



### Sändlista

Ert tjänsteställe, handläggare  
FinansdepartementetErt datum  
2017-03-22Er beteckning  
Fi2017/01289/DFVårt tjänsteställe, handläggare  
LEDS CIO, Helena Holmqvist, 08-788 84 31,  
Helena.holmqvist@mil.se

Vårt föregående datum

Vår föregående beteckning

### Försvarsmaktens yttrande över delbetänkande Digitalförvaltning.nu (SOU 2017:23)

## Sammanfattning

Försvarsmakten bejaktar i huvudsak delbetänkandets förslag men poängterar vikten av att förslagen bör kunna tillämpas olika för olika myndigheter. Försvarsmakten vill lyfta fram att myndighetens strävan är att, i kontakten med den offentliga förvaltningen, företag och enskilda, erbjuda digital kommunikation.

Försvarsmakten anser att myndigheten ska undantas från tvingande krav på digitalisering. Anledningen till detta är att Försvarsmaktens operativa uppgifter kräver att myndigheten har full rådighet och handlingsfrihet i val av hur uppgifter och information hanteras samt hur tekniska system och infrastrukturer utformas för att kunna verka i hela konfliktskalan fred, kris och krig. Försvarsmakten menar att myndigheten fortsatt ska ha rätt att meddela föreskrifter och utöva tillsyn inom eget verksamhetsområde vad avser skydd av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet.

För att minimera risken att skapa nya sårbarheter för hot utifrån avråder Försvarsmakten från att samla och hantera (lagra, bearbeta och överföra) all information och alla digitala tjänster i den offentliga förvaltningen<sup>1</sup> i en gemensam fysisk infrastruktur (molntjänst). Vidare avråder Försvarsmakten från att hantera de uppgifter och den information som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet i en gemensam fysisk infrastruktur (molntjänst).

<sup>1</sup> Framförallt avses de delar som berör totalförsvaret

(HHO)

Postadress  
Försvarsmakten  
107 85 Stockholm

Besöksadress  
Lidingövägen 24

Telefon  
08-788 75 00

Telefax  
08-788 77 78

E-post, Internet  
exp-hkv@mil.se  
www.forsvarsmakten.se



Försvarsmakten vill trycka på att den infrastruktur som tar hand om de civila och de militära delarna av totalförsvaret ska hållas åtskilda och att kommunikationen dem emellan bör ske med fåtalet användare.

## **Försvarsmaktens samlade syn på delbetänkandet och utredningens förslag**

Försvarsmakten har i sitt yttrande valt att samla myndighetens syn på delbetänkandet under ett fåtal rubriker. Detta angreppssätt har valts för att på ett tydligt sätt klargöra myndighetens ståndpunkt och för att undvika att upprepa liktydigt innehåll under flera olika förslagsrubriker.

### **Nationell digital infrastruktur är inte lämpligt för alla myndigheter**

I delbetänkandet framgår att utredarna och konsultföretaget Ramböll, som har haft Regeringskansliets uppdrag att bland annat ta fram en definition och en kartbild för den nationella digitala infrastrukturen, har olika syn på vad en nationell digital infrastruktur innebär. Försvarsmakten menar att det är nödvändigt för regeringen att ta fram en definition på en nationell digital infrastruktur som den offentliga förvaltningen har att förhålla sig till.

Försvarsmakten instämmer i att elektronisk kommunikation ska vara effektiv, säker och robust men hävdar att detta inte med säkerhet kan uppnås med en enda nationell digital infrastruktur. Att samla alla statliga myndigheter i en infrastruktur ökar risken för att obehöriga får åtkomst till information och skulle även riskera att skapa nya sårbarheter för hot utifrån då allt för mycket känslig information samlas på en plats.

Försvarsmakten menar att myndigheten ska undantas från krav på att ansluta till en nationell digital infrastruktur. Cyberrymden utvecklas i snabb takt och innebär strategiskt ett globalt gränslöst utrymme för att på distans genomföra attacker. I syfte att stärka skyddet av Sverige i cyberrymden har Försvarsmakten förmåga inom alla delar av dator och nätverksoperationer, CNO<sup>2</sup>. För att klara av detta måste Försvarsmakten kunna styra och utveckla digital infrastruktur inom egen myndighet. Den verksamhet som bedrivs inom myndigheten ställer särskilda krav på informationssäkerhet såsom sekretess och tillgång på information under de svåraste förhållanden.

Ytterst syftar säkerhets- och skyddskraven till att säkra tillgången till information och system vid krig men även vid fred och kris. Samtidigt som myndigheten ska säkra tillgången på information ska informationen och systemen hållas skyddad från motståndaren. Det är då av största vikt att grunden är lagd redan i fredstid eftersom det är då som aktörer genomför sina krigsförberedelser mot Sverige. Dessa förberedelser kan vara cyberattacker som genomförs för att störa och manipulera elektronisk kommunikation eller inhämtande av information som menligt kan påverka Försvarsmaktens operativa förmåga och riskera men för rikets säkerhet.

<sup>2</sup> Computer network operation



Försvarsmakten anser att det finns ett värde i att separera infrastrukturen för militär respektive det civila försvaret. Genom denna separation ges totalförsvaret ökad redundans, robusthet och minskad sårbarhet. En aktör som angriper delar i infrastrukturen eller en teknisk felfunktion kan därmed inte slå ut hela eller delar av både det militära som det civila försvarets infrastruktur samtidigt. Med separata nät kan dessutom det militära försvaret bibehålla full handlingsfrihet att lösa sina operativa uppgifter. Detta gäller exempelvis möjligheten att prioritera olika typer av kritisk trafik i näten.

### **Samlat ansvar för digitalisering behöver ta hänsyn till militära försvarets behov**

Försvarsmakten menar att regeringen bör precisera vad det samlade ansvaret ska innefatta, vilken roll myndigheten ska ha samt vilka uppgifter och vilket ansvar som ska åläggas myndigheten. Försvarsmakten förutsätter att myndigheten även fortsatt kommer att ha rätt att meddela föreskrifter och utöva tillsyn inom sitt verksamhetsområde vad avser skydd av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet.

Försvarsmakten vill trycka på att digitaliseringen och den digitala förvaltningen måste ta hänsyn till de särskilda behov och påfrestningar som kris och krig medför. Försvarsmakten ser även vikten av att belysa behovet av kontinuitetsplanering för att kunna upprätthålla kommunikation och tillgång till kritisk information även under svåra påfrestningar.

Det militära försvaret ska vara dimensionerat för att kunna verka i lägen när samhället är under svår påfrestning och behöver därför ha särskild handlingsfrihet inom digitaliseringsområdet. Detta för att bibehålla och utveckla sin operativa förmåga mot den mest kvalificerade motståndaren.

Försvarsmakten bejakar förslaget om att det inom den myndighet som får det samlade ansvaret ska finnas ett råd för samverkan. I detta råd bör Försvarsmakten ingå i syfte att påverka utvecklingen av digitaliseringen så att utvecklingen även stödjer Försvarsmaktens verksamhet och behov. Detta gäller verksamhet under fred så väl som under svår påfrestning, höjd beredskap och krig.

### **Behov av undantag från samlad styrning av digitaliseringen**

Försvarsmakten föreslår att myndigheten tillsammans med andra myndigheter med liknande krav som Försvarsmakten undantas från styrning av den digitala infrastrukturen och från styrning av digitala tjänster. En nationell infrastruktur riskerar att skapa nya sårbarheter för hot utifrån då allt för många myndigheters information är samlade på ett ställe. Stor del av den information som Försvarsmakten hanterar kräver hög säkerhet och högt skydd. Att låta all denna information överföras i en gemensam nationell infrastruktur kan skapa risker.

Utredningen slår fast att det i uppdraget för den myndighet som kommer att få samlat ansvar för digitaliseringen, ska ingå att ha ett brett samarbete med Statens servicecenter som i sin tur bland annat ansvarar för en gemensam statlig molntjänst för myndigheters IT-drift.



Försvarsmakten vill poängtera att myndigheten inte är ansluten till Statens Servicecenter. I den utredning som föranledde att statliga myndigheter blev anslutna till Statens Servicecenter undantogs Försvarsmakten. Skälen till detta var då och är nu att Försvarsmakten hanterar information, som om den blir röjd, kan riskera men för rikets säkerhet vilket innebär att det är direkt olämpligt för myndigheten att ingå i ett publikt statligt moln.

Försvarsmakten förstår vikten av att myndigheten som tilldelas ansvaret att hålla samman statliga myndigheters digitalisering även ska följa upp arbetet. Försvarsmakten vill dock poängtera att det är av största vikt att myndigheten fortsatt själv kan ta ställning till och fatta beslut om vilken information relaterat till Försvarsmaktens digitalisering som kan och bör lämnas ut till den myndighet som får det samlade ansvaret.

Utredningens förslag om att en ny bestämmelse införs i *förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte* innebär att myndigheter ska erbjuda elektronisk kommunikation i kontakten med enskilda. Även om Försvarsmakten strävar mot att erbjuda digital kommunikation i kontakten med enskilda anser myndigheten att det ska vara möjligt att välja annan typ av kommunikation när så anses vara lämpligt och att myndigheten därför ska undantas från bestämmelsen. Försvarsmakten anser att den nya bestämmelsen ökar risken att obehöriga får tillgång till sekretess- och skyddsrelaterad information och att bestämmelsen ökar risken för skapande av nya sårbarheter.

### **Behov av undantag från nyttjande av Mina meddelanden**

Försvarsmaktens ståndpunkt är att det ska finnas valfrihet för myndigheterna att ansluta sig till Mina meddelanden. I betänkandet framgår att regeringen i budgetproposition för 2015 angav att statliga myndigheter ska ansluta *relevanta* meddelandeflöden till Mina meddelanden. Vidare har regeringen meddelat att de överväger att göra det obligatoriskt för *lämpliga* statliga myndigheter att ansluta sig som avsändare till Mina meddelanden<sup>3</sup>.

Om en myndighet väljer att ansluta sig ska det åligga den myndigheten att besluta vilka meddelanden som ska distribueras via Mina meddelanden. Utredningen föreslår att arbetsgivaren ska erbjuda sin personal lönebesked via Mina meddelanden. För Försvarsmakten vars anställda omfattas av så kallad försvarssekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen är det direkt olämpligt att nyttja Mina meddelanden för att distribuera lönebesked. Försvarssekretess omfattar inte bara Försvarsmaktens personal utan även andra myndigheters personal inom totalförsvaret, såsom till exempel Polisen, jfr. Kammarrätten i Göteborgs dom 2007-11-14 (mål nr. 5613-07). Försvarsmakten avråder från att hantera (lagra, bearbeta och överföra) information som omfattas av lagen och som rör rikets säkerhet, i en gemensam fysisk infrastruktur som exempelvis molntjänst.

Försvarsmakten noterar att Mina meddelanden inte medger förmedling av meddelanden i den högsta skyddsklassen (4) och inte heller sådana som omfattas av sekretess med hänsyn till rikets säkerhet vad avser så kallad hemlig information enligt 4 § säkerhetsskyddsförordningen

<sup>3</sup> Remiss av betänkande digitalförvaltning.nu (SOU 2017:23) s. 155



(1996:633). Försvarsmakten avråder från eventuell utveckling mot att hantera denna typ av information i Mina meddelanden eftersom möjligheterna att skydda informationen mot en kvalificerad aktör bedöms små med rimliga medel. För meddelanden i de övriga skyddsklasserna är det viktigt att se över krav på säkerhet för brevlådeoperatörerna så att de hela tiden är lämpliga med hänsyn till informationens skyddsvärde och den aktuella hotbilden. Försvarsmaktens personal tillsammans med andra myndigheters personal kan omfattas av så kallad försvarssekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen.

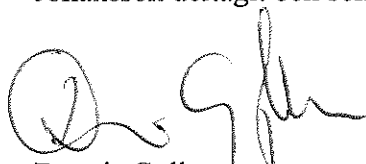
I 3 § förslag till förordning om infrastruktur för säkra elektroniska försändelser, framgår ett undantag för statliga myndigheter att teckna avtal som avsändare med Skatteverket och skicka elektroniska försändelser i infrastrukturen. Dock gäller undantaget endast efter beslut från regeringen. I författningskommentaren till 3§ nämns att undantaget kan gälla myndigheter som har väldigt lite kontakt med enskilda och företag så att en anslutning till infrastrukturen inte skulle ge någon vinst genom sänkta portokostnader, eller gälla myndigheter där det av säkerhetsskäl inte bedöms som lämpligt att skicka elektronisk post. Enligt Försvarsmaktens mening bör Försvarsmakten tillsammans med andra myndigheter inom försvarsområdet undantas från förslaget med hänsyn till att det av säkerhetsskäl är olämpligt att dessa myndigheter skickar elektronisk post. Ett sådant undantag bör framgå direkt av förordningstexten. Försvarsmakten hänvisar härvid till undantaget i 3 § förordningen om statliga myndigheters elektroniska informationsutbyte, som gäller Försvarsmakten tillsammans med andra myndigheter inom försvarsområdet.

Försvarsmakten anser även att motsvarande undantag av samma skäl bör formuleras i 2 § förslag till förordning om infrastruktur för säkra elektroniska försändelser.

-o0o-

I beredning av detta yttrande har deltagit försvarsjurist och personuppgiftsombud Anna Saarikoski, kommandörkapten Leif Östgaard, IT-arkitekt Åsa Ulwan, IT-säkerhetsstrategi Jan Wünsche.

Detta yttrande har beslutats av generallöjtnant Dennis Gyllensporre. I den slutliga handläggningen har dessutom generalmajor Fredrik Robertsson, kommandör Per-Ola Johansson deltagit och som föredragande analytiker Helena Holmqvist.



Dennis Gyllensporre  
Chef för Ledningsstaben



Helena Holmqvist



**Sändlista**

Finansdepartementet ([fi.registrator@regeringskansliet.se](mailto:fi.registrator@regeringskansliet.se), [fi.df.remissor@regeringskansliet](mailto:fi.df.remissor@regeringskansliet.se))

Som orientering

Försvarsdepartementet

Inom HKV

LEDS INRI

LEDS PLANEK

LEDS JUR

LEDS CIO

LEDS STAB ÖB/GD stöd

PROD

INS

MUST