Kapittel 4 Kommunikasjonssystemer for beredskap og krisehåndtering – teknologi og utfordringer

Mass Soldal Lund
Forsvarets høgskole/Cyberingeniørskolen, Lillehammer
Høgskolen i Innlandet, Institutt for organisasjon, styring, leiing, Rena

Innledning

Evna til kommunikasjon vil alltid være en avgjørende faktor i krisehåndtering. For vellykka krisehåndtering må ulike aktører koordinere innsatsen og dele informasjon; krisearbeidet må ledes, og kriseledelsen må bygge situasjonsforståelse. Evna til kommunikasjon vil i seg sjøl hvile på menneskelige, kulturelle, organisatoriske og teknologiske faktorer.[1] Dette kapittelet tar for seg de teknologiske midla som understøtter kommunikasjon i krisehåndtering mellom beredskapsaktørene, det vil si de informasjons- og kommunikasjonssystema de ulike beredskapsaktørene har tilgjengelig. Vi vil konsentrere oss om kriser der kommunikasjon spiller ei spesielt viktig rolle, eller som legger spesielt press på kommunikasjonsmidla. Etter en introduksjon om teknologi og tilhørende terminologi som omtales i kapittelet, vil vi drøfte tre problemstillinger relatert til bruk av kommunikasjonsteknologi i krisehåndtering: understøtting av samhandling, avhengighet av sårbare teknologier, og villede eller tilsikta handlinger som rammer kommunikasjonssystema. Så langt det er mulig, vil vi belyse problemstillingene med konkrete eksempler fra kjente hendelser.

Terminologi og teknologi

Det er lett å tenke på talesamband når det er snakk om kommunikasjon i krisehåndtering. Vi vil bruke de mer generelle begrepa *kommunikasjonsteknologi* og *kommunikasjonssystemer*, blant anna for å unngå en umiddelbar assosiasjon til klassiske håndholdte radioer. Disse begrepa markerer også at de teknologiske midla for kommunikasjon i beredskap og krisehåndtering kan være mer enn bare overføring av tale, sjøl om talesamband ofte spiller ei viktig rolle. I militær sammenheng vil man ofte bruke begrepet *kommando- og kontrollsystem*, som i tillegg til tale vil kunne støtte overføring av meldinger, filer, video, bilder, posisjoner og

[1] Bharosa et al. 2010: 50, 57; Manoj & Baker 2007.

Referanse: Lund, M. S. (2021). Kommunikasjonssystemer for beredskap og krisehåndtering – teknologi og utfordringer. I A.-K. Larssen (Red.), *Beredskap og krisehåndtering. Utfordringer på sentralt, regionalt og lokalt nivå* (s. 86–108). Cappelen Damm Akademisk.

andre sensordata. Det kan argumenteres for at det er de militære organisasjonene som har kommet lengst i forståelsen av hva som kreves av kommunikasjonssystemer for å være effektive verktøy for kommunikasjon i kriser og krisehåndtering. Bakgrunnen for dette er at de militære organisasjonene gjennom sitt oppdrag har et *behov* for å kunne kommunisere under alle slags forhold, inkludert i krise og krig, men også at de militære organisasjonene ikke er oppsplitta på den måten de sivile nødetatene og beredskapsorganisasjonene er, og derfor har hatt større *mulighet* for å utvikle enhetlige kommunikasjonssystemer på tvers av ulike våpenarter og funksjoner. I diskusjonen vil vi derfor referere til prinsipper utvikla for militære kommando- og kontrollsystemer.[2] Dette må sjølsagt ikke forstås som at militære organisasjoner «gjør alt riktig», mens sivile beredskaps- og kriseorganisasjoner «gjør alt feil». Sjøl om krisehåndtering vil bære større preg av samhandling enn av hierarkiske organisasjonsstrukturer, er konseptet med et kommando- og kontrollsystem overførbart som et system for å understøtte kommunikasjon mellom innsatsleder og mannskapene – og mellom enheter eller funksjoner – der kommunikasjonen foregår i krevende situasjoner og miljøer.[3]

Vi vil bruke *IKT* (informasjons- og kommunikasjonsteknologi) i den moderne betydninga som digital teknologi, men vil inkludere både digitale og analoge teknologier når vi kun omtaler kommunikasjonsteknologi. Vi vil se på et *system* som noe sammensatt av ulike komponenter og teknologier. Det er vanlig å beskrive kommunikasjonssystemer ved hjelp av lagdelingsmodeller. I en enkel lagdelingsmodell kan vi operere med:

- *Bærere*, som omfatter overføringsteknologiene, for eksempel VHF-radio eller fiberkabler.
- Et *infrastrukturlag*, som bruker bærere til å bygge en nettverksstruktur.
- Et *tjenestelag*, der infrastruktur utnyttes til å tilby en kommunikasjonstjeneste som for eksempel en samtaletjeneste eller en meldingstjeneste.

Et kommunikasjonssystem (er altså et system som) tilbyr en eller flere kommunikasjonstjenester over en eller flere underliggende teknologier. For et enkelt, analogt radiosamband (for eksempel walkietalkie) vil det ikke være mulig å skille tjeneste, infrastruktur og bærere fra hverandre, og lagdelingsmodellen vil kollapse. Men for mobiltelefoni vil vi kunne identifisere bærere som radio (mellom mobiltelefon og basestasjon)

[2] NATO 2017: 1-6–1-10.
[3] Bharosa et al. 2010: 51; Forsvaret 2019: 136–139; Rimstad et al. 2014: 30–32.

og fiber (mellom basestasjon og sentral). Infrastrukturlaget vil være nettverksfunksjoner som binder basestasjoner og sentraler sammen, og som oppretter forbindelse mellom mobiltelefoner. Samtaler og SMS vil utgjøre tjenestelaget.

Begrepa *kommunikasjonsinfrastruktur* og *ekom-infrastruktur*[4] brukes ofte om landsdekkende kommunikasjonssystemer (eller som dekker et anna stort geografisk område). En slik kommunikasjonsinfrastruktur vil bestå av *transportnett* for dataoverføring over store geografiske avstander og *aksessnett* som knytter sluttbrukere til transportnettet. I mobiltelefoni utgjør basestasjonene aksessnettet, mens basestasjonene og sentralene er kobla sammen ved hjelp av et transportnett. Begrepet *kjernenett* brukes gjerne om de komponentene sentralt i en infrastruktur som benyttes for å produsere tjenester. For mobiltelefoni vil dette typisk være databaser over hvor i nettverket den enkelte mobiltelefon befinner seg og de komponentene som oppretter samtaler mellom mobiltelefoner.[5]

Radiokommunikasjon

Begrepet *samband* vil for mange gi assosiasjoner til tovegsradio, med andre ord håndholdte, kjøretøymonterte eller stasjonære innretninger som kan sende og motta tale ved hjelp av radiosignaler. Dette er radioer med såkalt *push-to-talk*-funksjonalitet der det ikke er mulig å prate og lytte til samme tid, og der alle radioer innafor dekningsområdet (til radioen som sender), vil motta. Rekkevidda til slike radioer vil avhenge av frekvensen (og dermed også bølgelengda) til radiosignala og antennas høgde over bakken. Mest brukt er frekvensområdet *very high frequency* (VHF). Rekkevidda til VHF er *line-of-sight*, som vil si at den blir begrensa av hindringer i terrenget og jordkrumninga. Dekningsområdet til VHF kan likevel forlenges utover *line-of-sight* ved hjelp av reléer som mottar og videresender signala, eller permanente installasjoner i form av basestasjoner som gir dekning i et gitt område.[6] Maritim VHF (Kystradio) og Air VHF er eksempler på slike installasjoner.

Radiokommunikasjon kan også benyttes til transportnett. *Radiolinje* betegner retningsbasert radiokommunikasjon mellom to punkter. Endepunkta vil som regel være retningsbaserte antenner (paraboler) montert på master. Radiolinje vil være begrensa av *line-of-sight*, men kan tilby pålitelig dataoverføring med relativt høg kapasitet og kan kobles sammen i nettverk.[7] Et eksempel på bruk av radiolinje som transportnett er Norkring.

[4] Ekom er en forkortelse for *elektronisk kommunikasjon*.
[5] Cox 2014: 2, 23–25; Direktoratet for samfunnssikkerhet og beredskap 2015: 12; Nasjonal kommunikasjonsmyndighet 2017: 27–30; NOU 2015:13: 97–102.
[6] Onslow 2012.
[7] Saunders & Aragón-Zavala 2007: 6, 105.

Norkring er et datterselskap av Telenor som formidler TV- og radiosignaler for kringkasting over to landsdekkende datanettverk, der det ene er et autonomt nettverk bestående av radiolinjeforbindelser.[8]

Mobiltelefoni

Mobiltelefoni er ei form for teknologi som kalles *celleteknologi*. En mobiltelefon har en innebygd radio som kommuniserer med en basestasjon ved hjelp av radiosignaler. Et mobilnett er en infrastruktur som kobler sammen basestasjoner og sentrale komponenter i et nettverk. Dekningsområdet til en basestasjon er inndelt i flere sektorer som går under navnet *celler*, og en mobiltelefon vil til enhver tid være registrert med tilstedeværelse i ei celle. Fordi kapasiteten i ei celle er begrensa, vil mobilnettet typisk bestå av mange basestasjoner med kort rekkevidde i urbane og tettbygde områder, men av færre basestasjoner med lang rekkevidde i grisgrendte strøk. Sentrale komponenter i infrastrukturen administrerer mobiltelefonene som befinner seg i nettet. Andre- og tredjegenerasjons mobiltelefoni (2G/GSM og 3G/UMTS) er, som tradisjonell telefoni, bygd opp rundt telefonsamtalen, med datatrafikk som en sekundærtjeneste. I motsetning er fjerde- og femtegenerasjons mobilteknologi (4G/LTE og 5G) bygd som reine datanettverk der telefonsamtaler bare er en av flere tjenester over infrastrukturen.[9]

Satellitt

Satellittkommunikasjon er ei form for radiokommunikasjon som benyttes til både direktelinker og til telefoni. Fordelen med satellitter er sjølsagt høgda over jordoverflata, som gir større dekningsområde enn ei antenne på bakken. Satellitter har også den fordelen at de kan gi radiodekning på havet der det ikke finnes muligheter for å sette opp ei fast antenne, og på steder på landjorda med dårlig utbygd infrastruktur. En satellittlink fungerer prinsipielt på samme måte som radiolinje. To lokasjoner på landjorda kan oppnå forbindelse ved å rette direktive antenner mot en satellitt og la satellitten fungere som relé. Til satellittlink benyttes som regel geostasjonære satellitter. Det har den ulempa at det gir dårligere dekning jo nærmere polene en kommer, siden geostasjonære satellitter alltid vil befinne seg over ekvator. I tillegg vil det være begrensninger i overføringshastigheten det er mulig å oppnå. Satellittelefoni er celleteknologi som benytter lavbanesatellitter og fungerer som ei form for mobiltelefoni der basestasjonene går i bane rundt jorda. Siden det ikke benyttes geostasjonære

[8] Nasjonal kommunikasjonsmyndighet 2017: 33; Oslo Economics 2015: 13–14.
[9] Cox 2014: 2–27.

satellitter, er ikke geografi ei begrensning på samme måte som for satellittlink. I tillegg til at det er kostbart i bruk, er den store ulempa med satellittelefoni at det har svært begrensa kapasitet sammenligna med mobiltelefoni, siden hver celle vil være på størrelse med Sør-Norge.[10]

Nødnett

Nødnett er sambandsløsninga for nødetatene, det vil si politi, brann og redning og helsevesenet. I tillegg benyttes nødnettet også av andre beredskapsaktører som Sivilforsvaret, kommuner, kraftselskaper og frivillige organisasjoner som Røde Kors og Redningsselskapet. Nødnett er som mobilnettet bygd på digital celleteknologi. Det vil si at en nødnettradio på samme måte som en mobiltelefon kommuniserer med en basestasjon som gir dekning i et område (ei celle). Basestasjonene er knytta til et landsdekkende transportnett slik at det potensielt er mulig å kommunisere mellom to nødnettradioer i ulike deler av landet. [11]

Det er to hovedforskjeller mellom Nødnett og kommersiell mobiltelefoni. Istedenfor å opprette forbindelse mellom to enheter tilbyr nødnettet den samme typen funksjonalitet som man er kjent med fra tovegsradioer: Enhetene er *push-to-talk*, og talemeldinger blir med neglisjerbar forsinkelse kringkasta til andre enheter. Sjøl om overføringa går via basestasjoner, kan vi si at Nødnett simulerer tradisjonelt radiosamband. Likevel har nødnettet større fleksibilitet enn de tradisjonelle tovegsradioene. Ei melding vil ikke bli kringkasta til radioene innafor et geografisk dekningsområde, men til radioene i ei definert talegruppe. Talegruppene er ikke geografisk avgrensa, og det kan være flere aktive talegrupper parallelt i det samme geografiske området. Det er mulig å opprette en-til-en-samtaler mellom to radioer og også mellom en nødnettradio og en telefon i telenettet. Man kan med andre ord ringe ut fra en nødnettradio eller ringe inn til en nødnettradio. Nødnett har lav kapasitet for dataoverføring, men kan sende tekstmeldinger og rapportere egen posisjon fra innebygd GPS.[12]

Den andre store forskjellen mellom Nødnett og kommersielle mobilnett er at nødnettet er bygd med større *robusthet* i infrastrukturen, med andre ord er det designet for å tåle et gitt nivå av påkjenning og skal derfor kunne fungere i møte med forstyrrelser. En basestasjon i mobilnettet vil typisk ha én veg for å nå kjernenettet, mens basestasjonene til Nødnett er

[10] Andreassen et al. 2020: 4; Direktoratet for samfunnssikkerhet og beredskap 2014: 48; Saunders og Aragón-Zavala 2007: 6, 139, 331–332.
[11] Direktoratet for samfunnssikkerhet og beredskap 2019b: 24–26; Direktoratet for samfunnssikkerhet og beredskap 2020b: 6, 9–10.
[12] Direktoratet for samfunnssikkerhet og beredskap 2019b: 8, 16–20.

organisert i ringstrukturer med inntil åtte basestasjoner i hver ring. Det betyr at alle basestasjonene har to veger til kjernenettet og fortsatt vil være en del av nettverket dersom den ene av disse skulle falle ut. Ringene er bygd av fiber-, kobber- eller radiolinjer mellom basestasjonene. En basestasjon som mister forbindelsen til den sentrale infrastrukturen, kan fremdeles fungere lokalt og opprettholde samband mellom nødnettradioene som bruker basestasjonen. Nødnettradioene kan også operere uten basestasjoner, i såkalt direktemodus, og vil da fungere som tradisjonelle tovegsradioer. Nødnett har derfor mulighet for lokal *autonomi*, altså at deler av systemet kan fungere uavhengig av tilstanden til resten av systemet og andre systemer. Dette er en egenskap som ikke finnes i mobilnettet.[13]

Internett og ekom

Det er ikke til å komme unna at internett med tjenester som e-post, direktemeldinger, web-sider, sosiale medier, videostrømming og videokonferanser har blitt samfunnets viktigste kommunikasjonsinfrastruktur ved siden av telefoni. Det er en infrastruktur vi alle kjenner til og benytter oss av. Alle disse kommunikasjonstjenestene har et bruksområde i beredskapsarbeid og krisehåndtering, enten i kommunikasjon mellom ulike beredskapsaktører eller i kommunikasjon med innbyggere og offentlighet.[14] I offentlig sektor har krisehåndteringssystemet CIM blitt standarden for informasjonshåndtering under hendelser. CIM er et web-basert system som med litt ulike tilpasninger benyttes av kommunene, statsforvalterne, helseforetakene, departementa og etater som Direktoratet for samfunnssikkerhet og beredskap (DSB), Norges vassdrags- og energidirektorat (NVE), Statens vegvesen og Bane NOR. Hovedfunksjonene i CIM er loggføring, meldingsending, rapportering og informasjonsdeling. I og med at dette er en web-basert tjeneste vil det nødvendigvis forutsette internettilgang for effektiv bruk.[15]

Internett er kjennetegna ved at det er tilgjengelig for «alle», og ved at funksjonaliteten i infrastrukturlaget er definert av den såkalte internettprotokollen (IP). I et IP-nettverk vil internettprotokollen fungere som et homogeniserende lag, slik at kommunikasjonstjenestene ikke trenger å forholde seg til de underliggende bærerne. Internett er likevel avhengig av en landsdekkende ekom-infrastruktur med forbindelser til utlandet. Transportnettet i denne ekom-infrastrukturen består av fiberkabler, mens aksessnettet også kan bestå av kobberkabler i form av gamle telefon- og kabel-TV-kabler. Men vi må passe oss for å sette likhetstegn

[13] Direktoratet for nødkommunikasjon 2014: 6–11; Direktoratet for samfunnssikkerhet og beredskap 2019b: 9–12, 21–22; Nasjonal kommunikasjonsmyndighet 2017: 34; NATO 2017: 1-8–1-9.
[14] Bharosa et al. 2010: 51–52; Nasjonal kommunikasjonsmyndighet 2017: 25; NOU 2015: 13: 97.
[15] Fylkesmannen i Vestland 2019; Norges vassdrags- og energidirektorat 2014; NOU 2015: 13: 240.

mellom internett og ekom-infrastruktur; internett benytter ekom-infrastrukturen, men ekom-infrastruktur blir også benyttet til framføring av telefoni, TV-signaler og mer. I tillegg har mobilnettet, særlig med utbygginga av fjerdegenerasjons (4G) og etter hvert også femtegenerasjons (5G) mobilnett, blitt en viktig del av aksessnettet for internett.[16]

Samvirke

Krisehåndtering vil ofte involvere mange aktører, og det er anerkjent at god samhandling mellom beredskapsaktørene er en viktig suksessfaktor i håndtering av kriser. Det mest åpenbare eksempelet er håndteringa av terroraksjonene i Oslo og på Utøya 22. juli 2011, der problema med samhandling mellom ulike aktører har gjort at en del av fortellinga om 22. juli er blitt fortellinga om «ressursene som ikke fant hverandre».[17] Et eksempel på det motsatte er håndteringa av Viking Sky-hendelsen 23. mars 2019, der i alt 475 passasjerer blei evakuert med helikopter fra et cruiseskip i havsnød. Det var i alt mer enn 30 aktører involvert i håndteringa av hendelsen, i det som har blitt beskrevet som svært mange aktører i et «komplekst og krevende samspill». Håndteringa av hendelsen blir regna for å være svært vellykka, og godt samvirke mellom aktørene er oppsummert som en betydelig faktor i dette.[18]

Når vi ser på hendelser som dette, blir det klart at kommunikasjonssystema som skal understøtte beredskap og krisehåndtering, må forstås som sosiotekniske systemer, og det vil ikke alltid være mulig eller ønskelig å skille de teknologiske og organisatoriske sidene ved systema fra hverandre: Er det organisatoriske utfordringer som skaper de teknologiske utfordringene, eller er det teknologiske utfordringer som skaper de organisatoriske utfordringene?[19]

Beredskapsarbeidet i Norge er fundert på fire grunnleggende prinsipper: ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet.[20] Disse prinsippa får også konsekvenser for kommunikasjonssystema som skal understøtte krisehåndteringa. Ansvarsprinsippet medfører at departementa sjøl har primæransvaret for kommunikasjonssystemer som skal understøtte kriseledelse og krisehåndtering i egen sektor, likhetsprinsippet at de kommunikasjonssystema man benytter under ei krise, skal være mest mulig lik de kommunikasjonssystema man bruker til daglig, og nærhetsprinsippet at kommunikasjonssystemer for krisehåndtering må være tilgjengelige på alle organisatoriske

[16] Cox 2014: 7–9, 15; Nasjonal kommunikasjonsmyndighet 2017: 18–30; NOU 2015: 13: 97–102; Oslo Economics 2015: 5–17.
[17] NOU 2012: 14: 134.
[18] Direktoratet for samfunnssikkerhet og beredskap 2020a: 5, 29–36, 44–46.
[19] Bharosa et al. 2010: 57.
[20] Meld. St. 29 (2011–2012): 39–40; Meld. St. 10 (2016–2017): 19–21.

nivåer. Sagt litt enkelt er konsekvensen av dette at enhver aktør sjøl er ansvarlig for å ha tilgjengelig de kommunikasjonssystema som er nødvendig for å kunne håndtere ei krise.[21]

Samvirkeprinsippet blei innført som et resultat av erfaringene etter 22. juli 2011, og slår fast at beredskapsaktørene har et sjølstendig ansvar for å sikre best mulig samvirke med andre relevante aktører i beredskapsarbeid og krisehåndtering.[22] Kommunikasjon er ei nødvendig (men ikke tilstrekkelig) forutsetning for samvirke. Det vil si at samvirkeprinsippet vil stille krav til at kommunikasjonssystema som understøtter beredskap og krisehåndtering, også må understøtte samhandling og informasjonsdeling mellom relevante aktører og mellom organisatoriske nivåer. Det stiller spesielle krav til *interoperabilitet*, det at systema tillater aktørene å kommunisere på tvers.[23] Det mangler ikke erfaringer med tekniske løsninger «som ikke snakker sammen», og når hver aktør har ansvar for egne kommunikasjonssystemer, er faren stor for at systema ikke er kompatible. Under håndteringa av terrorangrepet på Utøya 22. juli 2011 hadde Oslo, Asker og Bærum og Søndre Buskerud politidistrikter Nødnett som sitt primære eller eneste samband og fikk ikke kommunisert med Nordre Buskerud politidistrikt, som fremdeles brukte det gamle, analoge politinettet. I tillegg var en del andre deltagende aktører, som Forsvaret, Sivilforsvaret, lokalt brannvesen og deler av ambulanse- og luftambulansetjenesten uten Nødnett. Konsekvenser av dette var at helseaktører som kom til området ved Utøya, gikk over til å benytte analog helsenettradio, og at mange var nødt til å gå over til mobiltelefon som sambandsmiddel.[24] I håndteringa av brannene i Lærdal 18.–19. januar 2014, i Flatanger 27. januar–2. februar 2014 og på Frøya 29.–31. januar 2014 var det store utfordringer med å holde oversikt over mannskaper i aksjon og ankomne eksterne ressurser, blant annet fordi sambandssystema var inkompatible, og det var utfordringer med bruk av mobiltelefoni (se også avsnittet om avhengigheter nedafor).[25]

Ved evalueringa av de fire hendelsene i 2011 og 2014 mente man at utfordringer som disse i stor grad skulle bli løst når utrullinga av Nødnett var fullført i 2015.[26] Vi ser her at samvirkeprinsippet i konteksten av kommunikasjonssystemer trekker i motsatt retning av de andre prinsippa for beredskap og krisehåndtering; det er et felles system som er løsninga på problema med interoperabilitet. Sjøl om utbygginga av nødnettet åpenbart har bedra situasjonen, skal man likevel være forsiktig med å tenke at det løser alle utfordringer. Viking

[21] NOU 2015: 13: 238–239.
[22] Meld. St. 29 (2011–2012): 5, 9, 39–40.
[23] NATO 2017: 1-7–1-8; NOU 2015: 13: 244.
[24] NOU 2012: 14: 305–307; Rimstad et al. 2014: 35–36.
[25] Direktoratet for samfunnssikkerhet og beredskap 2014: 24–34, 43–44, 46; PricewaterhouseCoopers 2014: 28–72.
[26] Direktoratet for samfunnssikkerhet og beredskap 2014: 48; PricewaterhouseCoopers 2014: 74.

Sky-hendelsen illustrerer dette. Sjøl om redningsaksjonen var vellykka og samvirket mellom aktørene var god, var det likevel utfordringer med kommunikasjonen fordi aktørene mangla en felles kommunikasjonsplattform, særlig på tvers av aktører som opererte til sjøs, i lufta og på land. Kommunikasjonen fra Hovedredningssentralen i Sør-Norge (HRS-SN) til Viking Sky og andre skip som deltok i redningsarbeidet, var over maritim VHF. Kommunikasjonen til helikoptra som evakuerte passasjerer, foregikk over Air VHF. Aktørene på land brukte Nødnett. De færreste av aktørene hadde tilgang til alle kommunikasjonsmidla; nødetatene har generelt ikke tilgang til VHF-samband, mens bare halvparten av helikoptra og ingen av de maritime aktørene hadde tilgang til nødnettet. HRS-SN hadde tilgang til alle kommunikasjonsmidla og måtte derfor stå for kommunikasjonen på tvers av VHF og nødnettet. De involverte kommunene Fræna, Molde og Kristiansund hadde ikke Nødnett til beredskapsformål og var derfor avhengig av brannvesenet for å få informasjon via nødnettet. Deler av koordineringa mellom aktørene skjedde også over mobiltelefon og e-post.[27]

Mens samvirkeprinsippet trekker i retning av Nødnett som felles samband for alle beredskapsaktører, svekkes samtidig de andre prinsippa for samfunnssikkerhet. Av størst praktisk konsekvens er trolig at likhets- og nærhetsprinsippa svekkes ved at aktører som i det daglige ikke benytter nødnettet (som kriseledelsen i en kommune), blir nødnettbrukere under kriser. Det betyr at nødnettet ikke nødvendigvis vil være *beredskapsklart* – tilgjengelig for å kunne dekke et umiddelbart behov – for alle aktører. Kombinert med mange aktive aktører på nødnettet ved store kriser kan dette føre til utfordringer med *skalerbarheten* av nødnettet, det vil si systemets evne til å tilpasse seg størrelsen på hendelsen når mange uerfarne aktører tar det i bruk. Evalueringer av både 22. juli-hendelsen i 2011 og Viking Sky-hendelsen i 2019 pekte på behovet for styrking av sambandsledelse og sambandsdisiplin.[28]

En annen grunn til at Nødnett ikke kan løse alle utfordringer, er at ikke alle sider ved samhandling og samvirke er best understøtta av talesamband. 22. juli-kommisjonen har vist til at politiet i juli 2011 mangla IKT-systemer som kunne gitt situasjonsforståelse til både operasjonssentralen og politipatruljene, for eksempel digitale kart, GPS-sporing og løsninger for overføring av bilder til operasjonssentralen.[29] Under håndteringa av Viking Sky-hendelsen gjorde mangelen på et egna system for registrering av evakuerte til at det var krevende å etablere et fullstendig situasjonsbilde, og aktørene på mottakssenteret, inkludert politiet,

[27] Direktoratet for samfunnssikkerhet og beredskap 2020a: 10, 36, 71–74.
[28] Direktoratet for nødkommunikasjon 2011: 21; Direktoratet for samfunnssikkerhet og beredskap 2020a: 10, 74; NATO 2017: 1-8, 1-10.
[29] NOU 2012: 14: 332–334, 336 454–455.

hadde ikke fullstendig oversikt og kontroll over de evakuerte. Registering blei gjort med penn og papir, og papirskjemaer med helseopplysninger blei fotografert og delt med private mobiltelefoner.[30] I begge tilfella var det altså mangel på et *kapabelt* system med tilstrekkelig funksjonalitet for å bygge situasjonsforståelse. Samhandling og samvirke fordrer med andre ord ikke bare kommunikasjonsløsninger for overføring av tale, men også IKT-systemer for å understøtte situasjonsforståelse og informasjonsdeling, systemer som kanskje er mer beslekta med militære kommando- og kontrollsystemer enn med nødnettet.[31]

Avhengighet

I håndteringa av nesten alle hendelser ser vi bruk av mobiltelefoni, og en tendens til å falle tilbake på mobiltelefoni når andre kommunikasjonssystemer er fraværende eller har mangler. Kanskje særlig to forhold bidrar til dette: Når mange aktører skal samhandle, er ofte mobiltelefoni et av de få kommunikasjonsmidla alle aktørene deler og har tilgang til, og mobiltelefon er for mange aktører det kommunikasjonsmiddelet de er vant til å bruke i hverdagen. Men det ligger i krisehåndteringas natur at man kan oppleve unormalt stress på ressurser man vanligvis kan regne med. Dette gjelder også for kommunikasjonssystemer og i høgeste grad for mobiltelefoni. Avhengigheten av kommunikasjonssystemer i krisehåndtering utgjør en betydelig utfordring, og avhengighet av mobiltelefoni egner seg godt for å illustrere dette.

Håndteringa av gras- og lyngbrannene i Flatanger og på Frøya i 2014 er eksempler på slik avhengighet. I Flatanger var utfordringene betydelige grunna dårlig mobiltelefondekning; kommunikasjonen til slukkemannskapene og eksterne ressurser var vanskelig, og ordonnanser måtte benyttes. På grunn av manglende mobildekning hadde innsatsleders kommandoplass kun én fasttelefonlinje tilgjengelig der den var etablert, og løpende rapportering og oppdatering av situasjonsbildet var derfor vanskelig. På Frøya falt sambandet ut under deler av innsatsen, og dårlig mobildekning og kort batteritid på mobiltelefonene skapte betydelige utfordringer. Det var vanskelig å holde kontakt med og oversikt over mannskaper og ankomne ressurser, og utfordringer med å koordinere innsatsen til både mannskaper og privatpersoner som var ute i terrenget.[32]

I disse tilfella var dårlig mobiltelefondekning utfordringa, men det finnes også eksempler på at krisa som håndteres, også er årsaka til kommunikasjonsproblema. I

[30] Direktoratet for samfunnssikkerhet og beredskap 2020a: 9, 64, 68.
[31] Bharosa et al. 2010: 50–52, 60–63; Meld. St. 28 (2020–2021): 32; NATO 2017: 1-7.
[32] Direktoratet for samfunnssikkerhet og beredskap 2014: 28–34; PricewaterhouseCoopers 2014: 43–72.

håndteringa av brannen i Lærdal i januar 2014 var det store kommunikasjonsmessige utfordringer. En av grunnene var at Telenor-bygget brant ned, noe som førte til at mobilnettet blei slått ut. Særlig i starten av redningsarbeidet bidro dette til «kaotiske tilstander». Sjøl om samband internt i etatene fungerte, var kommunikasjonen mellom aktørene i stor grad basert på mobiltelefoni.[33] Ekstremvær er en annen type hendelse med potensial til å ramme kommunikasjonssystemer. Ekstremværet Dagmar, som ramma Sør-Norge i romjula 2011, førte til store utfall i strømnettet og utfordringer med telefoni og internett. I mobilnettet var det største problemet at basestasjonene mista strøm, og at batteribackup gikk tom. I noen tilfeller mista også basestasjonene kontakt med infrastrukturen på grunn av skred, og noen basestasjoner blei ødelagt av ekstremværet sjøl. Utfordringene med telefoni gjorde det vanskelig for energiselskapa å innkalle mannskaper til feilretting i strømnettet, sjøl om energiselskapas interne VHF-samband stort sett fungerte godt. Gjenoppretting av mobilnettet krevde gjenoppretting av strømforsyning til basestasjonene, men energiselskapa måtte prioritere kritiske samfunnsfunksjoner, og det tok lang tid før de kunne prioritere basestasjoner.[34]

Etter at Nødnett var ferdig utbygd i 2015, har situasjonen forbedra seg betydelig. Nødetatene har et mer robust samband, avhengigheten av mobiltelefoni er redusert, og samhandling på tvers av aktørene er enklere. For eksempel viser oppsummeringa fra bekjempelsen av skogbranner sommeren 2018 at nødnettet fungerte etter hensikten.[35] Likevel viser (for eksempel) Viking Sky-hendelsen at nødnettet ikke fullstendig vil kunne fjerne avhengigheten av mobiltelefoni, spesielt når mange aktører er involvert. I tillegg er heller ikke nødnettet ufeilbarlig. Erfaringer med ekstremvær har vist at nødnettet, sjøl om det er mer robust enn mobiltelefonnetta, har en del av de samme utfordringene. Ekstremværet Tor, som ramma Sør-Norge 29.–30. januar 2016, førte til utfall i nødnettet. Store områder var uten dekning i korte perioder, og noen områder i lengre perioder. Utfalla skyldtes i hovedsak brudd på kommunikasjonslinjene inn til basestasjonene og i noe mindre grad andre feil i basestasjonene. Hovedproblemet med kommunikasjonslinjene var at antenner til radiolinjeforbindelser mellom basestasjonene blei blåst ut av posisjon, men også strømforsyning og nødbatterikapasitet i basestasjonene og i leide linjer mellom dem var ei utfordring. Mobilnettet opplevde også problemer under uværet, men i liten grad i de samme

[33] Direktoratet for samfunnssikkerhet og beredskap 2014: 24–28; PricewaterhouseCoopers 2014: 28–42.
[34] Norges vassdrags- og energidirektorat 2012: 5, 12–15; Post- og teletilsynet 2012: 11–13.
[35] Direktoratet for samfunnssikkerhet og beredskap 2018.

områda som nødnettet, og noen steder var også internettforbindelsen borte.[36] Politiet oppsummerte i etterkant at det hadde akseptable alternative sambandsmidler, mens 110-sentralene og AMK-sentralene mente de ville hatt betydelige utfordringer dersom en alvorlig hendelse hadde inntruffet der nødnettet var nede, eller hvis mobilnettet også hadde falt ut. Reserveløsningene ville bare gitt samband internt i etatene, og det var ingen alternative løsninger utenom mobiltelefoni som kunne gitt samband på tvers av etatene.[37] Også under ekstremværa Dagmar i jula 2011, Urd i desember 2016 og Knud i september 2018 var det utfall i nødnettet.[38]

Mobilnettet vil altså fungere som både supplement og *redundans* for nødnettet, et alternativt system for framføring av tale. En utfordring med dette er at mobilnettet og nødnettet er avhengig av den samme underliggende infrastrukturen. Flertallet av basestasjonene i nødnettet er samlokalisert i de samme mastene som basestasjoner i mobilnettet, og de bruker i stor grad de samme framføringslinjene for strøm og datatrafikk. Ved naturhendelser som ekstremvær vil nødnett og mobilnett være utsatt for de samme påkjenningene, og fysisk skade på master eller framføringslinjer kan potensielt slå ut både nødnett og mobilnett. Tilsvarende vil langvarig strømutfall i et geografisk område ramme basestasjonene og transmisjonslinjene til både nødnett og mobilnett i området.[39] Neste generasjons nødnett i Norge skal baseres på kommersielle femtegenerasjons (5G) mobilnett. Det vil skape enda større avhengighet mellom framtidas nødnett og mobilnett, men samtidig vil 5G-teknologien gi større fleksibilitet og skal ha bedre muligheter for å skape robusthet og autonomi enn tidligere generasjoners mobilteknologi.[40]

I eksempla ovafor har problemer med aksessnettet vært utfordringa og grunnen til at kommunikasjonstjenestene ikke har vært tilgjengelig. I slike tilfeller vil utfordringene i sin natur være lokale. Men kommunikasjonstjenester som telefoni, internett og nødnett er også avhengig av den delen av infrastrukturen vi har omtalt som transportnettet. Det er bare to kommersielle aktører som kan tilby landsdekkende datatransporttjenester: Telenor og GlobalConnect, der Telenor er den klart største. Andre aktører med landsdekkende transportnett som Altibox, Norkring og Forsvaret bruker hele kapasiteten til egen virksomhet og tilbyr ikke kapasitet til andre. Det vil si at alle leverandører av landsdekkende

[36] Bergman u.å.; DNV GL 2016: 2–3, 6, 8, 10, 17–19, 25, 27, 39; Norges vassdrags- og energidirektorat 2017: 37–38.
[37] DNV GL 2016: 21–24, 29.
[38] Holm-Nilsen & Wergeland 2018; Løland 2016; NOU 2015:13: 111.
[39] Direktoratet for nødkommunikasjon 2014: 5, 7–11; Direktoratet for samfunnssikkerhet og beredskap 2020b: 9; NATO 2017: 1-9.
[40] Meld. St. 28 (2020–2021): 109–112, 178.

kommunikasjonstjenester, inkludert mobiloperatørene Telia og ice, i større eller mindre grad er avhengig av tilgang til transportnettet til Telenor eller GlobalConnect. Det gjelder også Nødnett, som er helt avhengig av Telenor for å forbinde basestasjonsringene til kjernenettet og til kommunikasjon mellom regionene. Telenor er derfor ikke bare Norges største leverandør av internett og mobiltelefoni, men også ryggraden i hele ekom-infrastrukturen i Norge.[41] En illustrasjon av dette er at ikke bare Telenors mobilnett falt ut da Telenor-bygget i Lærdal brant ned i storbrannen i 2014, men også mobilnetta til NetCom, TeliaSonera og Tele2.[42] Det vil si at mobilnetta mangler autonomi, og at den tilsynelatende redundansen vi får ved å ha flere mobiloperatører og nødnett, til en viss grad er en falsk redundans.

Både Telenors og GlobalConnects transportnett har innebygd redundans ved at nettverka har ringstruktur og parallelle, fysisk og logisk adskilte framføringsveger. Det vil derfor kreve tre eller flere kabelbrudd eller andre feil samtidig for å «dele landet i to». Nasjonal kommunikasjonsmyndighet vurderer det som «mindre sannsynlig», men Norges lange og smale geografi gjør at det ikke er et umulig scenario. For eksempel opplevde Telenor store problemer i mobilnettet da de to hovedforbindelsene mellom Oslo og Trondheim falt ut på likt i mai 2011 – på grunn av graving i Gudbrandsdalen og en trevelt i Lørenskog utafor Oslo.[43]

På grunn av avhengigheten av Telenors kjernenett vil konsekvensene av en slik hendelse være store. Dette blir forsterka av at mange av tjenestene som går over nettverka, har sentraliserte kontroll- og styringsfunksjoner, for eksempel abonnementsdatabasen til en mobiloperatør. Delsystema har altså liten grad av autonomi, og fiberbrudd kan føre til uforholdsmessig store utfall av tjenestene. For krisehåndtering vil åpenbart konsekvensene være store dersom hendelsen også rammer kommunikasjonssystemer som benyttes til informasjon og koordinering av håndteringa, som mobiltelefoni og internett.[44]

Ekom-infrastruktur rammes ikke bare av fysiske feil som kabelbrudd. Logiske feil – feil i programvaren eller konfigurasjonen som styrer infrastrukturen, eller feil som følge av overbelastning – kan også gi utfall. Et eksempel er da alle Telenors mobilabonnenter var uten forbindelse i tre timer i oktober 2014 etter sletting av feil data i abonnementsdatabasen. Logiske feil kan i større grad enn fysiske feil rettes uten fysisk tilstedeværelse, men samtidig

[41] Ibid.: 172–173; Nasjonal kommunikasjonsmyndighet 2017: 17–21, 31–36; NOU 2015:13: 106–107; Oslo Economics 2015: 9–14.
[42] Oslo Economics 2015: 21.
[43] Nasjonal kommunikasjonsmyndighet 2016: 24; Post- og teletilsynet 2011.
[44] Nasjonal kommunikasjonsmyndighet 2016: 24; Nasjonal kommunikasjonsmyndighet 2017: 41; NOU 2015: 13: 107–110; Oslo Economics 2015: 23–26.

vil sentraliserte funksjoner og kompleksiteten i infrastrukturen gjøre at logiske feil kan gi utforutsette og store utfall i systema. Trenden er flere og mer avanserte kommunikasjonstjenester over de samme netta, noe som vil si at en større del av funksjonaliteten vil være i form av programvare. I tråd med det kan vi forvente at en større del av feila i framtida vil være logiske feil.[45]

Et eksempel på kombinasjonen av en fysisk og en logisk feil fant sted da deler av Øst-Finnmark var «tilnærmet ekom-døde» 30. november 2018. Slitasje hadde 28. november ført til brudd på en sjøkabel mellom Hammerfest og Gjesvær og dermed skapt et brudd i ringstrukturen i Finnmark. Sjøkabelskip blei rekvirert fra Bergen, men hadde estimert feilrettingstid på minst fem døgn. To dager etter førte en feilkobling i en nettverkskomponent i Vadsø til et nytt brudd i ringen, slik at området mellom Hammerfest og Vadsø i stor grad var uten elektronisk kommunikasjon fram til feilen blei retta fem timer seinere. Bruddet ramma mobiltelefoni, inkludert Telia og Ice, fasttelefoni og internett, og også nødnettet og kystradioen. I tillegg måtte lufthavnene i Vardø, Båtsfjord og Berlevåg stenge som resultat av bortfall av kommunikasjonssystemer.[46]

Villede handlinger

Ovafor har vi sett eksempler på kommunikasjonssystemer som er utsatt for naturhendelser eller ulike former for feil. Men hva om skaden på kommunikasjonssystema ikke er en utilsikta effekt av en hendelse, men ei villet handling? For ekom-infrastrukturen vil det fortsatt være snakk om fysiske og logiske feil, men da i form av sabotasje eller cyberangrep utført av en aktør med fiendtlige hensikter.[47] Vi har sett tilfeller der kommunikasjonssystema til sentrale norske aktører har blitt utsatt for etterretning ved hjelp av cyberangrep. I perioden 2008–2010 blei det avdekka alvorlige sikkerhetshull i det ugraderte nettverket til departementa (Depnett/U), og det har blitt spekulert i om utenlandske aktører har henta ut data. I 2012–2013 blei Telenor utsatt for omfattende industrispionasje, og i september 2020 og mars 2021 blei det avslørt cyberangrep mot Stortingets e-postsystem.[48]

Derimot vi har ingen eksempler på at norsk kjerneinfrastruktur har blir utsatt for cyberangrep eller sabotasje, og vi vil derfor ta utgangspunkt i et scenario beskrevet av DSB. I scenarioet har et cyberangrep retta mot sentrale komponenter i transportnettet til Telenor slått

[45] Direktoratet for samfunnssikkerhet og beredskap 2015: 40, 49; Nasjonal kommunikasjonsmyndighet 2017: 6, 37–40; NOU 2015:13: 110; Oslo Economics 2015: 18–21.
[46] Nasjonal kommunikasjonsmyndighet 2019: 3–7.
[47] Meld. St. 28 (2020–2021): 154; Oslo Economics 2015: 18.
[48] Riksrevisjonen 2010: 120–121; Fagerland et al. 2013: 2–7; Johansen 2011; Johansen 2013; Stortinget 2020; Stortinget 2021.

ut hele nettverket i fem dager.[49] Et slikt angrep vil være svært avansert, og vi må derfor forutsette at en kompetent og ressurssterk statlig aktør står bak. Siden ingen nasjoner i dag har motiv for å gjennomføre et slik angrep mot Norge, forutsetter scenarioet også en situasjon høgere opp i konfliktspekteret enn det vi har i dag. Den mest nærliggende faktiske hendelsen å sammenligne med vil trolig være «NotPetya-angrepet» mot Ukraina i 2017. NotPetya var en skadevare som 27. juni 2017 med raskt tempo spredde seg gjennom ukrainske IKT-systemer. Bakmennene hadde planta skadevare i ei oppdatering til en mye brukt programvare for skatterapportering i Ukraina. På et gitt tidspunkt blei NotPetya aktivert på alle datamaskiner der denne oppdateringa var installert. Når skadevaren på den måten hadde infisert ei datamaskin, var den designa til først å komme seg over på så mange andre maskiner som mulig, for deretter å kryptere alle filene og dermed gjøre datamaskina ubrukelig. NotPetya blir regna for å være den raskest spredende og mest destruktive skadevaren verden har sett, og den spredde seg også langt ut over Ukrainas grenser. Men som episenter var Ukraina hardest ramma. På slutten av dagen var fire sjukehus, seks kraftselskaper, to flyplasser, 22 banker og betalingssystemer og over 300 bedrifter angrepet – i tillegg til store deler av statsapparatet. Det har blitt anslått at i alt 10 prosent av datamaskinene i Ukraina i praksis blei sletta av skadevaren.[50] Dette var ikke et angrep som retta seg mot kjernen i ekom-systema, men kan sammenliknes med at 10 prosent av Norges datamaskiner på likt blei ramma av samme type skadevare som den som i januar 2021 slo ut IKT-systema til Østre Toten kommune. Det kan derfor illustrere det potensielle omfanget av et retta cyberangrep mot en nasjons IKT-infrastruktur.[51]

I DSB-scenarioet fører nettverksutfallet til store samfunnsmessige konsekvenser, særlig for helse og transport, på grunn av den sterke avhengigheten mange samfunnskritiske funksjoner har til ekom-infrastrukturen. En slik hendelse vil ramme bredt, både geografisk og på tvers av sektorer. Det vil derfor være et stort behov for samordning, koordinering og ledelse på nasjonalt nivå, og det må etableres kriseledelse på alle nivåer fra kommune til regjering. Behovet for informasjon i befolkninga vil være stort. Samtidig vil krisa i seg sjøl ramme evna til å håndtere krisa. Kommunene, fylkeskommunen og statsforvalterne er avhengig av e-post, mobil- og fasttelefoni, CIM og så videre for å kunne drive effektiv kriseledelse og for å rapportere til sentral kriseledelse. Tilsvarende vil ikke

[49] Direktoratet for samfunnssikkerhet og beredskap 2015: 14; Direktoratet for samfunnssikkerhet og beredskap 2019a: 204.
[50] Greenberg 2019: 179–189, 204–217.
[51] Kessel & Røsrud 2021; Solbakken 2021.

hovedredningssentralene kunne kommunisere eksternt, og media, inkludert NRK, vil ikke kunne formidle nyheter og heller ikke ha tilgang til kilder. Nødnumra vil ikke være operative, og Nødnett vil kun fungere lokalt. Det som finnes av alternative kommunikasjonssystemer, vil ikke kunne dekke opp for utfallet av telefoni og internett; radiosamband som VHF har rekkevidde som er begrensa til *line-of-sight*, og satellittelefoni er begrensa til en kapasitet på rundt hundre samtidige telefonsamtaler i Sør-Norge. I tillegg er dette utstyr som sjelden er i bruk, slik at erfaring med bruken vil være begrensa. Sentrale aktører vil kunne kommunisere seg imellom via Sikret offentlig nett (SON) – et dedikert fibernett mellom sentrale offentlige aktører i Oslo-området, uavhengig av kommersielle leverandører – men vil likevel operere i blinde hvis resten av samfunnet står uten effektiv kommunikasjon.[52] Konsekvensene av en hendelse som denne vil være uoversiktlige og store. Sannsynligheten vil *i dag* være liten, men det vil være vanskelig å utelukke scenarioer som dette dersom Norge skulle befinne seg i ei sikkerhetspolitisk krise. Nettopp fordi det er snakk om villede handlinger, som man må forvente at til en viss grad er målretta, vil ikke sannsynlighetsbetraktninger basert på for eksempel naturhendelser være overførbare.[53]

Samtidig trenger vi ikke å forutsette et slikt altomfattende scenario for å illustrere utfordringene med villede handlinger mot IKT-systemer. Cyberangrepet mot Helse Sør-Øst regionale helseforetak og Sykehuspartner helseforetak rundt årsskiftet 2017–2018 illustrerer utfordringene med kommunikasjon også i tilfeller der angrepet ikke er destruktivt. En angriper lyktes i romjula 2017 med å trenge inn i IKT-systema i helseregionen. Via en sårbar applikasjon eksponert mot internett klarte angriperen å komme seg inn i en av de tre regionale infrastrukturplattformene som Sykehuspartner forvalter for Helse Sør-Øst. Kompromitteringa blei oppdaga 9. januar 2018, og hendelseshåndteringa pågikk til 16. februar samme år.[54]

En av de prinsipielle utfordringene med kommunikasjon under et cyberangrep er at de kommunikasjonskanalene man vanligvis bruker, kan være kompromittert av angriperen, og at angriperen derfor vil kunne avlese kommunikasjon som gjelder håndteringa av hendelsen. For å unngå dette kan det være nødvendig å flytte kommunikasjonen over på alternative kanaler som man er sikker på at angriperen ikke har tilgang til. Dersom det er ugraderte systemer som er kompromittert, vil Nasjonalt begrenset nett (NBN) og Nasjonalt hemmelig nett (NHN) –

[52] Departementene 2019: 17–18; Direktoratet for samfunnssikkerhet og beredskap 2015: 26–48; Direktoratet for samfunnssikkerhet og beredskap 2019a: 204–207; Hattrem 2019; NOU 2015: 13: 241.
[53] Direktoratet for samfunnssikkerhet og beredskap 2015: 18; Direktoratet for samfunnssikkerhet og beredskap 2019a: 205–206.
[54] Bruvoll et al. 2020: 29–30.

dedikerte systemer for henholdsvis lavgradert og høggradert informasjon i norsk forvaltning – være naturlige alternativer.[55]

Håndteringa av cyberangrepet mot Helse Sør-Øst og Sykehuspartner var prega av mange aktører – i alt ni statlige og to kommersielle – og til dels betydelige utfordringer med bakgrunn i at deler av informasjonen og kommunikasjonen mellom aktørene var sikkerhetsgradert. Utfordringene skyldtes blant anna manglende tillit mellom aktørene, dårlige eller manglende rutiner for varsling, ulik kultur for autorisering og informasjonsdeling og ulik kompetanse og stammespråk – men også manglende tilgang til systemer for gradert informasjon, manglende erfaring med håndtering av gradert informasjon og manglende sikkerhetsklarering av involvert personell.[56]

Oppsummering

Kommunikasjon mellom involverte aktører er ei forutsetning for vellykka krisehåndtering, og kommunikasjonen forutsetter at aktørene har gode kommunikasjonssystemer som fungerer. For å kunne håndtere ulike typer hendelser, men også som resultat av prinsippa for beredskap og krisehåndtering (ansvar, nærhet, likhet) benyttes mange ulike kommunikasjonsteknologier og -systemer. Samtidig er trenden – i tråd med samhandlingsprinsippet som blei innført i 2012 – sentralisering og standardisering av kommunikasjonssystema for beredskap og krisehåndtering. Nødnett og CIM er eksempler på dette. Sjøl etter at nødnettet var ferdig utbygd i 2015, har mye hvilt på mobiltelefoni og internett, som er kommunikasjonssystemer alle har tilgang til, men som har begrensa robusthet og autonomi. En viktig grunn er at nødnettet mangler kapabiliteter ut over tale. For å bygge situasjonsbilde er beredskapsaktørene i stor grad avhengig av internettjenester. En annen grunn er at ikke alle aktører bruker Nødnett i det daglige og derfor ikke vil ha nødnettet som et beredskapsklart system. Den siste av disse utfordringene gjelder også for systemer for gradert informasjon.

Vi har sett på en rekke eksempler som illustrerer utfordringene som kan oppstå når kommunikasjonssystema ikke er tilstrekkelig interoperable, kapable og skalerbare, når hendelsen som håndteres, også rammer kommunikasjonssystema, og når hendelsen i seg sjøl er et villet, målretta angrep mot kommunikasjonssystema. Eksempla viser at beredskapsaktører tilstreber å kommunisere på tross av utfordringene, og at de er ofte svært kreative for å få det til. Men samtidig ser vi at fleksibiliteten i systema kanskje ikke er god nok, og at utfordringene må løses utafor systema.

[55] Departementene 2019: 17; Hattrem 2019.
[56] Bruvoll et al. 2020: 33–36, 45, 49–50, 53–54.

For å skape den interoperabiliteten, autonomien, redundansen og fleksibiliteten som til en viss grad mangler i summen av kommunikasjonssystema, kan internetteknologi og tjenesteorientering være en veg å gå. Internettprotokollen (IP) fungerer som et harmonerende infrastrukturlag som frigjør tjenestene fra bærerne. Sammensmeltinga av telefoni og internett, som vi ser både i fjerde- og femtegenerasjons mobilteknologi og i IP-telefoni, er et eksempel på dette. Ved å bygge kommunikasjonssystemer for beredskap og krisehåndtering over samme type lest vil vi kunne styrke interoperabilitet og fleksibilitet ved å standardisere på IP-baserte tjenester og styrke robusthet, redundans og autonomi ved å la tjenestene utnytte ulike underliggende teknologier og bærere. Når neste generasjons nødnett skal bygges på 5G-teknologi, kan dette potensielt gi ei åpning for en slik tankegang.

Litteraturliste

Andreassen, N., Borch, O. J. & Sydnes, A. K. (2020). Information sharing and emergency response coordination. *Safety Science, 130,* Artikkel 104895. https://doi.org/10.1016/j.ssci.2020.104895

Bharosa, N., Lee, J. & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers, 12*(1), 49–65. https://doi.org/10.1007/s10796-009-9174-z

Bergman, T. (u.å.). *Slik taklet Nødnett uværet Tor* [Lysarkpresentasjon]. Direktoratet for nødkommunikasjon.

Bruvoll, J. A, Thuv, Aa. & Enemo, G. (2020). *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene* (FFI-rapport 20/01560). Forsvarets forskningsinstitutt. https://publications.ffi.no/nb/item/asset/dspace:6767/20-01560.pdf

Cox, C. (2014). *An Introduction to LTE. LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications* (2. utg.). Wiley.

Departementene. (2019). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf

Direktoratet for nødkommunikasjon. (2011). *Bruk av Nødnett 22. juli 2011* (Rapport). https://www.nodnett.no/siteassets/bibliotek/rapporter/bruk-av-nodnett-22--juli-2011.pdf

Direktoratet for nødkommunikasjon. (2014). *Robusthet i transmisjon. Reservestrøm i transmisjonslinjer i Nødnett* (Rapport, offentlig versjon).

Direktoratet for samfunnssikkerhet og beredskap. (2014). *Brannene i Lærdal, Flatanger og på Frøya vinteren 2014. Læringspunkter og anbefalinger* (Rapport). https://www.dsbinfo.no/DSBno/2014/Rapport/branneniLaerdalFlatangerFroya2014/

Direktoratet for samfunnssikkerhet og beredskap. (2015). *Risikoanalyse av «Cyberangrep mot ekom-infrastruktur» – delrapport til Nasjonalt risikobilde 2014* (Delrapport). https://www.dsbinfo.no/DSBno/2015/Tema/Risikoanalyseavcyberangrepmotekominfrastruktur/

Direktoratet for samfunnssikkerhet og beredskap. (2018). *Nødnett – erfaringer etter skogbrannsituasjonene sommeren 2018* (Rapport). https://www.nodnett.no/siteassets/bibliotek/rapporter/erfaringer-etter-skogbranner---nodnett-2018.pdf

Direktoratet for samfunnssikkerhet og beredskap. (2019a). *Analyser av krisescenarioer 2019* (Rapport). https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

Direktoratet for samfunnssikkerhet og beredskap. (2019b). *Brukerevaluering Nødnett 2019. Landsdekkende brukerundersøkelse blant alle brukere i Nødnett* (Rapport). https://www.nodnett.no/siteassets/bibliotek/rapporter/brukerevaluering-2019.pdf

Direktoratet for samfunnssikkerhet og beredskap. (2020a). *Evaluering av Viking Sky-hendelsen* (Rapport). https://www.dsb.no/globalassets/dokumenter/rapporter/evaluering_av_viking_sky_hendelsen.pdf

Direktoratet for samfunnssikkerhet og beredskap. (2020b). *Nødnett i bruk. En oversikt over tekniske løsninger og funksjoner i Nødnett, samt retningslinjer for bruk* (Rapport, versjon 1.3). https://www.nodnett.no/siteassets/bibliotek/brukerveiledninger/nodnett-i-bruk-2020.pdf

DNV GL. (2016). *Evaluering etter ekstremværet «Tor»* (Rapport nr. 2016-0386, rev. 1.1).

Fagerland, S., Kråkvik, M., Camp, J. & Moran, N. (2013). *Operation hangover: Unveiling an Indian cyberattack infrastructure.* Norman Shark.

Forsvaret. (2019). *Forsvarets fellesoperative doktrine.* Forsvarsstaben.

Fylkesmannen i Vestland. (2019). *DSB-CIM brukarrettleiar for kommunane i Vestland. Grunnleggjande funksjonar* (Rapport). https://www.statsforvalteren.no/siteassets/fm-vestland/samfunnstryggleik-og-beredskap/krisehandtering-og-samordning/dsb-cim/dsb-cim-temaside/brukarrettleiar-dsb-cim-for-kommunane-vl.pdf

Greenberg, A. (2019). *Sandworm. A new area of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Hattrem, E. (2019, 17. juli). Hysj-nettet. Spesialkablene som skal forsvare Norge. *Vi Menn*. https://www.klikk.no/historie/hysj-nettet-6799389

Holm-Nilsen, S. & Wergeland, P. (2018, 24. september). «Knud» slo ut nødnettet: – Det er en skandale. *Nrk.no*. https://www.nrk.no/norge/_knud_-slo-ut-nodnettet_-_-det-er-en-skandale-1.14219126

Johansen, P. A. (2011, 12. oktober). Regjeringen tappet for store mengder data. *Aftenposten.no*. https://www.aftenposten.no/norge/i/PRyAb/regjeringen-tappet-for-store-mengder-data

Johansen, P. A. (2013, 17. mars). Spionerte på Telenor-sjefer, tømte all e-post og datafiler. *Aftenposten.no*. https://www.aftenposten.no/norge/i/P9d9e/spionerte-paa-telenor-sjefer-toemte-all-e-post-og-datafiler

Kessel, D. & Røsrud K. (2021, 8. februar). Østre Toten har vært uten datasystemer en måned etter hacking. *Nrk.no*. https://www.nrk.no/innlandet/kan-ta-et-halvt-ar-for-ostre-toten-a-rette-opp-dataangrep-1.15364106

Løland, L. R. (2016, 27. desember). Naudnettet svikta mange stader under «Urd». *Nrk.no*. https://www.nrk.no/vestland/naudnettet-svikta-mange-stader-under-_urd_-1.13293696

Manoj, B. S. & Baker, A. H. (2007). Communication challenges in emergency response. *Communications of the ACM*, *50*(3), 51–53. https://doi.org/10.1145/1226736.1226765

Meld. St. 29 (2011–2012). *Samfunnssikkerhet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld-st-29-20112012/id685578/

Meld. St. 10 (2016–2017). *Risiko i et trygt samfunn. Samfunnssikkerhet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

Meld. St. 28 (2020–2021). *Vår felles digitale grunnmur. Mobil-, bredbånds- og internettjenester.* Kommunal- og moderniseringsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-28-20202021/id2842784/

Nasjonal kommunikasjonsmyndighet. (2016). *EkomROS 2016. Risikovurdering av ekomsektoren* (Rapport). https://www.nkom.no/rapporter-og-dokumenter/ekomros-2016

Nasjonal kommunikasjonsmyndighet. (2017). *Robuste og sikre nasjonale transportnett – målbilder og sårbarhetsreduserende tiltak* (Rapport, versjon 2.0, offentlig versjon).

https://www.regjeringen.no/contentassets/e5a6166743d949e8a703f9feae23dc0f/robin_rapport.pdf

Nasjonal kommunikasjonsmyndighet. (2019). *Ekomutfall i Finnmark. Sjøfiberbrudd og feil i forbindelse med planlagt arbeid på Telenors sentral i Vadsø 30. november 2018* (Rapport). https://www.nkom.no/aktuelt/nkom-kritiserer-telenor-etter-utfall-i-finnmark/_/attachment/download/72e01e51-7295-4fb9-a1cc-6ecf787014b3:40489a121cced350279f25c89875387586306f6d/Rapport - ekomutfall Finnmark 30 november 2018.pdf

NATO. (2017). *Allied joint doctrine for communication and information systems* (AJP-6, utg. A, versjon 1). North Atlantic Treaty Organization.

Norges vassdrags- og energidirektorat. (2012). *Første inntrykk etter ekstremværet Dagmar, julen 2011* (Rapport nr. 3/2012). https://publikasjoner.nve.no/rapport/2012/rapport2012_03.pdf

Norges vassdrags- og energidirektorat. (2014). *Naturfareprosjektet: Delprosjekt 2. Beredskap og krisehåndtering. Delrapport 2 – Krisestøtteverktøy CIM – Anbefalinger* (Rapport nr. 76/2014). https://publikasjoner.nve.no/rapport/2014/rapport2014_76.pdf

Norges vassdrags- og energidirektorat. (2017). *Erfaringer fra ekstremværet Tor. Sammenlignet med erfaringer fra Dagmar 2011* (Rapport nr. 41/2017). https://publikasjoner.nve.no/rapport/2017/rapport2017_41.pdf

NOU 2012: 14. (2012). *Rapport fra 22. juli-kommisjonen*. Statsministerens kontor. https://www.regjeringen.no/no/dokumenter/nou-2012-14/id697260/

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

Onslow, D. (2012). *Two-way radio success. How to choose two-way radios, and other wireless communication devices for your business* (3. utg., versjon 3.1). IntercomsOnline.com. https://www.intercomsonline.com/v/vspfiles/downloadables/Free-Two-Way-Radio-Book.pdf

Oslo Economics. (2015). *Konsekvensutredning – Alternativer for styrket robusthet i landsdekkende kjernenett* (Rapport). https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/3.pdf

Post- og teletilsynet. (2011). *Dobbelt fiberbrudd i Telenors nett 23. mai 2011* (Rapport).

Post- og teletilsynet. (2012). *Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar* (PT-rapport nr. 2/2012). https://www.regjeringen.no/globalassets/upload/sd/ekstremvaeret_dagmar.pdf

PricewaterhouseCoopers (PwC). (2014). *Evaluering av brannene: Lærdal, Flatanger og Frøya* (Rapport). https://www.regjeringen.no/contentassets/1a669996f90945ba88e2ad3d11153774/brannevaluering.pdf

Riksrevisjonen. (2010). *Dokument 1 (2010–2011): Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2009*. https://www.stortinget.no/globalassets/pdf/dokumentserien/2010-2011/dok1-201011.pdf

Rimstad, R., Njå, O., Rake, E. L. & Braut, G. S. (2014). Incident command and information flow in a large-scale emergency operation. *Journal of Contingencies and Crisis Management, 22*(1), 29–38. https://doi.org/10.1111/1468-5973.12033

Saunders, S. R. & Aragón-Zavala, A. (2007). *Antennas and Propagation for Wireless Communication Systems* (2. utg.). Wiley.

Solbakken, H. A. (2021, 8. februar). Sensitiv pasientinformasjon kan være på avveie etter dataangrep. *Nrk.no*. https://www.nrk.no/innlandet/ostre-toten-kommune-angrepet-av-hackere-_-pasientinformasjon-og-helsedata-kan-vaere-pa-avveie-1.15321398

Stortinget. (2020, 8. oktober). *IT-angrepet på Stortinget: Potensielt skadeomfang er vurdert*. https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2020-2021/it-angrepet-pa-stortinget-potensielt-skadeomfang-er-vurdert/

Stortinget. (2021, 10. mars). *Stortinget utsatt for IT-angrep*. https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2020-2021/stortinget-utsatt-for-it-angrep/