med en trusselaktør. Det er mange forhold i vår moderne livsførsel som kan føre til at vi kan bli satt under press til å være illojale mot våre egne. Det er også en trend i samfunnet at brudd på taushetsklæring og sikkerhetsbestemmelser ikke ses på med samme alvorlighet som tidligere. Dette bidrar til å senke terskelen for å være illojal mot arbeidsgiver. Det er dessverre også slik at dersom det ikke er etablert

tilstrekkelige kontrollmekanismer så vil det nærmest være rasjonelt for noen å begå sikkerhetsbrudd.

I tillegg til militære problemstillinger som omfatter både Norge og NATO så må vi forvente at det foregår en nokså omfattende industrispionasje rettet mot teknologi og industriell metode og mot Norge i rollen som strategisk råvareleverandør. For å si det litt lettvint så har det aldri vært enklere å stjele informasjon enn det er nå. Samfunnet har gjort seg helt avhengig av informasjonsteknologi. Denne teknologien er svært vanskelig å sikre mot eksterne trusselaktører, men det er praktisk talt umulig å beskytte seg, dersom illojale medarbeidere samarbeider med disse trusselaktørene. En slik trussel blir derfor svært farlig for både sivile og militære strukturer som må beskytte sin konkurranseevne. Sikkerhetstiltak skal nemlig bidra til å beskytte det komparative fortrinnet.

I Forsvaret har vi lagt til grunn at vi med en relativ liten struktur kan få en relativ høy militær effekt ved å benytte høyteknologi og etablere et informasjonsovertak. Dersom trusselaktører kjenner til vår teknologi uten at vi selv er klar over det, så kan dette ha konsekvenser for vår operative evne. Det samme gjelder et antatt informasjonsfortrinn. En underdimensjonert eller dårlig ivaretatt militær sikkerhetstjeneste kan derfor føre til tap av operativ effekt og utsette soldater for høyere risiko.

Behovet for en effektiv sikkerhetstjeneste i Forsvaret

Forsvarets rolle mot ytre trusler som truer landets sikkerhet og selvstendighet er fundamental. Tapt operativ evne (forsvarsevnen) vil i prinsippet innebære svekket statssikkerhet. I dette perspektivet kan derfor ikke Forsvaret uten videre sammenlignes med andre statsetater, spesielt ikke hva angår sikkerhetsbehov.

Forsvarets operative evne vil alltid være avhengig av en rekke kritiske funksjoner. Det er viktig å identifisere de kritiske funksjonene fordi beskyttelsen av dem er den militære sikkerhetstjenestens hovedfokus. De kritiske funksjonene er igjen avhengige av en rekke verdier, forutsetninger og krav, eksempelvis spesialpersonell, informasjon, materiell, infrastruktur og spesielle objekter. Utfordringen er å avdekke sikkerhetsmessige svakheter eller sårbarheter og se disse i sammenheng med det aktuelle trusselbildet. På denne måten kan Forsvaret tilpasse og iverksette forebyggende sikkerhetstiltak. Fremtidig operativ evne er avhengig av at egne sårbarheter blir identifisert og tatt hensyn til, før en motstander evner å utnytte dem til sin fordel.

Den fortsatte omstillingen av Forsvaret har ytterligere forsterket behovet for en effektiv sikkerhetstjeneste gjennom økt sentralisering og ved at redundante organisasjonsledd fjernes (dvs enda flere egg i enda færre kurver enn tidligere).

Det er uansett ikke mulig å fjerne all risiko gjennom tekniske sikkerhetstiltak. Forsvaret har en relativ høy ambisjon om å etablere et Nettverksbasert Forsvar allerede i 2012. Dette innebærer at man må innrette sikkerhetstiltakene på en annen måte enn tidligere. Forebyggende sikkerhetstiltak må i fremtiden innrettes mot å etablere forsvarbare fysiske, logiske og organisatoriske strukturer. Med forsvarbare mener jeg proaktive tiltak som begrenser en motstanders offensive handlingsrom og

samtidig forsterker vår evne til å avsløre og bekjempe fiendtlige operasjoner før det er for sent. Slike forsvarbare strukturer forutsetter en helhetlig, kompetent og gjennomgripende sikkerhetsprosess hvor risikobildet blir kartlagt og håndtert. Dette kan bidra til å gi FSJ et større handlingsrom og en bedre beskyttelse av den operative evnen. Sikkerhetstjenesten i Forsvaret må derfor operasjonaliseres i takt med fremtidens krav til militære operasjoner. Det er vår erfaring i FOST at en sentralisering av viktige sikkerhetsfunksjoner bidrar til å synliggjøre risikobildet og sikkerhetsutfordringene i et mer helhetlig perspektiv.

Mye av det jeg har berørt så langt i dette foredraget kunne hver for seg vært tema for et eget foredrag. Jeg har beskrevet det på denne måten fordi jeg mener at det bidrar til å belyse et nokså omfattende behov for sikkerhetstjeneste i Forsvaret. Behovet er dessverre og merkelig nok – vil vi si - ikke blitt omtalt i andre dokumenter enn i FSJs Direktiv for den militære sikkerhetstjenesten. Vi jobbet iherdig for å få beskrevet behovet for sikkerhetstjeneste i Forsvarsstudien 2007. Dessverre nådde vi heller ikke her frem med våre innspill med unntak av forslaget om skifte av navn fra sikkerhetsavdeling til sikkerhetstjeneste. Dette bidrar til at man nå snakker om å redusere antall ansatte i FOST uten at det foreligger gode militærfaglige begrunnelser.

FSA og senere FOST er heller ikke i særlig grad viet oppmerksomhet i meldinger eller proposisjoner fra Forsvarsdepartementet. Dette kan ha gitt næring til at pressefolk og andre utenfor Forsvaret oppfatter og omtaler virksomheten som "en fjerde hemmelig tjeneste som har vokst frem i det stille". I forbindelse med medietrykket som vi har hatt etter en rapport avgitt av EOS-utvalget samt anmeldelse av FOST fra FD med påfølgende etterforskningen fra KRIPOS, har forsvarsledelsen etter mitt syn ikke redegjort tydelig nok for selve behovet for en militær sikkerhetstjeneste.

Med dette beveger jeg meg over på temaet nettverksovervåkning. Vår håndtering av dette oppdraget førte til at FOST nok en gang kom i medias søkelys den 10. juni i år.

FOST-saken

Tidlig om morgenen denne dagen mottar jeg en oppringning fra FSJs forværelse om straks å møte på FSJs kontor. Jeg har på det tidspunkt ikke den ringeste anelse om hva som er under oppseiling. En knapp halvtime etterpå mottar jeg en kort orientering fra FSJ om at FOSTs virksomhet på Jørstadmoen er mistenkt for å ha gjennomført ulovlig overvåkning av e-posttrafikken til statsministerens kontor og til slottet. Jeg får vite at KRIPOS er på vei for å gjennomføre en ransaking ved avdelingen. Det første tilfellet av ulovlig overvåkning skulle ha skjedd allerede i løpet av sommeren 2008 og det seneste tidlig på våren 2009.

Som sjef FOST var jeg på dette tidspunktet ikke kjent med at brukere utenfor Forsvaret benyttet seg av Forsvarets internettportal. Dette var avtaler som var inngått mellom FLO/IKT og disse brukerne uten at vi var orientert om dette.

Selv om FOSTs aktivitet ved det som betegnedes heter Forsvarets senter for beskyttelse av kritisk infrastruktur på Jørstadmoen er teknisk komplisert, har jeg som sjef allikevel hatt en god forståelse av aktiviteten og hvordan prosesser og oppgaver er organisert. Jeg ga derfor i en umiddelbar kommentar til FSJ uttrykk for at vi i den

sikkerhetsmessige overvåkningen av Forsvarets internettlinjer ikke leser innhold, men kun observerer såkalte metadata. Det vil si at FOST ikke "overvåker" brukerne av Forsvarets informasjonssystemer. Jeg kommer tilbake til hva dette innebærer.

Det veldig positive fra mitt perspektiv er at FSJ og sjef FST med det samme ga uttrykk for at de hadde full tillit til FOSTs ansatte inntil det motsatte var bevist. Dette ble også tydelig kommunisert utad.

Jeg skal ikke kommentere innholdet i selve etterforsknings-saken, men for å gi forsamlingen et innblikk i bakgrunnen til denne såkalte FOST-saken, vil jeg nevne noen vesentlige faktorer som kan bidra til å forklare hva nettverksovervåking er og hvorfor vi legger vekt på å gjøre dette.

Trusselnivået på internett er som nevnt ansett å være både høyt og komplekst. Risikoen for at Forsvarets internetteksponeerte tjenester kan bli utsatt for målrettede eller mer tilfeldige angrep er derfor stor. For å sikre Forsvarets internett-tilknyttede systemer er det implementert brannmurer, antivirusløsninger og andre statiske tiltak for å begrense de tjenester som eksponeres mot internett. Det dynamiske trusselbildet vi i dag står overfor på internett, og det faktum at det daglig oppdages nye sårbarheter i operativsystemer og applikasjoner, gjør det nødvendig for Forsvaret å iverksette tiltak for å redusere den restrisiko man står igjen med etter at statiske sikkerhetstiltak er iverksatt. Sikkerhetsmessig overvåking av Forsvarets internettforbindelser er et slikt tiltak.

Gjennom FSJs Direktiv for sikkerhetstjenesten i Forsvaret er jeg gitt både oppdrag og myndighet til å iverksette nettverksovervåking og kartlegge omstendighetene rundt sikkerhetstruende hendelser i Forsvarets informasjonssystemer. Videre har FD i iverksettelsesbrev til Forsvaret for både for 2008 og 2009 gitt oppdrag til Forsvarets sikkerhetstjeneste om å gjennomføre sikkerhetsmessig overvåking av Forsvarets informasjonssystemer. Det er disse dokumentene som har vært mitt hjemmelsgrunnlag for å utføre sikkerhetsmessig overvåking av Forsvarets informasjonssystemer.

Sikringen av Forsvarets internettaktivitet kom i gang tidlig i 2006 som et samarbeid mellom FLO/IKT og FSA.

FOST registrerer trafikk-metadata, som innebærer å registrere data om hvilke IP-adresser på innsiden av Forsvarets internettforbindelser som kommuniserer med IP-adresser på internett. Hvem som ligger bak IP-adressene på Forsvarets internettportal er det ikke FOST som har oversikt over, men FLO/IKT. Det registreres ikke innhold i kommunikasjonen.

Kort tid etter etableringen av nettverksovervåkningen i april 2006, ble det i et brev til FLO/IKT og Forsvarsstaben fra FSA sin side gjort rede for bakgrunnen for denne sikkerhetsmessige overvåkningen og hva den innebærer både i forhold til systemeier, som er FLO/IKT, og for brukerne. FLO/IKT ble i dette skrevet uttrykkelig pålagt å orientere alle brukerne av Forsvarets internettportal om dette nye sikkerhetsregimet.

Vi har ved avdelingen på Jørstadmoen hele tiden hatt et høyt fokus på personvern og etterrettelighet. Dette er nedfelt i gode ledelsesforankrede rutinebeskrivelser, og all

aktivitet blir løpende loggført. Derfor har FOST vært i svært god stand til å belyse overfor KRIPOS hva som har foregått i de sakene vi er anmeldt for.

Medietrykket som fulgte og den langtrukne etterforskningen fra KRIPOS har vært en kraftig belastning for de ansatte i FOST og i særlig grad de som driver med nettverksovervåkingen på Jørstadmoen. Som arbeidsgiver føler jeg derfor et stort ansvar overfor mine medarbeidere i forhold til å få forklart hva nettverksovervåking dreier seg om og på den måten bidra til at media og folk flest får korrekt informasjon om dette. Da saken verserte i pressen fikk jeg og mine ansatte munnkurv. Mediene hadde allikevel rikelig tilgang på detaljert informasjon som fra vårt perspektiv var tendensiøs og spekulativ. Vi sitter med et klart inntrykk av at mange av disse opplysningene som har kommet ut i media bare har vært kjent av folk på innsiden. Det er derfor grunn til å anta at dette kan ha vært gjort for å sette FOST i et dårlig lys.

Det som har vært særlig vanskelig å forstå i denne saken er at det fra politisk ledelse i FD har vært uttalt at de allerede tidlig på høsten 2008 mottok varsel om en mulig "ukultur" i FOST uten at det ble iverksatt effektive tiltak for å bringe fakta på det rene i forhold til dette. Dette fremgår av Statsrådets brev til Stortinget. Dersom det virkelig var en slik "cowboykultur" i FOST burde, etter mitt skjønn, departementet bidratt til at det ble gjennomført kontroll eller tilsyn hos oss for å avdekke dette. Jeg legger til at jeg aldri har blitt orientert om slik varsling om mulig ukultur i den virksomhet jeg leder. Verken jeg eller mine ledere har dermed hatt noen mulighet til å iverksette tiltak for å komme en påstått ukultur til livs.

Det hører med til historien at FD nylig har gjennomført en grundig inspeksjon av virksomheten vår på Jørstadmoen og i den sammenheng ikke funnet noe kritikkverdige.

For FOST har saken fått den dramatiske konsekvens at det i forslag til ny instruks forslås å overføre ansvaret for nettverksovervåkingen til andre aktører i Forsvaret. Begrunnelsen for dette synes å ligge i en sammenlikning med sivile aktører. Vi mener at det ikke er grunnlag for en slik sammenlikning og for oss vil dette i betydelig grad bidra til et redusert kompetansemiljø og en svekket tilgang til informasjon om sikkerhetstruende aktivitet mot Forsvarets IKT-virksomhet.

Dersom det ender med at KRIPOS konkluderer med at vi ikke har bedrevet det vi er anmeldt for – jeg sier det slik fordi jeg så langt ikke har fått innsyn i anmeldelsen, så gjenstår bare kritikken fra EOS – utvalgets rapport av 17. juni. Vi er slett ikke enige i konklusjonene i denne rapporten. Den er fremdeles høyt gradert, men vi har i et eget skriv til utvalget anbefalt at den avgraderes. En avgradering vil bidra til at det blir mulig å gå inn i disse problemstillingene. Dette blir vesentlig dersom det er dette som skal legges til grunn for en betydelig vingestekking av tjenesten.

Forsvarets senter for beskyttelse av kritisk infrastruktur har i lang tid vært viet betydelig oppmerksomhet for sitt meget høye profesjonelle nivå både fra utenlandske allierte og fra våre egne. Det har vært en rekke VIP-besøk på Jørstadmoen både fra forsvarsledelsen, politisk ledelse i FD og andre medlemmer av regjeringen. Mange har gitt uttrykk for forbauselse over det bildet som vi har kunnet vise frem og nesten uten unntak forlatt avdelingen med ordene "keep up the good work".

Det er viktig for meg å si at jeg er stolt av det arbeidet mine ansatte gjør og den profesjonelle holdningen de representerer. Jeg er også stolt av den måten de har båret den tunge børen det er å ha vært under etterforskning for å ha forbrutt seg mot norsk lov. Et stort antall har møtt frem her i kveld både for å gi meg litt moralsk støtte, men ikke minst for å vise at de ikke har noe verken å skjemmes over eller gjemme seg for.

Dermed vil jeg avslutningsvis si at som sjef opplever jeg at både sikkerhetsfaget og den enkelte medarbeiders motivasjon har fått seg et kraftig skudd for baugen som et resultat av denne saken.

Etter angrepet på Pearl Harbour viste amerikanerne en ekstrem besluttsomhet og vilje til innsats. Det varte ikke lenge før de hadde tatt igjen det tapte og mer til. Når det gjelder vår situasjon skorter det heller ikke på viljen, men vi er på nåværende tidspunkt i liten grad gitt mulighet til å påvirke vår egen situasjon og er derfor avhengige av at den sunne fornuft får råde i forhold til hvordan vår fremtidige virksomhet skal organiseres og reguleres.

Det er uansett et udiskutabelt militært behov for å være profesjonell på dette området. Konsekvensen av det motsatte illustreres godt gjennom det gamle ordtaket "ei lita tue kan velte et stort lass". Det passer også godt i denne sal å avslutte med et sitat fra Jens Christian Hauge som lyder som følger: "Det var først da vi tok sikkerheten på alvor at hjemmefrontens operasjoner fikk effekt."

Jeg ønsker dere alle et riktig hyggelig julegilde her i kveld og alt godt for den kommende høytiden.

Tusen takk for oppmerksomheten.