ETTERRETNINGSTJENESTEN

Vår saksbehandler
Udir Carsten Rapp
Tlf 510 4743

Vår dato 2009-12-17
Vår referanse 2009/000230-018/ETJ/ 430

Tidligere dato 2009-11-16
Tidligere referanse 2009/00484-55/FD I 4/FRI/204.3

Til
Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

Kopi til
Forsvarets sikkerhetstjeneste
Forsvarsstaben
Nasjonal Sikkerhetsmyndighet

Høring - Utkast til Instruks om sikkerhetstjeneste i Forsvaret

1 Bakgrunn

Etterretningstjenesten (E-tjenesten) viser til høringsbrev fra Forsvarsdepartementet om utkast til instruks om sikkerhetstjeneste i Forsvaret, med frist for å svare 5. jan 2010.

2 Hovedinntrykk

E-tjenesten mener de formelle rammene for den faglige virksomheten til Forsvarets sikkerhetstjeneste bør avklares og reguleres nærmere i instruks. Vi mener at utkastet til instruks adresserer de forholdene som er nødvendig i så henseende, men vi stiller spørsmål ved utformingen av enkelte av bestemmelsene. E-tjenestens nærmere kommentarer til utkastet gis i det følgende.

3 Generelle kommentarer

3.1 Navnet FOST versus FSA

E-tjenesten støtter forslaget om at Forsvarets sikkerhetstjeneste (FOST) skal skifte navn til Forsvarets sikkerhetsavdeling (FSA). E-tjenesten registrerte når FSA skiftet navn til FOST at det ble gitt ulike budskap om hensikten med navneendringen. På den ene siden ble det fremført at navneendringen ikke var ment å gjenspeile endringer i oppgavene. Samtidig ble det på annet hold fremført at FOST nå var blitt "den fjerde hemmelige tjenesten", og at det måtte få den konsekvens at FOST måtte få delta i enkelte EOS-forum de tidligere ikke hadde hatt en plass i.

Det vil være uheldig, også for FOST selv, dersom navnet som benyttes gir inntrykk utad av at FOST kan benytte mer inngripende metoder enn det som er tilfellet. Videre vil bruk av navnet FOST kunne føre til at allmennheten får inntrykk av at FOST er en EOS-tjeneste med nasjonale oppgaver i likhet med E-tjenesten, Nasjonal sikkerhetsmyndighet (NSM) og Politiets sikkerhetstjeneste (PST). De tre nevnte EOS-tjenestene er, i motsetning til FOST, gitt eget hjemmelsgrunnlag i lovs form, nettopp pga sine nasjonale og inngripende oppgaver.

3.2 Instruksens virkeområde og tittel

E-tjenesten har merket seg at instruksens tittel og formålsbestemmelse i utkastets § 1 viser til "sikkerhetstjeneste i Forsvaret". Likevel er det få bestemmelser i instruksen som gjelder andre aktører innen sikkerhetstjeneste i Forsvaret enn FSA. I praksis virker det derfor som instruksen

Postadresse
Pb 193 Alnabru
bedriftssenter
0614 Oslo

Besøksadresse
Lutvannsvn 60
Oslo

Sivil telefon/telefaks
23094000

Militær telefon/telefaks
510 4000

Epost/ Internett
Post.etterretningstjenesten@mil.no
www.forsvaret.no

Organisasjonsnummer
NO 974 7892 21 MVA

Vedlegg

stort sett er myntet på FSA. (Til sammenligning er forholdet motsatt i sikkerhetsloven med forskrifter, der de fleste bestemmelsene retter seg mot virksomhetene og ikke NSM.) E-tjenesten synes således at i forhold til instruksens tittel har den en "slagside" i retning av regulering av FSAs virksomhet spesielt. Andre målgrupper, som f eks militære sjefer på ulike nivåer, kan få problemer med å skille ut hvilke bestemmelser i instruksen som er relevante også for dem kontra kun relevant for FSA. E-tjenesten har imidlertid ingen konkrete forslag til endringer i så måte.

3.3 Gjengivelse av grunnleggende prinsipper

E-tjenesten registrer at det i utkastet, spesielt i kapittel 3 til 5, er foreslått en rekke bestemmelser som omhandler relevante rettsforhold. Forholdene omhandler blant annet grunnleggende prinsipper om hjemler, personvern og rettssikkerhet, som i stor grad allerede følger av andre rettskilder, men som kan være vanskelig å få oversikt over. Av pedagogiske og praktiske grunner støtter E-tjenesten den reguleringsmåten departementet her legger opp til.

3.4 Begrepsbruk: CND, IKT-sikkerhet og informasjonssikkerhet

I utkastet til instruks er det benyttet flere begreper som i stor grad overlapper hverandre. I utkastets §§ 2 sjette ledd, 4 første ledd bokstav c, 29 og 31, samt i tittelen til 30, benyttes begrepet *"CND"*. I §§ 29 og 30, samt i tittelen til kap 6, benyttes begrepet *"IKT-sikkerhet"*. Begrepene CND og IKT-sikkerhet er imidlertid brukt om hverandre i den hierarkiske strukturen for nevnte titler og bestemmelser, og fremstår i instruksen som synonymer. I § 22 benyttes derimot begrepet *"informasjonssikkerhet"*.

At begrepet informasjonssikkerhet er benyttet i § 22 er forståelig. Hele kap 4, som denne bestemmelsen står i, omhandler personvern og fremstår som et resymé av personopplysningsloven. I personopplysningsloven § 13 er nettopp begrepet informasjonssikkerhet benyttet.

E-tjenesten mener imidlertid at begrepsbruken for øvrig fremstår som noe forvirrende og lite enhetlig. Slik vi oppfatter det, gjenspeiler ikke begrepsbruken i instruksen forståelsen av tilsvarende begreper i andre sammenhenger. Information Assurance er et fellesbegrep for det vi i Norge kaller IKT-sikkerhet, og omfatter både Protective Security (forebyggende sikkerhet) og Security Operations (løpende/operativ sikkerhet). I NATO er Cyber Defence (CD) definert som den operative delen av begrepet Information Assurance, jf MC-0571. Computer Network Defence (CND) er definert som CD innen militære informasjonsoperasjoner, og benyttes på operasjonelt nivå i den militære strukturen, jf AJP-3.10. Vi synes ikke at ovennevnte begrepsforståelse gjenspeiles i bestemmelsene der CND er brukt.

Begrepet Cyber Security er benyttet av en del land, men med noe ulik betydning. I Norge har Cyber Security blitt oversatt til cybersikkerhet, og forsøkt brukt for å "revitalisere" informasjonssikkerheten innen spesielt det løpende/operative arbeidet i NorCERT og sektorvise CERTer. Begrepet cybersikkerhet fremstår imidlertid som for uavklart til at E-tjenesten synes det er noen god erstatning for CND-begrepet.

Innholdet i definisjonen av CND i utkastet er nærmest identisk med hvordan begrepene informasjonssikkerhet og IKT-sikkerhet er definert i mange andre sammenhenger. E-tjenesten støtter at instruksen bør fokusere på sikkerhet ved mer enn bare informasjon. Det vises til at de nye bestemmelsene om objektsikkerhet i og i medhold av sikkerhetsloven, er ment å beskytte objekter med funksjoner som er kritiske for samfunnet. Det omfatter sikkerhet ved digital og til dels elektronisk infrastruktur for øvrig, som igjen er viktig for funksjonaliteten til annen infrastruktur. Dvs at også f eks styringssystemer, som ikke kan karakteriseres som informasjonssystemer etter tradisjonell forståelse, må sikres. Dersom man ønsker å omfatte sikkerhet ved både informasjonssystemer og styringssystemer, anser E-tjenesten at IKT-sikkerhet er et tilstrekkelig dekkende begrep.

E-tjenesten mener at begrepet CND ikke bør benyttes i instruksen. Dersom andre begreper enn IKT-sikkerhet skal benyttes i formelle sammenhenger, vil det medføre utilsiktede og uheldige avgrensninger eller spesifiseringer. Vi anbefaler derfor at begrepet CND fjernes fra § 2 sjette ledd og at det erstattes med IKT-sikkerhet i §§ 4 første ledd bokstav c, 29, 30 og 31.

4 Kommentarer til de enkelte bestemmelsene

4.1 Utkastets § 3

I utkastets § 3 andre ledd pålegges den enkelte militære sjef å rapportere direkte til NSM og det vises til sikkerhetsloven og forskrift om sikkerhetsadministrasjon. I sistnevnte forskrifts kap 5 er imidlertid ansvarssubjektet for rapportering den enkelte "virksomhet". Både iht utkastets § 1 siste punktum og tidligere avklaring fra Juridisk avdeling i FD, er Forsvaret nå å anse som én og samme virksomhet i sikkerhetslovens forstand.

E-tjenesten har ikke innvendinger til at Forsvaret anses som én og samme virksomhet i sikkerhetslovens forstand. Vi stiller imidlertid av prinsipielle grunner spørsmål ved om det er heldig at den enkelte militære sjef skal rapportere direkte til NSM, når det er Forsvaret som virksomhet som er ansvarssubjektet. Det er et paradoks at det i instruksen har vært viktig å poengtere at det er Forsvaret som er å anse som virksomhet i sikkerhetslovens forstand, samtidig som man ikke helt vil ta konsekvensene av det, ved at det pålegges desentralisert rapportering til NSM. Utkastets bestemmelser vil i praksis redusere FSAs rolle til observatør av den direkte dialogen mellom militære sjefer og NSM. I tillegg vil NSM vanskeligere kunne oppfylle sin rolle som et overordnet og sektorovergripende tilsynsorgan også for Forsvaret, dersom enhver militær sjef skal rapportere direkte til NSM.

Gitt det virksomhetsbegrepet som utkastet legger til grunn, mener E-tjenesten at det er mer riktig at den enkelte militære sjef først rapporterer til FSA, og at FSA så rapporterer viktige saker videre til NSM. At rapporteringsveien i utgangspunktet skjer via FSA, behøver ikke være til hinder for at eventuell nærmere dialog, informasjon og undersøkelser på et senere stadium i saken, skjer direkte mellom militær sjef og NSM. FSA vil da få mulighet til å vurdere, ut i fra en saks art og omfang, om FSA som overordnet sikkerhetsorgan i Forsvaret selv skal ha den videre dialogen med NSM, eller om det er mer hensiktsmessig at det overlates til vedkommende militære sjef.

4.2 Utkastets § 4

E-tjenesten viser til begrepet risiko som er benyttet i utkastets § 4 første ledd bokstav d.

Begrepet risiko og risikobilde kan benyttes om mange forhold, ikke bare sikkerhet. Begrepene benyttes både innen virksomhetsstyring, HMS, samfunnssikkerhet, prosjektstyring og økonomiske forhold. E-tjenesten antar riktignok at det for målgruppen vil være liten tvil om hvilken type risiko FSA skal konsentrere seg om. E-tjenesten anbefaler likevel at det i utkastets § 4 første ledd bokstav d, for ordens skyld, presiseres at det er det *sikkerhetsmessige* risikobildet FSA skal holde oversikt over.

4.3 Utkastets § 9

E-tjenesten viser til utkastets § 9, spesielt første ledd fjerde punktum om at arbeidsgivers styringsrett og lov om militær politimyndighet *"...er ikke grunnlag for å gjennomføre forebyggende sikkerhetstjeneste".*

E-tjenesten mener § 9 går for langt i å begrense muligheten til helt legitime sikkerhetstiltak. Paragrafen reduserer sikkerhet til kun sikkerhetslovens fokus. Det gis inntrykk av at dersom et tiltak ikke er anvist i sikkerhetsloven med forskrifter, kan det heller ikke gjennomføres. Konsekvensen vil i praksis bli at Forsvaret pålegges større begrensninger i å innføre sikkerhetstiltak utenfor sikkerhetslovens virkeområde, enn det som gjelder for andre virksomheter. E-tjenesten mener imidlertid at sikkerhetsloven bare er ett av flere regelverk som omhandler krav til sikkerhet relevant for Forsvaret.

Slik vi ser det kan en rekke tiltak som kan anses som forebyggende sikkerhetstiltak, iverksettes nettopp med hjemmel i styringsretten eller lov om militær politimyndighet. Et eksempel kan være forbud mot bruk av minnepinner, slik E-tjenesten har innført. Det er et tiltak som ikke følger direkte av sikkerhetslovens krav. Tiltaket anses heller ikke som for inngripende i den personlige

integriteten, og dermed kan tiltaket bestemmes med hjemmel i arbeidsgivers styringsrett. Andre eksempler kan være styrkebeskyttelsestiltak og sikkerhetstiltak mot vinningskriminalitet, som bruk av militære vakters myndighet og kontroll av yttertøy og bagasje ved ut- eller innpassering av et område, fartøy eller bygg – dvs tiltak som kan sikre andre interesser og hensyn enn det sikkerhetsloven omhandler.

Selv om instruksen for øvrig gir en god fremstilling av de ulike rettslige rammene, savner E-tjenesten en redegjørelse for eller henvisning til regler om sikkerhetstiltak som utgjør inngrep i den *fysiske* integriteten til personer. E-tjenesten viser til at rettssikkerhet og personvern ved kontrolltiltak overfor arbeidstakere i virksomheten, også er ivaretatt i *arbeidsmiljøloven kap 9* som et vern mot at spesielt inngripende kontrolltiltak begrunnet i nettopp styringsretten. Vi mener det derfor bør tas inn en henvisning også til arbeidsmiljøloven kap 9 i denne paragrafen.

Sikkerhetsloven gir med andre ord ikke en uttømmende regulering av retten eller plikten til å innføre forebyggende sikkerhetstiltak. Paragrafen bør pga overnevnte endres til at dersom styringsretten skal benyttes som hjemmelsgrunnlag for sikkerhetstiltak, må tiltaket ikke være i strid med spesielt det ulovfestede legalitetsprinsippet, personopplysningsloven §§ 8, 9 og 11, sikkerhetsloven § 6 eller arbeidsmiljøloven kap 9.

4.4 Utkastets §§ 13 og 26

I utkastets §§ 13 og 26 er korttitlene *"etterretningstjenesteloven"* og *"etterretningstjenesteinstruksen"* benyttet.

E-tjenesten er klar over at nevnte korttitler er de offisielle korttitlene som benyttes i Lovdata, og at det i dagligtalen nok har liten betydning at man benytter disse korttitlene. Vi mener likevel at korttitlene er noe uheldige, da de gir inntrykk av at loven og instruksen omhandler all etterretningstjeneste som aktivitet, herunder etterretningstjeneste som utøves av *andre* enn E-tjenesten, som f eks Etterretningsbataljonen og ISTAR-elementer. Vi mener at langtittelen på regelverkene (*"Lov om Etterretningstjenesten"* og *"Instruks om Etterretningstjenesten"*) gir et mer korrekt inntrykk, dvs at regelverkene omhandler E-tjenesten.

E-tjenesten anbefaler at regelverkenes korttittel som er benyttet i utkastets §§ 13 og 26, erstattes med de formelle langtitlene.

4.5 Utkastets § 26

4.5.1 Første og andre ledd

Utkastet beskriver fagmyndigheten til FSA og E-tjenesten i utkastets § 26 første og andre ledd.

E-tjenesten antar at det, på tross av de foreslåtte bestemmelsene, for mange kan oppleves som noe uklart hvordan forholdet er mellom fagmyndighetene til FSA og E-tjenesten. For å gjøre det noe klarere, anbefaler vi at bestemmelsene omformuleres og at det legges til en fotnote. Vi foreslår derfor at paragrafens første og andre ledd erstattes med følgende: *"Sjef FSA er fagmyndighet og utøvende ansvarlig for militær kontraetterretning i Forsvaret, men er underlagt Sjef Etterretningstjenestens fag- og direktivmyndighet for etterretningsdisiplinene[1]"*. Videre forslag til fotnote 1: *"Med etterretningsdisipliner menes de ulike hovedkategoriene av metoder for innsamling av informasjon, herunder SIGINT, IMINT, NETINT, HUMINT og OSINT."*

4.5.2 Tredje ledd

I paragrafens tredje ledd ser det ut til å være en inkurie i formuleringen *"...skal ved behov anmode om informasjonsbehov og annen støtte fra..."*.

E-tjenesten antar intensjonen med formuleringen gjenspeiles korrekt ved å endre formuleringen til *"...skal ved behov anmode om informasjon og annen støtte fra..."* eller *"...skal fremme informasjonsbehov og annet behov for støtte fra..."*.

4.6 Utkastets § 27

4.6.1 Første ledd

I utkastets § 27 første ledd er det foreslått en bestemmelse om ansvarsforholdene for militær kontraetterretning i utlandet.

E-tjenesten mener den forslåtte bestemmelsen er uheldig formulert. Det fremgår at FSA er gitt et utøvende ansvar, samtidig som det skal skje innen rammen av norsk operativ sjefs bestemmelser. E-tjenesten tolker bestemmelsen dit hen at det åpnes en tredje kommandolinje (i tillegg til FOHs og E-tjenestens) for operasjoner i utlandet. Vi mener at etablering av nok en kommandolinje er uheldig da det vil være lite enhetlig i forhold til kontroll med nasjonale enheter i et operasjonsområde. Og dersom det ikke er meningen at det skal åpnes en egen kommandolinje for FSA, bør bestemmelsen endres for å tydeliggjøre kommandoforholdene.

Etter det E-tjenesten forstår, har Forsvarets operative hovedkvarter (FOH) v/ J2 pr i dag enkelte oppgaver også innen militær kontraetterretning. FOH har herunder en nasjonal J2X-funksjon for styring av Forsvarets samlede kontraetterretnings- og etterretningsressurser i et operasjonsområde (unntatt for E-tjenestens ressurser, der det i stedet er en koordinering mellom FOH og E-tjenesten). E-tjenesten savner således en omtale av FOHs rolle eller oppgaver i utøvelsen av militær kontraetterretning, f eks ved internasjonale operasjoner, øvelser og besøk fra allierte styrker.

Et alternativ til den foreslåtte bestemmelsen, er å fastsette at FSA skal ha det utøvende ansvaret for militær kontraetterretning, men at taktisk kommando (TACOM) for KE-elementer i et operasjonsområde skal avgis til f eks NCC. Ved TACOM under NCC sikres både nasjonal koordinering som del av FOHs J2X-funksjon og en tydeligere kommandolinje, samtidig som KE-elementene kan rapportere hjem til FSA. E-tjenesten anbefaler på denne bakgrunn at utkastets § 27 første ledd gjennomgås på nytt.

4.6.2 Andre og tredje ledd

E-tjenesten har merket seg forslagene om E-tjenestens rolle ved militær kontraetterretning i utlandet, jf utkastets § 27 andre og tredje ledd.

Det kan oppstå situasjoner der en person/aktivitet kan være kilde/mål både som ledd i kontraetterretningsvirksomhet, og som ledd i etterretningsvirksomhet innen rammen av E-tjenestens hjemmelsgrunnlag. Det er da viktighet å unngå at nasjonale KE-elementer og E-tjenesten benytter samme kilder uten å være klar over det, og derved skaper dobbeltrapportering fra kilder som fremstår som ulike. Videre bør det unngås at samme kilde "selger" samme informasjon til både nasjonale KE-elementer og E-tjenesten. Det må også unngås at KE-relaterte operasjoner i vanvare iverksettes mot etterretningsoperasjoner som er legitime, men pga dekket ikke fremstår som det, og forstyrrer disse.

I ovennevnte situasjoner må det i det minste skje en koordinering med E-tjenesten, som foreslått i paragrafens andre ledd, hvilket også er i samsvar med HUMINT-direktivet. I enkelte tilfeller er det også hensiktsmessig at E-tjenesten *overtar ansvaret* for å planlegge og gjennomføre operasjonen, jf tredje ledd. Selv om en slik overtakelse kun vil være aktuell i spesielle tilfeller, er det viktig at E-tjenesten – som normalt største aktør og med det videste nasjonale hjemmelsgrunnlaget for innhenting utenlands – på denne måten gis muligheten til å samordne en operasjon. E-tjenesten støtter av ovennevnte grunner forslaget til utkastets § 27 andre og tredje ledd.

4.7 Utkastets § 28

E-tjenesten er usikker på om § 28 andre ledd bokstav a og e er ment å innskrenke E-tjenestens utøvelse av intern sikkerhetstjeneste. Det vises til at FOST fra før er gitt begrenset myndighet og innsyn overfor E-tjenesten i sikkerhetssaker, av hensyn til skjerming av kapasiteter, metoder,

kilder og samarbeidende tjenester. E-tjenesten utøver og kontrollerer derfor selv sikkerheten internt på områder der FOST ikke har myndighet eller innsyn.

For å unngå tvil på området, anbefaler E-tjenesten at det føyes til et ledd i paragrafen om at oppgavene i andre ledd bokstav a og e, for E-tjenestens vedkommende, ivaretas av E-tjenesten selv (E-tjenestens interne sikkerhetstjeneste).

4.8 Utkastets § 29

Det står i utkastets § 29 andre punktum at NSM har et nasjonalt ansvar for å *"...produsere et oppdatert nasjonalt IKT-trusselbilde"*.

E-tjenesten mener bestemmelsen er uheldig formulert og etter sin ordlyd i strid med den prinsipielle ansvarsfordelingen som er fastsatt for NSM, E-tjenesten og PST. E-tjenesten og PST er ved hhv lov om Etterretningstjenesten og politiloven, gitt oppgaver innen analyse og vurderinger av trusler mot nasjonal sikkerhet. Det er ikke fastsatt noen begrensninger i dette ansvaret for bestemte type trusler, som f eks IKT-trusler, og det ville i så fall ha vært meget uheldig og lite logisk.

E-tjenesten mener pga overnevnte at kommaet i § 29 andre punktum bør erstattes med et punktum, og at den siterte formuleringen endres til *"NorCERT skal også, sammen med E-tjenesten og PST, produsere et oppdatert nasjonalt IKT-risikobilde"*.

4.9 Utkastets § 30

4.9.1 Første ledd bokstav b

I utkastets § 30 første ledd bokstav b fastsettes det at FSA har et *"utøvende ansvar for internkontroll med IKT driftsmiljøet/systemeier"*.

E-tjenesten stiller spørsmål ved om ikke begrepet internkontroll her brukes feil, i motsetning til i utkastets § 4 tredje ledd. Internkontroll betyr at man skal ha planlagte, systematiske og dokumenterte tiltak for å sikre ivaretakelse av lovpålagte krav og selvpålagte krav/interesser i en virksomhet. Internkontroll er altså ikke det samme som kontroll i betydningen tilsyn, revisjon eller evaluering, som muligens er det man egentlig har ment med bestemmelsen i utkastets § 30 første ledd bokstav b. Ikke bare FSA, men også driftsorganisasjonen for IKT, bør ha oppgaver som ledd i Forsvarets internkontrollsystem for IKT-sikkerhet. I bestemmelsen her bør det derfor heller fremgå at FSA har ansvaret for internt tilsyn, revisjon eller evaluering (avhengig av hva man vil oppnå) av sikkerheten ved driftsorganisasjonen for IKT og systemeier.

4.9.2 Første ledd bokstav c

E-tjenesten er usikker på rekkevidden av utkastets § 30 første ledd bokstav c og om FSA er gitt tilstrekkelig myndighet i så måte. Ved f eks alvorlige sikkerhetsbrudd, påvisning av store sårbarheter, akutte behov eller kriser, kan det være behov for hurtig reaksjon i form av nedstengning av berørte systemer. Myndighet til å gi slike pålegg kan være såpass inngripende for Forsvaret, at det bør avklares om FSA skal gis slik myndighet. Det bør fremgå tydelig i paragrafen om slik myndighet er gitt FSA direkte eller om FSA i stedet skal fremlegge slike saker til FSJ eller Sj FST for avgjørelse.

Arne Karstad (e f)
Assisterende direktør
Assisterende sjef Etterretningstjenesten