Direktoratet for nødkommunikasjon

Forsvarsdepartementet
Postboks 8126 Dep.
0032 OSLO

Deres referanse:	Vår referanse:	Dato:
2015/3139-7/FD V 3/MAY	17/244-2	27.02.2017

HØRING - NOU 2016: 19 SAMHANDLING FOR SIKKERHET - HØRINGSUTTALELSE FRA DNK

Det vises til Forsvarsdepartementets høringsbrev 17. oktober 2016 med frist 20. januar 2017 til å komme med innspill. Direktoratet for nødkommunikasjon (DNK) var ikke gjort kjent med at dette dokumentet var på høring, og tillater oss å komme med noen merknader selv om fristen er utløpt.

1. Innledning

Generelt er DNK positiv til de anbefalinger til ny sikkerhetslov som nå foreligger, og at det er viktig å gjøre endringer i lovverket for å ta hensyn til teknologiske, demografiske og sikkerhetsmessige endringer.

DNK er eier av nasjonal kritisk telekominfrastruktur (Nødnett) og tilbyder av elektroniske kommunikasjonstjenester ihht. ekomloven[1] (Nødnett-tjenester). Det er viktig for DNK at ny sikkerhetslov tar høyde for gjeldende utfordringsbilde for ekombransjen. Vi viser i den forbindelse til høringsinnspill fra andre aktører innen elektronisk kommunikasjon (Samferdselsdepartementet, Nkom, Telenor og Telia) og støtter i stor grad deres synspunkter.

DNK registrerer at Nødnett er lite omtalt i høringsnotatet, og den informasjon som er tatt inn er lite oppdatert. Det vises bl.a. til utredningen side 128, der det fremgår: «*Nødnett er et avlyttingssikret sambandssystem som skal gi bedre funksjonalitet, talekvalitet, dekning og kapasitet enn dagens samband*» (DNKs understrekning). Til dette skal det bemerkes at Nødnett har vært nødetatens samband i flere år, og Nødnett var landsdekkende i 2015. Politi og brannvesen har hatt Nødnett som primærsamband siden 1. desember 2015. Det er i dag nær 800 nød- og beredskapsorganisasjoner som er kunder av Nødnett, og nettet er det viktigste daglige kommunikasjonsmiddelet for en stor del av aktørene i totalforsvaret. Vi finner det derfor nødvendig å inkludere noe informasjon om Nødnett og DNK som telekomaktør i denne høringsuttalelsen.

Nødnett må defineres som *infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner,* og DNK er også i dag underlagt sikkerhetsloven. DNK er således en sentral aktør innen samfunnssikkerhet og beredskap. For å knytte nød- og beredskapskommunikasjon tettere sammen

[1] Jf. brev fra Nkom til DNK 3.12.2015 (DNK ref. 12/270-25)

Kontoradresse:	Postadresse:	Telefon sentralbord:	Telefaks:	Saksbehandler
Nydalen allé 37a Oslo	Postboks 7 Nydalen PIB 0410 Oslo	23 00 57 00	22 23 29 41	Berit Isaksen

Organisasjonsnummer: 990 382 840 MVA

med andre samfunnssikkerhetsområder vil DNK fra 1. mars 2017 bli en del av Direktoratet for samfunnssikkerhet og beredskap (DSB)[2] som avdeling for nød- og beredskapskommunikasjon.

2. Om Nødnett

Nødnett er et digitalt samband for politi, brannvesen, helsetjenesten og andre viktige samfunnsfunksjoner. Kjernebrukerne av Nødnett er de tre nødetatene brann, politi og helse. Disse etatene bruker radiosambandet som en viktig innsatsfaktor i sitt daglige arbeid. Samtidig er flere andre aktører med et nød- og beredskapsansvar tilknyttet Nødnett. En bred utnyttelse av Nødnett har vært et hovedmål fra begynnelsen av. Stortinget har flere ganger påpekt at flere brukergrupper skal få anledning til å ta i bruk Nødnett, og har omtalt Nødnett som en «pilar i totalforsvaret». Ulike kriser krever ulike aktører, og målet er at alle med et nød- og beredskapsansvar skal være tilknyttet Nødnett i 2020.

Nødnett er et mobilt radiosamband basert på TETRA-standarden, og består av ca. 2100 basestasjoner som gir dekning i om lag 86 % av Norges landareal. Sentrale nettverksnoder, basestasjonsutstyr, radiolinjeutstyr og driftstøttesystemer i Nødnett er eid av staten v/DNK. Enkelte deler av Nødnett er definert som skjermingsverdige objekter iht. objektsikkerhetsforskriften. Den daglige driften av Nødnett er satt ut til Motorola som overvåker og drifter nettet fra et driftssenter i Norge. Motorola utfører feilretting på alle komponentene som er eid av staten, og følger opp feilretting hos underleverandører.

En sentral føring ved byggingen av Nødnett (St. prop. Nr. 1, tilleggsnummer 3 (2004-2005)) var å utnytte eksisterende infrastruktur. Det er derfor inngått avtaler om bruk av eksisterende master og telelinjer der hvor det har vært mulig. Ca. 93 % av de ca. 2100 basestasjonene er innplassert hos andre. Telelinjene som knytter basestasjonene sammen med sentrale nettkomponenter er tradisjonelle, leide linjer fra Broadnet og Telenor. DNK har valgt å bygge radiolinjer mellom basestasjoner der det er fri sikt eller mangel på telelinjer fra tilbyder. Om lag 60 % av telelinjene til basestasjonene i Nødnett er dermed eid av DNK (radiolinjer), mens de resterende 40 % leies fra Broadnet og Telenor. Alle de lange telelinjene som benyttes i Nødnett er leide linjer.

3. Konkrete kommentarer til lovforslaget

Infrastruktur og informasjonssystemer

DNK støtter forslaget om at objektsikkerhet skal utvides til å gjelde både objekter og infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner. DNK ser også positivt på at informasjonssystemer skal omfattes av sikkerhetsloven og også kunne bli ansett skjermingsverdig.

DNK/Nødnett er allerede underlagt sikkerhetsloven, men med lovgivning som foreslått vil større deler av Nødnetts infrastruktur og systemer bli omfattet av sikkerhetslovens krav.

Som de fleste høringsinstanser har påpekt, gjenstår det en rekke punkter som må avklares i forskrift eller på annen måte. Ikke minst gjelder dette hvilke typer og deler av infrastruktur, objekter og informasjonssystemer som skal omfattes av den nye loven og hva som skal være terskelen for at infrastruktur og objekter skal anses som skjermingsverdig. Det er videre viktig at fagdepartement sikrer tydelige og forståelige utvelgelseskriterier og at det så langt mulig samsvarer på tvers av sektorer. Det vises også til NSMs uttalelse *«(f)or at en slik lov skal få ønsket effekt krever det, som utvalget påpeker, supplerende virkemidler. NSM mener en*

[2] For mer info se: https://www.regjeringen.no/no/aktuelt/regjeringen-samler-mer-ansvar-for-samfunnssikkerhet-i-dsb/id2516159/

rekke tiltak bør iverksettes for å bidra til å gi loven ønsket effekt».

DNK imøteser videre arbeid med retningslinjer for hvordan slike systemer skal identifiseres og utpekes, samt hvilke krav som skal stilles til forsvarlig sikring av slike systemer. Det kan være hensiktsmessig at disse vurderingene gjøres av de enkelte sektormyndigheter, som kan legge føringer for hva som er forsvarlig sikkerhet. Imidlertid må dette også samordnes tverrsektorielt. DNK (fra 1.3.2017 DSBs avdeling for nød- og beredskapskommunikasjon) bistår gjerne i dette arbeidet.

Som nevnt over, er Nødnett avhengig av andre leverandørers infrastruktur, bl.a. strøm og transmisjon. For å fungere er Nødnett avhengig av strøm og flere tusen telelinjer mellom basestasjoner og sentrale nettverkskomponenter. Nettet har dublerte komponenter, redundante telelinjer og reservestrøm for å redusere risikoen for utfall i Nødnett ved enkeltfeil eller strømbrudd.

Som også Telenor uttaler, er det den enkelte infrastruktureier som må håndtere inntrufne hendelser, og Nødnett er sårbart dersom f.eks. cyberhendelser inntrer i andre sektorer. Nødnett er søkt gjort robust ved redundans i både telelinjer og strømtilførsel, men vil likevel bli påvirket dersom det er omfattende utfall hos andre leverandører. DNK støtter derfor Telenors anførsel om at kritiske private virksomheter må inngå som del av krise- og beredskapsorganiseringen i Norge.

Personkontroll
Ved utbygging og drift av Nødnett er DNK og leverandør av Nødnett (Motorola) avhengig av internasjonale leverandører. Tilstrekkelig og nødvendig ekspertise har vist seg vanskelig å skaffe i Norge. Arbeidet med sikkerhetsklareringer og autorisering har vært omfattende, og DNK støtter derfor forslagene til endring av adgangsklarering av personell som skal ha fysisk eller logisk tilgang til skjermingsverdige objekter eller infrastruktur. Samtidig ser vi behov for at det sikres god kontroll med hvem som har tilgang til, og informasjon om sentrale/skjermingsverdige deler av Nødnett. DNK er derfor enige med SD som påpeker at det må være adgang til å kreve streng personkontroll av personell som skal ha tilgang til infrastruktur og objekter som er høyt klassifisert.

DNK støtter videre SDs anførsel om at bestemmelsene om personellsikkerhet også må gjelde for tilgang til informasjon om systemer, objekters utforming, sårbarhet mv.:

> *«Fysisk og logisk tilgang til objekter vil ikke bare kunne utgjøre en fare for sabotasje o.l., men vil også kunne gi personell inngående informasjon om objektets utforming, sårbarheter, mv. Dette er informasjon, som om den er nedfelt i et dokument, normalt er sikkerhetsgradert. SD stiller i lys av dette spørsmål ved det skillet som utvalget synes å trekke mellom tilgang til informasjon på den ene siden, og fysisk og logisk tilgang til objekter på den andre. Etter SDs vurdering bør spørsmålet om det skal gjennomføres en sikkerhetsklarering eller en enklere adgangsklarering, være knyttet til skadepotensialet ved at personell får tilgang – uavhengig av om tilgangen gjelder informasjon eller objekter.»*

Eierskapskontroll
DNK ser at det kan være problematisk om utenlandske eiere tar over kritisk infrastruktur i Norge. DNK støtter derfor innføring av en bestemmelse som kan sikre nasjonal eierskapskontroll over strategisk viktige selskaper, som er av kritisk betydning for nasjonale funksjoner. DNK

reiser også spørsmål ved om bestemmelsen også bør utvides til å omfatte tjenesteutsetting av drift av slik infrastruktur/systemer.

Dagens Nødnett er basert på TETRA-standarden, som gir gode tjenester for tale (grupper og en-til-en). TETRA gir imidlertid lite muligheter for mobilt bredbånd, som vi ser at Nødnett-brukerne vil bli mer avhengige av fremover. Ingen andre sammenlignbare land i verden har hittil basert sin nød- og beredskapskommunikasjon på bruk av vanlige, kommersielle mobilnett. Det vil bli for kostbart om det skal bygges et eget, dedikert Nødnett basert på LTE. Det mest sannsynlige scenariet – dersom Nødnett skal tilby datatjenester – er å leie kapasitet i de kommersielle mobilnettene. For å sikre Nødnett-brukerne robuste, «alltid tilgjengelige» tjenester, fordrer dette at det må settes en rekke krav til de kommersielle mobilnettene med hensyn til bl.a.:

- Prioritet
- Funksjonalitet (multicast, lokal autonomi, nasjonal gjesting)
- Dekning (øde områder, air-ground-air)
- Forsterkning av nettene (reservestrøm, redundant transmisjon)
- Sikkerhet i alle ledd (aksesskontroll, fysisk sikring, sikkerhetsklarert personell, håndtering av informasjon, eierskap, utstyrsleverandører, nasjonal uavhengighet)

Økonomiske konsekvenser av lovforslaget/kostnader ved sikringstiltak
I utredningen fremheves det flere steder at det forebyggende sikkerhetsarbeidet skal være samfunnsøkonomisk lønnsomt. Som også Telenor påpeker i sin uttalelse, vil vurderingen av hva som er samfunnsøkonomisk lønnsomt kunne variere fra virksomhet til virksomhet. DNK er enige med Telenor i at myndighetene må ta ansvar for å sette standandern for et forsvarlig sikkerhetsnivå på tvers av samfunnskritiske funksjoner, samt hva som skal legges til grunn for å beregne hva som er samfunnsøkonomisk lønnsomt.

Økte sikkerhetskrav vil medføre økte kostnader ved gjennomføring av nødvendige tiltak. Utbygging av Nødnett-infrastrukturen har skjedd gjennom statlige bevilgninger, mens kostnadene til drift dekkes av brukerne gjennom en abonnementsordning. Brukerne av Nødnett er i stor grad offentlige virksomheter med en nød- og beredskapsrolle. DNK vil advare mot en situasjon hvor betydelige kostnader knyttet til økt sikkerhet skal dekkes av brukerne, da det vil gi risiko for at enkelte aktører nedprioriterer å bruke Nødnett av økonomiske årsaker. DNK vil i den sammenheng påpeke at det må etableres en finansieringsmodell som sikrer at både investeringskostnader og driftskostnader fullfinansieres uten økte kostnader for brukerne.

4. Nødnett og gradert kommunikasjon

Utvalget skriver i kapittel 7.4.3 Elektronisk kommunikasjon *«Nødnett er likevel ikke godkjent for å kommunisere sikkerhetsgradert informasjon»*. Vi ønsker å knytte noen kommentarer til dette.

I DNKs årsrapport for 2015 står følgende: *«DNK har i 2015, i samarbeid med Nasjonal sikkerhetsmyndighet (NSM), gjennomført en vurdering om bruk av Nødnett for formidling av BEGRENSET informasjon. Studien konkluderte med at det kan være hensiktsmessig å arbeide videre med mulige løsninger som kan oppfylle de krav som stilles til denne typen gradert kommunikasjon.»*

DNK vil påpeke at det er viktig å skille mellom Nødnett-infrastrukturen og Nødnett-terminalene (sambandsradioene) som benyttes til å kommunisere over infrastrukturen, på samme måte som man må skille mellom en mobiltelefon og selve mobilnettet. For å kunne kommunisere

sikkerhetsgradert informasjon over Nødnett, må det finnes en godkjent Nødnett-terminal med tilstrekkelig kryptering og sikkerhetsmessig godkjenning av både maskinvare og programvare. NSM og DNK konkluderte i den nevnte studien at det vil kunne være mulig, men det krever videre arbeid og utredninger. Det har imidlertid ikke vært mulig å prioritere en videreføring av dette arbeidet det siste året.

Med vennlig hilsen

Tor Helge Lyngstøl
Direktør

Berit Isaksen
Leder, juridisk seksjon

Kopi:
Justis- og beredskapsdepartementet
Direktoratet for samfunnssikkerhet og beredskap