Sändlista

Ert tjänsteställe, handläggare	Ert datum	Er beteckning
Justitiedepartementet, Maria Pereswetoff-Morath	2017-03-15	Ju2017/02347/SSK

Vårt tjänsteställe, handläggare
LEDS CIO, Leif Östgaard, 08-788 75 00, leif.ostgaard@mil.se

Vårt föregående datum

Vår föregående beteckning

Svar före

Försvarsmaktens svar på remiss av promemorian Kommunikation för vår gemensamma säkerhet (Ds. 2017:7)

Sammanfattning och slutsatser

Försvarsmakten instämmer i att det finns ett behov av ett förbättrat ledningsstödsystem för aktörer inom allmän ordning, säkerhet, hälsa och i huvudsak för aktörer i det civila försvaret, och att den lösning som väljs bör säkerställa en tillräcklig statlig kontroll och rådighet över systemet.

Försvarsmakten noterar att utredningen avgränsat användarkretsens omfattning på samma sätt som den tidigare Rakelutredningen. Det innebär att de ytterligare behov som Försvarsmakten och andra aktörer inom totalförsvaret kan ha att kunna utbyta bl.a. uppgifter som innehåller försvarssekretess, sekretess som rör rikets säkerhet, inte omfattas av uppdraget och de förslag som utredningen lämnar. Den föreslagna lösningen kan därmed, enligt Försvarsmaktens bedömning i detta remissvar, utgöra ett tillräckligt ledningsstödsystem för det civila försvaret. Försvarsmakten avråder från utveckling av en systemlösning som ska kunna hantera utbyte av information med en hög grad av sekretess, inklusive försvarssekretess. Detta då Försvarsmakten bedömer att det nya systemet med rimliga åtgärder inte kommer att vara tillräckligt motståndskraftigt. En omfattande infrastruktur med eventuella anslutningar mot publika nät, såsom internet, i en kontext med sådant stort antal användare och användningsområden, underlättar cyberangrepp vilket med stor sannolikhet leder till informationsförluster.

Försvarsmakten har redan egna system med erforderlig sekretessnivå, och ett begränsat antal användare, anpassade för myndighetens egna operativa och taktiska behov vid höjd beredskap

och krig. Oavsett vilken sekretessnivå den nya systemlösningen kommer att uppnå behöver Försvarsmakten fortsätta utvecklingen av de egna systemen för att lösa det militära behovet. Därmed bör detta nya system i första hand kravställas utifrån övriga myndigheters och aktörers behov.

Försvarsmakten anser att det är nödvändigt att separera infrastruktur för det militära och civila försvaret så att totalförsvaret behåller redundans och robusthet mot såväl kinetiska vapen såväl som mot elektromagnetisk påverkan och cyberangrepp. Detta innebär att nuvarande inplaceringar i myndighetens infrastruktur kan behöva ses över med hänsyn till operativa behov och ett förändrat omvärldsläge.

Försvarsmakten anser vidare att fortsatt analys av hotbilden krävs så att systemlösningen får ett väl avvägt skydd. Det kan t ex vara aktuellt att förutom föreslagen driftcentral, NOC[1], även inrätta en säkerhetsövervakningsfunktion, SOC[2].

Försvarsmakten ställer sig bakom utredningens förslag om att 700 MHz-bandet används för denna typ av kommunikation, särskilt som det bidrar till att säkerställa Försvarsmaktens nyttjande av myndighetens befintliga system inom nu ianspråktaget utrymme, ca 380-395 MHz, och underlätta möjligheten för Försvarsmakten att kunna ge och ta emot militärt stöd från ett annat land, inklusive i enlighet med samförståndsavtalet mellan Sverige och NATO om tillhandahållande av värdlandsstöd. Denna effekt kan uppstå först när talkommunikation införs i ny systemlösning och Rakel avvecklats. Med tanke på spektrumfrågans betydelse för samhällets säkerhet och försvar menar Försvarsmakten att om tillräckligt spektrum inte kan säkerställas på annat sätt bör lämpliga lagstiftningsåtgärder övervägas.

Försvarsmakten bejakar utredningens förslag om att finansiering av det investeringsbehov som en ny lösning kräver förutsätts ske med stöd av de finansiella resurser MSB och Teracom AB disponerar i kombination med erforderlig lånefinansiering samt att kostnader för drift och underhåll av systemet bör avgiftsfinansieras med abonnemangsavgifter och de intäkter kommersiella operatörers inplaceringar innebär. Försvarsmakten har inte ytterligare granskat schablonberäkningar enligt utredningens bilaga 2 men delar utredningens beskrivning om att det kan finnas en risk för att kostnadsuppskattningar i RFI-svar tenderar att ligga i underkant jämfört med priser som offereras i en formell upphandling.

Försvarsmakten bejakar även utredningens förslag om att aktörer inte ska tvingas använda lösningen och dess funktioner där behov saknas eller skiljer sig åt vilket bör återspeglas i utformningen av abonnemangsavgiften som bör bygga på vilka tjänster som nyttjas.

Försvarsmakten vill poängtera att det inom myndighetens planering inte finns förutsättningar för att inrymma delar av en finansiering avseende utveckling, anskaffning eller vidmakthållande av ett nytt system. Ett införande som kräver två parallella system måste hanteras med en abonnemangskostnad som inte överstiger dagens, alternativt kompenseras. I annat fall kommer införandet att påverka Försvarsmaktens operativa förmåga.

[1] Network operations center
[2] Security operations center

Synpunkter på promemorian

Kapitel 3 Trender i samhälle och omvärld

Försvarsmakten delar uppfattningen att information ska kunna delas med höga krav på robusthet och sekretess [sid 44] men vill i sammanhanget påpeka att det inte innebär att systemen måste klara de särskilda krav som ställs på system som ska hantera försvarssekretess. För system där inte sådana krav ställs kan ökat fokus istället vara på robusthet och tillgänglighet.

Försvarsmakten instämmer i utredningens syn på att PTS behöver öka omfattningen av sitt arbete med totalförsvar och höjd beredskap. [sid 64] Dessa aspekter måste också få ett ökat genomslag i PTS spektrumförvaltning. Om en dedikerad samhällslösning med avsatt spektrum för samhällets säkerhet och försvar inte kan garanteras inom ramen för nuvarande lagstiftning bör dessutom lämpliga lagstiftningsåtgärder övervägas.

Kapitel 4 Användarkrets för säker mobil kommunikationslösning

Försvarsmakten delar utredningens bedömning att ingen större förändring av användarkretsen kommer att ske jämfört med Rakelsystemet. [sid 72] Det beror dock på när talkommunikation införs som funktionalitet. Försvarsmakten har enbart behov av talkommunikation för sina samverkansbehov i den föreslagna lösningen. Intill talkommunikation införs får Försvarsmakten liten användning av det nya systemet. Försvarsmakten bedömer att andra aktörer ger uttryck för behov av datakommunikation i detta system.

Kapitel 5 Aktörernas behov – krav som kan ställas

Försvarsmakten delar utredningens bedömning att kommunikationslösningen relativt snart bör omfatta talkommunikation. [sid 83] Införandet av talkommunikation gör att Rakelsystemet kan avvecklas varvid både infrastruktur och spektrum frigörs på ett sätt som stärker det militära försvaret samtidigt som antalet olika utrustningar som skall medföras minimeras.

Försvarsmakten delar även utredningens konstaterande att täckning och kapacitet i delar av landet måste kompletteras av rörliga resurser. Detta bedöms realistiskt för avlägsna platser eller där det är låg sannolikhet att samband behövs i större omfattning, men att kostnaden och hur dessa resurser ska hanteras behöver utredas vidare i sammanhanget.

Försvarsmakten vill särskilt understryka utredningens påpekande om att en utvidgad användarkrets och möjlig exponering mot internet talar emot användning där man hanterar försvarssekretess. [sid 91] Detta påpekande styrks även av de beskrivna behoven att erbjuda kopplingar till allmänna nät och tjänster [sid 92] samt interoperabilitet. Ett antagonistiskt angrepp kan ske på flera sätt varvid elektromagnetiska verkansmedel[3] och sofistikerade cyberattacker är två sätt, utöver kinetisk verkan, som kan påverka informationsinfrastrukturen på ett negativt sätt. Försvarsmakten avråder därför från utveckling av en systemlösning där

[3] Syftar på att antagonist via radio kan avlyssna trafik samt störa i syfte att förhindra kommunikation.

målsättningen är att hantera försvarssekretess. Rimliga åtgärder bedöms inte ge tillräcklig motståndskraft för att skydda den typen av sekretess. Försvarsmakten kan och bör därför vid särskilda fall även fortsatt tillhandahålla system avsedda för hantering av sekretess med hänsyn till rikets säkerhet. Vid behov inom det civila försvaret att hantera försvarssekretess bör ett för behovet anpassat system användas och eventuellt utvecklas.

Försvarsmakten delar utredningens uppfattning om att skälig regional autonomitet ska kunna upprätthållas och föreslår i linje med utredningen att indelning och prioritering av regioner görs i samverkan med Försvarsmakten inom ramen för totalförsvarsplaneringen. [sid 93]

Kapitel 7 Tekniska utgångspunkter

Försvarsmakten vill även understryka utredningens ställningstagande att den offentliga infrastruktur som ska användas ska vara lämplig [sid 127]. Försvarsmakten delar även utredningens bedömning att samlad kunskap är säkerhetskritisk och att information om infrastrukturen inte ska vara överdrivet öppen. [sid 167] Vid bedömning av lämplighet anser Försvarsmakten att det är nödvändigt att separera infrastruktur för det militära och civila försvaret för att ge totalförsvaret redundans och robusthet. Skälen för detta är att en antagonist som angriper på ovan beskrivet vis, alternativt en teknisk felfunktion, slår ut hela, eller delar av både det civila och det militära försvarets informationsinfrastruktur samtidigt. Med separata nät kan det militära försvaret ges full handlingsfrihet att lösa sina operativa uppgifter samtidigt som folkrättsliga aspekter beaktas.[4] Detta gäller således även för skyddade utrymmen och transmission för både kärnnät [sid 133] och stamnät [sid 135] och påverkar beslut om samlokalisering eller att ge andra aktörer tillträde [sid 140].

Försvarsmakten vill också, utifrån utredningens beskrivning av särskild funktionalitet för att uppnå högre säkerhetskrav, peka på det problematiska med att innehålla högre sekretess i nät där internetanslutningar och andra anslutningar till publika nät finns. [sid 137, 164] En anslutning till exempelvis internet medför en attackvektor för cyberangrepp som ger många aktörer inklusive statsaktörer möjlighet att attackera informationsinfrastrukturen för att störa funktionen och tillgänglighet i näten. Den ger även möjlighet att stjäla och överföra information till angriparen. Detta är även kopplat till synpunkterna på kapitel 4 och kapitel 8.

Kapitel 8 Utredningens förslag till kommunikationslösning

Försvarsmakten ställer sig bakom utredningens förslag om att 2x10 MHz ska avdelas i 700 MHz-bandet men föreslår därutöver att ytterligare 2x5 MHz ska avsättas samtidigt för att säkerställa talfunktionalitet. [sid 173, 181] Detta underlättar en framtida realisering av talfunktionalitet samt möjligheter till avveckling av Rakel.

Försvarsmakten ställer sig bakom och vill särskilt understryka vikten av utredningens påpekande om att Rakels frekvenser, ca 380-395 MHz, därmed görs tillgängliga för militär användning. [sid 182] Det bidrar till att säkerställa Försvarsmaktens nyttjande av

[4] Enligt den folkrättsliga distinktionsprincipen bör militär egendom (militära mål) så långt möjligt hållas åtskilda från civil egendom.

myndighetens befintliga system inom nu ianspråktaget frekvensutrymme samt bland annat det ytterligare behov av spektrum som verksamhet kopplat till möjligheten att ge och ta emot militärt stöd från ett annat land, inklusive i enlighet med samförståndsavtalet mellan Sverige och NATO om tillhandahållande av värdlandsstöd.

Försvarsmakten vill poängtera att nuvarande inplaceringar i myndighetens infrastruktur kan behöva överses med hänsyn till operativa behov och ett förändrat omvärldsläge. [sid 176] Skälen för detta är angivna ovan och syftar ytterst till att säkerställa att Försvarsmakten har full handlingsfrihet och operativ förmåga att försvara Sverige.

Försvarsmakten bejakar utredningens förslag om att aktörer inte ska tvingas använda lösningen och dess funktioner där behov saknas eller skiljer sig åt. [sid 177] Försvarsmaktens behov utgörs exempelvis av talkommunikation vid samverkan med det civila försvaret via denna mobila systemlösning, medan andra aktörer bedöms ha andra behov. När Försvarsmakten har behov av att dela information med försvarssekretess har Försvarsmakten system för detta. Intill att talkommunikation införs ser därför Försvarsmakten inget eget behov av att använda den nya systemlösningen.

Försvarsmakten delar utredningens bedömning att det krävs mer analys avseende bland annat känslighet och krav. [sid 187] I det fortsatta arbetet ser Försvarsmakten att informationssäkerhetsaspekter, med djupare analys avseende cyberhot, måste ingå som en grundförutsättning varvid behov av konfidentialitet/sekretess läggs på realistisk nivå. Lösningen bör även balansera åtgärder för robusthet för kärnnät och radioaccessnät. Syftet är att inte utvecklingen blir alltför kostnadsdrivande eller riskera en systemlösning som inte går att realisera. En antagonist kan exempelvis förutsättas ha kapacitet att förbigå eventuell kryptering vid ett långvarigt angrepp genom att infiltrera de tekniska systemen vilket ytterligare talar emot hantering av försvarssekretess. Detta arbete bör ske utifrån ett riskbaserat perspektiv med beaktande av att det parallellt bör genomföras en kontinuitetsplanering för de viktigaste verksamheterna. För att försvåra för en antagonist samt säkerställa hög tillgänglighet och robusthet bör det även finnas en säkerhetsövervakningsfunktion, SOC, i systemlösningen.

Kapitel 9 Kostnader och finansiering

Försvarsmakten ställer sig bakom utredningens förslag om att finansiering av det investeringsbehov som en ny lösning kräver förutsätts ske med stöd av de finansiella resurser MSB och Teracom AB disponerar i kombination med erforderlig lånefinansiering samt att kostnader för drift och underhåll av systemet bör avgiftsfinansieras med abonnemangsavgifter och de intäkter kommersiella operatörers inplaceringar innebär. [sid 193]

Under den valda lösningens inledande fas kan dubblering av abonnemang för tal- och datatjänster visa sig nödvändigt. [sid 193] Försvarsmakten delar utredningens beskrivning om att den period som behöver överbryggas innan nuvarande Rakel och kommersiellt upphandlade tjänster kan ersättas med ny lösning kan hanteras genom anpassade abonnemangskostnader för lösningen. [sid 205] Försvarsmakten förordar att så sker i syfte att inte menligt påverka Försvarsmaktens operativa förmåga.

Försvarsmakten delar utredningens beskrivning om att det kan finnas en risk för att kostnadsuppskattningar i RFI-svar tenderar att ligga i underkant jämfört med priser som offereras i en formell upphandling. [sid 194] Detta bör tas i beaktande vid fastställande av investeringens ekonomiska nivå. I övrigt har Försvarsmakten inte ytterligare granskat beräkningar i utredningens bilaga 2.

Utredningen anger att det för vissa aktörer/verksamheter kommer att erfordras kompletterande tjänster och skyddsnivåer, bland annat med avseende på krypteringsskydd, och att dessa kostnader ligger utöver den baskostnad som åsätts grundabonnemang. [sid 203] Försvarsmakten konstaterar att det för att nå högre kompletterande skyddsnivåer och försvarssekretess krävs omfattande investeringar i ett nytt system. Antalet aktörer och deras behov av dessa skyddsnivåer bedöms begränsat jämfört med behoven av en ersättare till Rakel. Försvarsmakten fortsätter därför utvecklingen av den egna infrastrukturen och ser en lösning som precis som idag bygger på att de aktörer som Försvarsmakten behöver dela försvarssekretess med ges tillgång till Försvarsmaktens system.

Utredningens förslag till kommunikationslösning bygger på möjligheter till ömsesidig inplacering av radioutrustning i statligt respektive kommersiellt ägd infrastruktur. [sid 203] Försvarsmakten vill återigen poängtera att inplacering i myndighetens infrastruktur kan behöva överses med hänsyn till Försvarsmaktens operativa behov.

Ärendets beredning

I beredningen av detta ärende har deltagit försvarsjurist Charlotta Viktorin, försvarsjurist och personuppgiftsombud Anna Saarikoski, överstelöjtnant Ola Kero, överstelöjtnant Joakim Kindahl, överste Mats Klintäng, civilingenjör Anna-Lena Berg och generalmajor Fredrik Robertsson.

Detta remissvar har beslutats av generallöjtnant Dennis Gyllensporre. I den slutliga handläggningen har dessutom överste Patrik Ahlgren deltagit och som föredragande kommendörkapten Leif Östgaard.

Dennis Gyllensporre
Chef för Ledningsstaben

Leif Östgaard

Sändlista
Justitiedepartementet

För kännedom
Försvarsdepartementet
Försvarets Materielverk

För kännedom inom HKV
GD
LEDS JUR
LEDS PLANEK
LEDS CIO
LEDS INRI
PROD
INS
INSS J6
MUST
HKV AVD