FMV

Datum	Diarienummer	Ärendetyp
2017-05-15	17FMV3307-2:1	1.5

Regeringskansliet
Justitiedepartementet
103 33 Stockholm

Er referens	Ert datum	Er beteckning
Maria Pereswetoff-Morath	2017-03-15	Ju2017/02347/SSK

Kommunikation för vår gemensamma säkerhet (Ds.2017:7)

Försvarets materielverk har tagit del av departementsskrivelsen *Kommunikation för vår gemensamma säkerhet (2017:7)* och har följande synpunkter att meddela i detta remissvar.

Sammanfattande synpunkter

FMV anser att utredningsförslagets inriktning kan och bör ifrågasättas. Fördelarna med den valda lösningen med ett statligt kärnnät är att staten har betydande kontroll, den bygger på etablerad kommersiell teknik samt att beroendet av kommersiella aktörer är minimerat. Nackdelarna är att föreslagen lösning tar relativt lång tid att etablera, kan bli dyr och innebär en uppenbar risk för eftersläpning gentemot tekniken på det kommersiella området.

FMV:s uppfattning är att utredningen inte presenterar några bevis eller tunga argument för att den valda lösningen skulle ge ett totalt sett robustare eller (för de primära användargrupperna) mer användbart nät än om samma pengar satsades på att förstärka publika mobilnät genom avtal eller subventioner etc. FMV menar därför att de fördelar som avses uppnås med ett kärnnät i statlig ägo behöver utredas ytterligare innan regeringen tar ställning i frågan.

Övergripande kommentarer

FMV anser att det bör göras mer djupgående prövningar av säkerhetsaspekterna i såväl ett statligt nät som i en kommersiell lösning. Bland annat bör det utredas hur bra skyddet kan bli om berörda användare i stället blir några i mängden i ett nät som betjänar alla, även allmänheten. Att på så sätt försöka ”försvinna i mängden” ger visserligen inte fullgott skydd mot sådan kvalificerad signalspaning som främmande makt kan förväntas utöva mot Försvarsmakten i krig, men om ett nytt nät utformas för icke-militära ändamål torde hotet vara lägre och ett sådant skydd tillräckligt.

Valet av lösning motiveras på sid 173 bl.a. med att offentliga och kommersiella strukturer och resurser kan nyttjas och balanseras så att funktionskrav, kontroll, säkerhet och ekonomi optimeras. Det framgår dock inte hur balanseringen har gått till för att förstå vilken betydelse funktionskraven och de andra aspekterna haft för valet av lösning och hur andra lösningar stått sig i konkurrensen. FMV anser att avvägningen mellan de olika alternativen borde ha redovisats mer i detalj. Någon underbyggd

FMV
Försvarets materielverk
115 88 Stockholm
Besöksadress: Banérgatan 62
Tel: 08-782 40 00
Fax: 08-667 57 99
registrator@fmv.se
www.fmv.se
Org.nr: 202100-0340
VAT nr: SE202100-0340-01

bedömning av för- och nackdelar med att helt eller delvis nyttja kommersiella nät låter sig inte göras utan en klar bild av vilken funktionalitet som kan erhållas där, och till vilket pris.

FMV bedömer vidare att principen att det statliga nätet ska skyddas och skydda användarna kan ifrågasättas. En god princip har länge tillämpats i militära nät; att nätet har ett grundskydd, ett ”självskydd”, men det ankommer på användarna att skydda sig och sin information. I den kommunikationsmiljö som kan förväntas om några år, som vi redan sett växa fram, är det ofta inte nåbarhet som är den kritiska faktorn. Internetkommunikation tar sig många former (WiFi, satellit, etc) och är därför i sig mycket robust. Men användarna måste ta stort ansvar för att skydda sig och sin information – något som redan sker i försvarets kryptotelefon[1] samt i helt kommersiella och världsspridda system som t.ex. Skype och WhatsApp.

I en lösning som bygger på kommersiella resurser bör en prioriteringsmekanism prövas, som i stället för en stel och ovillkorlig prioritering av i förväg utpekade användare som det föreslagna samhällsnätet innebär, utnyttjar mer dynamiska mekanismer som ger anpassning till rådande läge. Mekanismerna bör utformas för att i det längsta medge användning av bandbreddssnåla tjänster som t.ex. chat och SMS.

FMV kan också notera att utredningen talar om att nätet först på sikt ska bära även tal, genom en senare infasning av talbaserad kommunikation från Rakel. Många användare skulle alltså, får man anta, behöva dubbla terminaler innan denna infasning har skett. I kommersiella nät är det en självklarhet att en och samma terminal kan användas för alla funktioner. Tal ”på datanätet” (VoLTE) införs under 2017 av nätoperatörerna i Sverige och det kan ses som ett exempel på en av FMV befarad eftersläpning gentemot civil teknik om samhällsnätets aktörer skulle tvingas till dubbla terminaler under längre tid.

FMV anser vidare att

- det är oklart hur omfattande utbyggnad av statsägda basstationer som krävs utifrån lämplighet och nödvändighet för att uppnå en tillräcklig täckning och kapacitet,
- delar av de ekonomiska beräkningarna är diskutabla,
- behovet av permanent reservkraft är underskattat i kapitel 5,
- en djupare analys av den prioritering som erfordras i den föreslagna kommunikationslösningen saknas,
- det är otydligt hur roaming med kommersiella nät ska fungera, vilka användargrupper som berörs och vilken inbördes prioritet de ska ha,
- frågor kring cybersäkerhet generellt är otillräckligt beskrivna. Det som främst saknas är en bedömning av de hot som bedöms uppstå, och hur dessa kan motverkas,
- följande risker behöver behandlas (exempel):
  - Samtrafik med publika nät
  - Gränsyta mot Internet
  - Internationella gränsytor
  - En bred användargrupp, tydligen inkluderande allmänheten då Missing people nämns i rapporten. Det finns en målkonflikt mellan säkerhet och många betalande användare. Detta bör utredas vidare.

[1] Signalskyddssystem MGFI

Synpunkter i specifika avsnitt

Kapitel 4

Avsnitt 4.3 sid 72

Det är begripligt att funktioner som trygghetslarm och övervakningssystem skulle kunna nyttja systemet. Det är däremot oklart vad som ligger bakom tanken att det även ska ges möjlighet att larma 112. Vilken typ av användare avses där? Om det t.ex. är allmänheten som avses behöver det tydliggöras hur det är tänkt att fungera.

Avsnitt 4.3.3 sid 76-77

Strävan att en terminal (Smartphone eller motsvarande) i systemet ska kunna tillgodose användarens hela kommunikationsbehov är naturlig. Det behövs en riskanalys för att utröna vad det medför för risker om användaren exempelvis ska kunna surfa på Internet, vilket säkert är ett angeläget behov.

Kapitel 5

Avsnitt 5.2 sid 82-83

Det är oklart vad ambitionen att kunna involvera bl.a. allmänheten innebär i praktiken för den föreslagna kommunikationslösningen. Uppenbart är att det ur säkerhetssynpunkt kan innebära en väsentligt ökad exponering för t.ex. intrångsrisker.

Avsnitt 5.2.1 sid 83-84

Försvarsmaktens användning av nätet förutses avse samverkan med civila myndigheter medelst tal. Det innebär att det är först när talfunktionalitet tillförts som Försvarsmakten har nämnvärd nytta av nätet. Innan dess måste detta slags samverkan ske via Rakel. Flera skäl talar för att talfunktionalitet bör tillföras så tidigt som möjligt för att därmed kunna avveckla Rakel. Skälen för detta är:

- att talkommunikation ska överföras i nät med större tålighet än Rakel, vilket det nya nätet förutsätts ha,
- att perioden då många användare tvingas ha dubbla terminaler ska vara så kort som möjligt,
- att perioden med driftkostnader för två nät minimeras,
- att de frekvenser som Rakel använder ska frigöras.

Avsnitt 5.2.2 sid 88 ff

Avsnittet saknar diskussion om applikationernas betydelse för tillgängligheten. De applikationer som använder nätet kan beroende på sin utformning vara mer eller mindre kapacitetskrävande. I ett nät för verksamhetskritisk information är det angeläget att användarna kan få maximal nytta av den för tillfället tillgängliga kapaciteten. Det innebär att deras applikationer bör kunna minska sitt bandbreddsbehov när tillgången minskar, hellre än att upphöra att fungera. En möjlighet är att applikationer ska godkännas innan användning i samhällsnätet tillåts.

Avsnitt 5.2.4 sid 90, andra stycket

Vid t.ex. kris eller krig måste man förutsätta att långvariga och geografiskt utbredda elavbrott är sannolika. I sådana lägen kan reservkraft inte i någon nämnvärd omfattning ersättas av ”en dedikerad förvaltnings- och driftorganisation”, eller mobila enheter. Rapportens värdering i detta avseende synes felaktig. Erfarenheten från konsekvenserna av stormen Gudrun visar tydligt att även ”en dedikerad förvaltnings- och driftorganisation” som exempelvis Telias stod sig tämligen slätt vid ett utbrett och långvarigt elbortfall.

Avsnitt 5.2.5 sid 91-92

Det är otydligt vilka tjänster nätet avses erbjuda i säkerhetsavseende. Det kan tas för givet att lösningen innefattar skydd av information om nätet självt och dess abonnenter, samt av övrig skyddsvärd

information som erfordras för att tillhandahålla kommunikationslösningen. Det förefaller som lösningen därutöver ska medföra någon form av grundläggande skydd för användarnas information. Ambitionsnivån avgör hur kostnadsdrivande det blir, och vilken grad av integration som erfordras mellan användarnas informationssystem och kommunikationslösningen. Oklarheterna synes oroväckande stora vilket påtagligt påverkar bedömningen av förslaget.

Kapitel 8

Avsnitt 8.1.4

Det är oklart vilka användarkategorier (samhällsaktörer) i den föreslagna kommunikationslösningen som ska ha prioritet om/när de genom roaming styrs över till ett kommersiellt nät.

Cyber

Samtrafiken med kommersiella nät, genom nationell roaming eller på andra sätt, ger en gränsyta mot omvärlden som kan komma att attackeras av en antagonist. Särskilda åtgärder kommer att behövas för att skydda den föreslagna kommunikationslösningen mot sådana attacker. Det är väsentligt att utredningens förslag kompletteras i detta avseende.

Avsnitt 8.1.1 sid 177

Det finns viss målkonflikt i en eventuell vidgning av användarkretsen. Det ger en bredare ekonomisk bas, men medför samtidigt en utspädning av vad som är väsentliga samhällsaktörer vilket gör det än mer angeläget att ha en inbördes prioritering.

Avsnitt 8.1.2. sid 177-178

Kan kärnnätet anonymisera en abonnent när dess trafik kopplas över till kommersiella nät, dvs. göra det väsentligt svårare för utomstående att analysera den känsliga trafik det kan vara fråga om? Även om det inte går att dölja trafikens ursprung i samhällsnätet kan det vara värdefullt att anonymisera det enskilda abonnemangets innehavare.

Avsnitt 8.1.6. sid 181-182

FMV bedömer att det är väsentligt att, som utredningen anger, frekvenser nu använda för Rakel harmoniseras med euro0peisk planering och därmed görs tillgängliga för militär användning.

Avsnitt 8.3 sid 186-187

Den tidplan som anges i tabell 8.1 synes optimistisk. Om de prioriterade områdena är storstäder, huvudvägar mm. är det svårt att tro att det ska finnas en fungerande lösning där redan efter två år.

Kapitel 9

Abonnemangskostnad, sid 203

Den nu antagna abonnemangskostnaden, 500 kr/mån, kan vara rimlig även vid användning av en kommersiell operatörs nät, om betydande belopp avsätts för nätförstärkande åtgärder etc. Annars kan noteras att de svenska operatörerna varje kvartal anger snittintäkterna per abonnent (ARPU) till bara ungefär hälften av det beloppet. FMV har också vid upphandlingar funnit att marknadspriset ligger under hälften av det antagna beloppet.

Tabell 9.3 sid 205

I tabellen anges intäkterna för inplacering till 100 MSEK/år från år 6. Grunden för beräkningen framgår inte. Om man antar att det är de statligt ägda glesbygdssiterna som är aktuella och att samtliga 800[2] stycken har kommersiella inplaceringar så ger det 125 kSEK/glesbygdssite. Även om man gör

[2] Avsnitt 8.1.5

antagandet att det är två kommersiella inplaceringar per site, vilket ger en intäkt per site och inplacering på ca 62 kSEK, så verkar det högt räknat.

I den slutliga handläggningen har Claes Westergren stf chef SPL S&D, Lars Burström teknisk chef SPL Led DL, Mats Lindhé projektingenjör AL Led Nät och Christian Ramstedt verksamhetsutvecklare Ledstab deltagit. Den sistnämnde har tillika varit föredragande.

FÖRSVARETS MATERIELVERK

Johan Weidenberg
Tf chef Ledningsstaben

Christian Ramstedt
Ledningsstaben

Sändlista
Regeringskansliet, Justitiedepartementet
FMV arkiv