Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2016-03-15	2015-7213	1.0

En gemensam kommunikationslösning för samhället

Redovisning av regeringsuppdrag om säker och tillgänglig, mobil, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet hälsa samt försvar

Innehållsförteckning

Uppdraget

Myndigheten för samhällsskydd och beredskap (MSB) fick den 17 december 2015 ett regeringsuppdrag om säker och tillgänglig mobil, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar.[1]

Redovisningen inleds med en beskrivning av den kommunikationslösning MSB förordar, bedömda kostnader samt möjlig tidplan för skarp drift för denna. Vidare redovisas förutsättningar och överväganden för säker och tillgänglig mobil IP-baserad kommunikation. I enlighet med regeringsuppdraget redovisas krav och behov av säker och tillgänglig mobil IP-baserad kommunikation, kommunikationslösningar för aktörer inom allmän ordning, säkerhet, hälsa samt försvar och bedömda drifts- och investeringskostnader samt möjlig tidplan för olika alternativ.

Uppdragets genomförande

Regeringsuppdraget har givits till MSB och likalydande till PTS.

Arbetet med detta uppdrag har genomförts i tre delar. MSB har i uppdragets första del redovisat krav och behov av mobil IP-baserad kommunikation. PTS redovisade efter det översiktliga preliminära alternativ för kommunikationslösningar som, enligt PTS, inte tar hänsyn till behovet av säker kommunikation. MSB har sedan, i enlighet med uppdragets tredje del, redovisat bedömda kostnader och möjlig tidplan för skarp drift för de alternativ PTS redogjort för i sin redovisning.

Polismyndigheten och Försvarsmakten har deltagit i arbetet med krav och behov samt i bedömning av kostnader och tidplan för skarp drift. Polismyndigheten och Försvarsmakten har lämnat samråd. PTS har lämnat svar, i samrådet avseende bedömning av kostnader och tidplan för detta, i form av en beslutad promemoria där myndigheten beskriver sina synpunkter. Trafikverket har deltagit genom att lämna synpunkter gällande kommunikationslösning för transportsystemet.

MSB förordar en dedikerad kommunikationslösning

MSB förordar ett dedikerat rikstäckande radionät. Ett dedikerat nät är det lösningsalternativ som lever upp till de krav som aktörer inom allmän ordning, säkerhet, hälsa och försvar ställer. Dessa krav redovisas i avsnittet *Redovisning av krav och behov av säker, tillgänglig, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar*. Det rikstäckande radionätet kan kompletteras med nationella roamingavtal för samverkan i krishantering och för utökad kapacitet.

MSB:s förslag i sin helhet bidrar till såväl behovet av kommunikation för samhällsviktig verksamhet som till att realisera delar av regeringens mål om tillgång till bredband i hela landet. Lösningen skapar goda förutsättningar för likvärdiga samhällsomfattande tjänster i hela Sverige. Den skapar

[1] Regeringsbeslut II:28, 2015-12-17.

förutsättningar för snabb och skalbar användning och samverkan med frivilliga och privata aktörer. Den är kostnadseffektiv eftersom den uppfyller flera av samhällets behov. Den baseras på offentlig kontroll över kommunikationen och innebär att samhället och dess suveränitet kan vidmakthållas även när samhället utsätts för hot och påfrestningar.

För att kunna tillgodose aktörernas omedelbara behov av mobil datakommunikation, förordar MSB att utbyggnad av ett dedikerat nät realiseras stegvis. Det första steget är att etablera ett dedikerat offentligt kontrollerat kärnnät motsvarande PTS lösningsförslag ”Kommersiell lösning med dedikerat kärnnät”.[2] Först när hela det dedikerade rikstäckande radionätet är i skarp drift uppfylls alla krav som aktörer inom allmän ordning, säkerhet, hälsa samt försvar har, men för att tillgodose det omedelbara behovet kan ett dedikerat kärnnät etableras. Det tillgodoser *delar* av grundkraven för kontroll, spårbarhet och säkerhet, men inte kraven på täckning, tillgänglighet, robusthet och särskild funktionalitet. Ett dedikerat kärnnät förutsätter att kapacitet i ett eller flera kommersiella radionät upphandlas. När det dedikerade kärnnätet är etablerat kan aktörerna initiera en övergång från nuvarande kommunikationslösningar till ett delvis offentligt kontrollerat nät. Detta möjliggör för aktörerna att använda mobila bredbandstjänster med högre krav på kontroll, spårbarhet och säkerhet. Utbyggnad av radionätet kan pågå parallellt och bedöms ta 3,5 till 4,5 år. Tid för att genomföra upphandling och för att skapa regulatoriska och finansiella förutsättningar ingår inte i denna bedömda tid.

Den förordade lösningen med ett dedikerat radionät förutsätter att frekvenstilldelning av 2 x 10 MHz inom MFCN-delarna i 700 MHz-bandet[3] genomförs.

Täckning till nytta för samhället

Den dedikerade lösningen kommer att ha täckning och kapacitet i områden där det inte finns kommersiella incitament för utbyggnad och täckning, som även kommer allmänheten till del. MSB:s förordade lösning säkerställer därmed behovet av säker och tillgänglig kommunikation för samhällsviktig verksamhet och kan bidra till möjligheter att realisera delar av målet om tillgång till bredband i hela landet.

Kraven uppfylls och säkerställer samverkan

Aktörer inom allmän ordning, säkerhet, hälsa samt försvar ställer särskilda krav på offentlig kontroll, särskild funktionalitet, prioritet, informationssäkerhet, robusthet, kapacitet och täckning. Dessa krav uppfylls när den kommunikationslösning som förordas av MSB är i skarp drift.

Informationsdelning vid samhällsstörningar sker mellan en mängd olika aktörer (offentliga, privata och frivilliga) med olika krav på sekretess, tillgänglighet och skydd av sin information. De krav som samhällsviktig verksamhet ställer på en kommunikationslösning är mer omfattande än vad som normalt ingår i en kommunikationslösning för kommersiell användning. Kraven som ställs är dimensionerande för utformingen på kommunikationslösningen för samhällsviktig verksamhet, men inte

---

[2] PTS Dnr 15-11722, 2016-02-01.

[3] Mobile/Fixed Communications Networks, 703-733 MHz och 758-788 MHz.

exkluderande vilket innebär att även behov av kommunikation som inte har krav på sekretess kan tillgodoses.

Lösningen måste utifrån varje enskild händelse kunna användas av de aktörer som har uppgifter i olycks- och krishantering. Ett exempel är MSB:s behov att, inom ramen för sitt operativa uppdrag,[4] snabbt och skalbart kunna etablera skyddad och säker kommunikation. Detta även med aktörer som inte omfattas av förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, men som i den aktuella händelsen har en viktig funktion.

Krishantering kräver gränsöverskridande kommunikation. Idag samverkar Sverige i vardag och kris med de nordiska länderna.[5] Kommunikationslösningen ska t.ex. stödja det kommande fördjupade samarbetet mellan svensk polis och polisen i övriga nordiska grannländer. I och med allt mer gränsöverskridande kommunikation med samarbetspartners och aktörer i andra länder, blir det också allt viktigare att säkerställa att skyddsvärden i den information som delas är analyserade, kända och hanterade. Den kommunikationslösning som implementeras i Sverige får därför inte vara unik för Sverige, eftersom Sverige måste kunna hantera operativ samverkan över statsgränser. Norska DNK (Direktoratet for nødkommunikasjon) gör bedömningen att det är viktigt med en gemensam frekvensanvändning i de nordiska länderna i sin redovisning av frekvensbehov för mobil bredbandskommunikation i totalförsvaret, från mars 2016.[6]

Kostnadseffektivitet för samhället

Samhällets digitalisering innebär ett ökat behov av datatjänster för aktörer inom allmän ordning, säkerhet, hälsa samt försvar liksom för allmänheten. Med digitaliseringen kan de tjänster dessa verksamheter ska tillhandahålla till samhället effektiviseras. Avsaknaden av säker tillgänglig mobil IP-baserad kommunikation har inneburit att många verksamheter hamnat i en situation med flera parallella abonnemang och terminaler. Detta är fördyrande och skapar ett ineffektivt arbete för aktörerna.

Att säkerställa kommunikation för samhällsviktig verksamhet är ett offentligt åtagande, liksom att säkerställa tillgång till bredband för hushåll och företag. Det är relevant att jämföra investeringar i IT och digital infrastruktur med investeringar i annan infrastruktur såsom vägar, järnvägar eller elförsörjning. Om förverkligande av målet om tillgång till bredband i hela landet och säkerställandet av säker och tillgänglig mobil IP-baserad kommunikation för samhällsviktig verksamhet samordnas, bidrar det till mervärden för Sverige som helhet.

---

[4] MSB:s operativa uppdrag att MSB ska stärka, samordna och inrikta ansvariga aktörers hantering av allvarliga olyckor, kriser, katastrofer och krig, så att konsekvenserna begränsas.

[5] Haga-deklarationen II som skrevs under vid Nordiskt ministermöte rörande samhällsskydd och beredskap i Stockholm 4 juni 2013.

[6] Svar på: Oppdragsbrev – behov for frekvenser til framtidig nød- og beredskapskommunikasjon, Justis- og beredskapsdepartementet, 09.12.2015.

Aktörer inom allmän ordning säkerhet och hälsa samt försvar tillhandahåller samhällsservice till de som bor och vistas i Sverige. En rikstäckande kommunikationslösning bidrar till att skapa lika förutsättningar för samhällsservice över hela landet.

MSB anser att det är viktigt att det offentliga samutnyttjar infrastruktur så långt som det är möjligt, exempelvis samordnas kommunikationslösningen med framtida lösningar för kommunikationssystem för järnväg (FRMCS[7]) skapar det samhällsnytta. Ett arbete pågår att specificera ersättare till GSM-R[8]. Flera tjänster inom transportsystemet kan använda sig av kommunikationslösningen, såsom trafikövervakning. Det innebär att frekvensutrymme frigörs för kommersiell användning och att aktörerna kan undvika kostsamma och komplicerade leverantörsbyten.

Kommunikationslösningen ska också kunna användas för roaming av nödsamtal till 112 när de kommersiella näten inte är tillgängliga på grund av störningar eller på ställen där kommersiella operatörer inte har täckning. Möjlighet till roaming av nödsamtal till 112 innebär en ökad säkerhet för allmänheten och effektivare insatser.

Kommunikationslösningen och kringutrustning ska bygga på globala standarder för att undvika de kostnadsdrivande inlåsningseffekter som nischmarknader ger. En förutsättning för att undvika nischmarknadsproblem är att samhällsviktiga verksamheter tilldelas frekvenser inom MFCN-delarna[9] av 700 MHz-bandet. Arbetet med att utveckla standarder för LTE-teknik för att stödja samhällsviktiga verksamheters krav på särskild funktionalitet pågår i 3GPP[10], ETSI[11] och andra internationella organisationer med ett brett stöd från mobilindustrin och med medverkan av intressenter inom samhällsviktiga verksamheter. Att vara en del av massmarknaden ger ett större urval av utrustning, lägre priser, möjlighet till roaming med kommersiella nätverk och möjlighet att ta del av stordriftsfördelar som uppnåtts i kommersiella nät.

Offentlig kontroll i en föränderlig värld

Förändringar i världsläget och i vårt närområde, samt förändrade mönster i hotbilden såsom cyberattacker, sabotage och terrorism innebär att samhällets samlade resurser behöver användas effektivt för att ytterst värna svensk demokrati och suveränitet. Det gäller så väl i det förebyggande arbetet som i krishantering. Regeringens beslut från den 10 december 2015[12] att berörda myndigheter åter ska planera för civilt försvar är ett resultat av det försämrade säkerhetspolitiska läget i vårt närområde.

Kommunikation och informationsdelning som uppfyller de krav som aktörerna har inom totalförsvaret är en av grundförutsättningarna för totalförsvarsplaneringen. I Sverige råder idag förhöjd terrorhotnivå, nivå 3 på en femgradig skala, med flera samtidigt pågående nationella särskilda händelser och extraordinära händelser. Detta läge är inte en ”normal nivå” och

---

[7] Future Railway Mobile Communication System.

[8] Global System for Mobile Communications – Railways.

[9] Mobile/Fixed Communications Networks, 703-733 MHz och 758-788 MHz.

[10] 3rd Generation Partnership Project.

[11] European Telecommunications Standards Institute.

[12] Regeringsbeslut 5, 2015-12-10.

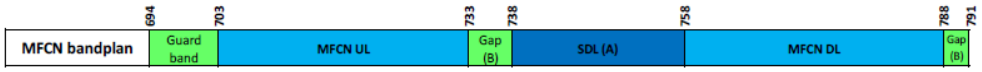
inte heller höjd beredskap eller krig, men ställer särskilda krav på kommunikationen för aktörer inom allmän ordning, säkerhet, hälsa samt försvar.

Aktörer inom allmän ordning, säkerhet, hälsa samt försvar utgör grunden i Sveriges krisledningsförmåga och ska ha förutsättningar att agera vid olika samhällsstörningar. Sveriges krisledningsförmåga ska inte kunna påverkas av kommersiella eller utländska intressen. MSB anser därför att kommunikationslösningen för samhällsviktig verksamhet behöver kontrolleras av det offentliga.

Förutsättningar

Tillgång till frekvenser

Behovet av mobil IP-baserad kommunikation som uppfyller samhällsviktiga verksamheters krav är omedelbar. 700 MHz-bandets egenskaper och att de tillgängliggörs 2017 gör det till ett kostnadseffektivt alternativ att avsätta minst 2 x 10 MHz i MFCN-delarna[13] på 700 MHz-bandet, till en kommunikationslösning för samhällsviktig kommunikation.



Bilden ovan visar bandplan[14] för 700 MHz-bandet.

Frekvensbehovet för mobil bredbandskommunikation är beräknat till 2 x 10 MHz exklusive kapacitet för t.ex. taltrafik. I ECC-rapport 199[15] har beräkningar gjorts för att bedöma kapacitetsbehovet genom att analysera trafikmängden i tre olika scenarier; vardaglig händelse, större händelse om än planerad eller oplanerad och en krissituation. När taltrafiken, som idag går i Rakelnätet, ska flyttas över till 700 MHz-bandet behövs ytterligare 2 x 3,2 MHz. Frekvenser på 700 MHz-bandet är också särskilt lämpade för att uppnå kraven på yttäckning samt inomhustäckning på ett kostnadseffektivt sätt.

De krav och behov som samhällsviktig verksamhet ställer redovisas i denna rapport och behöver omhändertas inom det regeringsuppdrag om den framtida användningen av 700 MHz-bandet (694–790 MHz), som PTS ska slutredovisa den 31 mars 2017[16]. En bedömning av samhällsnytta utifrån de säkerhetspolitiska förutsättningar som idag är tillämpliga behöver göras inom ramen för det uppdraget.

För att göra frekvensanvändningen för samhällsviktig kommunikation effektivare bör kommunikationslösningen inkludera vissa tjänster inom transportsystemet, t.ex. delar av det som idag är GSM-R. Arbete med att

---

[13] 703-733 MHz och 758-788 MHz.

[14] ECC (15)01.

[15] ECC Report 199, May 2013, User requirements and spectrum needs for future European broadband PPDR systems (Wide Area Networks).

[16] Uppdrag att utreda den framtida användningen av 700 MHz-bandet (694–790 MHz) Dnr: N2014/2008/ITP.

specificera ersättare till GSM-R pågår just nu inom UIC[17]. Specifikationen beräknas vara klar 2018.

Inom CEPT[18] pågår också arbete med harmonisering av frekvensbandet 694-791 MHz.[19] Beslutet förväntas att publiceras i juni 2016. Möjlighet till internationell interoperabilitet realiseras genom att länder använder gemensamma tekniska standarder. Därför är det en förutsättning att de samhällsviktiga verksamheterna i Sverige tilldelas frekvenser på 700 MHz-bandet som omfattas av LTE-ekosystem.[20] Eftersom arbete pågår med harmonisering ser MSB att det nu finns möjlighet att säkerställa att gemensamma resurser används effektivt. Om inte tillgång till frekvenser för samhällsviktig verksamhet säkerställs finns risk för att Sveriges krishanteringsförmåga påverkas negativt eller att Sverige kan komma tvingas att köpa tillbaka frekvenser.

Ett alternativ till 700 MHz-bandet som ibland framförs är 450-470 MHz-bandet. 450 MHz-bandet framställs som ett billigare alternativ eftersom det inte kräver lika många basstationer som 700 MHz-bandet. Ett annat argument är att det är tillgängligt 2020. Ett tredje är att samhällsviktig verksamhet är ett utpekat användningsområde i bandet. MSB ser att dessa argument ska ställas mot begränsad tillgång till användbar materiel och utrustning. Exempelvis finns det ett fåtal leverantörer på marknaden, som erbjuder mobiltelefoner anpassade till 450 MHz-bandet. Detta innebär att lösningen blir dyr och förutsättningarna för samverkan försvåras. Samhällsviktiga verksamheter riskerar också att inte kunna ta del av den framtida tekniska utveckling som sker på den kommersiella konsumentmarknaden. Vidare behövs minst 2 x 10 MHz i 700 MHz-bandet för samhällsviktig kommunikation. 450 MHz-bandet är därför inte ett realiserbart alternativ, eftersom motsvarande bandkapacitet inte är tillgängligt. Tilldelning av frekvenser inom 450-bandet påverkar övriga samhällsintressen, såsom satellitanvändning och försvar. Hela frekvensbandet styrs av internationell beslutad harmonisering och standardisering, vilket därför begränsar möjligheten att tilldela frekvensutrymme för samhällsviktig kommunikation på 450 MHz-bandet.

Reglering av kommunikationslösningen

I avsiktsförklaringen om digital förnyelse av det offentliga Sverige[21], beskrivs att myndigheter i större utsträckning ska dela och tillsammans utveckla digitala lösningar, istället för att varje myndighet utvecklar egna isolerade

---

[17] International Union of Railways.

[18] European Conference of Postal and Telecommunications Administration.

[19] CEPT ECC Draft decision 16(02), Harmonised technical conditions and frequency bands for the implementation of Broadband Public Protection and Disaster Relief (BB-PPDR) systems, mars 2016.

[20] TCCA (Tetra Critical Communication Association) och ECC (Electronic Communication Committee) rapport 199 identifierar LTE som gemensam teknisk standard och 700 MHz-bandet som förstahandsval som frekvensband i region 1 (ITU-Region 1 består av Europa, Afrika, Mellanöstern väster om Persiska viken inklusive Irak, f.d. Sovjetunionen och Mongoliet).

[21] Bilaga till protokoll nr III 5, vid regeringssammanträde den 29 oktober 2015, N2015/07455/EF.

komponenter och digitala tjänster. Detta ställer krav på såväl långsiktig förvaltning av den nationella infrastrukturen som juridiska förutsättningar.

MSB anser att en offentligt kontrollerad kommunikationslösning i kombination med en obligatorisk användning av denna, i väsentlig grad skulle bidra till samhällets krisberedskap. Den bör utformas med utgångspunkt från det ansvar användarna har att hantera olyckor, kriser och höjd beredskap samt civilt försvar. Det är vidare nödvändigt att tillfälligt, snabbt och skalbart kunna inkludera sådana externa resurser som behövs i det enskilda fallet, exempelvis frivilligorganisationer och privata aktörer. En författningsstadgad ensamrätt för den offentligägda kommunikationslösningen innebär att upphandlande myndigheter kan genomföra en direktupphandling.

Offentligt kontrollerad kommunikationslösning

MSB anser att kommunikationslösningen behöver vara offentligt ägd för att säkerställa att kraven på kvalitet och kvantitet uppfylls under oförändrade former. Uppgiften att tillhandahålla tjänster och lösningar ska vara utpekad och reglerad i författning.

Flerparten av aktörer med ansvar inom allmän ordning, säkerhet, hälsa samt försvar är upphandlande myndigheter. Som huvudregel gäller att även resurser som behövs för krisberedskap och höjd beredskap behöver upphandlas i konkurrens. De upphandlande myndigheterna kan idag i princip inte ställa sådana krav som enbart kan uppfyllas av den offentligägda kommunikationslösningen. Ett sätt att säkerställa att alla offentliga aktörer både kan och kommer att använda den offentliga kommunikationslösningen är att i författning reglera att det är obligatoriskt att ansluta sig till denna.

Genom att uppgiften att tillhandahålla kommunikationslösningen är utpekad och reglerad i författning kan abonnemangsavtal undantas från upphandling. Detta innebär att det som idag är reglerat som *”Tjänstekontrakt som en upphandlande myndighet tilldelar en annan upphandlande myndighet som på grund av lag eller annan författning har ensamrätt att utföra tjänsten är undantagna från upphandling”*[22] blir uppfyllt och abonnemangsavtal kan då tilldelas utan föregående annonsering. Det är nödvändigt att fortsatt utreda en sådan reglering.

För det fall kommunikationslösningen inte hamnar i offentligt ägo, bör den operatör som meddelas tillstånd för tillhandahållandet kontrolleras noggrant. Vidare behöver det ställas långtgående krav på informationshantering och säkerhet. Tillsyn av detta blir problematiskt, eftersom möjligheter att tilldela sanktioner eller återta tillstånd när tillståndsvillkor bryts inte är en ändamålsenlig åtgärd då ett avbrott i leveransen redan kan ha medfört en stor påverkan för svensk krishanteringssystem samt fara för liv, egendom och miljö.

Obligatorisk användning, operativ krishantering och elektronisk kommunikation

MSB föreslår obligatorisk användning av säkra, skyddade, tillgängliga och robusta kommunikationstjänster. Det bör regleras i författning att aktörer med ansvar att hantera olyckor, kris och höjd beredskap ska använda sig av säkra och robusta kommunikationslösningar. MSB understryker vikten av att den samverkan som behövs mellan aktörer inom krisberedskapen och

[22] 1 kap. 7 § lag (2007:1091) om offentlig upphandling.

totalförsvaret behöver kunna göras med stöd av säkra och robusta kommunikationssystem.

Regleringen kring elektronisk kommunikation behöver anpassas till de principer som det svenska krishanteringssystemet är uppbyggt på. MSB föreslår att användningsområdet ”samt försvar” inbegriper den civila verksamhet som ingår i totalförsvaret, vilka Försvarsmakten behöver kommunicera med. Resultatet av den utredning som pågår för att återuppta det civila försvaret bör användas för att definiera vilka användare som ska ingå i användarkretsen.

Fast och mobil kommunikation hör ihop

För att uppnå den tillgänglighet, informationssäkerhet och offentlig kontroll som krävs i den förordade kommunikationslösningen behövs ett geografiskt redundant transmissionsnät som realiseras genom offentligt ägda fibernät.

Ett utvecklat SGSI[23] i enlighet med NISU-utredningens[24] förslag innebär att det behövs ett fibernät som i huvudsak är baserat på statligt ägd infrastruktur. När staten äger och kontrollerar infrastrukturen kan staten såväl operativt som kvalitativt bestämma, prioritera och inrikta utvecklingen av funktionalitet. MSB delar NISU-utredningens bedömning att staten äger omfattande mängder av infrastruktur som skulle kunna användas för att bygga ett framtida SGSI.

MSB anser att utvecklingen av SGSI och utvecklingen av den föreslagna kommunikationslösningen behöver ses i ett sammanhang.

Samordna genomförandet av kommunikationslösningen med utvecklingen av svensk förvaltning

I arbetet med regeringsuppdraget har MSB identifierat flera pågående arbeten som påverkar, och påverkas av, arbetet med att säkerställa kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar.

Den nuvarande bredbandsstrategin lanserades 2009. I den revidering som nu sker anser MSB att även bredbanskommunikation för en effektiv förvaltning och för aktörer som tillhandahåller samhällstjänster inom allmän ordning, säkerhet, hälsa och försvar ska inkluderas. Ett digitaliserat samhälle kräver både bredband för enskilda och bredband för offentlig verksamhet för att kunna realisera de mervärden som digitaliseringen kan ge samhället. Pågående uppdrag om totalförsvarsplanering och gemensamma grunder för en sammanhängande planering för totalförsvaret och utredningen om försörjning av statens behov av it- och teletjänster med synnerliga säkerhetskrav[25] behöver vägas in i det fortsatt arbetet för att säkerställa kommunikation för aktörer och samhällsviktig verksamhet.

---

[23] Swedish Government Secure Intranet.

[24] Informations- och cybersäkerhet i Sverige, strategi och åtgärder för säker information i staten SOU 2015:23.

[25] Utredningen om försörjningen av statens behov av IT/teletjänster med synnerliga säkerhetskrav, Fö 2014:A.

I betänkandet *Statens bredbandsinfrastruktur som resurs*[26] beskrivs att informationssäkerhetsfrågorna har en allt större betydelse i takt med att allt mer av kommunikationerna går via bredbandsnät och mobilnät. Utredaren betonar dessutom att omvärlden förändrats och det säkerhetspolitiska läget i dag är ett annat än för bara några år sedan. Mobilitet är en förutsättning för användarnas fortsatta utveckling av arbetsmetoder och effektivisering av verksamheterna. Kommunikationssystemet Swedish Government Secure Intranet (SGSI) är ett skyddat fast intranät för utbyte av känslig och skyddsvärd information mellan svenska myndigheter. I betänkandet *Informations- och cybersäkerhet i Sverige*[27] föreslås att SGSI utvecklas samt att samtliga myndigheter som anges i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap ska anslutas.

Kommissionen överlämnade den 7 februari 2013 ett direktivförslag om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, det s.k. NIS-direktivet. [28] Direktivet är en del i den europeiska strategin för cybersäkerhet och innehåller ett antal krav som alla medlemsstaterna måste uppfylla. Exempelvis ska alla medlemsstaterna därför uppnå och vidmakthålla en miniminivå av informationssäkerhet och anta nationella strategier för nät- och informationssäkerhet. Tillsammans ska medlemsstaterna skapa en samverkansgrupp för att främja strategisk samverkan och utbyte av information mellan sig.

Finansiering av kommunikationslösningen

Planering och genomförande av samhällsviktig verksamhet behöver långsiktiga och förutsebara ekonomiska förutsättningar om statens medel ska användas effektivt. Flera beslut påverkar finansieringen av lösningen. Exempel beslut om användarkrets för kommunikationslösningen, vilka tjänster som kommunikationslösningen ska bära och på vilket sätt den kan ersätta befintliga kommunikationslösningar blir viktiga utgångspunkter. Likaså påverkas finansieringen av beslut om huruvida medel för förstärkningar avseende robusthet omfördelas till den gemensamma infrastrukturen. Beslut om huruvida kapacitet som inte används i kommunikationslösningen, kan göras tillgänglig för kommersiell användning, påverkar intäkterna.

Förvaltning och utveckling

Den kommunikationslösning som MSB förordar innebär initiala kostnader i form av investeringar och löpande kostnader i form av drift, förvaltning och utveckling. Kommunikationslösningen måste koordineras med teknikutvecklingen i omvärlden. En förutsättning för att realisera detta är att säkra en förvaltningsbudget som omhändertar uppgraderingar och vidareutveckling. Detta måste dock balanseras, så att den utveckling som görs omfattar välbeprövad teknik och säkerställer att förmågan hos användarna höjs. Det finns därför anledning att begränsa uppgraderingar och utveckling av en gemensam kommunikationslösning, så att införandet av ny teknik kan styras och anpassas utifrån behov och ekonomiska förutsättningar. Det är

---

[26] SOU 2016:1.

[27] SOU 2015:23.

[28] Direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen (KOM(2013)48).

därför betydelsefullt att göra en bedömning av förvaltningskostnaden för vald kommunikationslösning.

Redovisning och överväganden

Lösningsförslagen

I detta avsnitt beskrivs MSB:s bedömning utifrån de preliminära och övergripande lösningsförslag som PTS presenterade den 1 februari 2016. PTS identifierar fyra olika typer av cellulära lösningar: Kommersiell lösning, Kommersiellt radionät med dedikerat kärnnät, Dedikerat radionät och Hybridlösning. Se vidare avsnitt ”*PTS redovisning av kommunikationslösningar för aktörer inom allmän ordning, säkerhet, hälsa samt försvar*” nedan.

Utgångspunkt för MSB:s bedömning av de olika lösningsförslagen är de krav och behov som redogörs för i avsnittet ”*Krav och behov av säker, tillgänglig, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar*” nedan.

Tjänster i kommersiella radionät

PTS lösningsförslag ”Tjänster i kommersiella radionät” uppfyller inte de av MSB redovisade kraven på bland annat offentlig kontroll, robusthet, täckning, säkerhet och tillgänglighet. Användarorganisationernas praktiska erfarenheter av att använda de kommersiella tjänsterna visar att dessa inte lever upp till de krav som ställs i den operativa verksamheten. Dessa erfarenheter överensstämmer också med flertalet studier och rapporter[29] där det konstateras att en rent kommersiell lösning inte uppfyller de krav som aktörer inom allmän ordning, säkerhet, hälsa samt försvar ställer. Detta är också anledningen till att diskussioner förs om helt eller delvis dedikerade mobila bredbandsnät både på nationell och på internationell nivå inom t ex. FN och EU.

Användning av tjänster i kommersiella nät medför att samhällsviktiga verksamheter till stor del påverkas av de teknikval som görs i de kommersiella näten. Dessa teknikval kan vara oförenliga med de samhällsviktiga verksamheternas krav på långsiktighet och stabilitet. Behov av särskild funktionalitet för samhällsviktig verksamhet kan inte alltid tillgodoses i ett kommersiellt nät, då funktionaliteten inte överensstämmer med de kommersiella operatörernas affärsmodeller. Om inte särskild funktionalitet finns, inskränker det möjligheten till effektiva arbetssätt för samhällsviktiga verksamheter.

---

[29] Exempelvis ECC Report 199, User requirements and spectrum needs for future European broadband PPDR systems (Wide Area Networks), maj 2013 och

Kommissionens rapport “Is Commercial Cellular Suitable for Mission Critical Broadband?”, contract number: 30-CE-0603428/00-19, SMART number: 2013/0016.

Fördelar med tjänster i kommersiella radionät

- Tid för införande och övergång till skarp drift är kortare än för övriga alternativ.
- Tillgång till ett bredare frekvensspektrum då kommersiella aktörer har licens för flertal frekvensband t.ex. 800 MHz, 900 MHz, 1800 MHz med flera, innebär mer kapacitet och att inomhustäckning kan tillgodoses till viss del.

Nackdelar med tjänster i kommersiella radionät

- Lösningsförslaget uppfyller inte de grundläggande kraven på offentlig kontroll och informationssäkerhet. För att uppfylla övriga krav behövs viktiga investeringar i:
    - Robusthet, genom tillförsel av reservkraft samt genom utbyggnad av redundant transmission till basstationerna.
    - Täckning, genom utbyggnad av radionät där täckning saknas eller är bristfälligt.
- Ägarförhållanden kan inte säkerställas via avtal. Ägarskap av kommersiell infrastruktur kan hamna hos aktörer som inte beaktar samhällsviktiga verksamheters intressen.
- Kommersiella nät är primärt designade för nedladdning av stora mängder data, medan samhällsviktig verksamhets behov primärt är uppladdning.
- Frekvenshantering blir komplex vid användning av mobila förstärkningsresurser i form av ad-hoc radionät.
- Särskild funktionalitet som normalt inte finns i kommersiella nät behöver avtalas och tillföras. Exempelvis:
    - Prioritet
    - Direktsamtal mellan enheter (Proximity Services i LTE)
    - Push-to-talk (MCPTT, Mission Critical Push to Talk)
    - Gruppkommunikation (3GPP GCSE[30])

Kommersiell lösning med dedikerat kärnnät

PTS lösningsförslag ”Kommersiell lösning med dedikerat kärnnät” kan till viss del uppfylla kravbilden som beskrivs i avsnitt *Redovisning av Krav och behov av säker, tillgänglig, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar*. Lösningsförslaget förutsätter att investeringar görs i robusthetshöjande åtgärder i de kommersiella näten, i form av utökad reservkraft, redundant transmission samt kompletterande utbyggnad av täckningen. Över tid behöver särskild funktionalitet säkerställas som till exempel prioritet, direktsamtal mellan enheter, Push-to-talk och gruppkommunikation.

MSB bedömer att detta lösningsförslag är lämpligt som ett första steg till en lösning med ett dedikerat radionät för aktörer inom allmän ordning, säkerhet, hälsa och försvar. Lösningsförslaget kan dock inte ses som en slutlig lösning då ställda grundkrav bland annat avseende offentlig kontroll och informationssäkerhet inte kan tillgodoses fullt ut.

[30] Group Communication System Enablers.

Fördelar med kommersiell lösning med dedikerat kärnnät

- Det offentliga har kontroll över informationen i kärnnätet så som abonnentdata.
- Tillgång till ett bredare frekvensspektrum då kommersiella aktörer har licens för flertal frekvensband t.ex. 800 MHz, 900 MHz, 1800 MHz med flera, innebär mer kapacitet och att inomhustäckning kan tillgodoses till viss del.
- Införande av ny funktionalitet och uppgraderingar som ligger i kärnnätet kan styras och anpassas till de samhällsviktiga verksamheternas krav.
- Särskild funktionalitet, som normalt inte finns i kommersiella nät, kan enklare tillföras i och med ett dedikerat kärnnät.

Nackdelar med kommersiell lösning med dedikerat kärnnät

- Lösningsförslaget uppfyller inte de grundläggande kraven på offentlig kontroll. För att uppfylla övriga krav behövs viktiga investeringar i:
    - Robusthet, genom tillförsel av reservkraft samt genom utbyggnad av redundant transmission till basstationerna.
    - Täckning, genom utbyggnad av radionät där täckning saknas eller är bristfälligt.
- Ägarförhållanden kan inte säkerställas via avtal. Ägarskap av kommersiell infrastruktur kan hamna hos aktörer som inte beaktar samhällsviktiga verksamheters intressen.
- Kommersiella nät är primärt designade för nedladdning av stora mängder data, medan samhällsviktig verksamhets behov är primärt uppladdning.
- Frekvenshantering blir komplex vid användning av mobila förstärkningsresurser i form av ad-hoc radionät.
- Särskild funktionalitet som normalt inte finns i kommersiella nät behöver avtalas och tillföras. Exempelvis:
    - Prioritet
    - Direktsamtal mellan enheter (Proximity Services i LTE)
    - Push-to-talk (MCPTT, Mission Critical Push to Talk)
    - Gruppkommunikation (3GPP GCSE[31])

Dedikerat radionät

PTS lösningsförslag ”Lösningar med dedikerat radionät” innebär ett dedikerat nationellt landstäckande radionät, baserat på t.ex. kommersiell LTE-standard. MSB bedömer att lösningsförslaget kan uppfylla kravbilden som beskrivs i avsnitt ”*Redovisning av Krav och behov av säker, tillgänglig, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar”*.

Utbyggnad av ett dedikerat nationellt landstäckande radionät tar tid. Behoven av säker mobil bredbandskommunikation finns redan idag vilket medför att denna lösning måste realiseras i flera steg som initialt omfattar upphandling av dedikerat kärnnät (jmf PTS lösningsförslag ”Kommersiell lösning med

[31] Group Communication System Enablers.

dedikerat kärnnät"), följt av en hybridlösning (jmf PTS lösningsförslag "Hybridlösning" typ 2 och därefter av typ 1) under utbyggnadsfasen. När den dedikerade lösningen är realiserad kan ingångna nationella roamingavtal avslutas.

Fördelar med ett dedikerat radionät:

- Samhällsviktiga verksamheter konkurrerar inte med allmänhetens behov av att kommunicera vid större händelser och kriser. Prioritet kan realiseras utan att allmänhetens kommunikationsbehov åsidosätts.
- Det offentliga har kontroll över informationen i infrastrukturen.
- Kapacitet och täckning kan säkerställas på platser där de samhällsviktiga verksamheterna bedriver sin verksamhet även där det inte är kommersiellt motiverat att bygga täckning.
- Robusthet kan anpassas och säkerställas utifrån radionätets design utan hänsyn till kommersiella intressen.
- Kontroll och insyn hanteras inom det offentliga och ger möjlighet till kontrollerad behörighetsstyrning av åtkomst till data och tjänster.
- Införande av ny funktionalitet och uppgraderingar kan styras och anpassas till de samhällsviktiga verksamheternas krav.
- En offentlig aktör har möjlighet att garantera en långsiktighet och stabilitet som är en förutsättning i den offentliga verksamheten.
- Förenklad frekvenshantering vid användning av mobila förstärkningsresurser i form av ad-hoc radionät.

Nackdelar med ett dedikerat radionät:

- Ett dedikerat nät har ett begränsat frekvensutrymme t.ex. 2 x 10 MHz. Om frekvensutrymmet är för litet kan kapacitetsbrist uppstå till exempel vid större samhällsstörningar eller vid idag oförutsebar teknikutveckling som ställer krav på större frekvensutrymme än det tilldelade.
- Lågt frekvensutnyttjande i delar av det dedikerade radionätet då antalet användare är begränsat.

Hybridlösning

PTS ser ett antal olika grundläggande varianter på lösningar där det dedikerade och kommersiella nätens roll skiljer sig åt. De beskriver två exempel på möjliga varianter för en hybridlösning, typ 1: *Hybridlösning med nationellt täckande dedikerat "bas-nät"* och typ 2: *Hybridlösning med geografiskt begränsat dedikerat nät*. PTS lösningsförslag "Hybridlösning" är alltså en kombination av olika grader av dedikerat radionät och kommersiella radionät. Lösningsförslagen förutsätter att avtal med en eller flera kommersiella operatörer möjliggör att användarna vid behov kan använda flera operatörers nät via nationell roaming. Fördelningen av trafiken mellan de olika näten styrs i det dedikerade kärnnätet.

PTS beskriver typ 2 som ett nät som har täckning på platser som ses som särskilt viktiga vad gäller t.ex. kravet på säkerhet och tillgänglighet, där det ofta krävs hög kapacitet, eller där det finns kända brister i den kommersiella täckningen. MSB ser att det är problematiskt i förväg bedöma vilka platser som är särskilt viktiga vid hantering av olyckor och kriser och gör därmed en generell bedömning av detta lösningsförslag i avsnittet *"Summering av MSB:s bedömning av kravuppfyllnad, investerings- och driftskostander "* nedan.

Det dedikerade basnätet enligt typ 1 tillgodoser krav och behov och kan bära majoriteten av trafiken från de samhällsviktiga aktörerna. Kommunikationsutrustningen har dock möjlighet att vid behov växla till ett (eller flera) kommersiella LTE radionät. Det kommersiella nätet eller näten fungerar då som en kompletterande kapacitetsförstärkning eller backup i områden där täckning eller kapacitet behöver förstärkas.

Fördelar med en hybridlösning

- Fördelar med en hybridlösning är att användare i ett dedikerat radionät vid behov kan dra nytta av den kapacitet som återfinns i de kommersiella näten. Möjligheten att nyttja kommersiella nät underlättar hantering av driftavbrott vid till exempel uppgraderingar och servicefönster.
- Allmänheten kan nå 112 beroende på geografisk utbyggnad av det dedikerade radionätet.
- Hybridlösningar gör det möjligt att snabbare åstadkomma skarp drift då de kommersiella radionäten kan användas medan det dedikerade nätet byggs ut.
- Samhällsviktiga verksamheter konkurrerar inte med allmänhetens behov av att kommunicera vid större händelser och kriser. Prioritet kan realiseras utan att allmänhetens kommunikationsbehov åsidosätts.
- Förenklad frekvenshantering vid användning av mobila förstärkningsresurser i form av ad-hoc radionät.
- För övrigt samma fördelar med typ 1 som i ett dedikerat radionät.

Nackdelar med en hybridlösning

- Mer komplexa tekniska lösningar för t.ex. roamingfunktionalitet. Komplexitet medför större utmaningar för driftorganisationen vid t.ex. felsökning.
- Kostnadsdrivande lösning där kostnaderna för servicenivåavtal (SLA) med kommersiella aktörer är idag okänd.
- Hybridlösningar förutsätter tätt samarbete med den eller de kommersiella aktörerna som säkerställer att:
    - Funktionalitet som införs i det dedikerade nätet även införs i de kommersiella näten.
    - Servicenivåavtal kan övervakas och följas upp.

Summering av MSB:s bedömning av kravuppfyllnad, investerings- och driftskostnad

Nedanstående tabell summerar MSB:s bedömning av investerings- och driftskostnader för de fyra kommunikationslösningarna, deras kravuppfyllnad samt anger möjlig tidplan för skarp drift. Kravuppfyllnad har delats in i hög (H), medel (M), låg (L) och ingen kravuppfyllnad (-) efter hur pass väl de olika lösningarna uppfyller ställda krav. Kravuppfyllnad hög (H) är en förutsättning för att samhällsviktig verksamhet ska kunna använda lösningsförslagen.

	Tjänster i kommersiella nät	Kommersiell lösning med dedikerat kärnnät	Dedikerat radionät	Hybridlösning Typ 1	Hybridlösning Typ 2
Krav					
– Offentlig kontroll	-	M	H	M/H	
– Robusthet	H(*)	H(*)	H	H(*)/H	
– Täckning	H(*)	H(*)	H	H(*)/H	
– Informationssäkerhet	L	M	H	M/H	
– Prioritet	-	M	H	M/H	
– Långsiktighet	L	M	H	M/H	
– Särskild funktionalitet	L	M	H	M/H	
Kostnad					
– Investering	3 073 mnkr	3 189(**) mnkr	6 012 mnkr	3 189/6 012(**) mnkr	
– Drift	3 438 mnkr	4 163(**) mnkr	5 310 mnkr	4 163/5 310(**) mnkr	
Tidplan	1-2 år	1-2 år	3,5–4,5 år	1–4,5 år	

(*) Förutsätter utbyggnad av reservkraft, redundant transmission och kompletterande täckning.

(**) Investerings- och driftskostnader för roaming tillkommer.

Definitioner

MSB:s definition av kommunikationstjänster är inom ramen för redovisningen av detta regeringsuppdrag; de applikationer, tillämpningar och funktioner som möjliggör kommunikation inom och mellan användare. Detta motsvaras av elektronisk kommunikations med definitionen - Tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät.[32]

MSB:s definition av kommunikationslösning är den infrastruktur som bär kommunikationstjänsterna. Till detta kommer att kommunikationslösningen också förutsätter reglering och finansiering. Detta motsvaras av elektroniska kommunikationsnät med definitionen - System för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.

[32] Lag (2003:389) om elektronisk kommunikation. Kap 1. §7

Säker och tillgänglig mobil, IP-baserad kommunikation för aktörer inom allmän ordning säkerhet, hälsa samt försvar

Regeringsuppdrag II:28, 2015-12-17

Redovisning av krav och behov av säker och tillgänglig mobil, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar

Innehållsförteckning

1. Inledning

Myndigheten för samhällsskydd och beredskap har, i enlighet med regeringsuppdraget, i samråd med Polismyndigheten och Försvarsmakten i denna redovisning beskrivit vilka krav och behov aktörer inom allmän ordning, säkerhet, hälsa samt försvar har av säker, tillgänglig, mobil, IP-baserad kommunikation. Polismyndigheten och Försvarsmakten har lämnat samråd på denna redovisning.

I denna redovisnings avsnitt 1, redogörs för aktörer inom allmän ordning, säkerhet, hälsa samt försvars särskilda behov av mobil, IP-baserad kommunikation. I avsnitt 2, redovisas hur krav och behov inhämtats; vilka behov aktörerna har; vad som ska uppnås; vilka krav aktörerna ställer och vilka krav internationella utvecklingen ställer. I bilagor redovisas exempel på krav och behov, scenarier och viktning av hur verksamhetskritiska tjänster och funktioner är.

MSB har inom ramen för myndighetens ordinarie utvecklingsarbete inhämtat kraven och behoven av mobil IP-baserad kommunikation från övriga aktörer inom allmän ordning, säkerhet, hälsa samt försvar. Med MSB:s kunskap om Rakelanvändarnas behov och krav på mobil IP-baserad kommunikation anser MSB att detta underlag är representativt för aktörer inom allmän ordning, säkerhet, hälsa samt försvar. Samtidigt kan det inte uteslutas att vissa specifika krav eller behov från enskilda aktörer tillkommer eller förändras.

MSB, Polisen och Försvarmakten har i arbetet utgått ifrån att uppdraget omfattar det gemensamma behovet av kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar. Underlaget omfattar således inte Försvarsmaktens totala behov av kommunikation, utan de områden som avser samverkan med det civila försvaret inom Totalförsvaret.

I denna redovisning finns inte underlag från arbetet med regeringens uppdrag till Försvarsmakten och Myndigheten för samhällsskydd och beredskap avseende totalförsvarsplanering[1], med slutredovisning juni 2017, samt slutsatser från utredningen om försörjning av statens behov av it/teletjänster med synnerliga säkerhetskrav[2], slutredovisning december 2016. Underlag från ovan nämnda uppdrag och utredning är således ej tillgängliga men bör vägas in i den slutliga bedömningen avseende nationella behov och krav för aktörer inom allmän ordning, säkerhet, hälsa samt försvar. Resultatet av uppdraget till MSB och Försvarsmakten om gemensamma grunder (grundsyn) för en sammanhängande planering för totalförsvaret som ska redovisas den 10 juni

[1] Regeringsbeslut 5, Uppdrag till Försvarsmakten och Myndigheten för samhällsskydd och beredskap avseende totalförsvarsplanering, FÖ2015/0916/MFI, 2015-12-10.
[2] Fö2014:A

2016 kan också innebära att behoven av behov av säker och tillgänglig mobil, IP-baserad kommunikation ytterligare förstärks.

Datatjänster för samhällviktig verksamhet behövs redan idag

Behovet av mobil datakommunikation som uppfyller samhällsviktiga verksamheters[3] krav är omedelbar. Erfarenheterna och nulägesbilden av mobil datakommunikation i de allmänt tillgängliga kommersiella näten är att de inte motsvarar verksamhetens behov avseende tillgänglighet, täckning, kapacitet, prioritet och robusthet. Under den kartläggning och behovsinventering av kundbehoven av datatjänster som MSB genomförde under 2014, med ett tiotal aktörer inom allmän ordning, säkerhet, hälsa samt försvar beskrevs flera svårigheter med kommersiella operatörer. En klart framträdande brist med de kommersiella alternativen är att det inte går att avtala servicenivåer som motsvarar behoven. Vidare är frågor som säkerhet, tillgänglighet, robusthet och uthållighet anledningar till att aktörerna inte vågat ta steget fullt ut att realisera verksamhetskritiska satsningar på den mobila sidan. Samhällsviktig verksamhet efterfrågar en långsiktig, stabil operatör och leverantör av kommunikationstjänster som en förutsättning för att på ett säkert sätt genomföra vissa av sina effektiviseringsprogram i riktning mot ett mer mobilt arbetssätt.

MSB ser också att det ökade behovet av datatjänster i den operativa verksamheten innebär att många verksamheter hamnar i en situation med flera parallella abonnemang och terminaler. Detta är fördyrande och skapar ett ineffektivt arbete. Vidare ser vi att förmågan att agera samordnat minskar i takt med att verksamheterna skaffar sig egna lösningar.

Samhällsgemensamma lösningar som motsvarar aktörernas krav behöver anskaffas

Idag behöver Rakel kompletteras med högre kapacitet för överföring av data. Användarnas krav innebär också att den funktionalitet som Rakel idag tillhandahåller på sikt behöver omsättas med ny teknik. TCCA (TETRA and Critical Communications Association) gjorde 2011-2012 bedömningen att

---

[3] Med samhällsviktiga verksamheter inkluderas aktörer som hanterar allmän ordning, säkerhet och hälsa i kris och vardag. Dessa aktörer är desamma som omfattas av begreppet Public Protection and Disaster Relief (PPDR). PPDR definieras i ITU-R Report M-2033 som:
– Public protection (PP) radiocommunication: Radiocommunications used by responsible agencies and organizations dealing with maintenance of law and order, protection of life and property, and emergency situations.
– Disaster relief (DR) radiocommunication: Radiocommunications used by agencies and organizations dealing with a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as a result of complex, long-term processes.

TETRA kommer att fortsätta vara den standard som används för verksamhetskritiskt tal under de kommande 10 åren eller längre. MSB ser inte att Rakel kan avvecklas förrän det finns en annan teknisk lösning som erbjuder verksamhetskritiskt tal som är minst lika bra eller bättre än det som Rakel erbjuder idag och delar därför TCCA bedömning. Men, eftersom Tetrastandarden, som Rakel-systemet bygger på, inte kan leverera mobila datatjänster med sådan bandbredd som aktörerna inom allmän ordning, säkerhet, hälsa och försvar efterfrågar är det nödvändigt att initialt komplettera, inte ersätta, Rakel med en teknik som tillgodoser detta behov.

Användare av säker och tillgänglig, mobil, IP-baserad kommunikation

MSB ser att användarkretsen för kommunikationslösningar för samhällsviktig verksamhet är aktörer inom allmän ordning, säkerhet, hälsa och försvar. Detta inkluderar aktörernas olika användning såsom till exempel e-hälsa och ersättningssystem för GSM-R. Det förväntade antalet användare påverkas också av hur användare av it-/teletjänster med synnerliga säkerhetskrav definieras i den av Försvarsdepartementet tillsatta utredningen.[4] Slutredovisningen från utredningen lämnas senast den 1 december 2016.

Datakommunikation för samhällsviktig verksamhet behövs i hela hotskalan

Aktörerna inom allmän ordning, säkerhet och hälsa samt försvar har i uppdrag att säkerställa samhällets och medborgarnas trygghet och säkerhet. För den som drabbas av olyckor, sjukdomsfall, brott eller liknande är det helt avgörande att samhället kan agera snabbt och säkert. Ibland är det inte möjligt att stoppa händelser, varför skadeverkningarna behöver minimeras. För att utföra sina uppdrag är aktörerna beroende av ständig tillgång till en säker och effektiv mobil tal- och datakommunikation som säkerställer effektiva arbetssätt och möter verksamheternas mycket höga krav på mobilitet, robusthet, skydd, säkerhet och tillgänglighet. En fungerande kommunikation är en förutsättning för att leda, genomföra den operativa verksamheten och för att samverka med andra ansvariga verksamheter.

Tillgången till en ständigt fungerande kommunikationslösning är lika viktig i hela skalan, upp till höjd beredskap, eftersom tidsfaktorn alltid är direkt avgörande för om ett uppdrag eller en åtgärd ska lyckas eller misslyckas. En order eller ett uppdrag eller annan åtgärd måste gå fram omedelbart till mottagaren eller mottagarna. Konsekvensen om detta inte fungerar är att fler människor skadas och dödas, miljömässiga och ekonomiska värden går till spillo samt att personalens säkerhet äventyras. Ordergivning,

---

[4] Fö2014:A

informationsöverföring och informationshämtning sker med stöd av både tal och datakommunikation.

Resultatet av uppdraget till MSB och Försvarsmakten om gemensamma grunder (grundsyn) för en sammanhängande planering för totalförsvaret som ska redovisas den 10 juni 2016 kan också innebära att behoven av säker och tillgänglig mobil, IP-baserad kommunikation ytterligare förstärks. Förmåga att i fred planera inför höjd beredskap, precis som operativt agerande under en säkerhetspolitisk kris kräver kommunikationslösningar som är moderna, robusta och säkra.

Idag råder förhöjd terrorhotnivå, nivå 4 av 5, med flera samtidigt pågående nationella särskilda händelser och extraordinära händelser med hänvisning till t. ex. rådande migrantflöde. Detta läge är inte en ”normal nivå” och inte heller höjd beredskap eller krig, men ställer särskilda krav på kommunikationen inom och mellan ansvariga aktörer.

Förvarsmaktens primära behov för samverkan inom totalförsvaret är skyddad (krypterad) talförbindelse. Kommunikationslösningen avses användas av Försvarsmakten för informationsutbyte vid lagstadgad samverkan mellan Försvarsmakten och de civila delarna inom funktionerna allmän ordning, säkerhet och hälsa. Aktörer anslutna till kommunikationslösningen behöver kunna genomföra informationsutbyte digitalt i en skyddad gemensam kommunikationsplattform.

Förändrade mönster i hotbilden mot Sverige

Regeringens beslut från den 10 december 2015 att berörda myndigheter åter ska planera för civilt försvar är ett resultat av det försämrade säkerhetspolitiska läget i vårt närområde. Förändringar i världsläget och i vårt närområde, samt förändrade mönster i hotbilden såsom cyberattacker, sabotage och terrorism innebär att samhällets samlade resurser behöver användas effektivt för att ytterst värna svensk demokrati och suveränitet. Det gäller så väl i det förebyggande arbetet som i krishantering. Kommunikation och informationsdelning som uppfyller de krav som aktörerna har inom totalförsvaret kan vara en av grundförutsättningarna för totalförsvarsplaneringen.

En viktig aspekt i krishantering är att den ofta inte har några gränser. Internationell interoperabilitet är därför en viktig förutsättning för olycks- och krishantering vid samverkan med andra länder.

Myndigheter som har ett särskilt ansvar inför och vid höjd beredskap enligt Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och förordning (2015:1053) om totalförsvar och höjd beredskap ska återuppta planeringen för sin beredskap inom ramen för det civila försvaret. MSB understryker vikten av att den samverkan som behövs mellan aktörer inom krisberedskapen och

totalförsvaret behöver kunna göras med stöd av säkra och robusta kommunikationssystem.

Aktörerna ställer särskilda krav på mobil IP-baserad kommunikation

En kommunikationslösning för samhällsviktig verksamhet omfattar mer än vad som normalt sägs ingå i en kommunikationslösning för kommersiell användning. Detta beskrivs i Kommissionens rapport "*Is Commercial Cellular Suitable for Mission Critical Broadband?*"[5] Nedanstående punktlista är en redogörelse för de krav och egenskaper som ställs på mobil, IP-baserad kommunikation. I avsnitt 2.4 sker en fördjupning.

- Kommunikationslösningar som hanterar Sveriges krisledningsförmåga ska stå under svensk offentlig kontroll och lyda under svensk lagstiftning.
- Samhällsviktig verksamhet ska inom ramen för sitt uppdrag kunna kommunicera sekretesskyddade uppgifter och annan känslig information. Användarna behöver kunna hantera både öppen och hemlig information i kommunikationslösningen.
- Informationen ska vara tillförlitlig, inte kunna manipuleras och ska kunna skyddas mot obehörig åtkomst.
- Kommunikationslösningen ska alltid fungera och ha ett högt skydd mot otillåten påverkan samt stå emot t.ex. extrema väder och brand.
- Tillgänglighet behövs i hela landet. Aktörerna ska kunna lösa sina uppdrag var de än befinner sig.
- Kommunikationslösningen och kringutrustning ska bygga på globala standarder för att undvika de kostnadsdrivande inlåsningseffekter som nischmarknader ger. Detta gör det också möjligt att ta del av innovation och utveckling som sker på den publika marknaden. På så sätt uppnås en för samhället kostnadseffektiv lösning. Detta skapar också marknad för kommersiella aktörer.
- Användarna behöver långsiktiga och förutsägbara ekonomiska förutsättningar för såväl tjänster som kommunikationslösningar för att planera och finansiera sin verksamhet.
- Kommunikationslösningen ska möjliggöra gränsöverskridande krishantering.

[5] Contract number: 30-CE-0603428/00-19, SMART number: 2013/0016

2. Redovisning

MSB:s definition av *kommunikationstjänster* är i inom ramen för arbetet med detta regeringsuppdrag; de applikationer, tillämpningar och funktioner som möjliggör kommunikation inom och mellan användare. MSB:s definition av *kommunikationslösning* är den infrastruktur som bär kommunikationstjänsterna.

2.1 Inhämtning av krav

Kraven baseras på MSB:s kontinuerliga kravfångst från Rakels användarorganisationer, underlag från Försvarsmakten, Polisen och Trafikverket. MSB, Polisen och Försvarsmakten har också genomfört en workshop inom ramen för uppdraget. Krav har även hämtats från internationella arbeten genomförda av bland andra CEPT och ITU.

2.1.1 ECC:s rapport 199

MSB har tagit del av ECC:s rapport 199[6] som tar upp användarkrav och spektrumbehov för framtida europeiska bredbandssystem för aktörer inom samhällsviktig verksamhet (Wide Area Networks). Slutsatsen i rapporten är att det för datakommunikation för aktörer för samhällsviktig verksamhet behövs spektrum i intervallet 2x10 MHz under 1 GHz. Det kan finnas ytterligare spektrumbehov på nationell nivå för att tillgodose Direct Mode Operations (DMO), Air-Ground-Air (AGA), ad-hoc-nätverk och röstkommunikation. I rapport 199 konstateras att spektrumbehovet för aktörer för samhällsviktig verksamhet varierar mellan olika länder.

2.1.2 LEWP-RCEG[7] MATRIX OF APPLICATIONS[8]

Underlaget innehåller en översikt av applikationer för samhällsviktig verksamhet (s.k. PPDR-applikationer) med en kort beskrivning av speciella egenskaper för applikationerna. I samarbete mellan LEWP-RCEG och ETSI TC TETRA WG4[9] kompletterades matrisen senare med spektrumberäkningar. Resultatet blev att matrisen kan användas för detaljerad bedömning av spektrumbehov för olika scenarierna. Europeiska PPDR-organisationer är överens om matrisens innehåll och CEPT har erkänt den, som representativ för framtida PPDR-applikationer[10]. MSB har genomfört en jämförelse med

---

[6] ECC Report 199, User requirements and spectrum needs for future European broadband PPDR systems (Wide Area Networks), maj 2013.
[7] Law Enforcement Working Party – Radio Communication Expert Group
[8] ECC report 199, s.77
[9] ETSI Technical Committee (TC) TCCE (TETRA and Critical Communications Evolution) Working Group 4
[10] ECC Report 199, s. 23

statistik över svenska förhållanden och kan konstatera att matrisen är relevant för svenska överväganden.

2.1.3 FOI:s rapport om LTE[11]

FOI:s rapport identifierar att, för att använda LTE i samhällsviktiga och militära tillämpningar, måste ett antal särkrav beaktas och att dessa skiljer sig från de krav som ställs på publik användning. Till dessa egenskaper hör robusthet mot störningar, höga krav på informationssäkerhet samt en robust arkitektur som klarar av att delar av lösningen slås ut.

MSB ser, liksom FOI, att fortsatt arbete behövs kring åtgärder för förbättrad informationssäkerhet likaså bör störkänsligheten hos LTE hanteras för kritiska tillämpningar. Detta gäller särskilt i den övre delen av hotskalan. De särkrav avseende civil militär samverkan som FOI redogör för i sin rapport har tagits med i MSB:s underlag. För militärt bruk behöver även konsekvensen av att använda en cellbaserad arkitektur utredas.

2.1.4 Scenarier

Det är viktigt att förstå att kommunikation för samhällsviktig verksamhet måste kunna leverera rätt förmåga i hotskalans samtliga delar. I detta arbete har MSB därför tillsammans med Polisen och Försvarmaken utgått från flera scenarier, som sammantaget åskådliggör hela hotskalan: Från vardagshändelse och större en planerad eller oplanerad händelse, via samhällsomfattande kris exempelvis terrorism, till väpnat angrepp.

Beskrivningarna i scenarierna gör inte anspråk på att vara heltäckande utan syftar till att skapa större förståelse. Tjänsterna graderas i förhållande till hur verksamhetskritiska applikationerna och funktionerna är i de olika scenarierna; vardagshändelse; större planerad eller oplanerad händelse; samhällsomfattande kris; väpnat angrepp. För att dimensionera ett nät krävs fortsatta analyser och nätplanering. Kapaciteten och täckningen kommer att behöva justeras över tid samt utifrån tillgängliga lösningar och teknikutveckling som t.ex. 5G.

Vardagshändelse (PP1[12])
I rapport 199 exemplifieras vardagshändelser av typen PP1 med en trafikkontroll och en trafikolycka. I vår jämförelse har scenarier om en liten trafikolycka och en lägenhetsbrand använts, se *bilaga 2*.

[11] Long Term Evolution, vilket innebär standarden för 4G
[12] Report ITU-R M.2033, s.10

Större planerad eller oplanerad händelse (PP2[13])
I rapport 199 exemplifieras större planerad eller oplanerad händelse av typen PP2 med ett kungligt bröllop och social oro. I vår jämförelse har följande scenarier om en stor trafikolycka och ett statsbesök använts, *se bilaga 2*.

En händelse av typen PP2 kan inträffa var som helst, även på platser där kapaciteten i nätet inte är dimensionerad för större händelser pga. låg befolkningstäthet eller geografisk placering. Där kan extra kapacitet behöva tillföras för att hantera händelsen. Aktörer inom samhällsviktig verksamhet ställer därför krav på att nätkapaciteten ska kunna utökas eller prioriteras för berörda användargrupper med kort varsel.

Samhällsomfattande kris, exempelvis terrorism (DR[14])
Enligt rapport 199, genereras i katastrofscenariers (DR) inledande faser vanligtvis en hög trafikbelastning. Detta kan jämföras med trafikbelastningen vid scenarier för större planerad eller oplanerad händelser (PP2). Initialt kan trafiken i ett DR-scenario stödjas av ett nät för samhällsviktig verksamhet förutsatt att det fortfarande är i drift. I de senare faserna av DR-scenarier kan trafikbelastningen delas mellan olika celler i nätet och därmed blir jämförbar med vardagshändelse (PP1).

Till detta läggs att ytterligare liknande händelser kan inträffa på annan plats dvs. i andra celler i nätet. Då behöver extra kapacitet tillföras för att hantera händelsen. Aktörer inom samhällsviktig verksamhet ställer då krav på att nätkapaciteten ska kunna utökas eller prioriteras för berörda användargrupper med kort varsel. I en terrorismhändelse är det inte ovanligt att flera på varandra följande händelser sker. Vid t.ex. terrorism ställs stora krav på underrättelser och informationsdelning för att kunna hantera och förebygga.

Väpnat angrepp
Vid ett väpnat angrepp av typfall 2 kommer degradering ske av systemen i ökande takt. Detta kommer att innebära stor belastning på kvarvarande kapacitet, samt ett igångsättande av reservförfarande. Detta kan i sin tur ställa krav på ytterligare tillgång till spektrum och nationella resurser för att hantera detta. Kommunikationslösningen behöver kunna klara antagonistiska hot, såväl fysiska som logiska, samt ha skydd och beredskap mot elektronisk krigföring. Radiogränssnittet mellan terminal och basstation är en av de möjliga angreppspunkterna vid en väpnad konflikt. Stora krav ställs på kommunikationslösningens uthållighet för att medge att tillräcklig förmåga kan upprätthållas under väpnat angrepp.

---

[13] Report ITU-R M.2033, s. 11
[14] Report ITU-R M.2033, s. 11

Vid beslut om höjd beredskap inträder särskild lagstiftning. Regeringens befogenheter och mandat är dessutom utvidgade under höjd beredskap och Regeringsformen ger möjligheter till utökade befogenheter för enskilda myndigheter. Oavsett om annan lagstiftning träder i kraft vid väpnat angrepp, behöver kommunikationen för samhällsviktigt verksamhet säkerställas. Försvarsmaktens krav för dessa situationer är inte dimensionerande för kommunikationslösningen och det kommer inte användas för insatsledning eller för lösande av Försvarsmaktens stridsuppgifter.

2.2 Vilka behov har aktörerna av säkra och tillgängliga mobila, IP-baserade kommunikationstjänster?

De mobila, IP-baserade kommunikationstjänster som aktörerna behöver kan grovt delas in i två kategorier; tal och data.

2.2.1 Sammanfattat behov av talkommunikation

IP-baserade taltjänster motsvarar de behov av taltjänster som idag erbjuds i Rakel:

- Individsamtal och gruppsamtal med korta uppkopplingstider (< 200 ms för individsamtal och respektive 400 ms för gruppsamtal) mellan användare, såväl inom egen organisation som mellan organisationer.
- Upprätta talkommunikation med användare i andra nät, s.k. Inter System Interface (ISI) eller samtal till det publika telenätet.
- Direct Mode-samtal (DMO) för möjlighet att kommunicera utan kontakt med radioinfrastrukturen.
- Individsamtal och gruppsamtal mellan mark och luftfarkoster, s.k. Air Ground Air (AGA).
- Möjlighet att sätta upp ett fristående nät när det ordinarie drabbas eller riskerar att drabbas av avbrott samt när det ordinarie nätets prestanda inte räcker till eller befaras att inte räcka till.

Samhällsutvecklingen, och de förändringar i kommunikationsmönstren som det innebär, medför att sambandsmetodiken utvecklas. Detta leder till att nya krav på taltjänster kommer att ställas. Den tekniska utvecklingen kommer medföra att traditionella taltjänster kommer ersättas med VoIP (Voice over IP). Därför måste VoIP i framtiden uppfylla kraven för verksamhetskritisk kommunikation.

2.2.2 Sammanfattat behov beträffande överföring av data

Aktörer inom allmän ordning, säkerhet, hälsa samt försvar behöver kunna överföra och dela data mellan:

- Organisationer
- Individer
- Grupper
- Ledningscentraler och sambandscentraler
- Centrala och lokala databaser
- Maskin till maskin (M2M). Exempel på detta är övervakningsutrustning för kraftledningar som skickar information till driftcentraler, smarta fordon, smarta uniformer m.m.

Mobila IP-baserade kommunikationstjänster för dataöverföring måste hålla en kvalitet som möjliggör bildöverföring av video och högupplösta stillbilder till och från mobila enheter. Tjänsten ska kunna stödja mobila basstationer som vid behov kan ge utökad täckning och, eller, kapacitet (ad-hoc-nätverk). Detta för att exempelvis kunna tillhandahålla mobila ledningsplatser där det ordinarie nätets täckning och, eller, kapacitet är bristfällig.

Polis, ambulans och räddningstjänst kommer att utrusta fordon i utryckningsverksamheten med förmåga att skicka och ta emot strömmande video. Inom polisen kommer videokameror att ingå i den personliga utrustningen för både utrycknings- och spaningspersonal. Vid insatser, t.ex. vid statsbesök och idrottsevenemang som samlar många människor, är video med hög och låg upplösning ett nödvändigt verktyg i det förbyggande, åtgärdande, utredande och uppföljande arbetet, se vidare i *bilaga 1*.

2.3 Vad ska uppnås med kommunikationslösningarna?

Detta avsnitt beskriver på en övergripande nivå vad som ska uppnås med kommunikationslösningen, vilket också är grunden till samhällets krisledningsförmåga i det offentliga åtagandet.

En kommunikationslösning som fungerar när den behövs

Kommunikationslösningar för samhällsviktig verksamhet måste fungera när och där de behövs. När en enskild är i nöd och larmar måste det gå att förlita sig på att hjälpen kommer. Sker inte detta minskar förtroendet för samhället och i synnerhet för de aktörer som har ansvar att säkerställa allmän ordning, säkerhet, hälsa samt försvar. Kommunikationen inom och mellan aktörer inom allmän ordning, säkerhet, hälsa samt försvar, skiljer sig markant från kommunikationsmönstren i kommersiella nät. De är inte alltid förutsebara geografiskt och i fråga om när kapacitetsbehov uppstår. Större incidenter som flygplanshaverier eller terrorattacker är ovanliga, men kan hända när och var som helst. Lösningar som vanligtvis används av kommersiella operatörer innebär att tåligheten mot påfrestningar i näten, i form av t.ex. överbelastning

och avsiktlig störning, är begränsad. Detta beskrivs också i kommissionens rapport "*Is Commercial Cellular Suitable for Mission Critical Broadband?*"[15].

I ett nät för samhällsviktig verksamhet måste kraven på robusthet, tillgänglighet, säkerhet, täckning och prioritet säkerställas, överallt och alltid. Kontrollen över service och ägarförhållande för kommunikationstjänsten måste också säkerställas.

Kommunikationstjänster möjliggör effektivt arbete

Kommunikationslösningarna måste skapa förmåga hos samhällsviktig verksamhet att fullgöra sitt författningsreglerade uppdrag. Digitaliseringen av samhället är en viktig möjliggörare för detta och hur samhällsviktig verksamhet genomförs är därför statt i förändring det innebär t.ex. förändringar som utflyttade arbetsplatser för att komma närmare samhällsmedborgarna, mobila kontor, fjärrledning, smarta kläder, sensorer och obemannade farkoster.

Kommunikationslösningar för kommunikation vid samhällsstörningar ska bidra till effektiv informationsdelning. Informationsdelning mellan olika aktörer vid samhällsstörningar är en förutsättning för att ta rätt beslut och vara till stöd för krishanteringssystemets metodik.[16] Kommunikationslösningen ska kunna möjliggöra utbyte av information mellan aktörer, detta ställer krav på informationssäkerhet utifrån konfidentialitet, riktighet och tillgänglighet. En gemensam infrastruktur bidrar till att skapa enhetlighet i kommunikation och informationsdelning oavsett vilken kommunikationslösning som används. Grunden för en fungerande operativ verksamhet är att direkt kunna leda och styra de egna operativa resurserna samt att kunna samverka med andra aktörer. Flertalet av de händelser som kommer in via 112 till SOS Alarm kräver en väl fungerande samverkansförmåga.

Krisberedskapssystemet bygger på samverkan mellan ansvariga aktörer. Denna samverkan måste kommunikationslösningarna stödja. Framtida kommunikationslösningar måste också möta kraven på samverkan inom totalförsvaret.

Det finns också anledning att lyfta fram att kommunikationslösningen för polisens del även handlar om att realisera polisreformens huvudsyfte. Att komma närmare medborgarna är en av huvudinriktningarna för bildandet av Polismyndigheten. Polisen ska arbeta nära medborgarna i lokalsamhället över hela Sverige. Huvudinriktningen kommer från en bred parlamentarisk enighet. Den ställer krav på mobila bredbandslösningar och ytterligare krav som

---

[15] Contract number: 30-CE-0603428/00-19, SMART number: 2013/0016
[16] Gemensamma grunder för samverkan och ledning vid samhällsstörningar (MSB777), Gemensamma grunder för samverkan och ledning vid samhällsstörningar – Sammanfattning (MSB780)

redogjorts för. Ett krav som bör lyftas särskilt i anslutning till arbetet nära medborgarna är kravet på kommunikationslösningar under offentlig kontroll.

Kostnadseffektiva lösningar för staten som helhet

Kommunikationslösningar för aktörer inom allmän ordning, säkerhet, hälsa samt försvar består av en tät koppling mellan kommunikationstjänster och produkter (mjukvara och hårdvara). Kommunikationslösningarna ska ta del av innovation och utveckling för att uppnå en för samhället kostnadseffektiv lösning. Kostnadseffektiviteten uppnås bland annat genom långsiktiga och förutsägbara ändringar av såväl tjänster som kommunikationslösningar. Tillgång till kommersiell utrustning för såväl nät som för terminaler måste också säkerställas för att skapa kostnadseffektivitet.

Målsättningen är att till så stor del som möjligt använda lösningar som bygger på globala standarder avseende infrastruktur och dess kringutrustning. Detta för att skapa en så konstandseffektiv lösning som möjligt och undvika inlåsningar i nischmarknader. Behovet av verksamhetskritiska funktioner inom LTE har identifierats och standardiseringsarbete pågår inom 3GPP[17].

Under den kartläggning och behovsinventering av kundbehoven av datatjänster som genomfördes under första och andra kvartalet 2014 med ett tiotal aktörer inom allmän ordning, säkerhet, hälsa samt försvar beskrevs flera svårigheter med kommersiella operatörer. Av rapporten från denna kartläggning framgår att en klart framträdande brist med de kommersiella alternativen är att det inte går att avtala servicenivåer. Avtalen kan ändras ensidigt från operatörens sida under pågående avtalsperiod vilket medför stora konsekvenser för användarorganisationerna som arbetar med samhällsviktig verksamhet. Vidare så är frågor som säkerhet, tillgänglighet, robusthet och uthållighet anledningar till att aktörerna inte vågat ta steget fullt ut att realisera verksamhetskritiska mobila satsningar. Aktörerna efterfrågar en långsiktig, stabil operatör eller leverantör av kommunikationstjänster som en förutsättning för att på ett säkert sätt” genomföra vissa av sina effektiviseringsprogram i riktning mot ett mer mobilt arbetssätt. Ledord är nationell täckning, ekonomisk uthållighet och möjlighet att kunna avtala servicenivåer.

2.4 Vilka krav ställer aktörerna på kommunikationslösningarna?

2.4.1 Offentlig kontroll

Aktörer inom allmän ordning, säkerhet, hälsa samt försvar som påverkar Sveriges krisledningsförmåga ska ha förutsättningar att följa de beslut som finns och som kan bli aktuella vid olika beredskapsåtgärder. Kommersiella

[17] http://www.3gpp.org

intressen ska inte direkt- eller indirekt via utländska ägare och kommersiella villkor kunna påverka Sveriges krisledningsförmåga. Därför är en kommunikationslösning som står under svensk offentlig kontroll nödvändig.

Med offentlig kontroll över kommunikationslösningen kan säkerställas att data inte hamnar hos annan aktör för insamling, analys eller manipulering. Vidare gäller inte svensk rättsverkan utanför rikets gränser. Om t.ex. hemlig kameraövervakningssignal hamnar utanför rikets gränser påverkar detta kontrollen över bevismaterialet.

2.4.2 Särskild funktionalitet

Kommunikationslösningen ska erbjuda kort uppkopplingstid. Dessa behov tillfredsställs idag med Rakel. Kommunikationslösningen ska också erbjuda gruppsamtal som är implementerade så att de belastar nätet minimalt (jmf med funktionaliteten gruppsamtal i Tetra). Verksamhetskritiska gruppsamtal ställer andra krav än vanliga röstsamtal och är en viktig grundläggande funktion för aktörer inom allmän ordning, säkerhet, hälsa samt försvar. Specifikt för denna typ av gruppsamtal är bland annat effektiv och dynamisk gruppkommunikation med kort uppkopplingstid (300 millisekunder eller kortare) och prioriteringsfunktioner mellan individer och grupper. Behovet av speciella lösningar för verksamhetskritiska gruppsamtal är identifierat av bl.a. 3GPP och utveckling av standarder för detta inom LTE pågår. Mer information om detta arbete finns att läsa på 3GPP. Kommunikationslösningen för samhällsviktig verksamhet ska vidare erbjuda både företräde och prioritet för nödsamtal, så kallad pre-emption och priority.

Till detta kommer krav på funktionalitet motsvarande Direct Mode Operations (DMO), Air-Ground-Air (AGA) och ad-hoc-nätverk.

2.4.3 Prioritet

Aktörer inom samhällsviktig verksamhet ställer krav på att, vid resursbrist i nätet, kunna prioritera:

- Resurser för specifika användargrupper och roller.
- Mellan olika tjänster.

För att samhällsviktig verksamhet ska kunna utföra sitt uppdrag, kommer prioriteringar vara av yttersta vikt i en framtida kommunikationslösning. När olyckor och kriser uppstår ökar behovet för allmänheten att kommunicera med varandra. Därför är det viktigt att aktörer inom samhällsviktig verksamhet inte konkurrerar med allmänhetens möjligheter att kommunicera.

Exempel på funktioner och scenarion där prioritet förutsätts:

- Sjukvårdspersonal, polis, räddningstjänst m.fl. hamnar i nödläge och ”larmar” för att få understöd. I detta fall ska larmfunktionen ha högsta prioritet i infrastrukturen för att kontakt med en lednings-, eller sambandscentral ska kunna etableras och hjälp bistås den nödställda.

Larmet ska också omedelbart nå näraliggande egna resurser så att de kan komma till snabb undsättning.

- Ordergivning ska kunna prioriteras högre än vanlig talkommunikation för att information till fältoperativ personal ska kunna förmedlas på ett effektivt sätt.
- Positioneringsinformation ska kunna prioriteras högre än vanlig text-kommunikation då positionering är tätt kopplad till dirigering av de fältoperativa resurserna samt är en säkerhetsfunktion tätt kopplad till positionering av nödställd.
- Stillbilder och video ska kunna prioriteras vid t.ex. särskilda händelser där förmedling av lägesbild är kritiskt för insatsen.
- Flygsäkerhet ställer höga krav på kommunikation och kommunikationslösningar. Prioritet är därför en särskilt viktig funktion där trafik från flygledartornet alltid skall komma fram till personalen på marken. Förutom prioritet behövs funktionen ”pre-emption” som innebär att om det inte finns tillgänglig kapacitet så kopplas ett annat pågående samtal ned för att säkerställa att den prioriterade talgruppen eller anropet kan kopplas upp. Kraven på kommunikationen är reglerade i regelverk kring flygsäkerheten.[18]

2.4.4 Informationssäkerhet

Kommunikationslösningen och dess tjänster ska kunna hantera såväl öppen som sekretessbelagd information. Det är viktigt att en framtida kommunikationslösning för mobil IP-baserad kommunikation möjliggör informationsutbyte med aktörer som i sitt uppdrag använder publika nät, så som allmänheten, frivilligorganisationer, frivilliga resursgrupper och privata företag.

I den samhällsviktiga verksamheten hanteras en stor mängd information som berör den enskildes integritet. Den offentliga verksamheten ges ett förtroende att hantera känslig information om enskilda. Det ställer höga krav på att den offentliga verksamheten i enlighet med gällande lagstiftning kan skydda informationen från obehörig åtkomst

Informationsöverföringar i kommunikationslösningen ska kunna genomföras inom ramen för gällande lagstiftningar om sekretess, bland annat så finns ett uttryckt behov av att kunna förmedla uppgifter som omfattas av sekretess och rör rikets säkerhet (OSL 2009:400 kap 15 § 2). Samhällsviktig verksamhet ska med hänsyn till den enskildes personliga integritet och kraven på god verksamhetssäkerhet tryggt kunna kommunicera uppgifter som omfattas av sekretess och annan skyddsvärd information. Informationen ska skyddas mot

[18] EU 1035/2011, EG 482/2008, EG 1108/2009, TSFS 2012:6, TSFS 2013:7, TSFS 2013:5, ICAO Annex 11 med flera.

manipulation och obehörig åtkomst. Det gäller i alla lägen; från den enskilda olyckan till höjd beredskap.

Krav på autentisering
I bilaga 3 kan det utläsas krav på funktion ”positionering” som avser positioneringstjänst mellan inblandade enheter och ledningscentraler. En sådan tjänst ställer höga krav på autentisering i kommunikationslösningen för att säkerställa att rätt person eller användare eller enhet är den vars position som indikeras. En kommunikationslösning utan krav på autentisering av anslutna terminaler medför att de verksamheter som vill nyttja en positioneringstjänst inte kan vara säkra på att uppgifterna är korrekta. Således blir det positioneringsdata som skickas opålitligt.

Krav på spårbarhet
I bilaga 3 kan det utläsas krav på funktion ”registerslagningar”. De aktörer som ska nyttja framtida kommunikationslösningar har identifierat ett behov av att kunna göra registerslagningar för att får fram listor över icke identifierad person ellerförsvunnen person eller fordon. En myndighet som i det här exemplet kan antas vara polismyndigheten ställer från början höga krav på åtkomst till dessa register avseende spårbarhet för att kunna gå tillbaka för att se vem eller vilka personer som gjort vilka slagningar. Spårbarhet behövs för att stödja verksamheten, i det här fallet för att Polisen ska kunna utföra sina uppgifter.

Den samhällsviktiga verksamheten måste även i efterhand kunna granskas och ansvar kunna utkrävas. Det måste gå att rekonstruera kommunikationsflödet vilket ställer krav på bland annat spårbarhet. Det är ett krav i den offentlighetsprincip och transparens som ska råda i Sveriges offentliga verksamhet. Till exempel behöver man i efterhand kunna fastställa vem som fattade ett visst beslut eller i ett givet läge hade tillgång till en specifik information.

Krav på sekretess (konfidentialitet) och kontroll av informationsflöden
I flera av scenarierna beskrivna i bilaga 2 framgår det bland annat att uppgifter som omfattas av sekretess enligt OSL och rör rikets säkerhet eller patientdatalagen kommer att utbytas i framtida kommunikationslösning. Detta medför att krav på konfidentialitet avseende den information som utbyts mellan aktörer även avspeglas på kommunikationslösningen. För att förhindra obehörig åtkomst till information i kommunikationslösningen ställs därför särskilda krav tillträdesskydd (t.ex. fysisk åtkomst till master), skydd mot olovlig avlyssning (i t.ex. luftgränssnittet) och kontroll av de fysiska förbindelser som knyter samman kommunikationslösningen (kärnnätverket).

Tillgänglighet inom ramen för krav på informationssäkerhet
Den hotbild som finns mot Sverige innebär att det är troligt att en angripare kan försöka utarbeta skräddarsydda attacker mot samhällsviktiga verksamheter. Hotet kan sammanfattas som att ansluten utrustning kan användas som bas för en attack mot nätet i syfte att påverka t.ex.

tillgängligheten och, eller, informationen i nätverket. Verksamheterna kommer således att behöva förlita sig på ett avvägt risktagande avseende det samordnade totalförsvarssambandet, där behovet av att dela information vägs mot behovet av att skydda densamma.

Kraven som samhällsviktig verksamhet ställer är:

- Kommunikationslösningen för samhällsviktig verksamhet har krav på adekvat redundans i alla konfliktnivåer. De delar där det är ekonomiskt och tekniskt möjligt ska särskiljas från infrastruktur med kommersiella ägarförhållanden.
- Kommunikationslösningar ska vara byggda och designade på ett sådant sätt som begränsar att den exponeras. Skalskydd och tillträdesbegränsning är två sätt att realisera detta.
- Det måste finnas funktioner som begränsar access till nätet, för att minska risken för t.ex. DoS-attack[19] mot nät. Detta kan ske t.ex. genom autentisering.
- Det måste finnas funktioner som säkerställer att utrustning inte kan störa ut möjligheten för att nätet ska kunna övervakas och administreras.
- Det måste byggas upp funktioner som begränsar attackernas möjlighet att störa ut kommunikationen.

Aktörer inom allmän ordning, säkerhet, hälsa samt försvar ska kunna hantera information som är öppen såväl som sådan som omfattas av sekretess och rör rikets säkerhet. I scenarierna i bilaga 2 i avsnitt 2.2 och 2.3 framgår det att kommunikationslösningen ska kunna användas i samverkan mellan civila aktörer och Försvarsmakten. I detta ingår inte enbart scenariot väpnat angrepp utan även verksamhet som pågår innan ett sådant scenario realiseras. MSB, Polisen och Försvarsmakten gör den gemensamma bedömningen att uppgifter som omfattas av sekretess kommer delas mellan anslutna aktörer.

2.4.5 Robusthet

Robusthet uppnås genom krav på tillgänglighet; uthållighet, reciliens och informationssäkerhet. Krav på informationssäkerhet redogörs för i avsnitt 2.4.4.

Tillgänglighet
En kommunikationslösning för samhällsviktig verksamhet måste fungera i vardag och vid påfrestningar orsakade av naturen eller människan. En

[19] Denial of Service, en attack mot ett it-system i syfte att hindra normal användning av systemet, överbelastningsattack.

utmaning med kommersiella nät är att dessa tenderar att bli överbelastade eller otillgängliga under större händelser och påfrestningar. De blir då oanvändbara. Vid dessa tillfällen behöver samhällsviktig verksamhet kunna fungera som allra bäst och då är kommunikationerna avgörande. Tillgängligheten i ett nät för samhällsviktig verksamhet ska därför hålla en nivå som möter alla scenarier i bilaga 2.

Målsättningen för samhällsviktig kommunikation måste vara 100 % tillgänglighet men MSB är medvetna om att det finns omständigheter som gör att det svårt att uppfylla målet i praktiken. Men eftersom ett nät för samhällsviktig verksamhet är tänkt att fungera även under extrema väder, brand och höjd beredskap så måste det designas för att klara sådana omständigheter till skillnad mot kommersiella nät.

Reservkraft
Vid kraftbortfall ska kommunikationslösningen ha en uthållighet över tid. Idag åstadkoms detta i Rakel med reservkraftverk, batterikraft och överlappande täckning. MSB har använt Rakel-systemet som utgångspunkt och referens. Uthållighet över tid kan uppnås med reservaggregat t.ex. sju dygns dieseldrift som kan förlängas genom påfyllning av diesel. En framtida kommunikationslösning måste också kunna använda nya tekniker för att säkerställa robusthet och tillgänglighet t.ex. batteri kombinerat med bränslecellsteknik.

Redundans och reciliens
Kommunikationslösningen ska klara att vissa delar av lösningen slås ut utan att kommunikationen omöjliggörs. Detta innebär krav på inbyggd redundans och diversitet samt återställningstider som innebär att återställningsarbete initieras direkt. Organisationen för övervakning, drift och underhåll behöver vara dedikerad för att säkerställa tillgängligheten.

Förstärkningsresurser
Vid en påverkan på kommunikationslösningen i sådan omfattning att funktionaliteten degraderas, måste det finnas reservförfarande för att säkerställa en minsta nivå av kommunikation mellan aktörer inom allmän ordning, säkerhet, hälsa samt försvar över hela Sveriges yta. Detta bör ske t.ex. med möjlighet till mobila förstärkningsresurser i den minutoperativa verksamheten. Kommunikationslösningen behöver därför säkerställa att det finns tillgång till frekvenser för att snabbt utöka tillgängligheten och kapaciteten när och där det behövs inom ramen för det tilldelade frekvensutrymmet.

Förvaltning
Kommunikationslösningen ska förvaltas på ett sätt som löpande omhändertar användarnas operativa behov och förutsättningar. Detta ska ske bl.a. genom löpande anpassning av skyddsåtgärder som säkerställer tillgänglighet, robusthet och informationssäkerhet.

2.4.6 Kapacitet

För att aktörer inom allmän ordning, säkerhet, hälsa samt försvar ska kunna utföra sina uppdrag ställs det höga krav på kommunikationslösningens upplänk såväl som nedlänk avseende datakapacitet. Exemplifieringen i scenarierna ställer inte enbart krav på utökad täckning, utan även utökad kapacitet. Exempel på händelser som har ställt krav på att snabbt utöka kapacitet är insatserna i Ojnareskogen (Gotland, 2012), och Salem-demonstrationerna (2001-2010). De krav som ställs på kapacitet i kb/s per applikation finns redovisat av LEWP-RCEG.[20]

2.4.7 Täckning

Aktörer för samhällsviktig verksamhet behöver ha mycket god geografisk yttäckning för trafik 24/7/365. Tillförlitlig täckning krävs både inomhus och utomhus. Operativ täckning behöver också säkras för avlägsna områden och underjordiska eller otillgängliga områden (t.ex. tunnlar och källare). MSB är medveten om de stora kostnader som yttäckning är förenade med. För att nå en realistisk lösning behöver överväganden göras som säkerställer att yttäckning finns när aktörer inom allmän ordning, säkerhet, hälsa samt försvar behöver den att och möjlighet finns att förstärka och utöka nätet, när och där det behövs.

Behov för mycket god yttäckning kommer också av kraven att aktörerna snabbt ska kunna mobilisera sina resurser. Lösningen måste vara dimensionerad för händelser som uppstår sällan, och på i förväg okända platser, men som kräver stora resurser. Ytterligare resurser som antingen ökar täckning, kapacitet eller båda två behövs under pågående incident för täckning av lokaliserade områden. Därför behövs lösningar för mobila ad-hoc-nätverk.

2.5 Vilka krav ställer den internationella utvecklingen avseende operativ samverkan med aktörer från andra länder och internationella organisationer?

Dagens kriser och konflikter uppstår snabbt och tar inte hänsyn till några nationsgränser. Resurser måste kunna sättas in snabbt för att göra nytta. I och med allt mer gränsöverskridande kommunikation med samarbetspartners och aktörer i andra länder, blir det också allt viktigare att säkerställa att skyddsvärdena är analyserade, kända och hanterade. De slutsatser som Europeiska Kommissionen presenterar avseende förutsättningar för operativ samverkan med aktörer i andra länder måste vägas in i förslag på lösningar för

[20] ECC report 199, s.77

kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar i Sverige.[21]

Operativ samverkan omfattar såväl att ta emot som att lämna stöd till andra länder. I operativ samverkan har aktörerna behov av information från de länder som samverkan sker med. Målet är att de kommunikationslösningar som aktörer inom samhällsviktig verksamhet använder ska vara interoperabla. Detta innebär att andra länders aktörer inom samhällsviktig verksamhet ska kunna använda sin utrustning i Sverige och att svenska aktörer inom samhällsviktig verksamhet ska kunna använda sin utrustning i andra länder. Det kräver att aktörerna har tillgång till utrustning som stödjer harmoniserade frekvenser för aktörer inom samhällsviktig verksamhet.

Operativ samverkan med andra länder kräver att gemensamma analyser och lägesbilder kan skapas och delas. Eftersom analyser och lägesbilder av samverkan ofta är tvärsektoriell finns behov av information från många berörda aktörer. Denna information har olika nivåer av krav och behov som redogjorts för i svenska förhållanden. Nedan redogörs för ett urval av samarbeten och de krav som de ställer på kommunikation inom ramen för den operativa samverkan med aktörer från andra länder och internationella organisationer.

Den lösning som implementeras i Sverige får inte vara unik för Sverige. För att skapa bästa förutsättningar för en regional marknad för system och tjänster behöver vi eftersträva en lösning som möjliggör, och underlättar, operativ samverkan över nationsgränser. Detta gynnar också utvecklingen av gemensamma tekniska lösningar och standarder, vilket ger den bästa samhällsekonomiska effekten.

2.5.1 Nordiskt samarbete

Sverige har flera avtal om samarbete med de nordiska länderna. Sverige, Norge, Finland, Danmark och Island antog 2011 en nordisk solidaritetsförklaring. Den beskriver att de nordiska länderna ska samarbeta för att möta utrikes- och säkerhetspolitiska utmaningar i samband med potentiella risker som katastrofer, IT- och terrorangrepp. Det är därmed naturligt att Sverige kommer att be om stöd och stödja våra nordiska grannländer vid en samhällsstörning. Detta ställer krav på interoperabla kommunikationslösningar.

2.5.2 ISI- Nor–Swe

Inter System Interface Norge-Sverige (ISI Nor-Swe) är ett samarbetesprojekt mellan Direktoratet för nödkommunikation (DNK) och MSB. Målet med projektet är att möjliggöra effektiv kommunikation över landsgränserna mellan

[21] Is Commercial Cellular Suitable for Mission Critical Broadband? European Union, 2014. ISBN 978-92-79-38679-4

aktörer (polis, räddningstjänst, ambulans och tull) med stöd av svenska Rakel och norska Nödnett. Målet med projektet realiseras genom att näten kopplas samman via ett gränssnitt som tillåter svenska och norska blåljusaktörer att kommunicera över gränsen. Aktörerna kommer då kunna bistå varandra vid olyckor, kriser och andra händelser där resurser från annat land krävs. Rakel-mobilerna ska kunna användas i Norge och de norska Nödnett-mobiler i Sverige. MSB och DNK har inom ramen för projektet utvecklat processer, gemensamma riktlinjer för gränsöverskridande samverkan och utbildning för användarna när de nya funktionaliteterna tas i bruk. ISI-projektets utgångspunkt, gränsöverskridande kommunikation, skapar förutsättningar för aktörerna att leva upp till krav som operativ samverkan över landsgränsen ställer. En naturlig utveckling är att ISI-projektet ska utvidgas till att omfatta även Finland och Danmark.

ISI-projektet visar på dagens behov. Det framtida systemet måste i ännu högre grad stödja gränsöverskridande verksamhet eftersom sådan verksamhet bedöms öka i takt med övrig samhällsutveckling.

2.5.3 Polisens internationella operativa samarbeten

Polisen deltar i internationellt operativt polissamarbete. Det sker inom ramen för till exempel brottsutredningar, direkt med annan stats polisorganisation eller genom Europol, Schengensamarbetet, Interpol eller det nordiska polissamarbetet. Detta ställer krav på att operativa enheter från respektive land, genom en säker förbindelse, kan samverka under pågående insatser och dela lägesbilder, underrättelseinformation som minutoperativ samverkan i realtid. Samverkan kan till exempel gälla både i förväg kända händelser (t.ex. narkotikasmuggling eller människohandel) och hastigt uppkomna händelser som terrorism eller annan krissituation. Vid sidan om Prümrådsbeslutet antog RIF-rådet i juni 2008 även Atlasrådsbeslutet, vilket ger Europeiska polisiära insatsstyrkor möjlighet att hjälpa varandra främst vid terrorism.

I Europeiska Rådets rekommendation från 2009[22] beskrivs att effektivt samarbete över gränserna kräver lämpliga kommunikationsmöjligheter, inklusive kompatibla radiokommunikationssystem i gränsområden och mellan operativa tjänster från olika medlemsstater.

2.5.4 Internationella försvarssamarbeten

Inriktningen av Försvarsmaktens internationella samarbeten tar sin utgångspunkt i behovet av att skapa och använda förmågor. De operativa behoven är vägledande för Försvarsmaktens internationella samarbeten och utgör utgångspunkt för att värdera vilka samarbeten som ska genomföras. Den

[22] Draft Council Recommendation on improving radio communication between operational units in border areas 10141-09

svenska solidaritetsförklaringen[23], det nordiska och baltiska samarbetet, olika bilaterala samarbeten, medlemskapet i FN, EU och OSSE[24], och det nära samarbetet med Nato bildar det militärstrategiska sammanhanget för Försvarsmaktens agerande.

Interoperabilitet med våra tilltänkta samarbetspartners är en förutsättning för att kunna bedriva ett effektivt internationellt försvarssamarbete och för att kunna ta emot och ge militärt stöd samt kunna delta i internationella operationer i nära samverkan med andra länder och organisationer. Samarbetsmöjligheterna och utvecklad interoperabilitet med Finland ska här särskilt uppmärksammas och det fördjupade bilaterala försvarssamarbete mellan Danmark och Sverige realiseras. Oavsett samarbetsforum ska Nato:s processer, procedurer, metoder och standarder användas som grund för att uppnå efterfrågad interoperabilitet.

Tillgång till relevant frekvensspektrum vid nationell såväl som vid internationell krishantering, i och kring vårt närområde, är en förutsättning för att uppfylla regeringens krav på att säkerställa vår nationella säkerhet och att kunna bistå i enlighet med solidaritetsförklaringen. Sverige ska därför kunna ge och ta emot stöd såväl civilt som militärt.[25]

2.5.5 Samarbeten inom FN

MSB har fått i uppdrag av regeringen att se över hur MSB kan stödja med personal inom FNs fredsfrämjande insatser. Dessa insatser kan ha andra krav på kommunikationen än de humanitära insatserna som MSB vanligtvis samarbetar med FN kring. Vid tillgång till frekvensband i insatsområdet finns möjligheten av använda den ad hoc-lösning som är en del av kommunikationslösningen. MSB förutsätter att en framtida kommunikationslösning för samhällsviktig verksamhet uppfyller aktörernas krav och därmed innehåller tekniska förutsättningar som möjliggör ad hoc-lösningar. MSB ser att det ur ett krishanterings- och samhällsekonomiskt perspektiv är viktigt att kunna återanvända gjorda investeringar. Exempelvis avses användning i internationella insatser där en mobil ad hoc-lösning framtagen för samhällsviktig verksamhet kan användas för att skapa täckning och på det sättet möjliggöra kommunikation vid insatser i katastrofområden.

2.5.6 Samarbeten inom EU – Civil konflikthantering

Då insatser för civil konflikthantering ofta är politiskt känsliga har ibland en högre grad av säker kommunikation krävts. I bland annat insatserna i Aceh och Georgien har det ställts krav på krypterade GSM-telefoner. MSB står ofta för

---

[23] Sverige kommer inte att förhålla sig passivt om en katastrof eller angrepp skulle drabba ett annat EU-medlemsland eller nordiskt land. Sverige förväntar sig att dessa länder agerar på samma sätt om Sverige drabbas.
[24] Organisationen för Säkerhet och Samarbete i Europa
[25] Regeringens utrikesdeklaration 2015.

personal inom just områdena IT och kommunikation i dessa insatser. Vid tillgång till frekvensband i insatsområdet finns möjligheten av använda den ad hoc-lösning som är en del av kommunikationslösningen.

2.5.7 Förändrade förutsättningar utifrån internationellt pågående arbete

Inom internationella forum och EU skapas förutsättningarna för kommunikation i internationell operativ samverkan. Det finns stort intresse för att inkludera samhällsviktig verksamhet som en harmoniserad användning av spektrum. Intresset går att utläsa genom att arbetet t.ex. med 700 MHz-bandet där samhällsviktig verksamhet är ett utpekat användningsområde, har pågått i flera år. Kommissionen, Radio Spectrum Committee, har kommunikationsfrågor för samhällsviktig verksamhet på agendan.

CEPT har färdigställt rapporter avseende användarkrav och spektrumbehoven för framtida Europeiska bredbandssystem för samhällsviktig verksamhet (Wide Area-nätverk)[26], som används som stöd i arbetet med detta underlag. Rapporten om harmoniserade tekniska villkor för 694-790 MHz[27] färdigställs för närvarande. Rapporten om harmoniserade tekniska villkor och spektrumband för genomförandet av europeiska bredbandssystem för samhällsviktig verksamhet (BB-PPDR)[28] är färdigställd.

[26] ECC Report 199.
[27] ECC Report 60
[28] ECC Report 218

Bilaga 1

Exempel på krav och behov av datakommunikation

Nedan exempel är applicerbara på övriga aktörer med ansvar inom samhällsviktig verksamhet som t.ex. Tullen, Kustbevakningen, Kriminalvården, energibolagen m.fl.

Uppgifter om datakapacitetsbehov nedan är hämtade från LEWP-RCEG MATRIX OF APPLICATIONS. Datakapacitetsbehovet som är angiven till 768 kbps avser lågupplöst video. Högupplöst video som i praktiken kommer att användas kräver högre datakapacitet och är applikations- och implementationsberoende. Kraven för att kunna använda videoupptagningar i rättegångar för bevisvärdering är högupplöst video. Därför är högupplöst video ett dimensionerande krav.

Lednings- och beslutsstödsystem

- För överföring av order, avrapporteringar, lägesinformation mm med hjälp av text [10 000 bytes per transaktion DL/UL], kartor [50 000 bytes per transaktion DL], ritningar [50 000 bytes per transaktion DL], bild [100 000 bytes per transaktion DL/UL] och video [768 kbps UL/DL] mellan ledningscentral och yttre befäl och patruller.
- Positionering mellan inblandade enheter och ledningscentraler omfattande positionering av både fordons- och personlig utrustning [80 bytes per transaktion UL]. Förutom ett verksamhetsbehov är detta också ett säkerhetskrav för insatspersonal och således ett krav utifrån arbetsmiljöansvar.
- För dataslagningar [1 000 bytes UL, 50 000 bytes DL per transaktion].
- När en polispatrull färdas runt i geografin ska ledningsstödssystemet fortlöpande med automatik skicka relevant information till Patrullen. Det kan gälla personer och fordon som behöver kontrolleras. Det kan gälla händelser som behöver tillsyn. Det kan gälla utlovade åtgärder från medborgarlöften som ska uppfyllas med mera [50 000 – 100 000 bytes per transaktion DL].
- När en patrull ska gå in i en bostad ska patrullen i förväg med automatik få karta över området [50 000 bytes per transaktion DL], byggnadsritningar [50 000 bytes per transaktion DL], bilder [100 000 bytes per transaktion DL] över objektet. Patrullen ska få en tredimensionell animering av hur man bäst positionerar sig för att undvika att någon obemärkt lämnar platsen [100 000 bytes per transaktion DL].

För ett effektivt resursutnyttjande krävs ständigt uppdaterad resursöversikt som visar vilka enheter finns var och vad de arbetar med.

Brottsutredningssystem

- För överföring av text [10 000 bytes per transaktion DL], bild [100 000 bytes per transaktion DL] och video [768 kbps UL/DL] mellan ledningscentral, yttre befäl och patruller.

Video från och till polispatrull [768 kbps UL/DL]

- För att dokumentera lägesbild när man kommer till en brottsplats, olyckplats eller liknande. Både från fordonsmonterad och från personburen utrustning. För att användas för beslut om vidare åtgärder, t.ex. förstärkningsrörelser samt för att dokumentera för vidare utredning.
- Vid trafikövervakning t.ex. vid beteendeövervakning av stopplikt, omkörningsförbud, trafik i kollektivkörfält m.m.
- Personlig utrustning för att dokumentera ingripanden och förmedla lägesbild till ledningscentral vid ingripande mot folksamlingar eller ingripanden mot farliga personer.
- Personlig utrustning för övervakning vid publika evenemang som idrottsevenemang, statsbesök, demonstrationer m.m.
- För automatisk detektering av brottsmisstänkta eller farliga personer eller objekt vid publika evenemang som idrottsevenemang, statsbesök, demonstrationer m.m.
- Spaning vid brott.
- Spaning efter efterlysta.

Video från helikopter och obemannade farkoster [768 kbps UL]

- Vid statsbesök, idrottsevenemang, demonstrationer m.m.
- För automatisk detektering av brottsmisstänkta eller farliga personer eller objekt vid publika evenemang som idrottsevenemang, statsbesök, demonstrationer mm.
- Vid trafikövervakning från helikopter till patrull på marken eller till ledningscentral.
- Vid trafikövervakning från fordon.
- Spaning vid brott.
- Spaning efter efterlysta.
- Vid olyckor, t.ex. bränder, trafikolyckor.

Video från fasta installationer [768 kbps UL]

- För automatisk detektering av brottsmisstänkta eller farliga personer eller objekt vid publika evenemang som idrottsevenemang, statsbesök, demonstrationer m.m.
- För trafikövervakning avseende trafikflöden.
- För hastighetsövervakning.
- För övervakning på brottsutsatta platser.
- För övervakning av objekt.
- För automatisk detektering av brottsmisstänkta eller farliga personer eller objekt vid publika evenemang som idrottsevenemang, statsbesök, demonstrationer m.m.

Sjukvården

- Dataslagningar [1 000 bytes UL, 50 000 bytes DL per transaktion].
- Överföring av patientdata till och från ambulans, t.ex. patientjournaler [1 000 bytes UL, 50 000 bytes DL per transaktion] och EKG [15 kbps UL].
- Åtkomst till medicinska register och databaser, t.ex. FASS, Medline m.fl. [1 000 bytes UL, 50 000 bytes DL per transaktion].
- Överföring av kartor [50 000 bytes per transaktion DL].
- Video från ambulans till sjukhus. [768 kbps UL].
- Video vid vård i hemmet t.ex. för att hemtjänst ska kunna få diagnos på distans. [768 kbps UL/DL].
- Positionering av både fordon- och personlig utrustning [80 bytes per transaktion UL].

Räddningstjänsten

- Dataslagningar [1 000 bytes UL, 50 000 bytes DL per transaktion].
- Positionering av både fordon- och personlig utrustning [80 bytes per transaktion UL].
- Överföring av larm från smarta uniformer t.ex. gasdetektorer [1 000 bytes per transaktion UL].
- Åtkoms till register t.ex. farligt gods, RIB Kemdatabasen m.fl. [1 000 bytes UL, 50 000 bytes DL per transaktion].
- Överföring av kartor [50 000 bytes per transaktion DL].
- Överföring av byggnadsritningar [50 000 bytes per transaktion DL].

- Video från utryckningsfordon till och från ledningscentral [768 kbps UL/DL].
- Video från obemannad farkost till utryckningsfordon och ledningscentral vid t.ex. skogsbrand [768 kbps UL/DL].

Tillgång till sociala medier

- Vid olika typer av händelser vill de larmande (allmänheten) kunna skicka bilder och video till SOS Alarm och Polisen. För att genomföra insatserna är det ytterst värdefullt att personal kan få del av sådan materiel. Detta för att insatserna ska göras så effektivt och säkert som möjligt.

Identifierade krav av Trafikverket

- Kommunikation kopplat till ledningsfunktioner t.ex. Nationell operativ ledning, Regional operativ ledning, krisledning samt övriga ledningsfunktioner.
- Kommunikation mellan ledningsfunktioner och operativ personal i fält.
- Kommunikation med andra myndigheter samt andra externa parter exempelvis tågoperatörer.
- Kommunikationen som normalt sker med fasta kommunikationstjänster kan i kris behöva föras via säkra kommunikationstjänster.
- M2M-kommunikation mellan olika infrastrukturdelar.
    - Övervakning, kameralösningar, styrning av komponenter.
- Säkerhetskommunikation mellan fordon och infrastruktur exempelvis koppling mot järnvägens signalsystem ERTMS.

Bilaga 2

Scenarier

Scenarierna beträffande trafikolyckor och brand är typexempel på vad krisaktörerna har att hantera utifrån de larm som kommer in via 112. Det finns ett antal olika händelser som generar motsvarande behov av kommunikationsförmåga. Rutinmässigt hanterar aktörernas ledningscentraler flera olika samtidigt pågående sådana händelser. Frekvensen av händelser varierar över dygnet vilket SOS Alarm tydligt redovisar i sin verksamhetsstatistik.

Beträffande större händelser som omfattar fler användare så är frekvensen större i storstad jämfört med landsbygd. Det förekommer dagligen särskilda händelser i Stockholm, mycket ofta i Göteborg och Malmö, mera sällan i nivån residensstäder och väldigt sällan i mindre orter. Statsbesök har använts som typexempel men i samma härad finns högriskmatcher i fotboll och ishockey, demonstationer och liknande. Dessa typer av händelser förekommer flera gånger per vecka i t.ex. Stockholm. Antalet poliser som hanteras dessa händelser är mellan 100 och 1000 beroende på hotbilden. Vid riktigt stora insatser kan betydligt fler än 1000 poliser användas, samtidigt ska den vanliga ordinarie löpande verksamheten bedrivas. Förutom polisen berörs så gott som alltid även andra aktörer av denna typ av händelser.

Samhällsviktig verksamhet har samhällets uppdrag att hantera händelserna. Nyttan för aktörerna är att de kan utföra sina uppdrag. Nyttan för samhället är att medborgarna får det öppna demokratiska, trygga och säkra samhälle som man kräver. Nyttan av att det finns fungerande kommunikationslösningar är att insatser kan göras snabbare och effektivare och samverkan kan bedrivas bättre. Nyttan för samhället och samhällsmedborgarna är färre skadade och döda, mindre egendomsskador, minskat lidande och lägre kostnader.

Försvarsmakten anser att underlag ska inhämtas från Utredningen till Försvarsmakten och Myndigheten för samhällsskydd och beredskap avseende totalförsvarsplanering. Inom detta uppdrag anges ”*De antaganden som avser väpnat angrepp ska vara en utgångspunkt för en sammanhängande planering för totalförsvaret. De relevanta delarna av Försvarsmaktens försvarsplanering som avser höjd beredskap ska tillhandahållas av Försvarsmakten i en mellan myndigheterna överrenskommen ordning*.”

För beskrivna scenarier gäller att det alltid finns bakgrundstrafik som inte är relaterad till den specifika händelsen. Denna trafik måste adderas till den trafik som respektive scenario genererar. På samma sätt kommer vardagshändelse (PP1) finnas i bakgrunden till större planerade eller oplanerade händelser (PP2) samt krishändelser (DR).

Liten trafikolycka (PP1)

Detta scenario är till stor del baserad på idag rådande dataanvändning.

Till SOS Alarm i Jönköping inkommer en vardag i oktober vid 09.00-tiden via 112-samtal larm om att det skett en trafikolycka på riksväg 23 i norrgående riktning vid Östanå i Östra Göinge kommun. Den larmande som har passerat platsen uppger att en personbil har kört in i vajerräcket och att det ligger ett djur på vägen. Under larmoperatörens intervju med den larmande framkommer att det ser ut som att det också sitter en person i bilen. Den larmande kan på grund av trafikläget inte stanna och har fortsatt sin färd söderut.

Under tiden som den larmoperatör i Jönköping tar emot samtalet börjar en annan larmoperatör i Malmö som är inkopplad på medhörning av 112-samtalet att larma ut berörda räddningsenheter. Larm går till en ambulans som rycker ut från en ambulansstation i Broby. Larm går till räddningstjänstens larmcentral i Kristianstad som sedan larmar ut Räddningstjänst från Östra Göinge och räddningsbefäl från räddningstjänsten i Kristianstad. Därefter ringer den utlarmande SOS-operatören till Polisens ledningscentral i Malmö och förmedlar larmet till en operatör. Efter att operatören i polisens ledningscentral fått nödvändiga uppgifter larmas en polispatrull från Hässleholm som befinner sig i Osby. När den utlarmande SOS-operatören förmedlar larmet så meddelar operatören de larmade om vilken samverkanstalgrupp som ska användas under framkörningen till olyckplatsen. Operatörerna i ledningscentralerna hos SOS och polisen har tillgång till en positioneringslösning så att man kan följa sina egna enheters positioner och rörelser. Under framkörningen ringer fler personer 112 för att larma om olyckan. Det har uppstått viss köbildning i den norrgående körbanan eftersom vägen är blockerad. SOS informerar via samverkanstalgruppen enheterna som är på väg mot olycksplatsen om att köbildning uppstått så att man kan förbereda framryckningen och insatsen efter den förutsättningen. SOS meddelar därefter lokalradion om olyckan varpå lokalradion går ut i sändning och informerar trafikanterna om att en olycka har inträffat och att uttryckningsfordon är på väg. Så fort de olika enheterna från polis, räddningstjänst och ambulans fått sina uppdrag tar man kontakt med varandra via samverkanstalgruppen och kommer överens om framryckningen så att den kan ske på ett taktiskt bra sätt. Ambulansen kommer först framtill olyckplatsen och lämnar innan den stannat en så kallad vindruterapport till de övriga framryckande enheterna och ledningscentralerna. Ambulansen meddelar att det finns en bil som kört in i vajerräcket och blockerar vägen. En person sitter i bilen. En älg ligger på körbanan. När ambulansen stannat rusar ambulanspersonalen fram till bilen, konstaterar snabbt att personen som sitter i bilen kan befaras ha fått en nackskada. Med bärbar radio informerar ambulanspersonalen den framryckande räddningstjänsten om läget. Räddningstjänsten kan då förbereda att inför sin insats för att trygga omhändertagandet av den skadade. Under tiden har polispatrullen kommit till platsen och efter en gemensam lägesorientering med ambulanspersonalen vidtar man direkt åtgärder för att minimera att fler fordon riskerar att orsaka fler olyckor på platsen samt åtgärder för att säkerställa att den framryckande

räddningstjänsten kan komma fram. Fortlöpande sker kommunikation mellan enheterna, personal som lämnat sina fordon kommunicerar via bärbara radioapparater. När den första brandbilen från räddningstjänsten kommer till platsen förbereds åtgärder för att omhänderta den skadade. Brandmännen kommunicerar via bärbar radio med brandbil nummer två och med räddningsledaren som båda är på väg fram. När brandbil nummer två anlänt påbörjas arbetet med att flytta ut den skadade från fordonet. Parallellt arbetar delar av räddningsstyrkan med att förstärka skyddet av skadeplatsen så att inte fler fordon blandas in i olyckan. Polisen har kontakter med ledningscentralen för att kunna få fram jakträttsinnehavare och bärgare till platsen. Samtidigt arbetar man med att dokumentera olycksplatsen. Räddningstjänsten kapar taket på olycksbilen och tillsammans med ambulanspersonalen lyster man ut den skadade från fordonet. Den skadade flyttas in i ambulansen och ambulanspersonalen vidtar vårdande åtgärder i ambulansen för att säkerställa att den skadades tillstånd inte försämras. Via radio har ambulanspersonalen kontakt med akutmottagningen vid sjukhuset i Kristianstad. Information om patientens tillstånd avhandlas mellan ambulans. Och akutpersonal. Eftersom sjukhuset har tillgång tidigare vårduppgifter konstateras att vissa förebyggande vårdinsatser måste utföras redan under transporten vilket förmedlas till ambulanspersonalen. Under hela transporten till sjukhuset har ambulansen en fortlöpande kontakt med akutmottagningen och SOS.

Trafikolyckan medför att polisen måste omgruppera sina operativa enheter för att ersätta den polispatrull som beordrades till olyckan. En polispatrull från Hässleholm beordras därför till Osby. Under framkörningen informerar ledningscentralen om vilka arbetsuppgifter som man ska hantera i området. SOS omdirigerar en ambulans från Kristianstad till att placera sig mer strategiskt för att kunna ersätta Brobyambulansen om det kommer in nya larm från området. Trafikverkets ledningscentral informeras av polisens ledningscentral om olyckan. Trafikverkets ledningscentral beordrar ett av sina arbetsfordon till platsen för att provisoriskt åtgärda skadorna på vajerräcket och sätta ut varningsskyltar. Efter att räddningstjänsten, bärgare och personal från trafikverket röjt upp olycksplatsen och polisen genomfört sin utredningsdokumentation samt djuret omhändertagits av jakträttsinnehavaren avvecklas insatsen. Information om att vägen är fri förmedlas via SOS till lokalradion som går ut med ett sändningsmeddelande. De inblandade enheter avrapporterar fortlöpande till sina ledningscentraler som vid behov koordinerar sinsemellan så att man har en gemensam lägesbild.

Ovanstående beskriver hur olyckan hanteras i nuläget. Behovet är att minska insatstiden och samtidigt minimera riskerna för de drabbade, andra trafikanter och för räddningspersonalen. Ny teknik ger nya förutsättningar för att åstadkomma detta. En betydande del av talkommunikationen kan kompletteras med videoöverföring. Redan idag är många räddningsfordon utrustade med videokameror som fortlöpande dokumenterar både framkörningen och händelserna på olycksplatsen. Med en välfungerande

överföring till ledningscentralerna och mellan enheterna skulle personalen som först anländer inte behöva lägga tid på den första talade lägesbeskrivningen utan direkt kunna fokusera på räddande åtgärder. Lägesbeskrivning via videoöverföring kan också göras från UAV eller motsvarande och då ge lägesinformation redan innan första fordon anlänt till olycksplatsen. I den fortlöpande lägesrapporteringen skulle man spara tid om istället för att med tal beskriva händelseutvecklingen i stället kunde visualisera den via video till och mellan ledningscentralerna för att de ska få tillräcklig med information för att kunna ta beslut om kompletterande åtgärder. Gemensam lägesbild förkortar informationsvägarna och säkerställer att alla har tillgång till samma information samtidigt. Utvecklingen av smarta fordon och e-call förändrar scenariot avseende informationskedjan.

Lägenhetsbrand (PP1)

Detta scenario utgår ifrån att det finns den datakapacitet som krävs för att utföra insatserna på ett säkert och effektivt sätt.

Larm inkommer via 112 till SOS Alarm om att det brinner i en lägenhet i ett flerfamiljshus. Räddningstjänst, ambulans och polis larmas ut. Under utryckningen positioneras samtliga enheter och byggnadsritningar och åtgärdskalendrar skickas till räddningsfordonen. Räddningstjänsten sätter in rökdykare utrustade med detektorer för farliga ämnen, t.ex. gas. Mellan rökdykarledaren (som uppehåller sig utanför huset) och rökdykarna används en talgrupp som etablerar direktkommunikation mellan berörda enheter för fortlöpande radiokommunikation. Räddningstjänsten skickar upp en obemannad farkost för att få en överblick av brandspridningen. Informationen skickas till räddningsledaren i form av strömmande video. Informationen delas också med polisen och berörda ledningscentraler. Polisen spärrar av området, dokumenterar händelseförloppet och förmedlar lägesbilden till ledningscentralen via video. I övrigt bedrivs arbetet och sambandet på motsvarande sätt som vid trafikolyckorna. En rökskadad person anträffas och förs med ambulans till sjukhus. Under färd bedrivs prehospitalvård där patientinformation utbyts mellan sjukhus och ambulans. Polis och räddningstjänst avrapporterar och dokumenterar händelsen på plats.

Stor trafikolycka (PP2)

Informationsflödena vid en stor trafikolycka är i princip de samma som vid en mindre olycka, det som skiljer är volymerna. Initialt under framryckningen använder aktörerna en gemensam samverkanstalgrupp. Efter hand som man börjar agera på olyckplatsen använder polis, räddningstjänst och ambulans egna insatstalgrupper för den egna interna kommunikationen. Samverkanstalgruppen används enbart för fortlöpande samordning på befäls- och ledningsnivå. För trafikdirigering använder polisen ytterligare två talgrupper. Eftersom flödena redovisats tämligen detaljerat i föregående exempel så upprepas inte detta i följande scenario.

På E4 i utkanten av en större stad inträffar en trafikolycka mellan tre bilar. I bilarna färdas åtta personer varav fyra personer skadas. Det blir snabbt köbildningar och flera larm kommer in till SOS via 112. Ambulans, räddningstjänst och polis larmas/beordras till platsen. Fyra ambulanser, tre räddningstjänstfordon och tre polispatruller beordras till platsen. De utryckande enheterna kommer från olika positioner och anländer efter hand till platsen. Framryckning och andra initiala insatser är desamma som i föregående exempel. Den enda skillnaden är att fler är inblandade och att kommunikationen därför blir fördubblad. Eftersom trafiken är tät blir det snabbt långa köer. Efterhand inträffar ytterligare två olyckor i köerna med två respektive sex fordon inblandade. Ytterligar totalt tre personer skadas. Ytterligare två ambulanser, två räddningstjänstfordon och en polispatrull larmas. Eftersom polisen har en helikopter i närheten larmas den också till platsen för att man ska få en bättre överblick av trafikläget samt kunna säkerställa utryckningsvägarna. Ambulanserna överför fortlöpande medicinsk data till de akutsjukhus som ska ta emot de skadade.

Statsbesök (PP2)

I Stockholm hanteras varje år flera olika statsbesök. Under besöken sker vanligen utflykter till andra platser i riket. Insatsernas storlek beror på den hotbild som föreligger. För att upprätthålla säkerheten krävs en ständigt fungerande radiokommunikation. Den besökande har alltid ett antal medföljande, både sakkunniga och säkerhetspersonal. Alla förflyttningar sker med poliseskort. Eskorterna omfattar flera fordon och de ska starta respektive anlända till målen på exakt planerad tid. För att säkerställa färdvägen placeras polispatruller ut vid alla punkter där man kan befara någon risk, ex vid alla vägkorsningar, viadukter osv. När eskorten färdas ska trafikposter agera för att stänga av trafik vid vägkorsningar och övergångsställen mm. Om en risk plötsligt upptäcks eller befaras ska eskort styras om till en alternativ färdväg. Då måste samtliga patruller agera i enlighet med det ändrade läget. Eskorterna följs av ledningscentralen via video från helikoptrar, patruller och fasta kameror utmed färdvägen. På startplatser, utmed färdvägen och på ankomstplatser finns också videoövervakning med intelligenta applikationer som kan indikera på farliga personer och rörelser. Radiotrafik bedrivs fortlöpande med tal. Vid behov görs dataslagningar av patrullerna. I ledningsstödssystemet finns all planering för genomförandet. Patrullernas uppdrag, order kommuniceras fortlöpande med automatik med text och bilder från ledningsstödet. Beroende på insatsen storlek används mellan tio och fyrtio talgrupper samtidigt. En typisk eskortsträcka är från Arlanda till centrala Stockholm. Förutom polisen medverkar flera andra myndigheter och organisationer, även frivilligorganisationer. Av säkerhetsskäl beskrivs inte arbetet mer detaljerat i detta dokument. Olika statsbesök har olika hotbild. Statsbesöket överför en hotbild mot dels deltagare samt mot samhället i stort. Det finns i förväg överenskomna krav på t ex skydd och säkerhet som ställer krav på kommunikationslösningarna. Relation med annan stat riskerar att påverkas.

Kris, exempel terrorism, terrorattentat (DR)

Nedan scenario baseras på en samverkanövning som utförts av Polismyndigheten, SLL, Swedavia och räddningstjänsten. Av säkerhetskäl beskrivs inte scenariot mer detaljerat i detta dokument.

Scenariot inleds klockan 08.00 på morgonen. Då befinner sig uppskattningsvis 2-3000 personer i avgångshallen på terminal 5. Två personer beväpnade med automatvapen öppnar eld mot de som befinner sig i terminalbyggnaden. Anledningen till dådet är oklart. Attentatsmännen verkar inte ha en tydlig målgrupp. Aktionen är vad det verkar inte riktad mot något särskilt företag, stat eller liknande utan attentatsmännen verkar enbart försöka göra så stor skada som möjligt. Attentatsmännen rör sig över stora ytor i terminalbyggnaden och det finns skadade och döda både i Terminal 5 och Centralbyggnaden.

Det blir panik och kaos på platsen. De som befunnit sig i terminalbyggnaden flyr platsen. Dessa personer försöker ta sig så långt från platsen som möjligt och stannar följaktligen inte på de uppsamlingsplatser som finns. De är m.a.o. väldigt utspridda över hela området kring Arlanda. Svårt chockade personer kommer att påträffas runt omkring i området under övningen. Även de bilister, busschaufförer och andra trafikanter som befinner sig i anslutning till terminalbyggnaden försöker fly. Detta skapar trafikkaos och ett antal kollisioner med både personskador och skador på fordon som följd. Dessutom har de flyende personerna även använt sig av de befintliga nödutgångarna. Detta leder till att det nu finns chockade och eventuellt skadade personer även i transit och på airside.

På övriga delar av Arlanda har allmänheten ingen vetskap om vad som inträffat. De är för långt ifrån händelsen för att kunna höra eller på annat sätt uppfatta situationen. För att undvika ytterligare personskador måste dessa evakueras och föras i säkerhet i den mån det är möjligt.

Större händelser (inom polisen benämnda som särskilda händelser) ställer stora krav på både intern och extern kommunikation för samverkan, både via tal och data (Polis, räddningstjänst, Tull, SOS och sjukvård). Händelserna på Arlanda riskerar att ganska snabbt slå ut telekommunikationen då det befinner sig många personer på platserna och informationen kommer att spridas fort om vad som inträffat, både inom Sverige och i andra länder.

Det kan även bli internationella följdverkningar då flygplan på väg till andra flygplatser kan beröras utifrån misstankar om ev. bombhot. Ett terrorattentat på Arlanda kommer att skapa oro på många andra flygplatser. Stora krav på informationsspridning mellan aktörer med ansvar för samhällsviktig verksamhet och allmänheten.

För polisens del är det viktigt att utesluta eventuella ytterligare attentat och utreda aktuella brott, vilket kräver utrednings- och spaningsarbete, förutom att ta hand om själva händelsen. Möjligheten till video och bildöverföring kommer att ha en stor betydelse för effektiv genomförande av aktörernas uppgifter.

Säkerhetspolisen kommer att begära biträde för fast bevakning och tillsyn av olika objekt eller beskickningar, t.ex. Riksdagshuset och Rosenbad. Lediga resurser inom berörda aktörer inom samhällsviktig verksamhet kommer att kallas in för tjänstgöring vilket innebär att fler kommer att tillgång till resurser för tal och data.

Då syftet med terrordåd är att skapa oro och fruktan är det synnerligen viktigt att få ut information till allmänheten. Polisen kommer ha en stor uppgift med trygghetsskapande åtgärder vilket kräver möjlighet till kommunikation i de publika näten.

Väpnat angrepp (VA)

När händelseförloppen[29] inleds i respektive typfall förväntas ett allmänt fredstillstånd råda, utan några genomförda beredskapshöjningar. Typfallen utspelas inte vid någon given tidpunkt i framtiden utan är framtagna i perspektivet ”nu och framåt.” De är inte heller låsta till någon specifik utformning av landets försvar. För varje typfall redovisas först antagen situation och ett händelseförlopp.

Typfall 1:
Beredskapshöjning, mobilisering och transport till utgångsområden i typfallet berör mobilisering och koncentrering av Försvarsmaktens krigsförband, i ett läge där ett begränsat väpnat angrepp ännu inte inträffat, men kan vara förestående.

Situation och händelseförlopp:

Detta typfall avser en situation där ett internationellt skeende och en hotbild mot Sverige föranleder regeringen att besluta om höjd beredskap. Ett angrepp på Sverige föreligger inte, men kan tänkas vara nära förestående. Det militära försvaret ska då mobiliseras, varvid mycket korta tidskrav gäller; huvuddelen av krigsförbanden ska, efter beslut om höjd beredskap, kunna påbörja lösande av uppgift inom några dagar och samtliga delar inom en vecka. Efter mobilisering ska krigsförbanden transporteras från mobiliseringsorten till områden enligt grundförsvarsplan eller särskilt beslut.[30] Parallellt med detta ska det civila försvaret vidta åtgärder på sitt område som föranleds av beslut om höjd beredskap. Dessa två parallella processer torde medföra en avsevärd belastning på samhällsmaskineriet, inte minst på ledningsfunktionerna.

---

[29] FOI memo 5089, MSB dnr 2014-6080
[30] Äldre benämning för denna transportrörelse är koncentrering.

- Mobilisering och utgångsgruppering av Försvarsmaktens krigsförband innebär bland annat att:
- huvuddelen av krigsförbandens personal, vilken normalt inte tjänstgör på förband, ska ta sig till förbanden.
- vid förbanden ska personalen inmönstras, utrustas, förplägas, förläggas och sättas i arbete. Eventuellt genomförs inskjutning av vapen etc.
- materiel och förnödenheter som lagras centralt ska fördelas och föras ut till förbandens mobiliseringsplatser
- materiel och förnödenheter från lokala förråd utanför garnisonsområdet ska föras till förbanden och där fördelas – vissa av transporterna enligt denna och ovanstående punkt behöver skyddas.
- materiel på verkstad ska snabbt göras användbar och återföras till förbanden
- sådan materiel och sådana förnödenheter som Försvarsmakten/Försvarsmaktens logistik/Försvarets materielverk inte lagerför (i tillräcklig mängd) ska upphandlas, tas emot och distribueras till förbanden
- civila fordon (eller andra resurser) som Försvarsmakten ska ta i anspråk under längre tid ska ställas till Försvarsmaktens förfogande och inmönstras, samt att
- förband som fyllts upp med personal, materiel och förnödenheter ska förflyttas från mobiliseringsplats till tänkt operationsområde.

Ovanstående kan endast i ett fåtal fall genomföras enbart med Försvarsmaktens egna resurser. I de flesta fall krävs tillförsel av resurser inte bara från Försvarsmaktens logistik och/eller Försvarets materielverk, utan också i hög grad från civila aktörer. Som exempel kan nämnas den sista punkten ovan, där civilt stöd krävs såväl för själva transportrörelsen som för tankning, förplägning, inkvartering etc., under transporten och (initialt) i operationsområdet. Ett annat exempel är förnödenheter som skall köpas upp eller rekvireras vid mobilisering, såsom fordonsbränsle, livsmedel, hygienartiklar, bärbara datorer och batterier.

Typfall 2:
Angrepp med fjärrstridsmedel m.m., huvudsakligen mot civila mål i typfallet omfattar ett begränsat väpnat angrepp med fjärrstridsmedel mot civil infrastruktur, i syfte att påverka Sveriges vilja att agera i en pågående internationell kris.

Situation och händelseförlopp

I detta typfall riktar sig angriparen mot civila mål som elförsörjning, telekommunikationer, transportsystem etc. för att därmed försvaga eller lamslå

Sveriges vilja och förmåga att agera i en konflikt. Syftet är ytterst att påverka Sveriges vilja att agera i en pågående och eskalerande internationell kris. Angriparen vill inledningsvis dels demonstrera sin kapacitet, dels skapa allmän osäkerhet och rädsla. I ett senare skede är syftet främst att försvåra reparationer/åter-uppbyggnad och svensk mobilisering.

Händelseförloppet i typfallet är eskalerande, från mindre, dolda (dvs. med okänd angripare) och för Sverige svårtolkade attacker, till öppet angrepp från främmande makt. I ett första skede riktas dolda angrepp mot en rad samhällsfunktioner och ansträngningar görs för att dölja spåren och/eller att rikta misstankar åt annat håll. Sabotagegrupper och cyberangrepp används inledningsvis för att lokalt orsaka avbrott i el-, tele- och IT-system. Angriparen iscensätter även olyckor i form explosioner, haverier m.m. Geografiskt är målen utspridda över riket, även om storstadsområdena är något mer utsatta. Avbrott i kommunalteknisk försörjning i form av vatten, avlopp och fjärrvärme drabbar enskilda kommuner. Angreppen skapar successivt allt större osäkerhet i samhället och försvårar kommunikation och ledning. Utsatta kommuner får svårt att hantera situationen och behöver olika typer av stöd.

Angriparen övergår efter en tid från dolda till mer öppna attacker och ett hastigare förlopp. I det här skedet använder angriparen cyberangrepp, sabotagegrupper och fjärrstridsmedel, t.ex. kryssningsrobotar, mot viktiga funktioner i samhället. Obemannade system används för såväl underrättelseinhämtning som vapenbärare. Det står nu klart för Sverige att angreppen är antagonistiska och regeringen förbereder beslut om att höja beredskapen och mobilisera.

Efter 3-5 dagar med allt fler öppna attacker anbefaller regeringen höjd beredskap. Angriparen utökar i detta skede målkategorierna; symboliska och politiskt viktiga mål angrips nu öppet. Upprepade attacker mot knutpunkter lamslår transporter och kommunikationer, vissa ledningsfunktioner och -system slås ut, sjukvården blir allt mer överbelastad och allt större delar av landet saknar fungerande el- och VA-försörjning. Betalningssystemet fungerar endast i begränsad omfattning. Det finns i detta skede en stor vilja hos befolkningen att ”göra något”.

Typfall 3:
Angrepp med fjärrstridsmedel m.m., huvudsakligen mot militära mål i typfallet omfattar ett begränsat väpnat angrepp med fjärrstridsmedel mot militära mål i syfte att begränsa Sveriges militära förmåga att agera i den aktuella krisen.

Situation och händelseförlopp

I likhet med det föregående typfallet har angriparen här syftet att varna och straffa Sverige för ett visst agerande i en pågående internationell kris, vilken utgör den primära konflikten. Angreppen syftar också till att begränsa Sveriges militära förmåga att agera i den aktuella krisen. I detta typfall tillkommer också syftet att avväpna Sverige, det vill säga skapa ett läge där Sverige – oavsett

politisk vilja – inte militärt kan påverka den fortsatta krisens utveckling. När angreppen inleds har Sverige inte fattat beslut om eller genomfört militära eller civila beredskapshöjningar. Det gör man dock efter att de första angreppen skett.

Angriparen vill skapa goda förutsättningar för handlingsfrihet och vidare agerande från sin sida, politiskt och militärt. Detta inkluderar både agerande mot tredje part och mot Sverige, om Sverige efter ett inledande angrepp inte fogar sig. Angriparen strävar i inledningen av detta typfall att undvika att orsaka civila förluster, för att inte uppfattas som hänsynslös.

De medel som angriparen använder initialt är olika former av fjärrstridsmedel, inklusive kryssningsrobotar och ballistiska robotar, cyberattacker och specialförband för att utföra sabotage. Obemannade system utnyttjas för såväl vapeninsatser som spaning och underrättelseinhämtning. Attackflyg med styrda vapen används för uppföljningsangrepp.

I en första fas om 1-2 dagar utgörs målen för angreppet i första hand av Sveriges fjärrstridskrafter, främst i bas, samt de lednings- och understödsfunktioner dessa behöver för att nå effekt och ha uthållighet. Därtill bekämpas infrastruktur av kritisk militär betydelse (elkraft, telekommunikationer, kritiska broar/vägar). Därvid föredras mål med låg påverkan på omgivningen i form av döda och skadade.

Efter ett par dagar, där den svenska regeringen inte har vikit ner sig och svenska flyg- och marinsstridskrafter har bekämpats, riktas angrepp även mot svenska markförband samt mot eventuella marina enheter till sjöss. I detta ingår att begränsa eller hindra Försvarsmaktens möjligheter att mobilisera, förflytta förband, skydda sig mot angrepp, uppfatta läget och att genomföra väpnad strid. Därtill anfaller angriparen i denna fas civil och militär infrastruktur av särskild betydelse för mottagande av hjälp från tredje part, med syftet att få stöd till Sverige att framstå som farlig och osäker. Angreppen pågår 3-5 dagar.

Angriparen har möjlighet att eskalera konflikten i olika hänseenden, inkl. landstigning m.m. på svenskt territorium (se typfall 4).

Typfall 4:
Angrepp som omfattar landstigning och luftlandsättning mot viktiga områden i Sverige. Typfallet beskriver ett begränsat väpnat angrepp med fjärrstridsmedel mot militära mål och civil infrastruktur, i syfte att kraftigt begränsa Sveriges politiska vilja och militära förmåga att agera. Angreppet följs upp med landstigning och luftlandsättning mot begränsade områden från vilka angriparen med kvalificerade vapensystem kan dominera närområdet.

Situation och händelseförlopp

Angriparens syfte är att kraftigt reducera Sveriges förmåga att agera i en aktuell internationell kris, genom att fysiskt förneka oss och tredje part militär

handlingsfrihet i närområdet och samtidigt öka sin egen handlingsfrihet. Angriparen söker generellt i detta typfall att uppnå sina mål så fort som möjligt, samt att kraftigt försvaga Sveriges möjligheter till ledning, beslutsfattande och agerande. Strävan är att genomföra angreppet så snabbt som möjligt, med utnyttjande av överraskningsmomentet, och nå effekt innan Sverige eller tredje part hunnit agera effektivt. Operationens strävan till överraskning och snabbhet betyder att angriparen tar större taktiska/operativa risker än vad som är doktrinärt ”normalt” och att landstigning/luftlandsättning påbörjas så snart Sveriges fjärrstridskrafter, ledningssystem och infrastruktur m.m. har reducerats i tillräcklig omfattning.

En ökad politisk och militär spänning inklusive tecken på anfallsförberedelser före angreppet har noterats, varför Sverige har vidtagit smärre förberedelser inom militär, polisiär och övrig civil beredskap. Dock sker angreppet utan föregående tydlig strategisk/operativ varning, varför förberedelserna inom det militära försvaret och enstaka myndigheter endast är marginella.

Angreppet inleds med en våg av fjärrstridsmedel (kryssningsrobotar kombinerade med ballistiska robotar; ca 100-200 stycken) och sabotagegrupper. Cyberattacker sker mot viktiga funktioner. Mål är svenskt flyg och flotta i bas, reservbaser, förråd för kvalificerad ammunition, bränsle, reservdelar etc., markförband med hög tillgänglighet, det militära försvarets ledningsorgan och kommunikationsnoder, samt centralförråd. Ett mindre antal insatser görs mot civil infrastruktur av särskild betydelse (el, tele och väg/järnväg). Vissa insatser som stör den politiska och den militära ledningen genomförs med sabotagegrupper. Områden och infrastruktur av särskild betydelse för tillförsel av hjälp utifrån blockeras eller neutraliseras med sabotage eller fjärrstridsmedel.

Attackerna har avsedd verkan. Det militära försvaret drabbas, el- och telenät i Mellansverige och vissa regioner är utslagna för minst några dagar och förflyttningar på väg/järnväg försvåras allvarligt. Fortsatta angrepp försvårar berörda aktörers försök till reparationer och mättar Sveriges motståndskraft. Skadeutfallet militärt och civilt på svensk sida är i de flesta fall måttligt, utom på ett fåtal särskilt drabbade orter, samt på platser där fjärrstridsmedel av misstag har träffat bostadshus.

Ett svenskt område av stor strategisk/operativ betydelse besätts av fallskärmstrupp och andra markstridsenheter. Luftlandsättning och landstigning sker även i mindre omfattning mot ett sekundärt område. Luftlandsättningarna och landstigningarna understöds av attackflyg.

Efter de första attackerna beslutar regeringen om högsta beredskap och om mobilisering. Ansvariga aktörer försöker bedöma vad som har skadats och den påverkan skadorna får, samt vad som inom angripna system inte slagits ut och därmed har blivit mer skyddsvärt. De militära resurser som inte har slagits ut reorganiseras på bästa möjliga sätt för verkan och överlevnad, samtidigt som

mobilisering ska genomföras. Detta är mycket krävande och försvåras av att ledningsfunktioner har varit mål. Svåra prioriteringar är nödvändiga.

Angriparen framgrupperar attackhelikoptrar, kvalificerat luftvärn och kustrobotar till tagen terräng i syfte att öka sin egen och minska Sveriges och tredje parts handlingsfrihet.

Ett ultimatum utfärdas av angriparen, med innebörden att Sverige inte kommer att tillfogas ytterligare skada och angriparen kommer att dra sig tillbaka, på villkor att Sverige avbryter samarbete med tredje part och i stället samarbetar med angriparen. Om Sverige inte fogar sig och i stället gör motstånd får Sveriges regering svara för följderna. Angriparen uppmanar ”fredsälskande” svenskar att påverka regeringen i denna riktning.

Total förfluten tid från angreppets inledning till när ultimatumet löper ut är tre dygn.

Statistik

Nedan redogörs för statistiskt underlag för att visa på antalet händelser som ligger till grund för scenario av typen PP1.

Utveckling av antal 112-samtal till SOS Alarm AB som handlar om räddnings-, vård- eller polisärenden:

	2012	2013	2014
Vård	824 668	851 471	871 519
Räddning	94 746	102 449	106 286
Polis	600 647	617 173	660 856

Källa: Årsredovisning 2014 SOS Alarm

Händelser från anrop till 112 fördelade per län:

Län	Räddning	Varav samverkan med vård	Vård	Varav samverkan med polis	Övriga ärenden	Totalt
Blekinge län	1 449	976	14 452	343	274	16 175
Dalarnas län	4 303	4 073	27 825	635	361	32 489
Gotlands län	1 034	866	4 740	93	142	5 916
Gävleborgs län	2 913	2 748	26 950	923	467	30 330
Hallands län	2 856	2 049	27 607	771	490	30 953
Jämtlands län	2 148	1 691	11 529	265	110	13 787
Jönköpings län	3 998	3 121	28 113	715	513	32 624
Kalmar län	2 395	1 611	25 465	535	415	28 275
Kronobergs län	1 989	1 319	14 706	274	264	16 959
Norrbottens län	2 476	1 506	23 670	667	95	26 241
Skåne län	15 146	9 957	116 738	3 154	2 221	134 105
Stockholms län	20 323	15 238	168 098	3 994	4 609	193 030
Södermanlands län	2 986	2 790	22 740	635	494	26 220

Uppsala län	3 659	2 840	22 840	577	537	27 036
Värmlands län	4 035	3 247	24 127	657	661	28 823
Västerbottens län	2 177	1 410	22 356	581	192	24 725
Västernorrlands län	3 323	2 449	25 062	603	244	28 629
Västmanlands län	2 346	2 164	24 543	760	601	27 490
Västra Götalands län	18 647	11 896	159 570	4 802	2 268	180 485
Örebro län	2 086	1 539	25 400	811	430	27 916
Östergötlands län	4 264	4 069	37 753	1 035	550	42 567
Övrigt	1 733	1 340	17 235	481	674	19 642
Totalt	106 286	78 899	871 519	23 311	16 612	994 417

Källa: Årsredovisning 2014 SOS Alarm

Vidarekoppling från anrop till 112 fördelade per län

Län	Utländska larmcentraler	Flygräddning	Polis	Jourhavande präst	Kustbevakning	Socialjour	Jourhavande tandläkare	Tips om smuggling	Övrigt	Totalt
Blekinge län	2	5	8 216	1 342	4	92	8	7	0	9 676
Dalarnas län	5	1	16 811	1 562	0	1 293	11	13	0	19 696
Gotlands län	1	1	2 774	74	1	187	5	6	0	3 049
Gävleborgs län	6	1	18 416	4 084	4	700	11	24	3	23 249
Hallands län	12	9	16 641	1 047	4	1 383	8	8	4	19 116
Jämtlands län	6	0	6 678	774	0	216	10	10	2	7 696
Jönköpings län	6	4	18 268	4 021	0	2 104	10	15	3	24 431
Kalmar län	8	4	11 334	3 591	3	278	1 219	8	4	16 521
Kronobergs län	3	2	10 589	2 128	0	399	2	2	3	13 128
Norrbottens län	43	6	15 065	2 830	1	257	187	8	2	18 399
Skåne län	95	10	88 337	13 738	8	255	5	81	45	102 574
Stockholms län	119	36	170 041	24 738	19	2 966	166	161	13	198 259
Södermanlands län	12	1	22 696	1 279	4	2 642	8	15	0	26 657
Uppsala län	11	5	19 283	3 402	0	942	11	16	0	23 670
Värmlands län	21	2	17 094	2 141	0	593	6	22	0	19 879
Västerbottens län	16	3	11 604	4 738	1	1 128	1 441	8	4	18 943
Västernorrlands län	6	1	17 386	4 398	2	181	33	14	1	22 022
Västmanlands län	2	3	21 410	3 955	1	421	763	8	0	26 563
Västra Götalands län	48	26	108 063	21 369	23	3 864	116	65	19	133 593
Örebro län	7	0	19 517	2 415	0	546	4	6	3	22 498
Östergötlands län	16	4	27 495	6 302	1	552	11	22	0	34 403
Övrigt	12	2	13 138	1 784	2	284	65	8	4	15 299
Totalt	457	126	660 856	111 712	78	21 283	4 172	527	110	799 321

Källa: Årsredovisning 2014 SOS Alarm

Antal polisutryckningar och deras fördelning

	2014
Totalt antal utryckningar	1 182 469
Varav utryckningar för trafikförseelser	41 295

Källa: Polisens Årsredovisning 2014

Antal till polisen inkomna ärenden och deras fördelning

	2014	2013	2012
Totalt antal ärenden	1 255 643	1 222 099	1 224 593
Varav ärenden för trafikförseelser	41 295	37 493	42 124

Källa: Polisens Årsredovisning 2014

2.5.8 Användning av statistiskt material från SCB

Nedan tabell visar befolkningens procentuella fördelning.

Invånare/km^2	< 300	300 - 3 000	> 3 000
Befolkning i %	10,85	22,76	66,39
Andel av area i %	92,74	5,82	1,43

Källa: SCB:S befolkningsdatabas 2014-12-13

Befolkning 2014-12-31 (st)	9 845 155
Sveriges area (km^2)	431 706

Källa: SCB:S befolkningsdatabas 2014-12-13, samt GPW v3 avseende area

Bilaga 3

Viktningstabell

Tabellen nedan ger en allmän översikt av vanliga tjänster och funktioner inom samhällsviktig verksamhet som återfinns i de olika scenarierna. Tjänsterna är grupperade efter en uppskattad dataförbrukning för dessa. Tjänsterna har viktats utifrån hur verksamhetskritiska dessa är i scenarierna. Viktningen är gjord i sammarbete mellan MSB, Polismyndigheten och Försvarsmakten och uppdelad enligt följande; mycket viktig (H); viktig (M) och mindre viktig (L) i varje givet scenario. Beräknat kapacitetsbehov för respektive tillämpning återfinns i LEWP-RCEG matris samt delar av bilaga 1.

Tjänst	Funktion	Exempel	Viktning			
Låg dataförbrukning			PP1	PP2	DR	VA
Tal	Enhet till enhet	Kommunikation till/från/mellan fältoperativ personal	H	M	H	H
	En till många	Gruppkommunikation	H	H	H	H
	”Walkie-talkie” kommunikation, direktkommunikation	Direkt enhet till enhet kommunikation utan kontakt med övrig infrastruktur	H	H	H	H
	Push-to-talk	Push-to-talk	H	H	H	H
	Förtur/prioritet	Selektiv prioritet, ordergivning, omedelbar tillgång till ”talkanalen”	H	H	H	H
	Säkerhet	E2EE-kommunikation (enhet till enhet, gruppkommunikation och kommunikation med ledningscentraler)	M	H	H	H
Faksimil	Enhet till enhet	Statusmeddelanden, textmeddelanden	L	L	M	L
	En till många	Utskick av initial ärendedata	L	L	M	L
Meddelanden	Enhet till enhet	Status- textmeddelanden, kortare e-post	H	M	H	H
	En till många	Utskick av incident/skadeplatsinformation, signalement	H	H	H	H
Prioritet	Prioritet, omedelbar tillgång	Larmfunktioner (röd knapp), ”man down”-funktion	H	H	H	H

	till resurser i infrastrukturen					
Telematik	Positionering	Positionering mellan inblandade enheter och ledningscentraler omfattande positionering av både fordons- och personlig utrustning	H	H	H	M
	Sensordata	M2M kommunikation, t.ex. avläsning av kraftledningsutrustning, personliga gaslarmssensorer	H	M	H	M
		EKG från ambulans	H	H	M	-
Dataslagningar (minimal datastorlek)	Mall-baserade slagningar	ANPR, misstankeregister (PERSON/FORDON), CBRNE/farliga ämnen.	H	H	H	H
	Mall-baserad avrapportering	Avrapportering rutinärenden	M	M	L	M
Medium dataförbrukning						
Meddelanden	E-post, eventuellt med bilagor	Kommunikation via epost, chattfunktionalitet	L	L	L	L
Dataslagningar (medium datastorlek)	Registerslagningar	Överföring av patientjournaler	H	H	H	-
		Listor över icke identifierad person/försvunnen person/FORDON,	H	H	M	H
		Skicka kartor och tilläggsinformation (extra information om byggnader, placering av enheter, vägar, kartöverlägg m.m.)	H	M	M	-
Överföring av textbaserad information	Dataöverföring	Avrapportering av icke rutinärenden, skicka alla typer av briefing information från ledningscentral till berörda enheter	L	M	M	M
		Registersökningar	H	H	M	H
		Åtkomst till styrdokument och lagar	L	L	H	L
Bildöverföring	Upp/nedladdning av komprimerade bilder	Biometri (fingeravtryck)	H	H	H	H
		Identitetshandlingar	H	H	H	H
		Överföring av byggnadsritningar	H	H	H	H
Telematik	Fordonstelematiksystem	Fordonsdiagnostik, smarta fordon	M	L	H	L
Video	Upp/nedladdning av	Överföring av tidigare inspelat videomaterial	H	L	L	L

	komprimerad video	Video från skadeplats till ledningscentral samt operativ personal på skadeplats, från helikopter	H	H	H	H
		Hjälmkamera för observation med lägre kvalitet, som kan kopplas om till högre kvalitet om behov uppstår	H	H	H	H
Interaktiv kommunikation	Direktmeddelanden Positionering	Tvåvägskommunikation	H	H	H	H
		Direkt/interaktiv kommunikation via kartsystem	H	H	H	H
Hög dataförbrukning						
Databasåtkomst	Tillgång till Intranät/Internet	Mobila ledningscentraler, mobila vårdinrättningar	H	H	H	H
	Surf (från de mobila enheterna)	Tillgång till sociala medier och information från allmänheten, Överföring av multimedia och tyngre databasinformation	L	L	H	L
Automatiserade tjänster	Fjärrstyrning	Styrning och kommunikation med bombrobotar, obemannade farkoster	H	H	H	H
Video	Strömmande realtidsvideo	För att dokumentera lägesbild när man kommer till en brottsplats, olyckplats eller liknande. Både från fordonsmonterad och personburen utrustning	H	H	H	H
		Video vid vård i hemmet ex för att hemtjänst ska kunna få diagnos på distans.	H	M	H	L
		För automatisk detektering av brottsmisstänkta eller farliga personer eller objekt vid publika evenemang som idrottsevenemang, statsbesök, demonstrationer mm	H	H	H	H
		Video från helikopter och obemannade farkoster vid statsbesök, idrottsevenemang, demonstrationer, bränder	H	H	H	H
Bildöverföring	Bilder med hög upplösning	Överföring av byggnadsritningar, sprängskisser, övervakningsbilder	H	H	H	H

PROMEMORIA

Datum	Vår referens	Sida
2016-02-01	Dnr: 15-11722	1(22)

Spektrumavdelningen
Johan Stake
08-678 55 93
johan.stake@pts.se

Kommunikationslösningar för aktörer inom allmän ordning, säkerhet, hälsa samt försvar

Sammanfattning

PTS redovisar i denna pm översiktligt olika alternativ som finns för en mobil, ip-baserad kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa samt försvar, i enlighet med regeringsbeslut II:28.

Denna pm innehåller endast en översiktlig beskrivning av några olika alternativ som finns, utan att göra anspråk på att vara heltäckande. Det finns många delar av kommunikationslösningarna som kan organiseras annorlunda vilket ger ytterligare lösningar, inte minst beträffande ägande-, och nätförhållanden.

PTS identifierar i nedanstående redovisning fyra olika typer av cellulära lösningar: kommersiell lösning, kommersiellt radionät med dedikerat kärnnät, dedikerat radionät, och hybridlösning. Utöver detta beskrivs även andra lösningar, satellit och militära system, och kompletterande system, videolänk och temporära nät. Slutligen redovisas en översikt av ett antal frekvensområden och tillståndstider för dessa.

1 Bakgrund

Den 18 december 2015 fick Post- och telestyrelsen (PTS) i regeringsbeslut II:28 i uppdrag att till den 18 mars 2016 redovisa till regeringen vilka möjliga kommunikationslösningar det finns för aktörer inom allmän ordning, säkerhet, hälsa samt försvar.

Myndigheten för samhällsskydd och beredskap (MSB) har i samma regeringsbeslut fått i uppdrag att beskriva vilka behov aktörer inom allmän ordning, säkerhet, hälsa samt försvar har av mobil, ip-baserad kommunikation, inklusive bland annat vad som ska uppnås med kommunikationslösningarna och vilka krav som aktörerna ställer gällande informationssäkerhet, yttäckning, kapacitet och funktion. Dessutom ska MSB bedöma vilka drifts- och investeringskostnader olika lösningar medför, vilket MSB ska genomföra i samråd med PTS, Polismyndigheten och Försvarsmakten.

Den 18 december skickade PTS en skrivelse till MSB och bad om ett antal uppgifter rörande aktuella aktörers behov, vad kommunikationslösningarna ska uppnå, funktioner och krav [1]. Den 18 januari inkom MSB med ett yttrande som svar på PTS förfrågan [2]. PTS har därefter efterfrågat förtydliganden och kompletteringar av informationen i yttrandet.

Vid ett möte den 13 januari efterfrågade MSB att PTS den 1 februari övergripande redogör för olika möjliga lösningar för MSB, vilket PTS fullföljer med denna pm.

Mot bakgrund av den mycket begränsade tid PTS har haft till förfogande för att ta fram denna redovisning innehåller den endast en ytterst grov översikt av några olika alternativ för den typ av mobila ip-baserade kommunikationslösning som efterfrågas i regeringsbeslutet. Den korta tid PTS har haft till förfogande har inte heller medgett att PTS i annat än begränsad omfattning baserat redovisningen i denna pm på det yttrande som MSB lämnade till PTS den 18 januari.

[1] PTS dnr 15-11722.
[2] MSB dnr 2015-7213. MSB har utarbetat informationen i samråd med Polismyndigheten och Försvarsmakten. Krav har också inkommit från Trafikverket.

I samband med samrådet har PTS fått synpunkter och underlag från många intressenter inklusive kommersiella operatörer och utrustningstillverkare. Dessa kan läsas i sin helhet på PTS hemsida under ärendet.[3]

Lösningarna i denna pm redovisar PTS arbete såhär långt och är därför en preliminär kartläggning av lösningar och information. Informationen och beskrivningarna av lösningarna kan komma att ändras allteftersom arbetet med regeringsuppdraget fortskrider och ny information framkommer. Därför ska informationen och lösningarna i denna pm ses som preliminära och PTS kan inte utlova att informationen i denna pm kommer att vara samma som i den slutliga regeringsrapporten.

PTS kommer härefter att fortsätta kartlägga lösningar samt fördelar och nackdelar med de olika lösningarna i enlighet med regeringsbeslut II:28, och redovisa detta i en rapport till regeringen den 18 mars.

[3] http://www.pts.se/sv/Dokument/Remisser/2015/Samrad-i-utredning-om-framtida-mobila-kommunikationslosningar-for-blaljustjanster---15-11722/

2 Generellt om behov för mobil ip-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar

I denna pm gör PTS antagandet att aktörer inom allmän ordning, säkerhet, hälsa samt försvar ska tolkas som de verksamheter som idag omfattas av MSB:s uppdrag inom radiokommunikationssystemet för skydd och säkerhet (Rakel-systemet) såsom Polisen, Tullverket, Kustbevakningen, räddningstjänsten, akutsjukvården (kallat blåljusmyndigheter), alarmeringsföretag som bistår dessa myndigheter för alarmering och dirigering, samt den verksamhet inom Försvaret som är avsedd att stötta och samverka med sådan civil verksamhet.[4] Dessa kallas i denna pm för samhällsviktiga aktörer.

För att specifika lösningar för mobil ip-baserad kommunikation ska kunna utvärderas krävs att det finns en tydlig kravbild i form av funktionalitet, krav och behov. En noggrann utvärdering av vilka behov aktörerna har bör ligga till grund för analysen, och motivet bakom respektive krav och behov bör granskas, inklusive hur verksamhetskritisk funktionen är. Först därefter går det att avgöra vilka av aktörernas kommunikationsbehov och krav på kommunikationslösningar som drar nytta av att realiseras gemensamt och vilka som bäst genomförs via andra/egna lösningar. Avvägningar kommer även i praktiken att behöva göras vad gäller olika funktionalitet eller krav, vägt mot kostnader och verksamhetsnytta.

Någon sådan detaljerad utvärdering vad gäller ip-baserad kommunikation har inte genomförts i Sverige. Däremot gjordes en motsvarande utvärdering för det nuvarande kommunikationssystemet Rakel[5]. I syfte att här ändå kunna säga något om olika möjliga kommunikationslösningar har PTS fristående identifierat några aspekter och funktionaliteter som brukar anses centrala för mobil ip-baserad kommunikation generellt, samt särskilt för aktörer inom allmän ordning, säkerhet, hälsa samt försvar (se definition ovan). Denna beskrivning är dock mycket schematisk och syftar endast till att kunna identifiera några lösningar som kan vara aktuella att titta närmare på i det här sammanhanget.

[4] SOU 2003:10 Trygga medborgare - säker kommunikation
[5] SOU 2003:10 Trygga medborgare - säker kommunikation

2.1 Behov av täckning och tillgänglighet

Möjlighet att nå kommunikationstjänster i olika delar av landet är viktigt, och täckning är därför en central fråga att utvärdera. När man analyserar täckningsbehoven kan det vara relevant att ställa kraven i relation till täckningen i de nät som finns idag.

Dagens Rakel-system täcker 99,84 % av Sveriges befolkning och 95 % av landets yta, undantaget fjällvärlden (där fjällvärlden motsvarar i storleksordningen 7 – 8 % av landets yta).[6] Vad avser cellulära nät så har kommersiella operatörernas mobiltelefoninät en yttäckning för tal som (med antagandet om en typisk smartphone där signalen inte dämpas av kroppen) motsvarar drygt 90 % av landets yta inklusive fjällvärlden och ca 99,997% av landets befolkning.

Datatäckningen i de kommersiella näten förbättras kontinuerligt i och med den pågående 4G-utbyggnaden, och 2016 förväntas datatäckningen närma sig de nivåer som idag gäller för tal. Med samma antaganden som den kommersiella taltäckningen ger detta en förväntad yttäckning på omkring 85 % och en befolkningstäckning som överstiger 99,9% för 10 Mbit/s. Behövs högre nivåer av yttäckning även i otillgängliga områden såsom i fjällvärlden eller nationalparker är satellitlösningar extra intressanta att titta på.

När det gäller behov av tillgänglighet så är den i viss utsträckning beroende av behoven på täckning eftersom behov av täckning är ett geografiskt tillgänglighetsbehov. Behoven på tillgänglighet i detta fall blir styrande för hur kommunikationslösningen ska kunna hantera avbrott i tjänsten och hur länge sådana avbrott kan tolereras, som t.ex. avgrävda kablar, försörjning av el och reservkraft (dieselaggregat eller batterier), felaktigt handhavande, förstörd utrustning eller terminalutrustning eller andra avbrott såsom störningar. Detta måste säkerställas och kravställas i alla led, t.ex. hur stark effekt ska en basstation sända på, hur långt elavbrott ska ett reserv-elaggregat kunna hantera eller ska en enskild tjänsteman ha en extra terminal i händelse av att den huvudsakliga går sönder och/eller ska denne bära med sig extra batterier till terminalen/erna.

2.2 Behov av kapacitet

Behovet av kapacitet är i hög grad beroende av vilken funktionalitet som ska användas. I detta fall måste man också skilja mellan sådana behov som är verksamhetskritiska och sådana behov som kan vara bra att ha och på ett

[6] https://www.msb.se/sv/Produkter--tjanster/Rakel/Om-Rakel/Tackning, PTS gör antagandet att dessa siffror gäller för en fordonsmonterad terminal med 5 Watt uteffekt och yttre monterad antenn.

generellt plan underlätta arbete eller i vissa fall spara tid i det vardagliga arbetet som i sig inte är tidskritiskt. Ytterligare är det nödvändigt att analysera hur verksamheten påverkas om inte kommunikationslösningen uppnår högt ställda behov och hur verksamheten kan anpassas efter detta.

Behovet av kapacitet är också beroende av geografisk lokalisation och hur länge en viss kapacitet behövs.

2.3 Behov av säker kommunikation

När det gäller behov av konfidentialitet måste det klarläggas vilken typ av information som ska hanteras i kommunikationslösningen, hur skyddsvärd den är och hur tidskritiskt skyddet är. Om kommunikationslösningen ska hantera uppgifter som rör Sveriges säkerhet som har hög grad av sekretess under lång tid ställs helt andra krav på kommunikationslösningen jämfört med om kommunikationslösningen ska hantera uppgifter som förvisso är känsliga men som är av operativ karaktär och där informationen inte kan skada insatsen om den kommer ut när insatsen är avslutad. Dessutom finns det en skillnad i säkerhetsfunktioner beroende på om de ska vara på applikationsnivå eller på nätnivå. Om nätets säkerhet ligger i applikationerna kan känslig information sändas över de flesta sorters infrastruktur, medan om säkerheten ligger i näten finns det begränsningar i sändningarna.

På samma sätt kommer behovet av riktighet – d.v.s. att informationen inte obehörigen förvanskas – vara viktig för hur kravställningen utformas. Om det finns behov av spårbarhet måste krav ställas på loggningsfunktion och lagring av dessa samt säkerhet för loggarna. Finns andra behov av trafikdatalagring måste funktionalitet och lagring för denna typ av information också kravställas.

Informationssäkerheten i de olika typer av lösningarna påverkas av flera faktorer. En sådan faktor är lagstiftning där kommersiella operatörer har vissa skyldigheter[7] att vidta åtgärder för att upprätthålla informationstillgångars tillgänglighet, konfidentialitet och riktighet.

Utöver denna grundläggande nivå, är det möjligt att addera särskilda säkerhets-funktioner, exempelvis kryptografiska skydd, och också vidtala om andra åtgärder för att skydda både innehållet i elektronisk kommunikation och annan information.

[7] Enligt lagen (2003:389) om elektronisk kommunikation och föreskrifter som utgår från denna lagstiftning.

Vad gäller dedikerade nät så finns det förutom kryptografiska skydd också större möjligheter att kontrollera de tekniska lösningar som säkerställer informationssäkerheten i radionätet, och att bygga in skydd i hårdvaran. Valet av transmissionslösning kan påverka kraven och lösningarna för att säkerställa informationsskyddet i nätets olika delar.

Denna pm kommer inte vidare behandla lösningar för att säkerställa behov av säker kommunikation.

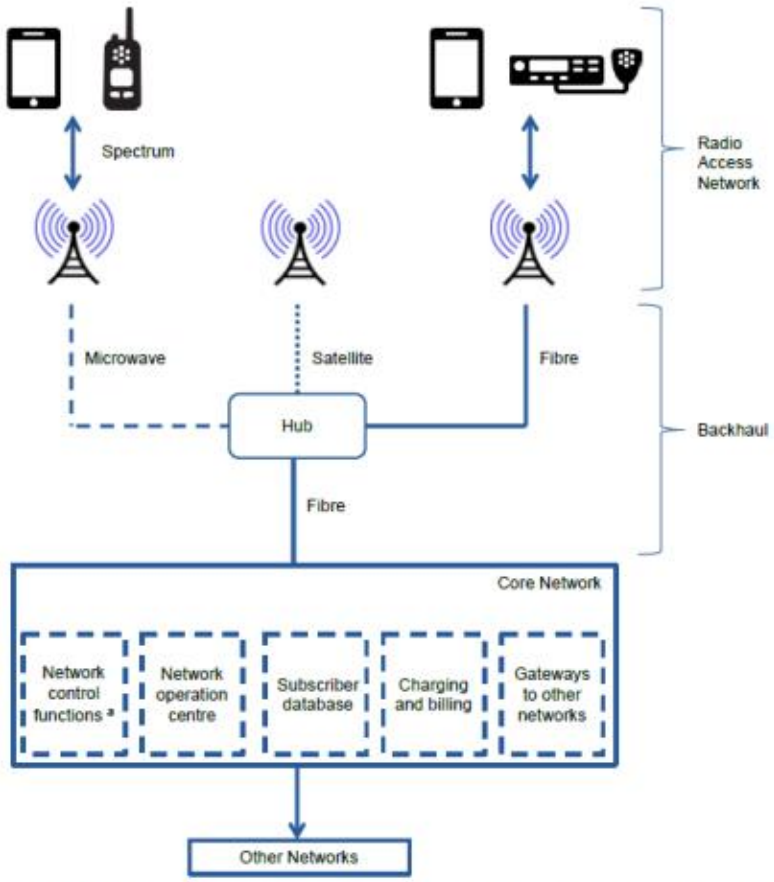
2.4 Behov av särskilda funktioner

En kommunikationslösning anpassad för aktörer inom allmän ordning, säkerhet, hälsa samt försvar ställer troligtvis speciella krav på särskilda funktioner i nätet, exempelvis prioritering. Andra tänkbara funktioner är exempelvis push-to-talk, direktsamtal mellan enheter, tak på uppkopplingstid mm. Denna pm kommer inte att behandla eller ta hänsyn till sådana särskilda funktioner som kan vara aktuella för en kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa samt försvar.

3 PPDR i cellulära bredbandsnät

En cellulär lösning för samhällsviktig kommunikation kan beskrivas utifrån tre olika delar: radionät, transmissionsnät och kärnnät. Hur dessa hänger samman förklaras av nedanstående bild[8] där radionät motsvaras av ”Radio Access Network”, transmissionsnät motsvaras av ”Backhaul”, och kärnnät motsvaras av ”Core Network”.

Figure 5.2 **Key elements of a mobile network**



a 'Network control functions' are functions that different elements of the core undertake when managing a call or data session on a mobile network, such as user authentication, assigning resources, traffic management, and cell handover.

Sources: Alcatel-Lucent (2009, 2010); Gras (2015).

[8] Bilden är från Productivity Commission 2015, *Public Safety Mobile Broadband,* Research Report, Canberra.

3.1 Tjänster i kommersiella radionät

3.1.1 Beskrivning

Denna lösning innebär att man använder en eller flera mobiloperatörers kommersiella radionät som bärare av trafiken. Operatören man har kontrakt med ansvarar i detta fall även för abonnemang, kundhantering, kundsupport och fakturering. Vid en upphandling av tjänst kan man i detta fall ställa specifika krav angående den funktionalitet, tillgänglighet och integritet/säkerhet som anses vara nödvändig för aktörer inom samhällsviktig verksamhet[9]. Kraven som ställs i en sådan upphandling kan också omfatta ändringar av ägarkontrollen av nätet.

En variant på samma tema är att istället upprätta en Mobil Virtuell Nätverks Operatör (MVNO) för samhällsviktig verksamhet utan egen infrastruktur. Denna kan då upphandla kapacitet centralt från en eller flera mobiloperatörer men ansvarar för abonnemang, kundhantering, kundsupport och fakturering gentemot kunderna inom området samhällsviktig verksamhet. I övrigt är denna lösning lik den förstnämnda. Beskrivningarna i följande avsnitt ska därför anses giltig för båda dessa varianter.

3.1.2 Radionätet

Den aktiva utrustningen i radionätet ägs och kontrolleras av kommersiella aktörer. Trafik från samhällsviktig verksamhet överförs inom samma frekvensutrymme och med samma utrustning som används för att hantera trafiken från allmänhet och operatörens övriga kunder. Mobiloperatören uppgraderar dock sitt radionät med den extra funktionalitet och de förstärkningar som krävs för att uppfylla de krav som angetts i upphandlingen.

Om man slutit ett avtal som tillåter kundspecifik nationell roaming[10] eller krisroaming med en eller flera ytterligare mobiloperatörer så kommer man även ha tillgång till samtliga radionät som dessa operatörer har vilket ger möjlighet till större yttäckning samt ökad robusthet och redundans.

3.1.3 Transmissionsnätet

Transmissionsnätet för de kommersiella näten är en kombination av operatörens egna förbindelser över egen eller hyrd svartfiber, hyrda förbindelser och radiolänkförbindelser. Detta omfattande IP-nät är idag i stora delar redan utbyggt med redundans och geografisk diversitet. Beroende på i

[9] Vi likställer ”samhällsviktig verksamhet” med kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar.
[10] Koppling från en operatör till en annan.

upphandlingen ställd kravbild så kan delar av nätet behöva uppgraderas och/eller förstärkas.

3.1.4 Kärnnätet

Samma kärnnät används som för den kommersiella trafiken, detta ägs och kontrolleras av den kommersiella operatören som är helhetsleverantör av kommunikationstjänsten. Beroende på vilka krav som ställts i upphandlingen kan operatören dock behöva göra förändringar i sitt kärnnät och i sin drift- och underhållsorganisation.

3.1.5 Frekvenser

Lösningen använder sig av det frekvensutrymme som är tilldelat och i framtiden kommer att tilldelas till de kommersiella mobiloperatörerna[11]. Redan idag finns kommersiella LTE nät med god yttäckning utbyggda i de låga frekvensbanden under 1 GHz, exempelvis i 450 MHz, 800 MHz och 900 MHz. Vidare finns LTE-nät i 1,8 GHz, 2,1 GHz och 2,6 GHz som förstärker kapaciteten i områden som har en hög konsumtion av datatrafik. Mer spektrum lämplig för kapacitetsförstärkningar kan förväntas erbjudas marknaden i öppna urvalsförfaranden kommande år. Ytterligare kapacitet i frekvensband som är bra för yttäckning förväntas byggas ut i 700 MHz bandet efter den 1 april 2017.

3.1.6 Täckning

Täckningen i detta fall är som utgångspunkt den/de kommersiella operatörernas täckning. Om man upphandlat avtal i vilket det ingår kundspecifik nationell roaming eller krisroaming så kommer man ha tillgång till den kombinerade täckningen från de i avtalet ingående operatörerna. Eventuella täckningskrav som går utöver den som redan erbjuds av den kommersiella operatören behöver dock ingå som en del i upphandlingen.

3.1.7 Kapacitet

Den stora mängden tillgängligt kommersiellt spektrum, i kombination med det tätt planerade radionäten (antal basstationer per yta) gör att kapaciteten i de kommersiella LTE näten är idag generellt mycket god och förväntas öka med tiden. Detta medför att förutsättningarna är goda för de kommersiella radionäten att täcka kapacitetsbehovet i de mest kapacitetskrävande situationerna. Samhällsviktig verksamhet kan då få prioritet i nätet, eventuellt utan större påverkan på operatörernas övriga trafik. Genom att tillföra mer frekvensutrymme till de kommersiella aktörerna kan också den totala kapaciteten i näten vidare utökas med samma mängd som skulle tillföras vid implementation av separat dedikerat nät i samma frekvenser, dock med

[11] Tilldelas efter ett öppet urvalsförfarande, t.ex. en auktion enligt 3 kap.8§ LEK 2003:389.

skillnaden att kapacitetsökningen i de geografiska områden där aktörer inom samhällsviktig verksamhet vid varje specifik tidpunkt inte använder hela kapacitetstillskottet kan användas av andra kunder. Beroende på kravställningen kan även tillfällig kapacitetsökning ske genom exempelvis mobila basstationer såväl vid planerade händelser som vid oförutsedda krissituationer.

3.1.8 Tillgänglighet

Tillgängligheten i det kommersiella nätet kommer att beror på en rad faktorer som inkluderar t.ex. antalet basstationer, transmissionslösning och redundanta förbindelser, tillgång till reservkraft, serviceorganisation m.m. Nivån på denna kommer att vara ett resultat av de krav som ställs i upphandlingen. Höga robusthetskrav vad gäller t.ex. redundans och reservkraft för alla noder i nätet kan dock vara mycket kostsamma vilket förväntas återspegla sig i prisbilden för de tjänster som upphandlas.

3.2 Kommersiell lösning med dedikerat kärnnät

3.2.1 Beskrivning

Denna lösning innebär liksom föregående lösning att en eller flera av mobiloperatörers kommersiella LTE radionät och transmissionsnät används som bärare av trafiken. Men till skillnad mot ovan så implementeras ett för samhällsviktig verksamhet dedikerat kärnnät. Målet med detta är att få ökad kontroll över centralnätfunktionalitet och abonnentrelaterad data.
Med detta alternativ omfattas viss infrastruktur och funktionalitet inte av upphandlingen av kapacitet från de kommersiella operatörerna. Det är dock fortfarande lika viktigt att upphandlingen ställer de specifika krav på radionätet som anses vara nödvändiga för aktörer inom samhällsviktig verksamhet.

3.2.2 Radionätet

På samma sätt som i föregående fall ägs och kontrolleras den aktiva utrustningen i radionätet av kommersiella aktörer och trafik från samhällsviktig verksamhet överförs inom samma frekvensutrymme och med samma utrustning som används för att hantera trafiken från allmänhet och företag.
För en mer omfattande beskrivning se avsnitt 3.1.2 ovan.

3.2.3 Transmissionsnätet

Samma förutsättningar som anges i avsnitt 3.1.3 ovan.

3.2.4 Kärnnätet

Ett separat kärnnät dedikerat för den samhällsviktig verksamet implementeras. Med införandet av detta separata kärnnät går det att garantera direkt kontroll över vissa delar av nätet och därmed även över kundrelaterad data. Ett dedikerat kärnnät ger också bättre förutsättningar för en tät integration mellan LTE-nätet och TETRA-nätet.

I detta fall finns två alternativ för ägande och kontroll av kärnnätet.

1. Ett separat kärnnät dedikerat för den samhällsviktig verksamet, där de aktiva noderna ägs och kontrolleras av en statlig aktör.
2. Ett separat kärnnät dedikerat för den samhällsviktig verksamet, och där de aktiva noderna ägs och kontrolleras av en kommersiell aktör under kontrakt och översyn från staten.

3.2.5 Frekvenser

Samma förutsättningar som anges i avsnitt 3.1.5 ovan.

3.2.6 Täckning

Samma förutsättningar som anges i avsnitt 3.1.6 ovan.

3.2.7 Kapacitet

Samma förutsättningar som anges i avsnitt 3.1.7 ovan.

3.2.8 Tillgänglighet

Samma förutsättningar som anges i avsnitt 3.1.8 ovan.

3.3 Lösningar med dedikerat radionät

3.3.1 Beskrivning

Detta alternativ innebär att byggandet av ett dedikerat nationellt landstäckande radionät, baserat på t.ex. kommersiell LTE-standard.

3.3.2 Radionätet

Den aktiva utrustningen i radionätet är för denna lösning dedikerad, och radionätet bär enbart trafik för samhällsviktig verksamhet. Liksom för det nuvarande Rakel-nätet ägs en stor del av infrastrukturen (t.ex. masterna) av kommersiella aktörer. Den aktiva utrustningen kan placeras i egna teknikbodar, eller inhyrd plats i en kommersiell bod där åtgärder vidtas för att uppnå ett adekvat skalskydd.

När det gäller den aktiva utrustningen (t.ex. radiobasstationerna) kan man tänka sig två olika alternativ för ägande och kontroll:

1. Den aktiva utrustningen ägs och kontrolleras av en statlig aktör.
2. Den aktiva utrustningen ägs och kontrolleras av en kommersiell aktör under kontrakt och översyn från staten.

Till skillnad från det nuvarande Rakel-nätet som använder rundstrålande antenner byggs ett yttäckande LTE-nät normalt sett med sektoriserade basstationer, där varje basstation typiskt har tre antennriktningar. PTS känner

inte till något kommersiellt LTE-nät som använder sig av rundstrålande antenner, och en sådan lösning skulle ge en betydligt sämre täckning och erbjuda en lägre kapacitet jämfört med ett sektoriserat nät.

Antalet basstationer i nätet är starkt beroende på behovet av täckning och kapacitet samt kravet på eventuell redundans, samt även frekvensband.

3.3.3 Transmissionsnätet

Även transmissionsnätet i denna lösning är dedikerad, och skulle, liksom för det nuvarande Rakel-nätet, vara uppbyggt med en kombination av fiberanslutningar och radiolänkförbindelser. När det gäller ägande och kontroll av transmissionsnätet ser PTS följande alternativ (som eventuellt även kan kombineras):

1. Anslutningarna i transmissionsnätet hyrs av en kommersiell aktör
2. Alla aktiva utrustning transmissionsnätet (både radiolänkutrustning och aktiva noder i fiberanslutningarna) ägs och kontrolleras av en statlig aktör.

3.3.4 Kärnnätet

Kärnnätet i denna lösning är också dedikerad för samhällsviktig kommunikation. Tekniskt sett motsvarar lösningen i stort sett den kommersiella lösning med ett dedikerat kärnnät som beskrivs i kap 3.2.4. När det gäller ägande och kontroll över kärnnätet finns följande alternativ.

1. Ett separat kärnnät dedikerat för den samhällsviktig verksamet, där de aktiva noderna ägs och kontrolleras av en statlig aktör.
2. Ett separat kärnnät dedikerat för den samhällsviktig verksamet, och där de aktiva noderna ägs och kontrolleras av en kommersiell aktör under kontrakt och översyn från staten.

3.3.5 Frekvenser

Ett dedikerat radionät kräver tillgång till frekvenser. För att uppnå kraven på yttäckning med ett rimligt antal basstationer bör dessa frekvenser ligga under 1 GHz (vilket även är den slutsats som ECC Rapport 199 och 218 gör). PTS kan konstatera att det finns ett antal potentiella frekvenslösningar, exempelvis i banden 450 MHz, 700 MHz och 900 MHz (se vidare kapitel 5).

3.3.6 Täckning

Täckningen från det dedikerade radionätet beror på utbyggnaden av nätet. Vilket/vilka frekvenser som används har en inverkan på hur kostsamt det blir att bygga ut täckning på så sätt att låga frekvensband når längre och därmed medger färre basstationer för samma täckning.

3.3.7 Kapacitet

Kapaciteten i det dedicerade nätet beror på frekvenslösningen i kombination med hur tätt nätet byggs (antal basstationer per yta). Olika lösningar skulle kunna vara exempelvis 2x3 MHz, 2x5 MHz och 2x10 MHz.

3.3.8 Tillgänglighet

Tillgängligheten i ett dedikerat nät beror på en rad faktorer som inkluderar t.ex. antalet basstationer, transmissionslösning och redundanta förbindelser, tillgång till reservkraft, serviceorganisation m.m. PTS noterar att höga robusthetskrav vad gäller t.ex. redundans och reservkraft för alla noder i nätet kan vara mycket kostsamt.

3.4 Hybridlösning

3.4.1 Beskrivning

Denna lösning innebär att trafiken bärs av en kombination av ett dedikerat radionät och ett eller flera kommersiella radionät. PTS ser ett antal olika grundläggande varianter på lösningar där det dedikerade och kommersiella nätens roll (och därmed kravbild) skiljer sig åt.

3.4.2 Radionätet

Radionätet är här är en kombination av ett dedikerat radionät och kommersiella radionät. Avtal med en eller flera kommersiella operatörer möjliggör att användarna vid behov kan använda flera operatörers nät via roaming. Fördelningen av trafiken mellan de olika näten styrs genom funktionalitet i kärnnätet, och LTE-standarden gör det möjligt utifrån en mängd parametrar (även differentierat mellan olika användare) på ett önskat sätt styra trafiken mellan de olika näten. Avtalen med de kommersiella operatörerna kan även vara förenade med villkor, t.ex. att trafiken från samhällsviktig verksamhet ges prioritet i näten. Om avtalet tillåter kundspecifik nationell roaming med en eller flera ytterligare mobiloperatörer så kommer man även ha tillgång till de radionät som dessa operatörer har.

Nedan följer två exempel på möjliga varianter för en hybridlösning.

- **Hybridlösning med nationellt täckande dedikerat ”bas-nät”**
  För denna lösning består det dedikerade radionätet av ett nationellt PPDR-nät som fungerar som ett slags ”bas-nät”, vilket under normala driftförhållanden kan bära majoriteten av trafiken från de samhällsviktiga aktörerna. Terminalerna i har dock även möjlighet att vid behov växla till ett (eller flera) kommersiella LTE radionät. Det kommersiella nätet eller näten fungerar då som en kompletterande kapacitetsförstärkning eller backup i områden med dålig täckning eller

driftavbrott i PPDR-nätet.

- **Hybridlösning med geografiskt begränsat dedikerat nät**
  I denna variant på hybridlösning består radionätet av ett eller flera kommersiella radionät i kombination med ett antal lokala, geografiskt begränsade dedikerade nät. Det kommersiella radionätet ger nationell yttäckning och kapacitet, men i områden som ses som särskilt viktiga vad gäller t.ex. kravet på säkerhet och tillgänglighet, där det ofta krävs hög kapacitet, eller där det finns kända brister i den kommersiella täckningen kompletterar man radionätet med ett lokalt dedikerat nät.

3.4.3 Transmissionsnätet

Transmissionen för det dedikerade radionätet kommer att vara ett dedikerat nät enligt samma princip som beskrivs för den dedikerade lösningen (kapitel 2.3). Den samhällsviktiga trafiken som går i kommersiella radionätet använder även den kommersiella operatörens transmissionsnät.

3.4.4 Kärnnätet

Denna lösning har ett dedikerat kärnnät. Men när en terminal använder det kommersiella radionätet kommer även den samhällsviktiga trafiken att gå genom det kommersiella kärnnätet.

3.4.5 Frekvenser

Det dedikerade radionätet i en hybridlösning kräver tillgång till frekvenser som är dedikerade till samhällsviktig kommunikation. För att en hybridlösning med ett nationellt täckande dedikerat nät ska bli mindre kostsam bör frekvenser i relativt låga frekvensband användas för att uppnå god yttäckning med ett lägre antal basstationer (se vidare kapitel 5).

Om det dedikerade radionätet har ett begränsat täckningsområde och t.ex. främst ska ge täckning och/eller kapacitet i och omkring större städer så bör frekvenser i högre band användas (se vidare kap 5).

3.4.6 Täckning

Täckningen i ett hybridnät motsvarar den sammanlagda täckningen från det dedikerade och kommersiella radionätet. Detta gör att kravet på täckningen från det dedikerade radionätet bör kunna vara lägre, vilket borde möjliggöra en mer ekonomisk lösning med färre basstationer, jämfört med en helt och hållet dedikerad lösning.

3.4.7 Kapacitet

Beroende på utformning möjliggör lösningen att terminalerna vid behov kan utnyttja kapacitet i det kommersiella radionätet vilket ger större möjligheter att med en begränsad bandbredd i det dedikerade radionätet täcka kapacitetsbehovet i de mest kapacitetskrävande situationerna (främst simultan videoöverföring till eller från flera användare i nätet).

3.4.8 Tillgänglighet

Möjligheten för terminalen att växla nät gör att den totala tillgängligheten för användaren blir högre än den som uppnås i respektive när var för sig.

4 Övriga och/eller kompletterande lösningar

4.1 Lösningar som utgår från militära system och teknik

Försvarsmakter har vanligtvis tillgång till ett flertal olika kommunikationsnät med olika egenskaper. En del av dessa nät används för att möjliggöra mobil datakommunikation och har utvecklats för att fungera även i situationer där tillgången till annan kommunikationsinfrastruktur är begränsad och då det i övrigt råder utmanande förhållanden.

Beroende på den samlade nationella behovsbilden för aktörer inom allmän ordning, säkerhet, hälsa och försvar kan delar som baseras på militära kommunikationssystem eller militär teknik[12] vara en del av en total lösning för att täcka det samlade identifierade behovet av mobil kommunikation, inte minst om behov och användningsområden går utöver det för det nuvarande Rakel-systemet.

4.1.1 Radionätet

Det finns flera sätt att möjliggöra mobil datakommunikation inom begränsade områden utgående från tillgänglig militär teknik. Normalt är den underliggande infrastrukturen rörlig eller flyttbar. Det finns också möjligheten att etablera kommunikation mellan rörliga enheter helt utan annan infrastruktur än radioterminaler.[13]

4.1.2 Kärnnätet

Militära kommunikationsnät för mobil kommunikation är normalt inte uppbyggda så att radionätet är beroende av anslutning till ett kärnnät för att upprätthålla kommunikation inom (ett begränsat) täckningsområde. Därmed finns det inte en centraliserad hantering av abonnenter eller övriga funktioner som kan associeras med kärnnät i ett kommersiellt, cellulärt kommunikationsnät. Radionätet kan dock vara anslutet till ett transmissionsnät för att möjliggöra kommunikation över stora avstånd.

4.1.3 Transmissionsnätet

De tekniska skillnaderna mellan militära kommunikationssystem och de system som används för icke-militära tillämpningar är störst i radionätet och mer

[12] Exempel på sådan teknik är skydd mot telekrigsinsatser (ökad störtålighet) och särskilda informationssäkerhetsskydd som kan tillföras till de kommunikationslösningar som tidigare har använts för kommersiella ändamål.
[13] Genom så kallade ad hoc-nät.

begränsade i övriga nätdelar. Transmissionsnätet, som förbinder ett radionät med täckning inom ett geografiskt avgränsat område med andra nät, består ofta av radiolänk- och satellitbaserade lösningar (vid internationella operationer).

4.1.4 Frekvenser

Militära radiokommunikationssystem utnyttjar normalt dedicerade frekvenser som avsatts för detta bruk. Försvarsmaktens frekvensanvändning i Sverige beslutas på samma sätt som annan radioanvändning av PTS enligt 3 kap 3 § i Lag (2003:389) om elektronisk kommunikation, efter hörande av Försvarsmakten och vederbörlig behovsprövning.

I den utsträckning som militär teknik används för att förbättra särskilda egenskaper i kommersiella system, exempelvis för att ge förbättrad tålighet mot elektromagnetiska störningar, kan de sammanlagda frekvensbehoven påverkas utan att de möjliga frekvensbanden (enligt tidigare avsnitt) ändras.

4.1.5 Täckning

Hur lång räckvidd en sändare i ett militärt radiokommunikationssystem har är liksom för andra trådlösa kommunikationssystem, starkt frekvensberoende.

4.1.6 Kapacitet

Kapaciteten för militära kommunikationssystem är generellt lägre jämfört med dagens kommersiella mobila kommunikationsnät under normala omständigheter. Militära system kan dock förväntas bibehålla hela eller delar av kommunikationsförmågan även i situationer som avviker väsentligt från det normala.

4.2 Satellit

För att uppfylla behovet av mobil kommunikation även på platser där ett cellulärt mobilnät normalt sett inte kan ge täckning kan satellittjänster vara en potentiell möjlighet.

Satellitlösningar för bredband som finns på marknaden idag kan möjligöra både mobil och fast bredbandsuppkoppling över hela Sverige. Lösningarna är dock inte fullt optimerade för mobilitet, men detta håller på att förändras med en pågående uppbyggnad av nya satellitsystem.

Exempelvis har EchoStar Mobile fått ett paneuropeiskt mobilsatellit (MSS) tillstånd i 2 GHz-bandet vilket kommer kunna ge mobil satellittäckning till

handenheter i hela Sverige. Systemet är för tillfället under uppbyggnad[14]. Dessutom möjliggör utvecklingen av elektriskt fasstyrda adaptiva antenner att terminaler kan börja använda de stora frekvensmängder som finns i fastsatellitfrekvensband för fordonsburna mobila tillämpningar[15].

Både traditionella operatörer av geostationära satellitsystem och nya aktörer som planerar stora konstellationer av lågflygande icke stationära satelliter[16] arbetar med dessa lösningar. Denna typ av lösningar kan också kombineras med en liten LTE-basstation i fordon för att ge lokal täckning till mobilterminaler[17] i vilket fall satelituppkoplingen snarare är att se som en del i transmissionsnätet.

4.2.1 Frekvenser

I 2 GHz bandet finns det 2st paneuropeiska MSS-tillstånd om 2*15 MHz vardera[18]. En av tillståndshavarna har identifierat PPDR som en lämplig marknad att adressera vilket gör att 2*15 MHz är aktuella i detta sammanhang. Tillstånden tillåter även utbyggnad av ett komplementerande markbaserat nät i samma frekvensband, något som i praktiken möjliggör utbyggnad av ett mobilnät på dessa frekvenser.

För FSS finns det reglering och harmonisering som gör det möjligt att använda FSS-frekvensband för jordstationer i rörelse. I Sverige finns det undantag för satellitterminaler för denna typ av användning i 14,0-14,5 GHz och 29,5-30 GHz banden. Dessa undantag gäller sändning från satellitterminaler till satelliter – sändningar från satelliter till satellitterminaler behöver inte tillstånd i Sverige, och kan ske i ett antal olika FSS band.

4.2.2 Täckning

Det finns ett antal olika satelitsystem som redan har nationell täckning för fast/nomadiskt bredband i Sverige, dessa är framförallt FSS system med satelliterna i en Geostationär bana. EchoStar Mobile har som en del i tilldelningsprocessen för sitt paneuropeiska MSS tillstånd accepterat ett 100 % täckningskrav i Sverige, detta skall vara uppfyllt senast den 1 december 2016.

---

[14] EchoStar Mobile's satellite network can provide a robust and secure communications network for the PPDR sector, http://echostarmobile.com/

[15] Kymeta answers the questions of the two dominant constraints in the mobile communications industry: coverage and capacity, http://www.kymetacorp.com/technology/the-problem-we-solve/

[16] How a Va. Startup Plans to Launch 648 Satellites, http://dcinno.streetwise.co/2016/01/26/va-based-internet-satellite-co-oneweb-plans-2016-raise-hiring/

[17] Vehicle Cell Network For First Responders, http://oneweb.world/#use

[18] Komissionsbeslut 2009/449/EG om urval av operatörer av alleuropeiska system som tillhandahåller mobila satellittjänster, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:149:0065:0068:EN:PDF

De nya satellitsystemen med stora konstellationer av lågflygande satelliter utlovar global täckning för bredbandstjänster t.ex. utlovar One-Web att uppnått detta innan slutet av 2019.

För samtliga satellittjänster gäller att täckningen framförallt kan anses vara för utomhusbruk till mobila och nomadiska terminaler. För täckning inomhus behöver dessa lösningar kompletteras med lokala markbundna lösningar.

4.2.3 Kapacitet

De FSS satellitsystem som redan är i drift har idag kapacitet på över 1 Gbit/s per spotbeam (motsvarar täckningsområdet för en cell i ett mobilsystem) med en eller ett flertal spotbeams som överlappande täcker olika delar av Sverige[19].

Även om MSS i 2 GHz bandet förväntas ha begränsad kapacitet på grund av den begränsade frekvensbandbredd om 2*15 MHz som tilldelats, så tillåter även tillståndet att man bygger ut ett komplementerande marknät. Detta gör att MSS operatören i praktiken har rättighet att bygga ut ett komplementerande mobilnät i samma frekvensområde, något som kraftigt kan utöka den kapacitet som kan erbjudas.

De nya satellitsystem med stora konstellationer av lågflygande icke stationära satelliter som nu är under uppbyggnad planeras för att kunna erbjuda mycket hög kapacitet. Med undantag för markkomponenten i 2GHz MSS som i praktiken skulle vara ett mobilnät, bör dock kapaciteten jämfört med den som kan uppnås i ett nationellt mobilsystem anses som lägre. Detta gör att satellitlösningarna främst lämpar sig som komplement till ett nationellt LTE basserat mobilnät.

4.3 Videolänk

Videolänkförbindelser ses som en kompletterande kommunikationskanal som kan tillfredsställa vissa behov av kommunikation. Exempelvis kan kommunikation mellan mark och flygfarkost (AGA) ske på detta sätt, eller annan överföring av rörlig bild som inte behöver ske direkt mellan terminaler i det cellulära bredbandsnätet.

Beroende på typen av användning så finns det en rad potentiella både civila och militära frekvensband i olika frekvensområden.

[19] Eutelsat KA-SAT http://www.eutelsat.com/en/satellites/the-fleet/EUTELSAT-KA-SAT.html

4.4 Temporära nät

Temporära nät ses inte heller i denna redovisning som en komplett lösning, utan som ett komplement. Beroende på användning och scenario behöver lösningen för temporära kommunikationsbehov inte nödvändigtvis vara en integrerad del av det cellulära bredbandsnätet. Behovet av temporär kapacitet och täckning med lösningar skulle kunna tillfredsställas med hjälp av separata system som använder sig av frekvenser i andra band än de som används för det cellulära bredbandsnätet som normalt sett bär den samhällsviktiga trafiken.

5 Frekvensband och tillståndstider

Nedan följer en förteckning av olika frekvensband med deras respektive tillståndstider.

Frekvensband och tillståndstider

Frekvensband	Tillstånd går ut
450 MHz	2021
700 MHz	2017
900 MHz	2025
1,8 GHz	2027
1,9 GHz	2025
2,3 GHz	2018
2,6 GHz	2024
3,5 GHz	2018
3,7 GHz	2023
26 GHz	2022
28 GHz	2025

Rakel-nätet använder idag frekvenser runt 380 MHz, som blir ”lediga” om Rakel ersätts av en mobil bredbandslösning.

PTS tilldelar idag temporära, lokala tillstånd för videolänk i samband med olika evenemang, exempelvis runt 2 GHz och 2,8 GHz. Då det rör sig om temporära tillstånd finns det ingen tillståndstid som går ut. Runt 5 GHz finns det även band som är harmoniserade både inom och utanför Europa för Broad Band Disaster Relief (BBDR). Olika militära frekvensband skulle kunna vara möjliga beroende på verksamhet och Försvarsmaktens framtida behov av frekvenser.

Alla tillstånd i frekvensband som används för radiotrafik i de kommersiella mobilnäten är förenade med villkor som möjliggör att frekvenserna delas med annan användning. Ett eventuellt behov att utöka täckning eller kapacitet när ett kommersiellt nät har ett driftavbrott skulle kunna tillfredsställas genom att man temporärt använder den kommersiella operatörens frekvenser i det område där det är driftavbrott. Utanför tätbefolkade områden skulle man kunna tänka sig en lösning där man för att lokalt utöka täckning och kapacitet för samhällsviktig kommunikation temporärt använder sig av höga frekvensband som normalt sett inte används av mobiloperatörer i dessa områden.

Säker och tillgänglig mobil, IP-baserad kommunikation för aktörer inom allmän ordning säkerhet, hälsa samt försvar

Regeringsuppdrag II:28, 2015-12-17

Redovisning av bedömda drifts- och investeringskostnader samt möjlig tidplan för skarp drift av olika alternativ

Innehållsförteckning

Inledning

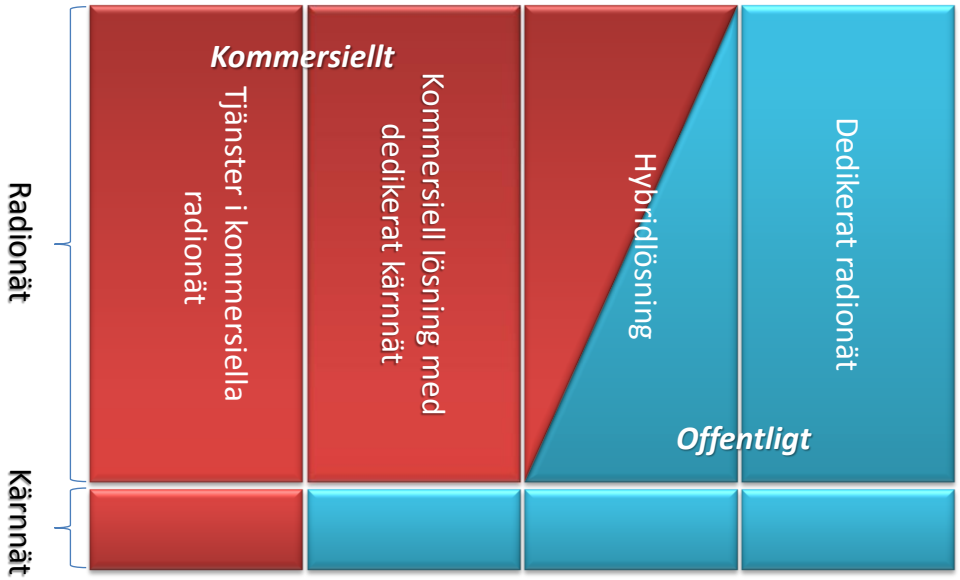
Myndigheten för samhällsskydd och beredskap har, i enlighet med regeringsuppdraget, i samråd med Polismyndigheten och Försvarsmakten i denna redovisning gjort en bedömning av drifts- och investeringskostnaderna samt redovisat en möjlig tidplan för skarp drift för olika lösningar. Samråd har också genomförts med Post- och telestyrelsen (PTS).

De krav och behov som hänvisas till och ligger till grund för bedömda kostnader är de som redovisas i dokumentet ”Säker och tillgänglig mobil, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar, regeringsuppdrag II:28, 2015-12-17, Redovisning av krav och behov av säker och tillgänglig, IP-baserad kommunikation för aktörer inom allmän, ordning, säkerhet, hälsa samt försvar”.

PTS har redovisat tänkbara lösningar för kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar, inom ramen för samma uppdrag[1]. MSB har använt lösningar som PTS redovisade den 1 februari som underlag för bedömningar av kostnaderna.

MSB har under hösten 2015 beräknat drifts- och investeringskostnader för ett dedikerat offentligt ägt mobil bredbandsnät. För att kvalitetssäkra dessa beräkningar inom ramen för regeringsuppdraget samt för att bedöma kostnaderna för övriga lösningar som PTS presenterat, genomförde MSB under februari 2016 en informationsinhämtning[2] (även kallat Request For Information). MSB har fått svar från sammanlagt 13 respondenter. Huvuddelen av respondenterna har åberopat affärssekretess.

[1] *Kommunikationslösningar för aktörer inom allmän ordning, säkerhet, hälsa samt försvar* (PTS diarienummer 15- 11722)
[2] *Förfrågningsunderlag RFI – säker och tillgänglig mobil IP-baserad kommunikation* (MSB diarienummer: 2016-667)



Figur 1. Illustration av PTS lösningsförslag.

Figur 1 visar hur de olika lösningarna delas in utifrån ett ägar- och kontrollperspektiv gällande kärnnät och radionät[3]. Röd markering i figuren avser kommersiell styrning och kontroll av infrastruktur, medan blå markering avser offentlig styrning och kontroll av infrastruktur. En hybridlösning kan variera från begränsad till fullständig offentlig kontroll.

[3] Med kärnnät avses infrastruktur för kontroll av; användare, användarinformation, behörigheter, säkerhet och tjänster. Radionätet skapar geografisk täckning och säkerställer kapacitet.

Redovisning

Nödvändiga kompletteringar som innebär kostnader
Samtliga lösningar som presenteras i denna rapport måste kompletteras med följande för att ge en fullständig bild av kostnaden:

- Lösningarna innebär att inplaceringar görs på redan tillgängliga installationsplatser där detta är möjligt.
- Inplacering i Försvarsmaktens installationsplatser innebär att särskild lagstiftning måste beaktas, såsom säkerhetsskyddslag och tillträdesförordningen, vilket kan påverka möjlighet till och kostnad för inplacering.
- De driftskostnader som redovisas innehåller inte avskrivningskostnader, utan investeringskostnaden redovisas separat.
- Samtliga lösningar behöver kompletteras med tidplan och kostnader för genomförande av en eller flera upphandlingar.
- Lösningarna omfattar begränsad täckning i fjällvärlden. Krav är talkommunikation med möjlighet att snabbt utöka med datakapacitet vid behov. Denna utökning ingår inte i de bedömda kostnaderna.
- Lösningarna innehåller ingen extra utrustning för inomhustäckning.
- Med särskild funktionalitet avses det som redovisas i ”Redovisning av krav och behov av säker och tillgänglig mobil, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar” avsnitt 2.4.2. Sådan funktionalitet avtalas genom tecknande av servicenivåavtal (SLA).
- Nationell roaming innebär att datatrafiken kan fördelas mellan olika operatörer, vilket hanteras genom avtal.

Reservkraft
MSB har för att uppnå robusthet på sju dygn räknat med dieselaggregat på cirka 80 procent av installationsplatserna. MSB bedömer att motsvarande komplettering behövs också för de kommersiella operatörerna.

Tjänster i kommersiella radionät

Beskrivning
Denna lösning innebär att det är möjligt att använda en eller flera mobiloperatörers kommersiella kärn- och radionät som bärare av trafiken. Vid en helt kommersiell lösning i dess enklaste utformning kan tjänsten köpas t.ex. i form av abonnemang. Driftskostnaden består då av abonnemang och styrs av flera olika faktorer som t.ex. antal användare, hur mycket data som ingår och bindningstid. Tilläggstjänster som t.ex. prioritet och annan funktionalitet som är nödvändig medför extra kostnader.

Den abonnemangskostnad som redovisas bygger på genomsnittet av de fyra största mobiloperatörernas företagsabonnemang för mobilt data, som inkluderar 50 GB data per månad och bindningstid 0 - 3 månader. Om en högre datakapacitet krävs innebär detta högre kostnader.

Kommentarer till krav som samhällsviktig verksamhet ställer
Inkomna RFI-svar är ofullständiga gällande kostnader för de tjänster eller förutsättningar som behövs för att svara upp till kraven. MSB har gjort en bedömning av kostnaden för denna lösning men har således inte kunnat verifiera dessa i de inkomna RFI-svaren.

MSB:s bedömning är att detta lösningsförslag inte uppfyller de grundläggande kraven på offentlig kontroll och informationssäkerhet. För att uppfylla övriga krav behövs väsentliga investeringar göras i t.ex. utökad täckning, reservkraft och andra robust- och säkerhetshöjande åtgärder i transmission samt verksamhetskritisk funktionalitet.

Prioritet för samhällsviktig verksamhet behöver säkerställas i de kommersiella näten. Om prioritet inte regleras i författning innebär det en tillkommande eller ökad kostnad.

Investeringskostnaden för detta lösningsförslag bedöms vara 3 073 mnkr.

Driftskostnaderna bedöms vara 3 438 mnkr under en 10-årsperiod.

Tidplan
Tidplanen för att realisera denna lösning påverkas av hur lösningen utformas och avgränsas, av upphandling och därefter av kompletterande åtgärder för att uppfylla kraven, som t.ex. nätutbyggnad, strömförsörjning och bygglov. Lösningen beräknas kunna tas i drift med grundläggande funktionalitet efter 12 månader, ytterligare 12 månader behövs för att samtliga krav ska kunna vara uppfyllda.

	Kostnad
Geografiskt redundant kärnnät	Ej tillämplig
Utökad täckning	592 mnkr
Reservkraft	1 760 mnkr
Radionät inklusive installation	Ej tillämplig
Transmission	Ej tillämplig
Robusthöjande åtgärder i transmissionsnät	721 mnkr
Övervakningssystem	Ej tillämplig
Etablering och projektering	Ej tillämplig
Summa investeringskostnad	**3 073 mnkr**
Driftskostnad	Ej tillämplig
Abonnemangskostnader	3 438 mnkr
Nationell roaming	Okänd
SLA/särskild funktionalitet	Okänd
Summa driftskostnader	**3 438 mnkr**

Kommersiell lösning med dedikerat kärnnät

Beskrivning
Denna lösning bygger på ett separat offentligägt dedikerat och redundant kärnnät med geografisk spridning och tillträdesbegränsade lokaler. En eller flera mobiloperatörers kommersiella LTE-radionät och transmissionsnät används som bärare av trafiken. Denna lösning innebär att kärnnätet är offentligt ägt och radionätet ägs av en eller flera kommersiella operatörer.

Kraven på kommunikationstjänster för samhällsviktig verksamhet uppfylls genom kontinuerlig uppgradering och aktivering av tjänsterna i kommande 3GPP/LTE-standarder. De nödvändiga prioritetsfunktionerna kommer att finnas i LTE-standarden och kan aktiveras i nätet eller näten. Befintlig transmission behöver kompletteras och förstärkas med ytterligare förbindelser där så krävs och är möjligt.

Den abonnemangskostnad som redovisas bygger på genomsnittet av de fyra största mobiloperatörernas företagsabonnemang för mobilt data, som inkluderar 50 GB data per månad och bindningstid 0 - 3 månader. Om en högre datakapacitet krävs innebär detta högre kostnader.

Kommentarer till krav som samhällsviktig verksamhet ställer
Lösningen kräver ett dedikerat kärnnät under offentligt ägande och kontroll.

Nätet eller näten behöver kompletteras med nya basstationer för att uppnå täckningskravet.

Nätet eller näten behöver utrustas med reservkraft för att uppnå kraven på tillgänglighet.

Investeringskostnaden för detta lösningsförslag bedöms vara 3 189 mnkr.

Driftskostnaderna bedöms vara 4 163 mnkr under en 10-årsperiod varav 725 mnkr avser kärnnätet.

Tidplan
Lösningen beräknas kunna tas i drift med grundläggande funktionalitet efter 12 månader, ytterligare 12 månader behövs för att samtliga krav ska kunna vara uppfyllda.

	Kostnad
Geografiskt redundant kärnnät	116 mnkr
Utökad täckning	592 mnkr
Reservkraft	1 760 mnkr
Radionät inklusive installation	Ej tillämplig
Transmission	Ej tillämplig
Robusthöjande åtgärder i transmissionsnät	721 mnkr
Övervakningssystem	Ej tillämplig
Etablering och projektering	Ej tillämplig
Summa investeringskostnad	**3 189 mnkr**
Driftskostnad	725 mnkr
Abonnemangskostnader	3 438 mnkr
Nationell roaming	Okänd
SLA/särskild funktionalitet	Okänd
Summa driftskostnader	**4 163 mnkr**

Dedikerat radionät

Beskrivning
Denna lösning inkluderar ett dedikerat radionät, kärnnät och transmission inklusive nätövervakning under offentlig kontroll som täcker behov och krav som aktörerna inom allmän ordning, säkerhet, hälsa samt försvar ställer.

MSB bedömer att denna lösning kommer att bestå av 5 500 basstationer för att uppnå den yttäckning och kapacitet som krävs. Bedömning förutsätter användningen av 700 MHz-bandet. För att uppnå den tillgänglighet som krävs i nätet består denna lösning av ett geografiskt redundant kärnnät som sammankopplas via offentligt ägd fiber, dubbla transmissionsvägar till varje basstation samt batterier och dieselaggregat för basstationer. Dieselaggregat används för 80 procent av installationsplatserna.

Vid eventuell inplacering av utrustning hos kommersiella operatörer krävs avtal avseende säkerhets- och skalskyddsnivåer.

Kommentarer till krav som samhällsviktig verksamhet ställer
Kraven på kommunikationstjänster för samhällsviktig verksamhet uppfylls genom kontinuerlig uppgradering och aktivering av tjänsterna i kommande 3GPP/LTE-standarder.

Investeringskostnaden för denna lösning är 6 012 mnkr,

Driftskostnaden över 10 år är 5 310 mnkr.

Tidplanen
Tidplanen för att implementera ett dedikerat radionät uppskattas till mellan 3,5 och 4,5 år för fullt utbyggt nät, men delar av nätet kan tas i bruk redan efter 1 år.

	Kostnad
Geografiskt redundant kärnnät	116 mnkr
Utökad täckning	592 mnkr
Reservkraft	1 760 mnkr
Radionät, inklusive installation	1 650 mnkr
Transmission	1 469 mnkr
Robusthöjande åtgärder i transmissionsnät	Ingår
Övervakningssystem	45 mnkr
Etablering och projektering	380 mnkr
Summa investeringskostnad	**6 012 mnkr**
Driftskostnad	5 310 mnkr
Abonnemangskostnader	Ej tillämplig
Nationell roaming	Ej tillämplig
SLA/särskild funktionalitet	Ingår
Summa driftskostnader	**5 310 mnkr**

Hybridlösning

Beskrivning
En hybridlösning kan definieras på olika sätt och kan sträcka sig från en lösning med dedikerat kärnnät och kommersiellt radionät till en lösning med dedikerat kärn- och radionät som kan kompletteras med kommersiellt radionät för kapacitet- och eller yttäckning.

Kommentarer till krav som samhällsviktig verksamhet ställer
En fördelning av kostnaderna för en hybridlösning påverkas av hur lösningen definieras. Exempelvis är fördelningen av antalet basstationer mellan det offentliga och en eller flera operatörer en faktor som påverkar investeringskostnaden. Samma resonemang gäller för investeringar i reservkraft och transmission.

Investeringskostnaden för detta lösningsförslag bedöms vara mellan 3 189 mnkr och 6 012 mnkr.

Driftskostnaderna bedöms vara mellan 4 163 mnkr och 5 310 mnkr under en 10-årsperiod.

Tidplanen
Tidplanen för att implementera en hybridlösning är beroende av hur lösningen fördelas mellan det offentliga och de kommersiella operatörerna och

uppskattas till mellan 1 och 4,5 år för fullt utbyggt nät, men delar av nätet kan tas i drift tidigare.

	Kommersiell lösning med dedikerat kärnnät	Dedikerat radionät
Geografiskt redundant kärnnät	116 mnkr	116 mnkr
Utökad täckning	592 mnkr	592 mnkr
Reservkraft	1 760 mnkr	1 760 mnkr
Radionät, inklusive installation	Ej tillämplig	1 650 mnkr
Transmission	Ej tillämplig	1 469 mnkr
Robusthöjande åtgärder i transmissionsnät	721 mnkr	Ingår
Övervakningssystem	Ej tillämplig	45 mnkr
Etablering och projektering	Ej tillämplig	380 mnkr
Summa investeringskostnad	**3 189 mnkr**	**6 012 mnkr**
Driftskostnad	725 mnkr	5 310 mnkr
Abonnemangskostnader	3 438 mnkr	Ej tillämplig
Nationell roaming	Okänd	Ej tillämplig
SLA/särskild funktionalitet	Okänd	Ingår
Summa driftskostnader	**4 163 mnkr**	**5 310 mnkr**

Sammanställning av de fyra lösningsförslagen

	Tjänster i kommersiella radionät	Kommersiell lösning med dedikerat kärnnät	Dedikerat radionät	Hybridlösning
Investering	3 073 mnkr	3 189 mnkr	6 012 mnkr	3 189 – 6 012 mnkr
Drift	3 438 mnkr	4 163 mnkr	5 310 mnkr	4 163 – 5 310 mnkr
Tidplan	1–2 år	1-2 år	3,5–4,5 år	1–4,5 år

Figur 2. Sammanställning.

Ovanstående tabell är en summering av MSB:s bedömning av investerings- och driftskostnad för de fyra kommunikationslösningarna samt redovisning av möjlig tidplan för skarp drift.

	Tjänster i kommersiella radionät	Kommersiell lösning med dedikerat kärnnät	Dedikerat radionät	Hybridlösning
Investering	0,4 - 3,8	0,6 – 4	1,6 - 8,9	0,3 - 5
Drift	ca 1,8	0,3 - 0,8	0,3 - 6,9	0,3 - 1,5

Figur 3. Kostnadsspann i mdkr för inlämnade RFI-svar.

Ovanstående tabell illustrerar kostnadsspann på inlämnade RFI-svar. Beloppen för lösningarna är inte direkt jämförbara då kravuppfyllnaden varierar. Exempelvis med avseende på hur väl kravspecifikationen uppfylls. De lägre beloppen innehåller t ex inte kostnader för nödvändig reservkraft för att skapa robusthet.

REGERINGEN

Regeringsbeslut **II:28**

2015-12-17

Ju2015/00044/SSK
Ju2015/09907/SSK

Justitiedepartementet

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad

Uppdrag om säker och tillgänglig mobil, ip-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar

Regeringens beslut

Regeringen uppdrar åt Myndigheten för samhällsskydd och beredskap (MSB) att i samråd med Polismyndigheten och Försvarsmakten beskriva vilka behov aktörer inom allmän ordning, säkerhet, hälsa samt försvar har av mobil, ip-baserad kommunikation. Post- och telestyrelsen (PTS) ska bistå med relevant sakkunskap.

Av MSB:s redovisning ska framgå:

- vilka behov aktörerna har av säkra och tillgängliga mobila, ip-baserade kommunikationstjänster,
- vad som ska uppnås med kommunikationslösningarna,
- vilka krav som aktörerna ställer på kommunikationslösningarna, bland annat gällande informationssäkerhet, yttäckning, kapacitet och funktion, exempelvis utifrån olika scenarier, samt
- vilka krav som den internationella utvecklingen avseende operativ samverkan med aktörer från andra länder och internationella organisationer ställer.

Regeringen uppdrar åt PTS att redovisa tänkbara lösningar för kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar. PTS ska bland annat beakta den information som framkommer under arbetet enligt första stycket. PTS ska också inhämta synpunkter från utredningen *Försörjningen av statens behov av it/teletjänster med synnerliga säkerhetskrav (Fö2014:A)*. Även synpunkter från övriga relevanta intressenter ska inhämtas. MSB ska bistå med relevant sakkunskap. PTS ska inte lämna förslag som innebär en inskränkning av utrymmet för marknäten för radio och tv.

Postadress 103 33 Stockholm
Besöksadress Rosenbad 4
Telefonväxel 08-405 10 00
Telefax 08-20 27 34
E-post: ju.registrator@regeringskansliet.se

Av PTS redovisning ska framgå:

- vilka dedikerade frekvensband med beaktande av nuvarande frekvensanvändning och placering i frekvensband, som skulle kunna utnyttjas av aktörer inom allmän ordning, säkerhet, hälsa samt försvar för säkra och tillgängliga mobila, ip-baserade kommunikationslösningar,
- vilka alternativ som finns till sådana dedikerade frekvensband,
- vilka tidplaner som skulle gälla för de olika alternativen,
- hur Försvarsmaktens behov av frekvensutrymme kan tillgodoses,
- vilka fördelar och nackdelar som finns med de olika alternativen samt vilka åtgärder som skulle kunna vidtas för att begränsa eventuella nackdelar,
- vilka konsekvenserna blir för andra samhällssektorer om de olika frekvensbanden reserveras för ovanstående ändamål, samt
- vilka faktorer som är viktiga i ett internationellt sammanhang.

Regeringen uppdrar även åt MSB att i samråd med PTS, Polismyndigheten och Försvarsmakten göra en bedömning av drifts- och investeringskostnaderna samt redovisa en möjlig tidplan för skarp drift av de olika alternativen.

Uppdragen ska redovisas till Regeringskansliet senast den 18 mars 2016.

Skälen för regeringens beslut

Bättre mobiltäckning och bredbandstillgång är en viktig prioritering för regeringen. Dessutom har användningen och behovet av mobila bredbandstjänster inom flera sektorer ökat kraftigt under de senaste åren. Detta medför att efterfrågan på frekvensutrymme ständigt ökar.

Behovet av utvecklade kommunikationstjänster för aktörer inom allmän ordning, säkerhet, hälsa samt försvar är stort och ökande. För att myndigheterna ska kunna fullgöra sina uppdrag är säkra system för såväl talkommunikation som mobila bredbandslösningar avgörande. Nuvarande datakapacitet i det gemensamma radiokommunikationssystemet för skydd och säkerhet (Rakel- systemet) räcker inte till för att tillgodose användarnas krav på datakommunikation.

PTS förvaltar radiospektrumet och tilldelar tillstånd att använda olika delar av frekvensutrymmet enlig lagen (2003:389) om elektronisk kommunikation. Den myndighet som vill använda ett visst frekvensutrymme ansöker om att få göra detta hos PTS, med undantag för Polismyndigheten, Säkerhetspolisen, Försvarsmakten m.fl. som PTS tilldelar spektrum i dialog med myndigheterna.

Eftersom PTS har i uppdrag att förvalta radiospektrumet är de bäst lämpade att bedöma vilka frekvensutrymmen som kan användas för aktörer inom allmän ordning, säkerhet, hälsa samt försvar. För att PTS ska kunna bedöma detta behövs en tydlig beskrivning av de behov aktörerna har. MSB, som bl.a. har i uppdrag att förvalta och utveckla Rakel-systemet, är bäst lämpade att i samråd med Polismyndigheten och Försvarsmakten beskriva detta behov, bland annat genom att ange vilka typer av kommunikationstjänster som det finns behov av hos avnämarna i form av funktioner. Av beskrivningen bör även framgå hur verksamhetskritiska dessa behov är. MSB ska därför förtydliga behoven och bedöma de investerings- och driftskostnader som de olika alternativen skulle innebära. PTS ska redovisa tänkbara lösningar för kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar.

På regeringens vägnar

Anders Ygeman

Tor-Björn Åstrand

Likalydande till

Post- och telestyrelsen

Kopia till

Statsrådsberedningen/SAM
Justitiedepartementet/PO
Försvarsdepartementet/ MFI och SUND
Finansdepartementet/BA och KSÄ
Näringsdepartementet/ITP och SB
Kulturdepartementet/MF
Myndigheten för radio och tv
Försvarsmakten
Försvarets materielverk
Försvarets radioanstalt
Polismyndigheten
Säkerhetspolisen