

Robust kommunikasjonsinfrastruktur for samhandling i krise



▲ Bildet viser Telenors telesentral, som også ble flammens bytte i storbrannen i Lærdal natt til søndag 19. januar 2014. (Foto: Hove Media)

Kan nye digitale tjenester bidra til mer effektive brann- og redningsinnsatser i Norge, og hvor robuste er disse løsningene, gitt den eksisterende kommunikasjonsinfrastrukturen?

Med utgangspunkt i denne problemstillingen har FFI-prosjektet «Robust tjenesteinfrastruktur for ledelse og samhandling i krise» (RUTIL) studert hvilke informasjons- og kommunikasjonssystemer brannvesenet bruker i sin redningsinnsats, samt hvordan sårbarheter i den underliggende infrastrukturen kan få konsekvenser for redningsinnsatsen.

Brannvesenet, kommunikasjonsystemer og sårbarhet

I henhold til «Brann- og eksplosjonsvernloven» er det kommunene som skal sørge for etablering og drift av et brannvesen som kan ivareta forebyggende og beredskapsmessige oppgaver. Brannvesenet har derfor lokal tilhørighet, og er den viktigste tekniske førstelinjeinnsatsen i den norske redningstjenesten. Brannvesenet

samarbeider tett med de andre nødetatene og har også et utstrakt samarbeid med andre statlige, private og frivillige beredskapsressurser.

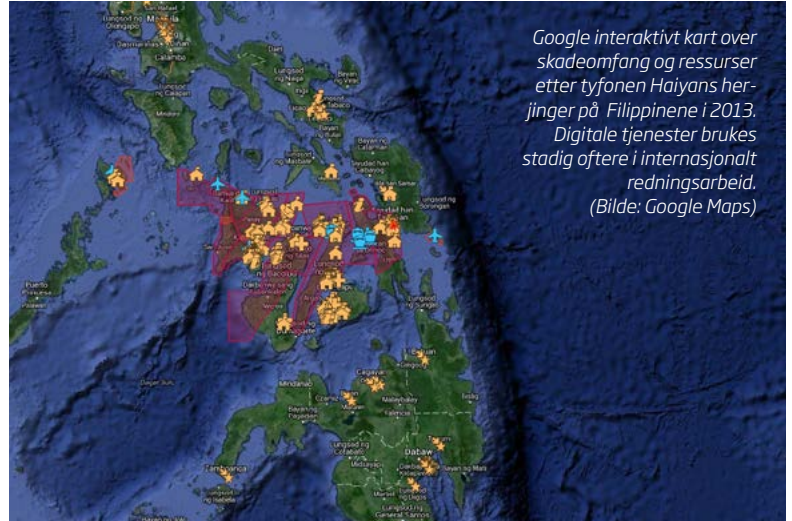
Brannvesenet har eget samband og ressursstyringssystem. Det gamle analoge systemet FAS (Fag Alarm System) er nå i ferd med å bli erstattet av Digitalt Nødnett. Digitalt Nødnett har flere fordeler i forhold til gammelt analogt nett – det tilbyr bedre funksjonalitet, kryptering og muligheter til å operere lokalt innenfor et geografisk avgrenset område gjennom direkte kommunikasjon terminal til terminal. Selv om Nødnett er designet med høy grad av robusthet, kan likevel redusert funksjonalitet eller tilgang til tjenestene oppstå i enkelte scenarier. Dette skyldes blant annet Nødnettets sentraliserte

oppbygging, avhengighet av elektrisitet og en sterk avhengighet til den offentlige kommunikasjonsinfrastrukturen. Det offentlige transportnettet utgjør en grunnleggende forutsetning for det meste av sivil kommunikasjon i Norge. Denne er sårbar overfor både naturskapte og menneskeskapte hendelser, samt for teknisk svikt, strømbrydd og systemfeil.

Denne sårbarheten er også geografisk betinget. Transportnettet utgjør ryggraden i alle sivile kommunikasjonstjenester i Norge. Det meste av trafikken går her, og utfall kan få nasjonale konsekvenser. Til sammenlikning vil et tilsvarende utfall i et aksessnett, for eksempel ved at enkelte basestasjoner faller ut, ofte kun få lokale konsekvenser for et begrenset antall sluttbrukere. Et viktig poeng er at Nød-



▲ Brannvesenet er den viktigste tekniske førstelinjeinnsatsen i den norske redningstjenesten. Bildet viser en brannslukking i Fetsund. (Foto: Scanpix)



Google interaktivt kart over skadeomfang og ressurser etter tyfonen Haiyans herjinger på Filippinene i 2013. Digitale tjenester brukes stadig oftere i internasjonalt redningsarbeid. (Bilde: Google Maps)



nett spesielt og sivil kommunikasjonsinfrastruktur generelt er dimensjonert for å fungere i «ordinære situasjoner», og ikke store katastrofer som varer over tid. Det er nettopp under slike situasjoner at man trenger Nødnett aller mest.

Digitale beredskapstjenester i norsk krisehåndtering

Gjennom internasjonale katastrofer de siste årene har vi sett at sosiale medier og mobilkommunikasjon spiller en stadig viktigere rolle i redningsarbeid og at befolkningen selv kan bidra. Det er stor innovasjon på området humanitære digitale beredskapsverktøy. Informasjonsdeling og integrasjon på tvers av organisasjonsgrenser krever åpne dataskjema og standardiserte grensesnitt, men her det også utfordringer: I tillegg til uønsket

geotagging og fareeksponering av personell som er truet av autoritære regimer, kommer tradisjonelle cybertrusler som hacking, manipulasjon av informasjon og nektelsesangrep. Den økte teknologiske avhengigheten utgjør i seg selv en sårbarhet.

Erfaringer fra internasjonalt hjelpearbeid viser at digitale beredskapstjenester utgjør et stadig viktigere bidrag til å skape et bedre situasjonsbilde for alle involverte i en krise. Men i større katastrofer, stormer og ved storbranner er brann- og redningsinnsatsen prisgitt sårbarhet i den underliggende informasjons- og kommunikasjonsinfrastrukturen. Dette gjør slike digitale beredskapstjenester upålitelige, men dette vil først bli oppdaget når det virkelig gjelder.

Når slike tjenester eksempelvis blir utviklet for nødetatene, bør vi samtidig utvikle funksjoner med nødvendig sikkerhet, pålitelighet og beredskap overfor svikt i underliggende infrastruktur, som tjenestene er avhengig av. I denne utviklingen kan det være hensiktsmessig å se på hvordan Forsvaret har utviklet sin infrastruktur.

Kontakt
Janne Hagen
janne.hagen@ffi.no