FORSVARET
Forsvarsstaben

Vår saksbehandler
Hans Kristian Herland, hherland@mil.no
+4723 09 67 08, 0510 6708
FST

Vår dato 2010-01-08

Vår referanse 2009/019659-023/FORSVARET/ 005

Tidligere dato

Tidligere referanse

Til
Forsvarsdepartementet

Postboks 8126 Dep
0032 OSLO
NORGE

Kopi til
Etterretningstjenesten
Forsvarets Sikkerhetstjeneste
INFORMASJONS- OG KOMMUNIKASJONSTJENESTER

Høring - Utkast til instruks om sikkerhetstjeneste i Forsvaret

Det vises til tidligere referanse hvor Forsvarsdepartementet (FD) ba om merknader til utkast til instruks om sikkerhetstjeneste i Forsvaret.

I lys av oppmerksomheten Forsvarets sikkerhetstjeneste (FOST) har hatt i den senere tid er det vesentlig at rammene for sikkerhetstjeneste i Forsvaret er entydige og klare. Forsvarsstaben (FST) understreker følgende forhold:

- Den prinsipielle rollefordelingen mellom FD, Forsvaret og Nasjonal sikkerhetsmyndighet (NSM) må ligge fast. FOST er underlagt Forsvarssjefen.
- NSM utøver rollen som nasjonal sikkerhetsmyndighet iht Sikkerhetsloven, og gir pålegg og råd til Forsvarssjefen samt fører tilsyn med sikkerhetstjenesten i Forsvaret. FOST er fagmyndighet for sikkerhetstjeneste i Forsvaret på vegne av FSJ. FOST mottar, konkretiserer og iverksetter pålegg fra NSM innen Forsvaret.
- Etterretning-, overvåkning- og sikkerhetsutvalgets (EOS) rolle ift til aktørene i linjen samt til evt andre utvalg må være entydig og klar. Den foreslåtte etableringen av Sikkerhetsforum (S-forum) og Tilsynsutvalget for FOST (TFF) innebærer ytterligere to fora som skal følge opp sikkerhetstjenesten og FOST. FST støtter etableringen av S-forum, men er i tvil om det er hensiktsmessig at FD etablerer et eget tilsynsutvalg for FOST gitt at NSM har ansvaret for tilsynet med sikkerhetstjenesten i Forsvaret. Tilsyns- og ansvarslinjene må være klare.
- Det er behov for å klargjøre og styrke hjemmelsgrunnlaget relatert til FOSTs virksomhet.

FST gir i vedlegg[A] merknader til noen av utkastets paragrafer.

FD har mottatt eget høringsinnspill fra Etterretningstjenesten (E-tj) og FST velger derfor, for helhetens skyld, å vedlegge innspill mottatt fra FOST[B] og Forsvarets logistikkorganisasjon/Informasjons- og kommunikasjonstjenester[C] (FLO/IKT).

FST anbefaler at FD gjennomfører et arbeidsmøte med berørte parter ifm videre arbeid med instruksen.

Jan Eirik Finseth (ef)
Viseadmiral
Sjef Forsvarsstaben

[A] Vedlegg: Merknader til "Utkast til instruks om sikkerhetstjeneste i Forsvaret
[B] Vedlegg: 2009-12-17 2009/019659-21 Høring - Utkast til instruks om sikkerhetstjeneste i Forsvaret
[C] Vedlegg: 2009-12-10 2009/019659-20 Høring - Utkast til instruks om sikkerhetstjeneste i Forsvaret - Merknader fra FLO/IKT

Merknader til "Utkast til instruks om sikkerhetstjeneste i Forsvaret

§ 1. Formål og virkeområde

FST viser til merknaden fra FOST og foreslår å endre andre avsnitt til: Forsvaret er i denne instruksen å betrakte som en virksomhet, og Forsvarssjefen er virksomhetens leder. Herunder medfører instruksen ingen endring i virksomhetens rapportering til NSM.

Avsnittet er selvmotsigende samtidig som det innebærer at hver enkelt sjef skal rapportere sikkerhetstruende hendelser direkte til NSM og ikke til FSJ. Dette vil medføre at FSJ ikke gis grunnlag til å drive risikohåndtering i Forsvaret, som han ift Sikkerhetsloven er pålagt.

Forsvaret er å anse som en virksomhet, hvorav FOST er sikkerhetsmyndighet og har rapporteringsplikt til NSM. Forsvarets avdelinger er ikke egne virksomheter og har derfor ikke direkte rapporteringsplikt til NSM. Rapportering skal gå tjenestevei internt i Forsvaret til FOST og videre til NSM i henhold til gjeldende lover og bestemmelser.

§ 2. Definisjoner

FST ber FD vurdere om det er nødvendig å benytte begrepet Computer/Cyber Network Defence (CND) i instruksen og om det er andre begreper som heller kan benyttes for eksempel IKT-sikkerhet. FST viser for øvrig til E-tj og FOST sine innspill til definisjoner.

§ 3. Organisering og utøvelse av forebyggende sikkerhetstjeneste i Forsvaret

FST viser til kommentaren til §1 hvor Forsvaret må anses som en virksomhet og at rapportering skal skje gjennom FSA til NSM.

§ 4. FSA

Det vises til innspill fra E-tj og FOST.

§ 5. Foreleggelse og rapportering til FD

FST anbefaler å fjerne pkt c hvor FD ønsker at FSJ skal rapportere anskaffelse av nye sensorer/kapasiteter. Dette begrunnes i at FD er involvert i "alle" materiellanskaffelser samt at begrepene sensorer/kapasiteter er svært generelle begreper.

§ 8. Tilsynsutvalget for FSA

FST anbefaler paragrafen strøket og at et slikt tilsyn ikke etableres. NSM sin rolle ift FSA bør i tilstrekkelig grad ivareta tilsynsrollen.

§ 9. Overordnede juridiske rammer

FST viser til E-tj sine merknader knyttet til at paragrafen i sin nåværende form i for stor grad kan avgrense arbeidsgivers styringsrett. FST anbefaler at FD utreder denne problemstillingen ytterligere.

§ 12. Bistand til politiet og andre sivile offentlige myndigheter

FOST fremmer betenkninger til paragrafen slik den nå står med henvisning til FOR 2003-02-28 nr 220: "Instruks om Forsvarets bistand til politiet" som i sin § 2 fastslår at denne instruksen ikke gjelder for forebyggende sikkerhetstjeneste. FST anbefaler at FD utreder denne problemstillingen ytterligere.

§ 13. Forholdet til etterretningstjenesteloven

Det vises til E-tj innspill.

§ 26. Generelle bestemmelser (Særlig om militær kontraetterretning)

Det vises til E-tj innspill som foreslås ivaretatt i endelig instruks.

FST ber FD vurdere å endre passusen om at FSA *ved behov skal anmode om* informasjonsbehov og annen støtte fra E-tj og Politiets sikkerhetstjeneste (PST) til at disse tjenestene rutinemessig må videreformidle vurderinger og varsler om trusler mot Forsvaret til FSA. Dette for å gjøre FSA i stand til å gjennomføre kontinuerlige risikovurderinger for Forsvaret.

§ 27. Militær kontraetterretning i utenlandsoperasjoner
FST viser til E-tj innspill og behovet for å sikre at det ikke oppstår dobbeltrapportering og fare for misforståelser ved at kilder rapporteres både til en nasjonal kontraetterretnings-enhet og til E-tj.

Videre understrekes viktigheten av å koordinere kontraetterretningen med Forsvarets operative hovedkvarter (FOH) og E-tj.

Siste avsnitt i denne paragrafen anbefales vurdert på nytt. Ansvaret for kontraetterretning ligger hos sjef FSA og dette ansvaret kan ikke delegeres til annen militær sjef uten at dette er avklart i linjen opp til Forsvarssjefen (FSJ).

§ 28. Militær kontraetterretning i Norge i fredstid
Både E-tj og FOST har egne forslag til innspill til denne paragrafen. FST henviser til dette innspillet for nærmere vurdering.

§ 29. Ansvarsforhold (Særlig om IKT-sikkerhet i forsvarssektoren)
FST anbefaler at E-tj innspill til andre punktum tas til følge: "NorCert er en del av NSM og har nasjonalt ansvar...". må endres til at "NorCert skal også, sammen med E-tj og PST, produsere et oppdatert nasjonalt IKT-risikobilde".

FST anbefaler at FD vurderer å utdype denne paragrafen ytterligere for å få frem FSJs selvstendige ansvar for militære operasjoner. Forsvaret skal ha et nært samarbeid med NSM, men FSJ har ansvaret for militære operasjoner og må fortløpende forvalte risiko i disse operasjonene. NSM bør ha tilgang til informasjon fra nettovervåkingen, men ikke inngå som beslutningstaker i en militær operasjon ledet av FSJ.

§ 30. Ansvaret for CND i Forsvaret
FST mener at denne paragrafen ikke er tilstrekkelig gjennomarbeidet og at det videre arbeid må få til en klarere rollefordeling mellom de ulike partene uten at dette bør reguleres i detalj i denne instruksen. Det henvises her til innspill både fra E-tj , FOST og FLO/IKT.

FST foreslår at begrepet CND ikke benyttes i dokumentet og at en heller bør omtale IKT-sikkerhet.

§ 31. Samarbeidet mellom NSM og Forsvaret
Paragrafen bør gis mer substans eller utgå.

§ 32. Beredskap
Paragrafen bør gis mer substans eller utgå.

Forsvarets Sikkerhetstjeneste

Vår dato	Vår referanse
2009-12-17	2009/019659-021/FORSVARET/ 005
Tidligere dato	**Tidligere referanse**
2009-10-02	2009/00484-45/204.3

Til
Forsvarsstaben

Kopi til
Etterretningstjenesten
Forsvarets operative hovedkvarter
INFORMASJONS- OG KOMMUNIKASJONSTJENESTER
INI

Høring - Utkast til instruks om sikkerhetstjeneste i Forsvaret

1 Bakgrunn

Forsvarets sikkerhetstjeneste (FOST) viser til oppdraget gitt fra Forsvarsstaben (FST) til FOST om å koordinere Forsvarets innspill i fm høring på instruks om sikkerhetstjeneste i Forsvaret.
Etter anmodning fra FOST godkjente FST en utsatt svarfrist til 17 des 2009.

Interne høringsinstanser i Forsvaret har vært E, INI, IKT og FOH. FOST har mottatt muntlig høringsinnspill fra INI. E har meddelt at de svarer Forsvardepartementet direkte. Det er ikke mottatt tilbakemeldinger fra IKT og FOH.

2 *Drøfting*

Vedlagt følger forslag til tekst som tilbakemelding til FD på høringen. I den muntlige tilbakemeldingen fra INI fremkom at det er intern uenighet i Forsvaret vedrørende ansvar for sikkerhetsmessig nettverksovervåking. INI mener denne bør ligge i sin egen organisasjon for å ivareta det helhetlige ansvar for informasjonsinfrastrukturen. FOST viser til møte mellom sjef FST, sjef INI, sjef IKT og sjef FOST i september i år, der dette ansvarsforholdet var et tema. Sjef FST besluttet da at ansvaret for sikkerhetsmessig overvåking skal ligge hos sjef FOST.

Sjef FOST har lagt dette til grunn i utarbeidelsen av svarbrevet for høringen.

3 Konklusjon

Vedlagt følger forslag til svarbrev fra Forsvaret til Forsvarsdepartementet som svar på "Høring – utkast til instruks om sikkerhetstjeneste i Forsvaret".

Terje Alvsaker (ef)
Oblt
Fungerende sjef Forsvarets
sikkerhetstjeneste

Postadresse	Besøksadresse	Sivil telefon/telefaks	Epost/ Internett	Vedlegg
OSLO MIL/Akershus 0015 OSLO	Langkaia 1, 6 etg inng A 0015 OSLO	/ **Militær telefon/telefaks** 99/0500 3699	forsvaret@mil.no www.mil.no **Organisasjonsnummer** NO 986 105 174 MVA	0

Tilbakemelding på instruks

1. Generelt

Det vises til skriv fra Forsvarsdepartementet av 2 okt 2009 vedrørende "Høring – utkast til instruks om sikkerhetstjeneste i Forsvaret".

Forsvaret er av den oppfatning at en slik instruks bør være av generell karakter. Bla bør ikke strukturelementer i Forsvaret nevnes med navn, bare med funksjon; slik at instruksen ikke behøver revidering hver gang Forsvaret omorganiserer eller endrer navn på strukturelementer.

Forslag til instruksen medfører for Forsvaret to vesentlige forhold som vil medføre betydelige endringer for håndtering av sikkerheten i etaten. Det ene er det foreslåtte navneendringen, og det andre er overføring av ansvar for nettverksovervåkingen fra FOST til "driftsenheten". Begrepet "driftsenheten" er brukt gjennomgående i utkastet. Dette er et uformelt og ukjent organisatorisk begrep i Forsvaret. Det antas at man her sikter til FLO/IKT eller til INI, men dette er uklart.

Høringsutkastet avklarer usikkerheten rundt begrepet "virksomhetens leder" og fastslår at Forsvarssjefen er virksomhetens leder i Sikkerhetslovens forstand. Dette er en nødvendig og god avklaring som er avgjørende for en god sikkerhetstjeneste i Forsvaret. Betydningen av begrepet virksomhetens leder er ikke gjennomgående gjenspeilet i forslaget til instruks da det fremkommer en del inkonsistens i forhold til ansvarsbeskrivelser.

I det etterfølgende er hver enkelt paragraf kommentert der det er relevant. Noen ganger har det vært formålstjenlig å kommentere konkret, mens andre steder i dokumentet har forståelsen for paragrafen vært uklar slik at det er kommentert på et generelt grunnlag.

§ 1. Formål og virkeområde

Instruksen medfører ingen endringer i forholdet mellom NSM og Forsvarets virksomhet innen forebyggende sikkerhetstjeneste. Herunder medfører instruksen ingen endringer i virksomhetenes rapporteringsplikt til NSM i medhold av sikkerhetsloven med forskrifter. Forsvaret er å anse som én virksomhet i instruksens forstand.

Andre avsnitt bør endres til: Forsvaret er i denne instruksen å betrakte som en virksomhet, og Forsvarssjefen er virksomhetens leder. Herunder medfører instruksen ingen endring i virksomhetens rapportering til NSM.

Begrunnelse: Avsnittet er selvmotsigende samtidig som det innebærer at hver enkelt FDUS/EDUS skal rapportere sikkerhetstruende hendelser direkte til NSM og ikke til FSJ. Dette vil medføre at FSJ ikke gis grunnlag til å drive risikohåndtering i Forsvaret, som han ift Sikkerhetsloven er pålagt.

Forsvaret er å anse som en virksomhet, hvorav FOST er sikkerhetsmyndighet og har rapporteringsplikt til NSM. Forsvarets avdelinger er ikke egne virksomheter og har derfor ikke direkte rapporteringsplikt til NSM. Rapportering skal gå tjenestevei internt i Forsvaret til FOST og videre til NSM i henhold til gjeldende lover og bestemmelser.

§ 2. Definisjoner

Med "FSA" menes i instruksen her Forsvarets sikkerhetsavdeling.

I høringsutkastet har man endret navnet fra FOST til FSA. Forsvaret viser til skriv fra Forsvarsdepartementet av 20. okt 2008 vedrørende navneendring fra FSA til FOST. FD legger i nevnte skriv vekt på " FD er enig i at dagens navn - Forsvarets sikkerhetsavdeling (FSA) - ikke fullt ut er dekkende for sikkerhetstjenestens funksjon og rolle i Forsvaret, og at navnet derfor bør

endres på en måte som understreker at tjenesten er Forsvarets øverste fagmyndighet på området i etaten".

Dersom navnet igjen skal endres må det begrunnes og redegjøres for skriftlig. FD må altså gå tilbake på det grunnlaget/begrunnelsen de tidligere la til grunn for at FSA skulle bli en tjeneste. Det forbindes tilsynelatende heft med det nåværende navnet FOST. En navnendring tilbake til FSA tolkes derimot som en irettesettelse og mistillit til organisasjonen. På nåværende tidspunkt er denne mistilliten urettmessig og basert på feilaktige opplysninger. Navnendring tilbake til FSA vil trolig gjøre det vanskeligere for FOST å gjenoppbygge tillit, og igjen medføre at FOST blir mindre relevant som myndighet og aktør innenfor sikkerhetstjenesten i Forsvaret.

Forslag:
Navnet på organisasjonen bør være resultatet av en ny og ryddig prosess som bidrar til å gjenskape tillit til organisasjonen. Navnet bør derfor være noe nytt, for eksempel Forsvarets sikkerhetsmyndighet.

Femte avsnitt Med "militær kontra etterretning" menes.... bør endre til: *Med militær kontra etterretning menes i denne instruksen; "de aktiviteter som omfatter identifisering og tiltak mot de trusler mot sikkerheten som representeres av fremmed etterretningstjeneste, organisasjoner eller ved enkeltpersoner som er involvert i terrorisme, spionasje, sabotasje, subversjon og organisert kriminalitet (TESSOC)".*

Begrunnelse: NATOs definisjon iht ACO Directive 65-3, som Norge har ratifisert, bør benyttes samt at norske ord må benyttes helt ut i definisjonen i denne instruksen.

Computer Network Defence (CND) er et av tre elementer i Computer Network Operations (CNO). Definisjonene er hentet fra NATOs Allied Joint Publication 3.10

"CND is action taken to protect against disruption, denial, degradation or destruction of information resident in computers and computer networks or the computers and networks themselves."

CND er alle tiltak for å beskytte informasjonen i IT-systemene. Dette innbefatter eksempelvis alt fra fysisk sikring, autorisasjon og klarering til kryptering og tekniske implementeringer.

§ 3. Organisering og utøvelse av forebyggende sikkerhetstjeneste i Forsvaret

Enhver militær sjef plikter innenfor eget ansvarsområde og rammen av gjeldende regelverk [å]....overholde de øvrige plikter som følger av forskrift 29. juni 2001 nr. 73 om sikkerhetsadministrasjon, herunder [å] rapportere direkte til NSM. Militær sjef kan ikke overlate dette ansvaret til FSA eller andre,....

Ref kommentar § 1. Militære sjefer representerer ikke egne virksomheter, og skal derfor ikke rapportere direkte til NSM. FOST har på vegne av FSJ det overordnede ansvaret for sikkerheten i Forsvaret og skal på vegne av virksomheten rapportere til NSM i henhold til gjeldende bestemmelser.

Formuleringen kan dessuten feiltolkes dit hen at FOST er pliktig til å rapportere ALLE sikkerhetstruende hendelser/virksomhet til NSM. Dette vil i så fall innebære langt strengere føringer for rapportering til NSM en sikkerhetsloven tar høyde for.

I henhold til forskrift om sikkerhetsadministrasjon skal virksomheter rapportere til NSM:

1. § 5-2 Ved kompromittering av informasjon gradert konfidensielt eller høyere.
2. § 5-6 Dersom det oppdages sikkerhetstruende hendelser eller sikkerhetsbrudd vedrørende informasjon sikkerhetsgradert av utenlandske myndigheter eller internasjonale organisasjoner.

3. §5-7 Ved politianmeldelse av sikkerhetstruende hendelser
4. §5-8 Særbestemmelser for kryptosikkerhet.
    a. §7-7 I tilfeller av fjerning eller uautorisert fravær av krypto forvalter eller stedfortreder.
    b. Virksomheter som mottar kryptomateriell direkte fra NSM skal kontrollere beholdningen og sende beholdningsrapport til NSM.
    c. Rapporter som gjelder nasjonalt kryptomateriell skal sendes til NSM.

Dersom alle militære sjefer skal rapportere direkte til NSM er det trolig at kvaliteten på Forsvarets innrapportering til NSM vil lide under mangel på systematisering, integrering og en helhetlig analyse.

At militære sjefer skal rapportere alt til flere instanser vil medføre at et allerede komplekst rapporteringsregime blir mer komplekst. Dette vil resultere i at informasjonsflyten blir vesentlig dårligere. Konsekvensen kan bli at risikobildet i Forsvaret blir mangelfullt og at hverken FOST eller NSM sitter med det totale risikobildet for Forsvaret og at risikostyringen i Forsvaret blir skadelidende.

Et mer komplekst rapporteringsregime kan dessuten medføre forvirring i forhold til ansvar- og rollefordeling og hvem som gjør hva i forhold til den innrapporterte informasjonen.

§ 4. FSA

FSA skal rapportere til NSM om endringer i sikkerhetstilstanden i Forsvaret.

Endres til: *FOST skal rapportere til NSM i henhold til sikkerhetsloven med forskrifter.*

Begrunnelse: Innrapporteringen til NSM ut over det lovpålagte krav bør ikke bli beskrevet i dette dokumentet, men i en egen samarbeidsavtale mellom organisasjonene.

I samarbeidsavtalen bør rapporteringsforholdet mellom FOST og NSM presiseres slik at det oppstår en forventningsavklaring både hos FOST og NSM på hva det skal rapporteres på, og hvor ofte det skal skje. Uavklarte forventninger til innrapportering kan medføre unødig støy og mangel på forutsigbarhet som igjen kan medføre at planlegging og gjennomføring av innrapportering blir mangelfull.

Tillegg i pkt f: ....militær kontra etterretning i NATO (NCIA og NCIR) og i .....)

Begrunnelse: Sjef FOST er som nasjonalt kontaktpunkt for militær kontra etterretning i NATO og i bilaterale samarbeidsforhold ansvarlig for funksjonene NATO Counterintelligence Authority (NCIA) og NATO Counterintelligence Representative (NCIR) som beskrevet i ACO Directive 65-3 som Norge har ratifisert.

§ 5. Foreleggelse og rapportering til Forsvardepartementet

Pkt c. I utkastet lyder "Anskaffelse av nye sensorer/kapasiteter"; dette synes å være svært unødvendig å ha med i en slik instruks, all den tid alle materiellanskaffelser gjøres gjennom FD på prosjektbasis. Siste setning er også upresist formulert, derfor en den endret. Paragraf 5 kan derfor lyde som følger:

FSJ skal forelegge følgende saker for Forsvardepartementet:

a. Etablering av samarbeid og avtaler med utenlandske aktører

b. Saker av særlig viktighet eller prinsipiell karakter

FSJ skal holde departementet orientert om relevante endringer i sikkerhetstilstanden i Forsvaret.

FSJ fastsetter interne rapporteringsrutiner i Forsvaret, oppover, nedover og sideordnet.

§ 7. Sikkerhetsforum

Forsvaret ser det som vanskelig å kommentere denne paragrafen, all den tid mandatet for et slikt forum er en del av grunnlaget.

§ 8. Tilsynsutvalget for FSA (TFF)

TFF etableres for å styrke departementets tilsyn med FSA,....

§ 8 bør strykes

Begrunnelse: Etterforskningen av FOST saken fastslår at FOST ikke har forbrutt seg på gjeldende regelverk. Derfor vil grunnlaget for å etablere enda et kontrollregime for FOST - "Tilsynsutvalget for FSA" (TFF) – falle på sin egen urimelighet og dessuten være grunnløst og unødvendig.

Klare rammer for utøvelsen av sikkerhetstjeneste i Forsvaret, eksisterende kontrollregime og evt ansettelse av en personvernrådgiver/juridisk rådgiver burde være tilstrekkelig for å sikre en legitim og effektiv sikkerhetstjeneste.

Ved å etablere nye tilsynsordninger, er tilsynsapparatet som rettes mot FOST snart like stort og omfattende som FOST-organisasjonen i seg selv. Resultatet er at FOST må bruke uforholdsmessig mye stabskraft for å imøtekomme alle tilsyn og inspeksjoner.

§ 9. Overordnede juridiske rammer

Paragrafen er tilnærmet en repetisjon av sikkerhetsloven. Setningen "Under utførelse av forebyggende sikkerhetstjeneste skal det ikke anvendes metoder som er krenkende for den personlige integritet" er underlig, og nødvendigheten av denne setningen må vurderes.

§ 12. Bistand til politiet og andre sivile offentlige myndigheter

Bistand på norsk territorium til støtte for politiet skal følge bestemmelsene i kgl. res. 28. februar 2003 nr. 220 om Forsvarets bistand til politiet.

I henhold til FOR 2003-02-28 nr 220: Instruks om Forsvarets bistand til politiet, § 2, så gjelder denne instruksen ikke for Den forebyggende sikkerhetstjeneste.

Bistand på norsk territorium til støtte for andre sivile offentlige myndigheter enn politiet skal forelegges Forsvarsdepartementet via kommandovei for avgjørelse.

Forslag: For at den forebyggende sikkerhetstjenesten skal være effektiv i særskilte tilfeller, så bør § 12 også beskrive unntak fra prosedyre og evt alternativ prosedyre.

Begrunnelse: Det er verdt å merke seg at tiltak i forbindelse med den forebyggende sikkerhetstjenesten ofte er tidskritisk. Operasjoner i samarbeid med politiet må i noen tilfeller iverksettes umiddelbart for å forhindre sikkerhetstruende hendelser og virksomhet mot Forsvaret. Ved særskilte tilfeller kan § 12 andre ledd medføre sterke begrensinger for FOST og i verste fall medføre at FOST ikke rekker å iverksette nødvendige tiltak - i samarbeid med politiet - for å forhindre sikkerhetstruende virksomhet mot Forsvaret. Konsekvensene kan være fatale for Forsvaret.

§ 26. Generelle bestemmelser

Sjef FSA er fagmyndighet og utøvende ansvarlig for militær kontra etterretning i Forsvaret.

Innenfor militær kontra etterretning er FSA underlagt Etterretningstjenestens fag- og direktivmyndighet for aktuelle etterretningsdisipliner.

Det tolkes dit hen at FOST kan gjennomføre innhentingsoperasjoner med egne innhentingsressurser innenfor rammene av lov, fag- og direktivmyndighet.

Tillegg til tredje avsnitt: *For å iverksette forebyggende tiltak og beskytte Forsvaret på en effektiv måte, så er FOST avhengig av at PST og E-tjenesten rutinemessig videreformidler vurderinger og varsler om trusler mot Forsvaret til FOST.*

Begrunnelse: FOST gjennomfører kontinuerlige risikovurderinger for Forsvaret. I dagens dynamiske og komplekse trusselbilde kan FOST ikke basere dette på periodiske trusselvurderinger. FOST gjennomfører egen innhenting, herunder åpne kilder, rapporter om sikkerhetstruende hendelser, inspeksjoner, undersøkelser, sårbarheter, Forsvarets kapabiliteter (verdier), bilaterale forbindelser, NATO-kanaler og militær kontra etterretning. Dette, sammen med E-tjenestens og PSTs trusselvurderinger, gir grunnlaget for FOSTs risikovurderinger.

§ 27. Militær kontra etterretning i utenlandsoperasjoner

Første avsnitt bør endres til: *I militære operasjoner i utlandet har FOST et overordnet ansvar for å ivareta nasjonal kontra etterretning, utøve nasjonal militær kontra etterretning og være kontaktpunktet for militær kontra etterretning, innen for rammen av norske nasjonale bestemmelser og operasjonens regelverk, jf. § 11 annet og tredje ledd.*

Tredje avsnitt strykes.

Begrunnelse: Ansvar og oppgaver tillagt sjef FOST, herunder militær kontra etterretning, kan ikke overføres til annen militær sjef.

Sjef Etterretningstjenesten skal ikke ha ansvar for militær kontra etterretning. Dersom sjef E-tjenesten skal overta sjef FOSTs rolle i operasjoner i utlandet, vil dette medføre uklarheter omkring ansvarslinjer og myndighetsforhold, samt bidra til usikkerhet om hvem som er ansvarlig for den militære kontra etterretningen.

Avhengighet av tillatelse fra andre for å utøve eget ansvar svekker sjef FOSTs autoritet og handlingsrom. Militære kontra etterretningsoperasjoner vil alltid være godkjent av FSJ og det bør tilligge FSJ å avgjøre ansvars- og oppgavefordeling i Forsvaret. 2X-strukturen i NATO og nasjonalt vil sikre at ressurser ikke overlappes, at aktivitetene blir koordinert og at innhentet informasjon blir samordnet. Sjef FOST har i dag et naturlig og godt samarbeid med andre allierte og bilaterale militære kontra etterretningstjenester.

§ 28. Militær kontra etterretning i Norge i fredstid

Dette tolkes dit at FOST sin bistand til politiet og et utøvende samarbeid mellom FOST og PST i forbindelse med å utøve tiltak til hensikt å avdekke og hindre ulovlig etterretningsvirksomhet mot Forsvaret og Forsvarets aktiviteter er uproblematisk.

Andre avsnitt bør allikevel endres til: *På norsk territorium i fredstid skal FOST:*

a. Identifisere og kartlegge trusselaktører mot Forsvaret

b. Sammenstille og analysere informasjon om trusler og trusselaktører mot Forsvaret

c. Foreta undersøkelser ved sikkerhetstruende hendelser i og mot Forsvaret

d. Foreta undersøkelser ved sikkerhetstruende hendelser i militær infrastruktur, eid av Forsvaret, hvor FSJ er systemeier

e. Ved øvingsaktivitet og alliert militær trening i Norge beskytte deltagende enheter mot sikkerhetstruende virksomhet (TESSOC)

f. Støtte Forsvarets sjefer og avdelinger med styrkebeskyttelse

g. Briefe og debriefe personell som kan tenkes å bli utsatt for TESSOC-trusler

h. Dele kontra etterretninger som nødvendig med PST, E-tjenesten, NSM og allierte/bilaterale militære sikkerhetstjenester

i. Bidra i gjennomføringen av tiltak for å redusere risiko og sårbarheter i forsvarsstrukturen

j. Være Forsvarets kontaktpunkt mot PST, allierte og bilaterale samarbeidspartnere

k. Være forberedt på å støtte PST ved anmodning

Begrunnelse: Forsvarets kapasiteter er spesialiserte, teknologigavhengige og gjensidig avhengige på tvers av forsvarsgrenene. Forsvarsstrukturen er nå i betydelig grad antallsmessig mindre (manglende redundans) enn tidligere, og den enkelte avdeling og enhet har større slagkraft. Dette tilsier at den konsekvensmessige verdien av hver enkelt avdeling/enhet har økt. Alvorlig sikkerhetstruende aktivitet mot *en* avdeling kan derfor få konsekvenser i hele Forsvarsstrukturen. Liten- eller manglende redundans tilsier at tap av en avdeling eller styrkekomponent medfører betydelige konsekvenser for kampevnen. Dette nødvendiggjør en gjennomgående og mer aktiv sikkerhetstjeneste som kan detektere trusler før de materialiseres.

Som statens maktutøver mot ytre trusler, deltaker i operasjoner utenlands og innehaver av høyteknologi våpen og kompetanse, har Forsvaret høy fokus fra ulike trusselaktører. Det unike interne rapporteringssystemet i Forsvaret medfører at antall potensielle sikkerhetssaker innen TESSOC er høyt.

PST har erfaringsmessig ikke kunnet bruke sine ressurser innledningsvis på Forsvarets saker innen TESSOC. Først når FOST har undersøkt og identifisert en mulig trusselaktør, har PST vist interesse for å tildele ressurser for håndtering av saken. En indikasjon på trusselaktivitet er ikke tilstrekkelig for å åpne en sak for PST. Ved sammenstilling av rapporterte saker og innhentet materiale fra FOST selv, vil imidlertid grunnlaget for at PST kan forfølge saken være bedre. I tillegg har det i flere av sakene der FOST og PST har samarbeidet vært behov for militær kompetanse. Et slikt samarbeid gir derfor synergi mellom PST og FOST.

§ 29. Ansvarsforhold

Sikkerhetsloven beskriver ansvarsforhold for forebyggende sikkerhetstjeneste. Loven m/ forskrifter fordeler ansvar mellom Nasjonal sikkerhetsmyndighet, virksomhetens leder og systemeier. I stort beskriver Sikkerhetsloven krav som må være på plass for systemer som skal behandle sikkerhetsgradert informasjon eller informasjon som må beskyttes spesielt. Sikkerhetslovens krav kan betraktes som en delmengde av CND, og man innfører uklarheter i ansvarsfordelingen ved å bruke begrepet i instruksen.

FSJ selvstendige ansvar for militære operasjoner er ikke beskrevet. Forsvaret skal ha et nært samarbeid med NSM, men FSJ har ansvaret for militære operasjoner og må fortløpende forvalte risiko i militære operasjoner. NSM bør ha tilgang til informasjon fra nettverksovervåkingen, men

ikke inngå som beslutningstager i en militær operasjon ledet av FSJ. FOST skal ha gode grensesnitt med NSM/NorCERT for løpende og gjensidig informasjonsutveksling.
Grunnlaget for sikkerhetstjenestens operative fokus er beskrevet i flere NATO dokumenter (1234) Disse NATO dokumentene integrerer OPSEC, CND, EMSEC og Force Protection (FP) i militær planlegging og gjennomføring av operasjoner. Det er den militære sjefens ansvar å ivareta dette. Det er derfor viktig at instruksen for militær sikkerhetstjeneste utvikles innenfor rammene av NATO doktriner i tillegg til norsk lov.

§ 30. Ansvaret for CND i Forsvaret

FSJ er i kraft av virksomhetens leder ansvarlig for forebyggende sikkerhet i Forsvaret. FOST er på FSJ vegne virksomhetens leder og er ansvarlig for at krav i lov og forskrift blir fulgt.

Denne paragrafen er ikke tilstrekkelig gjennomarbeidet. Her er det flere forhold som i beste fall er uklar i forhold til kravene i lov og forskrift. Man innfører nye begreper i forhold til lovverket og styrer FSJ på et uhensiktsmessig detaljnivå.

Eksempelvis er det sannsynligvis lovbrudd å legge ansvaret for konfidensialitet, integritet og tilgjengelighet til "driftsavdelingen". Dette er åpenbart et ansvar som tilligger systemeieren, og at sikkerhetssjefen i Forsvaret forvalter restrisikoen i systemene på vegne av systemeieren.

Paragrafen beskriver overføring av ansvaret for sikkerhetsmessig nettverksovervåking fra FOST til "driftsenheten".

Overvåkning av drift og sikkerhet bør være skilt fra hverandre slik at ikke samme organisasjonsledd har ansvaret for begge deler. Dette er i henhold til best practice innenfor overvåkning og kontroll. Det bør være to separate overvåkningssenter hvor ett tar for seg overvåkning av drift og vedlikehold, mens et annet tar for seg sikkerhetsmessig overvåkning.

Trusselaktører, innsideproblematikk og kontroll med tjenesten
Forsvarets kritiske infrastruktur er utsatt for trusselaktører. Trusselaktører benytter forskjellige angrepsvektorer inn i infrastrukturen for å skaffe seg informasjon, manipulere informasjon eller gjøre informasjonstjenestene utilgjengelige. Angrepsvektorene kan være direkte gjennom internett eller indirekte ved å skaffe seg fysisk tilgang til nettverket, f eks ved hjelp av hjelpere på innsiden (innsidere/utro tjenere).

I forslaget til ny instruks ønsker FD å overføre utførelsen av nettverksovervåkingen til "driftsavdelingen". FOST sin oppgave er i følge utkastet å føre kontroll med denne funksjonen. Ved å legge nettverksovervåkingen til driftsenheten vil denne kontrolltjenesten bli lagt til samme organisasjonsledd som har et stort antall driftspersonell/systemadministratorer med utvidete rettigheter i systemene. Forsvaret mener dette er en uheldig løsning da systemadministratorer og nettverksovervåking er plassert i samme organisasjon.
FOST er definert som et inspeksjonsobjekt av EOS-utvalget. NSM fører i dag tilsyn med FOST - og FD gjennomfører inspeksjoner. Videre er FOST underlagt internkontroll av FST. Dette er kontrollfunksjoner som fullt ut er i stand til å ivareta kontroll med tjenesten.

---

[1] Allied Joint Doctrine AJP-01© spesielt pkt 0408

[2] Allied Doctrine for Joint Operations AJP-3(A), spesielt pkt 0133 og 0134

[3] Guidelines for Operational Planning (GOP) spesielt pkt 3-10

[4] Allied Joint Doctrine for Information Operations AJP 3.10, spesielt pkt 0123, 0124, 0129 og Annex 2a

Nettverksovervåkingen som FOST gjennomfører i dag er underlagt god kontroll, og den foreslåtte ansvarsfordelingen gir ikke bedre kontroll med nettverksovervåkningen.

Sikkerhetsetterretninger bør komme fra flere kilder og sensordisipliner. Dette har da naturligvis konsekvenser også for arbeidet med å drive kontra etterretning. CND bidrar til flerkildeinnhenting og økt kvalitet på etterretninger.
Ulike sensorer og forsvarsmekanismer som er en del av kontra etterretningen og det generelle sikkerhetsarbeidet i Forsvaret bør naturligvis være integrert i en og samme organisasjon for å sikre en effektiv utnyttelse av kapasiteter og en helhetlig forvaltning av risikobildet og styring av sikkerhetsarbeidet i Forsvaret. CND bør være underlagt samme sjef som kontra etterretning. I motsatt fall er det en fare for at både kontra etterretning og CND mister deler av sitt potensial som følge av at disse opptrer isolert fra hverandre. Sikkerhetsetterretninger som indikerer trussel mot rikets sikkerhet skal utveksles med PST og E-tjenesten (og NSM). Denne informasjonsutvekslingen utføres av FOST som har grensesnitt mot de hemmelige tjenestene. Dette taler for at nettverksovervåkingen må utføres av FOST. Det er ikke hensiktsmssig at driftsavdelingen oppretter grensesnitt mot de hemmelige tjenestene.

En endring av ansvarsfordelingen for nettverksovervåking som foreslått i instruksen vil forringe kvaliteten på sikkerhetsbildet (risikobildet) som FOST forvalter på vegne av FSJ, og det vil ikke styrke kontrollen med tjenestens nettverksovervåking.

Kosteffektiv tjeneste, økonomi og praktiske utfordringer
FOST er i dag pålagt oppdraget med døgnkontinuerlig nettverksovervåking av systemene. FOST har hentet ut betydelige synergier mellom driften av Forsvarets alarmsentral (FAS) og nettverksovervåking. Denne felles alarmsentralen bemannes med personell trent til å håndtere begge funksjoner. En overføring av nettverksovervåkingen fra FOST til "driftsenheten" vil følgelig medføre betydelige personell- og infrastrukturkostnader.
FOST har i dag bygd opp en betydelig kompetanse innenfor informasjonssikkerhet på Jørstadmoen. I tillegg til kompetanse på nettverksovervåking innehar dette personellet en betydelig stabskompetanse på mastergradsnivå. En overføring av personellet til "driftsenheten" gjør at FOST mister stabskraft innenfor fagområdet informasjonssikkerhet.
Det er i instruksen også lagt opp til splitting av fagmiljøer ved at FOST skal ha igjen kompetanse på Computer Forensics (CF), Opsec og Emsec. Dette er kompetansekrevende fagområder som vanskelig kan trenes til akseptabel standard uten et minimum av personell som danner et fagmiljø. Det er en forhøyet risiko for at et slikt kompetansemiljø vil bli for lite og vil forringes ved oppsplitting av nettverksovervåking og øvrig kompetansemiljø.
I tillegg vil en overføring medføre oppbygging av et konkurrerende miljø innen informasjonssikkerhet i driftsenheten. Fagmiljøene innen informasjonssikkerhet er små og sårbare, og en oppsplitting vil følgelig desimere den faglige kraften.

Ansvaret for nettverksovervåking i Forsvaret må ligge i FOST. Dette sikrer at grensesnittet mellom NSM og FOST for nettverksovervåking blir best mulig ivaretatt.

Det er derfor formålstjenlig at sikkerhetsmessig nettverksovervåking forblir i kompetansemiljøet for sikkerhet i FOST.

§ 31. Samarbeid mellom NSM og Forsvaret

Den foreslåtte teksten gir overhodet ingen avklaring av ansvarsområdene og bidrar til uklare linjer mellom sivil etat (NSM) og Forsvaret.
Dersom denne paragrafen skal beholdes må det defineres hva slags myndighet og ansvarsområder hhv NSM og FSA har. Disse rollene er langt på vei beskrevet i Sikkerhetsloven med forskrifter.

§ 32. Beredskap
Det er uklart hva denne paragrafen gir av merverdi i forhold til FSJ sikkerhetstjeneste. Dette må fremgå for at paragrafen skal ha mening.

Konklusjon

Utkastet til ny instruks om sikkerhetstjeneste i Forsvaret beskriver oppgaver og ansvar på detaljnivå i Forsvarets organisasjon og begrenser FSJ evne og handlingsrom til å organisere sikkerhetsarbeidet effektivt og hensiktsmessig. Samlet innebærer utkastet i nåværende form en begrensning i FOST sin evne til å beskytte Forsvarets kapabiliteter på vegne av Forsvarssjefen.

Et eventuelt nytt navn på FOST bør være resultat av en ny og ryddig prosess som bidrar til å gjenskape tillit til organisasjonen.

Det er avgjørende at sikkerhetsmessig nettverksovervåking forblir i kompetansemiljøet for sikkerhet i FOST.

FORSVARET
Informasjons- og kommunikasjonstjenester

Vår saksbehandler
Petter Christensen, pchristensen@mil.no
+4767 86 20 06, 0515 2006
IKT/LED/STAB

Vår dato 2009-12-10

Vår referanse 2009/019659-020/FORSVARET/ 005

Tidligere dato

Tidligere referanse

Til
Forsvarets Sikkerhetstjeneste

Kopi til
Forsvarets Logistikkorganisasjon
Forsvarsstaben

HØRING - UTKAST TIL INSTRUKS OM SIKKERHETSTJENESTE I FORSVARET - MERKNADER FRA FLO/IKT

1 Bakgrunn

FLO/IKT viser til skriv av 2. oktober 2009 fra Det kongelige Forsvarsdepartement, HØRING – UTKAST TIL INSTRUKS OM SIKKERHETSTJENESTE I FORSVARET.

Her følger våre merknader.

2 Drøfting

2.1 Generelt

FLO/IKT er opptatt av at sikkerhetstjenesten i Forsvaret gjennom sin adferd og sin organisering skaper tillit og tiltro internt så vel som eksternt. Dette setter store krav til aktørene og hvorledes disse løser sine oppgaver.

FLO/IKT har over lengre tid påpekt viktigheten av dette og behovet for en klargjøring av utøvelsen av sikkerhetstjenesten i Forsvaret, spesielt innen området informasjonssikkerhet. *Utkast til Instruks om sikkerhetstjeneste i Forsvaret* er et godt bidrag til dette.

2.2 Merknader til det enkelte kapittel

2.2.1 Kapittel 1, 3, 4 og 5

Ingen merknader

2.2.2 Kapitel 2

Begrepet *Enhver militær sjef* bør endres til *Enhver sjef*. Dette vil omfatte Forsvarsjefens direkte underlagte sjefer (FDUS) og BRA sjefer[1], uavhengig av om de er sivilt eller militært ansatt.

Presiseringen av FSA som sentral stabsfunksjon med overordnet ansvar for forebyggende sikkerhetstjeneste i Forsvaret er klargjørende. Dette gjør det lettere for enheter i og utenfor Forsvaret å forholde seg til FSA samtidig som det er stilt strenge krav til faglig kompetanse, notoritet og internkontroll i enheten, jevnfør § 4. Kravet vil bidra til økt sporbarhet og kvalitetssikring av forebyggende sikkerhetstjeneste i Forsvaret.

[1] Ref Direktiv for virksomhets- og økonomistyring

Med henvisning til §5, 1. ledd, bokstav C anbefaler FLO/IKT at begrepene *sensorer/kapasiteter* presiseres og begrenses til virkeområdet til instruksen.

2.2.3 Kapittel 6

FLO/IKT ser det som riktig at departementet bruker et eget kapittel om IKT-sikkerhet i forsvarssektoren. Selv om *IKT sikkerhet* ikke er et entydig begrep i Forsvaret (lov og forskrift bruker begrepet informasjonssikkerhet) så berører dette alle både i og utenfor Forsvaret.

Innen CND er det spesielt viktig å skille mellom rollen til FSA med overordnet ansvar for forebyggende sikkerhetstjeneste i Forsvaret, systemforvalter med ansvar for de tekniske løsninger og systemer som benyttes og IKT driftsorganisasjonene med ansvar for daglig drift av systemene i h. t. de bestemmelser som er fastsatt av systemforvalter, FSA og NSM. Dette er i tråd med prinsipper og føringer som fremgår av Direktiv for materiellforvaltning i Forsvaret med underliggende bestemmelser. Det er her viktig å merke seg at Forsvaret har én systemforvalter, FLO, mens det er flere IKT driftsorganisasjoner som INI, LOS DVU og Sambandsbataljonen i brigaden.

FLO/IKT anbefaler at det helhetlige ansvar for totalsikkerheten i systemene legges til systemforvalteren og at driftorganisasjonene får ansvaret for daglig drift og håndtering av sikkerhetstruende hendelser.

FLO/IKT foreslår derfor følgende endringer i § 30:

FSA har:

a. *overordnet ansvar for informasjonssikkerhet i Forsvaret*
b. *overordnet ansvar for håndtering av sikkerhetstruende hendelser*

Systemforvalter har:

a. *ansvar for systemets sikkerhetsarkitektur og nødvendig konfigurasjonssyring av denne, herunder at kravene til informasjonssystemsikkerhet etterleves*
b. *ansvar for å utgi regelverk nødvendig for forsvarlig forvaltning, drift og vedlikehold av systemet i dets levetid, kontrollere at disse etterleves og påpeke avvik.*

IKT-driftsorganisasjonene har:

a. *ansvar for daglig drift og vedlikehold av systemene, herunder sikkerhetsmessig overvåking og håndtering av sikkerhetstruende hendelser (insident)*
b. *ansvar for rapportering av sikkerhetsmessige feil og mangler til systemforvalter, herunder behov for tekniske endringer (change)*

FLO/IKT anbefaler at *Forsvarets senter for beskyttelse av kritisk infrastruktur* (FSKI) beholdes samlet som et fagmiljø som på overordnet nivå og i forlengelsen av NorCERT utvikles videre til et norsk MILCERT.

3 Konklusjon

FLO/IKT imøteser ny *Instruks om sikkerhetstjeneste i Forsvaret*. FLO/IKT anbefaler at instruksens kapittel 2 og 6 justeres i samsvar med merknader som fremkommer av dette skriv.

Elisabeth Natvig
Flaggkommandør
Sjef FLO IKT