Säkerhetspolisen

PM

Datum
2018-09-18

Diarienummer
2018-10207-5

Mottagare
Utredningen om radiospektrumanvändning i framtiden N 2017:7
Att: Huvudsekreterare Ylva Mälarstig

Er referens
N 2017:7.
Huvudsekreterare Ylva Mälarstig

Säkerhetspolisens svar på frågor ställda av utredningen om radiospektrumanvändning i framtiden (N 2017:7)

Säkerhetspolisen har från utredningen om radiospektrumanvändning i framtiden (N 2017:7) fått en framställan om önskemål att ta del av information och synpunkter på radiospektrumanvändning i framtiden. Utredningen har sammanställt ett antal frågor som Säkerhetspolisen ombetts besvara. Nedan redovisas frågorna och Säkerhetspolisens svar på dessa.

Vad vill Säkerhetspolisen framföra i relation till bifogat uppdrag?

Säkerhetspolisen ser ett framtida ökat behov av säkra trådlösa och mobila kommunikationslösningar. Delar av dessa behov kan fortsatt tillfredsställas genom kommersiella aktörer medan andra delar bör, med avseende på höga säkerhets- och tillgänglighetskrav, hanteras av ett statligt kontrollerat nät. Med andra ord så kommer det finnas behov av flera olika typer av lösningar för trådlös kommunikation. Staten måste ta höjd för olika typer av förändringar i säkerhetsläget och därför säkerställa kommunikations-lösningar som inte är beroende av eller kan påverkas och styras av utländska aktörer. Säkerhetspolisen vill också framföra behovet av att tillfälligt kunna nyttja radiofrekvenser, som kan vara tilldelade till annan aktör, för egen utrustning att användas i den operativa verksamheten. I dessa fall kan den operativa omständigheten göra att det inte finns tid för en frekvensdialog med Post och Telestyrelsen.

Teknikutvecklingen, som kan exemplifieras med 5G, innebär särskilda utmaningar i möjligheterna att möta interna och externa hot mot nationell säkerhet, terrorism och grov kriminalitet. Säkerhetspolisen vill därför starkt betona vikten av att även fortsättningsvis kunna verkställa hemliga

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se

tvångsmedel och lagring av historiska trafikuppgifter för att upprätthålla och säkerställa grundläggande trygghet för invånarna, samhället och landet. I det perspektivet är de utredningar rörande datalagring (SOU 2017:75) och hemlig dataavläsning (SOU 2017:89) också viktiga att beakta för utredningen kring framtida radiospektrumanvändning.

Teknikutvecklingstrenden innebär att kommunikationen ska ske så långt ut i nätet så nära användaren som möjligt (ref: EDGE Computing) i syfte att öka bandbredden och samtidigt minska fördröjningar i nätet. Säkerhetspolisen vill i det perspektivet framhålla behovet av kontroll, dvs. hur radiospektrumet används i realiteten. En teknik, som används av leverantörer av elektronisk kommunikation, är NFV (Network Function Virtualisation) vilken innebär att det som tidigare löstes i fysisk utrustning nu verkställs av programvara. Det innebär att nätverksfunktioner under pågående drift kan flyttas till annan utrustning på en ny geografiskt plats. NFV och SDN (Software Defined Networking) är tekniker som ger förutsättningar för att lösa nätverkstjänster i molnet (Cloud Computing). NFV och SDN är relativt nya tekniker där säkerhetsskyddsmekanismer inte är fullt utvecklade men sannolikt kommer att vara lösta 2027 – 2047. Däremot kvarstår frågor om var utrustningen som används är geografiskt lokaliserad, vilken lagstiftning som är tillämplig och vilken tillgänglighet som kan säkerställas om utrustningen finns i en annan jurisdiktion.

Säkerhetspolisen ser att trådlös kommunikation och andra radiospektrum-baseradetjänster är relativt lätta att störa ut. Det finns kommersiellt tillgänglig störutrustning, vilken är lätt att införskaffa på Internet, som kan innebära att kriminella stör ut exempelvis polisens radiokommunikation för att underlätta sin egen brottsliga verksamhet. Denna typ av störningar kan leda till allvarlig fara för liv och hälsa. Säkerhetspolisen vill därför framhålla att straffsanktioner mot användning eller införskaffande av illegal radiostör-utrustning måste skärpas.

Säkerhetspolisen har tagit fram ett utkast till styrande principer (se bilaga 1) som kan utgöra en vägledning för hur staten ska kunna säkerställa att nya vitala elektroniska kommunikationsnät, som ofta nyttjar radiospektrum, kan möta krav på skydd av Sveriges säkerhet. Dessa principer ska ses som ett förslag till att också möta målen i den Nationella säkerhetsstrategin, dvs. värna befolkningens liv och hälsa, samhällets funktionalitet samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter. Förutsättningen för att nå dessa mål är att säkra Sveriges politiska oberoende samt att Sveriges territoriella integritet kan upprätthållas.

Säkerhetspolisen ser vidare att för tillstånd till radiofrekvenser eller radiospektrum ska besluten föregås av noggrann beredning där Försvarsmakten och Säkerhetspolisen bör ha ett avgörande inflytande. Säkerhetspolisen anser att det finns ett behov av att tillståndsgivaren också

ges möjlighet att återkalla ett frekvens- eller radiospektrumtillstånd då nationella säkerhetsintressen så kräver. Försvarsmakten och Säkerhetspolisen bör ha möjligheten att initiera sådana ärenden då särskilda skäl föreligger.

Hur ser framtida behov av trådlös kommunikation och andra radiospektrumbaseradetjänster ut inom Säkerhetspolisens område åren 2030-2047?

Säkerhetspolisen utgår ifrån att nuvarande kommunikationslösning Rakel är nedlagt redan före 2030 och då uppstår behovet av en ersättare med motsvarande funktioner samt en utökning med mobila bredbandstjänster i ett skyddat nät. Det framtida behovet av trådlös kommunikation förväntas öka generellt, även för ”Public Protection and Disaster Relief”-användare (PPDR) och då inte minst för Säkerhetspolisen. Bandbreddskrävande applikationer, exempelvis högupplöst realtidsvideo, är viktiga verktyg för Säkerhetspolisen.

Säkerhetspolisens behov av ”Internet of Things” (IoT) kommer sannolikt att öka främst i säkerhetsskyddsverksamhet men också i operativ verksamhet där olika sensorer kommer att bli avgörande för förmågan att förebygga, avslöja, utreda och åtala för brott som rör Sveriges säkerhet eller terrorism.

Vilken teknikutveckling eller utveckling av användarnas behov kan eventuellt förväntas ske inom sektorn som påverkar framtida behov av trådlös kommunikation och andra radiospektrumbaseradetjänster?

I likhet med utvecklingen för andra samhällsaktörer kommer behovet av trådlös kommunikation och andra radiospektrumbaseradetjänster att öka. Teknik för ansiktsigenkänning och andra biometriska identifikations-lösningar i realtid går framåt och förväntas bli viktiga redskap för Säkerhetspolisen. Även behovet av övervakning av geografiska platser i form av t.ex. kameraövervakning förväntas öka. I många fall ställer detta krav på realtidsöverföring av högupplösta bild- och ljudströmmar via radiospektrumbaseradetjänster. Ett annat exempel är kroppskameror som kan vara ett hjälpmedel för att stödja medarbetare eller att dokumentera händelseförlopp. Drönare som hjälpmedel för spaning och övervakning är andra tekniker vilka är av intresse för Säkerhetspolisen. Säkerhetspolisen ser också behovet av att använda olika typer av sensorer (IoT), som ofta är baserade på trådlös kommunikation, i den preventiva verksamheten men också i den brottsutredande verksamheten.

Vilka politiska mål och visioner är relevanta för utredningen att beakta?

Regeringens bredbandsstrategi att hela Sverige år 2023 bör ha tillgång till stabila mobila tjänster av god kvalitet överensstämmer med PPDR-användarnas behov av mobila kommunikationstjänster. Infrias bredbands-strategin så är PPDR-användarnas behov av täckning uppfyllda om 10-30 år. Det som behöver säkerställas är PPDR-användarnas tillgång till tjänsterna samt att informationssäkerheten ligger på en acceptabel nivå. Tillgången till tjänsterna kan säkerställas genom prioritetsfunktioner eller dedikerade frekvenser. Höga krav måste också ställas på kommunikations-lösningen när det gäller drift- och informationssäkerhet.

Klimatförändringarna kan förväntas ge mer extrema väderförhållanden, vilket kan påverka anläggningar och antenner. Yttre hot från olika typer av aktörer ökar. Säkerhetspolisen vill understryka att tillgänglighet till kommunikationslösningar och dess funktioner är mycket viktigt vid extrema påfrestningar på samhället, såsom terrorattacker. Vid dessa tillfällen har PPDR-aktörer en mycket viktig roll och ofta är trådlös kommunikation (både tal och data) en avgörande framgångsfaktor för att uppdragen ska kunna utföras. Vid dessa tillfällen är det av mycket stor vikt att PPDR-användarnas behov av radiospektrum kan mötas. Det är viktigt att betona att detta också gäller i vardagen, vid s.k. vardagshändelser, men då är sannolikt behovet av radiospektrum något lägre. Säkerhetspolisen ser därför att omfattningen av tillgängligt radiospektrum ska kunna variera över tid.

Säkerhetspolisen vill betona vikten av att i framtida elektroniska kommunikationslösningar kunna verkställa hemliga tvångsmedel och lagring av historiska trafikuppgifter för att upprätthålla samt säkerställa grundläggande trygghet för invånare, samhället och landet.

Säkerhetspolisen anser att kommunikation, där användande av radiospektrum, är en mycket viktig förutsättning för att tillgodose invånarnas trygghet, säkerhet och hälsa. I det perspektivet är det av vital betydelse att det finns mekanismer för att bedöma, kontrollera och om nödvändigt justera villkoren för marknadsaktörer som agerar i Sverige. En av utgångspunkterna, som också anges i den nationella säkerhetsstrategin, är att Sveriges territoriella integritet kan upprätthållas.

Den svenska strategin mot terror lyfter också upp värdet av att skapa och minska samhällets sårbarhet genom att skydda känslig information, samhällsviktiga anläggningar och kritisk infrastruktur. Säkerhetspolisen ser att kommunikationssystem, vilka använder radiospektrum, som tillhandahåller vitala förutsättningar för Sverige att fungera (ex. mobiltelefonnät som 4G och kommande 5G) är sådana anläggningar och således kritisk infrastruktur som är särskilt skyddsvärd.

Vilken övrig information, rapporter eller undersökningar kan vara relevanta för utredningen att beakta med tanke på uppdraget?

Säkerhetspolisen har tidigare yttrat sig i utredningar bland annat Ds 2017:7 gällande säker och tillgänglig, mobil, IP-baserad kommunikation för aktörer inom allmän ordning, säkerhet, hälsa samt försvar. Dessa yttranden är fortfarande relevanta.

Vidare ser Säkerhetspolisen att SOU 2017:75 Datalagring – brotts-bekämpning och integritet samt SOU 2017:89 Hemlig dataavläsning kan vara relevanta för att beskriva brottsbekämpande myndigheters behov. De särskilda yttranden och remissvar som Säkerhetspolisen lämnat till dessa utredningar kan ytterligare beskriva de behov och utmaningar som ny elektronisk kommunikation kan medföra i brottsbekämpningen.

Säkerhetspolisen kan konstatera att NFV idag inte har de säkerhetsmekanismer som kan säkerställa skyddet av uppgifter som är av betydelse för Sveriges säkerhet. För utredningen kan det arbete som utförs i ETSI, European Telecommunication Standardisation Institute, vara värdefullt att följa (Se ETSI GS NFV-SEC 14).

Detta yttrande har beslutats av biträdande säkerhetspolischef Charlotte von Essen. I handläggningen har biträdande chefsjuristen Annica Runsten deltagit, föredragande har varit seniora strategiska rådgivaren Kurt Alavaara.

Charlotte von Essen
Biträdande Säkerhetspolischef