FFI-rapport 2015/01926

«Med krisekommunikasjonsplanen i lomma» – mobilapplikasjoner til krisehåndtering i totalforsvaret

Janne Hagen og Hilde Hafnor

FFI Forsvarets forskningsinstitutt

«Med krisekommunikasjonsplanen i lomma» – mobilapplikasjoner til krisehåndtering i totalforsvaret

Janne Hagen og Hilde Hafnor

Forsvarets forskningsinstitutt (FFI)

29. mars 2016

FFI-rapport 2015/01926

1343

P: ISBN 978-82-464-2712-6
E: ISBN 978-82-464-2713-3

Emneord

Informasjon og kommunikasjon

Mobilkommunikasjon

Samfunn og sikkerhet

Totalforsvar

Nettverksbasert forsvar

Godkjent av

Hilde Hafnor	Forskningsleder
Anders Eggen	Avdelingssjef

Sammendrag

FFI-prosjektet «Smart samhandling i det nye informasjonslandskapet» (Sinett) setter søkelyset på militært-sivilt samarbeid og mer effektiv samhandling i Forsvaret ved bruk av sivil teknologi som smarttelefoner, skytjenester og mobilapplikasjoner (apper). Mobilteknologi har vist seg å ha et stort potensial som samhandlingsverktøy ved større internasjonale katastrofer. Denne rapporten diskuterer mulighetene for å ta i bruk mobilapplikasjoner som ledd i arbeidet med å håndtere kriser i Norge. Spesielt ser rapporten på mulighetene for å bruke mobilapplikasjoner som verktøy for krisekommunikasjon. Innledningsvis stiller vi derfor forskningsspørsmålet: Hva er mulighetsrommet for bruk av mobilapplikasjoner i sivil-militær krisehåndtering?

I kriser vil beslutningstakere typisk oppleve informasjonsunderskudd som innebærer for dårlig tid til vurdering og generelt stor usikkerhet. Usikkerheten er knyttet til situasjonen og til informasjonen som blir presentert. Den store utbredelsen av smarttelefoner gir muligheter til å utvikle mobilapplikasjoner som kan bedre situasjonsforståelsen. Smarttelefoner gjør det mulig å dele sanntidsinformasjon uavhengig av geografisk sted. Brukerne trenger bare internettilknytning. Mobilteknologien bidrar dermed til bedre situasjonsforståelse og beslutninger. Bruk av mobilteknologi kombinert med skytjenester gir også potensial for å utvide kapasiteten og tilby tilgjengelighet «overalt». Samtidig reiser bruk av denne typen sivil teknologi noen sikkerhetsmessige spørsmål. En annen utfordring er gyldigheten til og kvaliteten på data som finnes åpent tilgjengelig på internett.

Rapporten ser spesielt på krisekommunikasjon. Innenfor dette området finnes det allerede mange verktøy for å utvikle apper. Dessuten finnes det både gratis og kommersielle apper for krisekommunikasjon. Selv om disse appene har mange gode funksjoner, er de ikke designet for å dekke det norske totalforsvarets behov for funksjonalitet og sikkerhet. De kan likevel inspirere til å utnytte det potensialet som mobilteknologi etter hvert representerer når det gjelder å oppnå mer fleksible løsninger og å få informasjonen nærmere brukeren og de oppgavene som skal løses. Med dette som bakteppe presenterer rapporten et mulig konsept for å gjøre informasjon og funksjonalitet tilgjengelig i form av mobilapplikasjoner til krisehåndtering i totalforsvaret.

Rapporten konkluderer med at det er et stort mulighetsrom for å utnytte mobilteknologi med tanke på å oppnå mer fleksible løsninger og for å tilgjengeliggjøre informasjon helt ned på enkeltmannsnivå i sivil-militær krisehåndtering. Dette vil også kunne styrke nærhetsprinsippet ved at man blir i bedre stand til å kunne utføre og ferdigstille en økende mengde av oppgaver på stedet, forutsatt at infrastrukturen sørger for at informasjonen når fram til brukeren. I det videre forskningsarbeidet vil det være naturlig å se på muligheten for å utvikle en eller flere demonstratorer som kan bidra til å øke kunnskapen ytterligere på dette området, også på infrastruktursiden og bakenforliggende systemer. Dette vil øke kunnskapen ikke bare innenfor temaer som informasjonsdeling, situasjonsforståelse og samhandlingsevne internt i totalforsvaret, men også innenfor området strategisk kommunikasjon som eksempelvis informasjon til offentligheten.

English summary

The FFI project ”Smart collaboration in the new information landscape” explores civil-military collaboration and more effective military cooperation by using civil technology like smart phones, cloud services and mobile phone applications. Smart phone technology has proven to be an effective tool in crisis management in international catastrophes. The report describes the opportunities for using smart phones, mobile applications and eventually cloud services in crisis management in Norway. The report focuses in particular on the technological opportunities in crisis communication. The report addresses the following research question: *What are the opportunities to use smart phones and apps as tools for crisis management and civil-military collaboration?*

Catastrophes are stressful situations where the decision makers, first responders, military staff and civil stakeholders are challenged by lack of timely and relevant information, time pressure and a high degree of uncertainty. The uncertainty is related to the huge amount of available information. The widespread dissemination of smart phones among the population provides, however, unused opportunities for stakeholders and crisis responders to share real time information across the civil and military sector. Mobile technology and mobile apps provide opportunities to produce a shared situational awareness and improve the decision making. Smart phones and cloud services offer opportunities for scalability of services and availability everywhere as long as you have an internet connection. The use of such technology raises at the same time some basic security questions. Another challenge is related to the validity and quality of data found on the Internet.

Crisis communication is an area where there are already several tools for developing mobile apps. In addition, there are free and commercial apps available. Even though these apps offer many services, they are still not designed to serve the specific need of the Norwegian civil emergency preparedness or the needs of the defense sector. Current available apps can however inspire future developments within mobile technology in order to provide increased flexibility and user-centric solutions.

The report concludes that there are considerable opportunities for leveraging mobile technology to achieve more flexible solutions and to make information available down to the individual level in civil-military crisis management. This will also strengthen the stated aim that those closest to the incident should be able to handle it locally (“nærhetsprinsippet” in Norwegian), provided that the underlying infrastructure ensures that the information reaches the user.

Further research work will be directed towards the development of one or more demonstrators that can contribute to increased knowledge in this field, including the infrastructures and back-end systems. The work should not be limited to information sharing, situational awareness and civil and military collaboration, but should also cover topics like strategic communication and information to the public.

Innhold

Forord

Norge er blant de land i verden der digitaliseringen har kommet lengst. Digital Agenda for Norge, utgitt av Kommunal og moderniseringsdepartementet (KMD), skisserer et høyt ambisjonsnivå og en målsetning om fortsatt digitalisering. I henhold til rapporten Global Cyber Security Index & Cyberwellness Profiles (2015) rangerer Norge som nr. 1 i Europa og nr. 5 på verdensbasis. Denne sammenligningen viser at Norge, sett opp mot andre land, ligger godt an med tanke på å ha på plass nødvendig lovverk innenfor cyber, ha tekniske systemer og organisasjoner på plass, samt ha etablert samarbeid mellom offentlige etater. Det er ikke alle land som har en slik «infrastruktur» på plass. Selv om kommunikasjonsinfrastrukturen er sårbar for både naturgitte og menneskelige trusler, slik som det framgår av NOU 2015:13 «Digital sårbarhet – sikkert samfunn», er det viktig å se på de mulighetene som teknologien tross alt gir.

Rapporten bygger videre på FFIs forskning på samhandling i nettverk og Nettverksbasert Forsvar, og forskning på samfunnssikkerhet og cybersikkerhet. Samfunnssikkerhetsforskningen især har vist at totalforsvaret mangler digitale mobile verktøy til krisehåndtering og krisekommunikasjon. Den brede utbredelsen av smarttelefoner og Norges modning i forhold til digitalisering representerer et mulighetsrom, men også noen utfordringer.

Rapporten oppsummerer kunnskapsstatus og skisserer et mulig konsept for mobilapplikasjoner som krisehåndteringsverktøy. For å illustrere konseptet, tar rapporten utgangspunkt i en app for krisekommunikasjon.

Rapporten er skrevet som en del av «Smart samhandling i det nye informasjonslandskapet» (Sinett 3.0)-prosjektet og «Cybermakt og informasjonsoperasjoner i et nytt trusselbilde» (CITRUS)-prosjektet ved FFI. Vi vil takke våre kollegaer Bård Reitan, Ann-Kristin Elstad, Sigmund Valaker, Federico Manchini, Henning André Søgaard, Torgeir Broen, Bjørn Olav Knutsen og Frank Trethan Johnsen for kommentarer til rapporten.

17. februar 2016

Janne Hagen og Hilde Hafnor

1 Innledning

Økt krav til effektiv samhandling mellom nivåer og på tvers av domener, spesialiteter og profesjoner er stadig oftere fremhevet som løsningen på fremtidens utfordringer, både i militær og sivil sektor og i samvirket mellom dem. Moderne informasjons- og kommunikasjonsteknologi (IKT) blir ofte i samme åndedrag trukket frem som et av de viktigste virkemidlene for å få til en betydelig økt samhandlingsevne. Samtidig opplever man at mye av arven i militær og offentlig sektor, i form av teknologiske silosystemer og "høye hierarkier", forsinker informasjonsflyt og hemmer evnen til samhandling.

Ser man dette i et totalforsvarsperspektiv vil det å sammenkoble militære og sivile aktører helt ned på enkeltmannsnivå via digitale nettverk og tjenester kunne bli av stor betydning for den *operative samhandlingsevnen* i nasjonal krisehåndtering. Det å ha tilgang til og dele informasjon der man til enhver tid er, fremkommer som et stadig sterkere behov og krav i operativ virksomhet ettersom både trusselbildet og mangfoldet av oppgaver stadig endrer seg. Med billige og brukervennlige håndsett, stadig bedre nettverk og mer fleksible sikkerhetsløsninger, kompetente brukere og et økende spekter av tjenester og tilfang av informasjon, vil dette kunne representere et viktig element i arbeidet med å etablere mer effektive samarbeidsmekanismer mellom Forsvaret og det sivile samfunn i totalforsvaret.

FFI-prosjektet «Smart samhandling i det nye informasjonslandskapet» (Sinett 3.0) setter søkelyset på sivilt-militært samarbeid i en nettverksbasert kontekst, og mer effektiv samhandling i Forsvaret ved bruk av sivil teknologi som smarttelefoner, skytjenester og mobilapplikasjoner. Slik teknologi anses som et godt utgangspunkt når Forsvaret skal samhandle med sivile aktører. Mobil-applikasjoner har også vist seg å ha et stort potensial som samhandlingsverktøy ved større internasjonale katastrofer. I denne rapporten diskuteres mulighetsrommet for å ta i bruk mobil-applikasjoner som ledd i arbeidet med å håndtere kriser i Norge. Spesielt ser rapporten på mulighetsrommet for å bruke mobilapplikasjoner som verktøy for krisekommunikasjon.

1.1 Bakgrunn

I forsvarsforskningen nasjonalt og internasjonalt samt i Forsvaret generelt, kan vi observere flere aktiviteter som har å gjøre med økt operativ utnyttelse av sivil kommunikasjonsteknologi og metoder. Av aktiviteter i Forsvaret kan for eksempel nevnes LTE-mulighetsstudien (CYFOR, 2015) og det pågående eksperimentprosjektet EP 1667 *SMART – Gjennomgående felles situasjonsbilde på enkeltmannsnivå*. Fra internasjonale aktiviteter nevnes det nederlandske PROMISE[1]-prosjektet (Promise, 2015). Dette prosjektet har tatt frem og eksperimentert med en kommando og kontroll (K2)-løsning basert på kommersielle smarttelefoner/nettbrett og tilgjengelige apper, men med tilpasset operativsystem, for å se på egnetheten av sivil teknologi i militær K2. Erfaringene fra PROMISE er såpass lovende at det vil bli etterfulgt av PROMISE 2.0 i 2016 (Johnsen, 2016).

[1] Forkortelse for PROject Multi-Touch Information System Experiment.

Sinett-prosjektserien ved FFI har siden 2007, i et infrastruktur- og anvendelses perspektiv, studert hvordan teknologistøttet samhandling kan bli mer effektiv i det «nettverksbaserte» Forsvaret (NbF). Erfaringene fra prosjektet er relevante også med tanke på sivilt-militært samarbeid. Sinett-miljøet har gjennom flere år eksperimentert med ulike IKT-baserte løsninger, samhandlings-modeller og prosesser rundt informasjonsdeling fra den sivile sfære og introdusert dette til ulike oppgaver i det militære domenet for å vurdere muligheter og utfordringer ved teknologien. Resultatene har vært svært lovende og indikerer at her vil det være mye å hente. Eksempelvis viser prosjektets resultater fra tidligere studier knyttet til mobile informasjonsplattformer at det er høye forventninger til bruk av teknologi som smarttelefon/nettbrett, tjenester og samhandlings-modeller fra den sivile sfære inn mot militære og sivil-militære oppgaver, men at det per i dag har liten kompatibilitet med dagens militære prosesser og måter å jobbe på.[2] På samme tid avdekker resultatene at teknologien allerede er i operativ bruk "under radaren" fordi den oppleves som så nyttig og nødvendig at den tvinger seg frem utenom de offisielt støttede teknologiene. Bruken blir da noe "ukontrollert" og ufokusert.[3] Dette er en type bruk som mest sannsynlig ikke vil forsvinne, fremtidig bruk av smarttelefoni for militære applikasjoner forventes heller å øke, men Forsvaret kan ved enkle grep gjøre denne bruken «mer riktig» og mindre risikofylt. Videre bør det være mulig offisielt å legge til rette for at denne teknologien konstruktivt kan benyttes inn i nye samhandlingsarenaer og bidra til mer effektive måter å samhandle på.

I eksperimentene har prosjektet brukt kombinasjoner av kommersielle og egenutviklede løsninger (demonstratorer). En av demonstratorene utviklet i prosjektet er et teknologisk rammeverk og økosystem for utvikling av mobilapplikasjoner for Forsvaret (Mlab). I Mlab kan brukerne eksperimentere og bygge sine egne mobilapper uten å ha spesielle programmeringskunnskaper (Bergh, 2014, Bergh, 2015a, Bergh, 2015b). Den opprinnelige intensjonen med Mlab var å lage noe som Forsvarets høyskole (FHS) kunne bruke i Advanced Distributed Learning (ADL), men har forøvrig også vakt interesse utenfor forsvarskretser for å utvikle apper som ikke er spesifikt forsvarsrelaterte. Prosjektet har også utviklet et demonstratorsystem, Collective Environment Interpretation (CEI)-systemet, et slags «sosialt taktisk rapporteringssystem" som har en Android-app. I CEI blir all informasjon (egen posisjon, egenrapporterte observasjoner og kommentarer) presentert i en ny type felles situasjonsbilde. Systemet legger opp til interaktive prosesser i situasjonsbildet hvor man i fellesskap bygge et bilde i sann tid, som i sum representerer en kollektiv fortolkning av miljøet. Ved å tilrettelegge for en gjennomgående felles dialog rundt elementer i operasjonsmiljøet skal det bidra til en bedre og mer dynamisk fortolkning av situasjonen og til økt felles situasjonsforståelse. CEI betraktes som en demonstrator for en ny klasse kommando, kontroll og informasjonssystemløsninger (K2IS) som vektlegger åpenhet, høy tilgjengelighet, enkelhet i bruk og som virker på mobile plattformer. [4] Essensen ligger på det vi

[2] Se for eksempel Elstad A-K og B.K. Reitan: "Mobile information platforms in the military domain", *NOKOBIT* 23 (2015).
[3] I Forsvaret gir dette opphav til det man kaller «*Shadow IT*» eller «*Stealth IT*».
[4] Reitan, et al., En ny klasse kommando og kontroll informasjonssystemer (K2IS) – eksperimenter med smarttelefoner og samhandling, FFI-rapport 2015/02298

kaller datasentriske løsninger som gir økt organisatorisk og operativ fleksibilitet[5] og som bygger på åpen og tilgjengelig teknologi.[6] Videre har prosjektet også utviklet metoder og gjennomført empiriske studier med fokus på sammenheng mellom struktur og prosess (kongruens), fleksibilitet, tillit, bruk av samhandlingsteknologi og organisatorisk effektivitet i Forsvaret.[7]

Sinett-prosjektets resultater kan derfor være interessante også med tanke på forskning på krisehåndtering i en sivil-militær kontekst. Prosjektet setter søkelyset på sivilt-militært samarbeid og bruk av sivil teknologi som smarttelefoner, skytjenester og mobilapplikasjoner (apper). Slik teknologi anses som et godt utgangspunkt når Forsvaret skal samhandle med sivile aktører. Erfaring fra internasjonalt nødhjelpsarbeid har også vist at selv i store katastrofer kan denne type teknologi være nyttig og bidra til et bedre felles situasjonsbilde og til mer effektiv ressursbruk[8]. Bruk av slik teknologi er også forbundet med risiko; herunder risiko for avlytting, ubevisst bruk av manipulerte data, og ikke minst avhengighet av en sårbar sivil kommunikasjonsinfrastruktur. Likevel, og til tross for mulige utfordringer, er teknologien i så bred bruk internasjonalt, at også Forsvaret bør vurdere hvordan den kan understøtte Forsvarets operasjoner og samarbeidet med sivile aktører. Særlig interessant blir teknologien i grenseflaten mellom sivile og militære aktører og det samarbeidet som er nødvendig når Forsvaret skal bistå i sivilt hjelpearbeid.

I henhold til Forsvarssjefens Militærfaglige Råd (FMR)[9] må «*Forsvaret fortsette å investere i ny og avansert teknologi, som åpner for nye måter å løse oppgaver på. Når teknologien tillater nye systemer, som gir tilsvarende eller større effekt til lavere kostnader, bør erstatning av dagens løsning iverksettes. Utviklingen innen enkelte kategorier materiell, for eksempel IKT, skjer meget hurtig og krever tilsvarende hurtig utskiftning i Forsvaret for å være relevant. Innen denne kategorien og enkelte andre er det formålstjenlig med systemer utviklet på grunnlag av tilgjengelig sivil teknologi for å redusere investerings- og driftskostnadene for Forsvaret*.» Denne rapporten diskuterer derfor muligheter og utfordringer i tilknytning til bruk av mobilteknologi og apper for sivilt-militært samarbeid innenfor krisehåndtering. Vi har valgt å anskueliggjøre mulighetsrommet ved å fokusere på krisekommunikasjon spesielt. Denne aktiviteten er felles med FFIs prosjekt Cybermakt og informasjonsoperasjoner i et nytt trusselbilde (CITRUS).

1.2 Problemstilling

I følge Direktoratet for samfunnssikkerhet og beredskap (DSB) vil offentlige og private virksomheter kunne bli involvert i flere forskjellige typer kriser i framtiden. Noen er så store at de defineres som samfunnskriser; da er en rekke myndighetsorganer involvert, og koordinering av

[5] Det vil si støtter flere formater og i stor grad frakoblet organisasjonens hierarki og operasjonsmønster.
[6] Se Reitan, 2010; Karlsen og Reitan, 2014, Reitan et al. 2015a, Reitan et al. 2015b.
[7] Bjørnstad, A. L., og Elstad, A-K., Utvikling og evaluering av spørreskjema med fokus på organisasjon og bruk av samhandlingsteknologi, FFI-rapport 2015/00046, og Elstad, A-K et al., Erfaringsrapport – analysestøtte knyttet til organisasjon og samhandling under Gram-øvelsene 2011–2013, FFI-rapport 2015/00045.
[8] Hagen, J.M. og V.Q, Pham, Brannvesenets behov for robust informasjonsinfrastruktur for samhandling i krisesituasjoner, Kjeller: FFI-Rapport 2014/01704.
[9] Forsvarsjefens fagmilitære råd, Forsvaret, 2015: 25.

situasjonsbilder, medieuttalelser og ansvarsforhold blir komplisert og utfordrende. Andre kriser håndteres mer lokalt og av få myndigheter, mens det finnes kriser (eksempelvis ulykker og branner) som kun rammer én enkelt virksomhet[10].

Rapportens formål er å studere mulighetsrommet for bruk av mobilapplikasjoner til krisehåndtering, og krisekommunikasjon spesielt. Dette gir følgende forskningsspørsmål:
Hva er mulighetsrommet for bruk av mobilapplikasjoner i sivil-militær krisehåndtering?

- Hva finnes av gratis og kommersielle mobilapplikasjoner for krisekommunikasjon og hvilke behov dekker disse løsningene?
- Hva vil være de største mulighetene og utfordringene for å ta i bruk slik teknologi?
- Hvilket informasjonsbehov kan dekkes av mobilapper?

1.3 Metode

Vi har valgt en utforskende tilnærming til alle tre problemstillingene og diskuterer de utfordringer som totalforsvaret har når det gjelder samhandling i kriser opp mot de muligheter som sanntids-deling av informasjon på tvers av etater kan gi.

Samhandlingsutfordringene er av både organisatorisk og teknologisk karakter. De organisatoriske utfordringene er skapt over lang tid som følge av ansvarsdeling, sektorlovverk og organisasjons-kultur i ulike offentlige etater. De teknologiske utfordringene er gitt som følge av lang tids utvikling av IKT-arkitekturen i offentlige etater, der ulike etater har valgt IT-løsninger som ikke kan kommunisere med hverandre.

Rapporten bygger på litteraturstudier og informasjon som finnes i forskningsdatabaser og åpent tilgjengelig på internettet.

1.4 Rapportens oppbygging

Kapittel 2 gir en introduksjon til krisehåndtering og lærdom fra kriser.

Kapittel 3 gir en introduksjon til totalforsvaret og sivilt-militært samarbeid, og hvilke utfordringer Totalforsvaret har når det gjelder samhandling og bruk av IKT.

Kapittel 4 diskuterer begrensninger og muligheter for krisekommunikasjon.

Kapittel 5 gir en oppsummering av app-utvikler verktøy og noen eksempler på mobilapper som andre har utviklet. Disse appene dekker krisekommunikasjon og omdømmestyring. De er valgt ut kun som eksempler, ikke fordi vi har rangert dem som de beste. I tillegg gis en oversikt over verktøy for opinionsanalyse som kan ha relevans for krisekommunikasjon og kontroll med narrativets utvikling.

[10] *Tema. Risiko- og krisekommunikasjon*, September 2014. Rapport utgitt av Direktoratet for samfunnssikkerhet og beredskap (DSB), s 10.

Kapittel 6 drøfter begrensninger om muligheter for bruk av mobile applikasjoner i krisehåndtering.

Kapittel 7 presenterer en idé til et konsept for å utvikle en mobilapplikasjon for krisekommunikasjon. Konseptet er utviklet for bruk i totalforsvaret.

Kapittel 8 oppsummerer konklusjonen og skisserer veien videre.

2 Lærdom fra reelle kriser

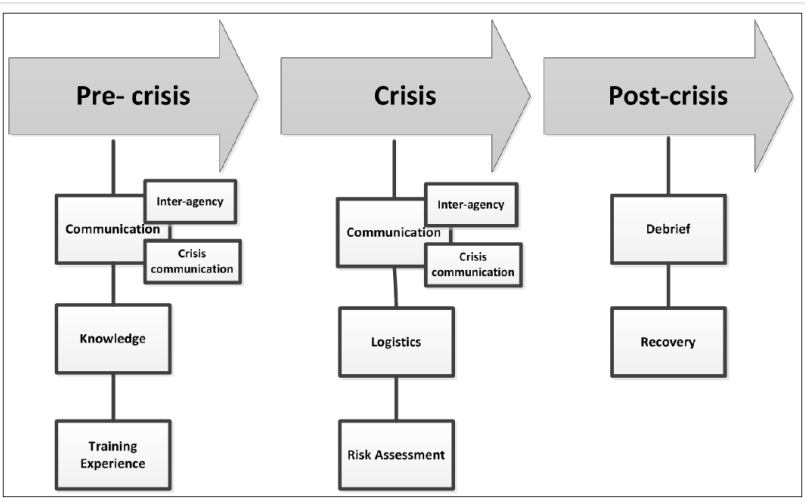
FFIs forskningsmiljø på samfunnssikkerhet har deltatt i prosjektet ELITE (Elicit to learn crucial post-crisis lessons) [11], finansiert av den europeiske unionen (EU). Erfaringene herfra dekker kun naturkatastrofer. Prosjektet samlet erfaring fra henholdsvis skogbranner[12], jordskjelv og flom. Store jordskjelv har hatt enorme skadevirkninger i de samfunn der en er rammet av katastrofen. Tilsvarende har flom og branner i Norge hatt store konsekvenser for befolkning og infrastruktur. Eksempler er flommen i pinsen 2011 og brannene i Lærdal og i Flatanger (2014).

Erfaringene som er innhentet i ELITE-prosjektet kan være til nytte, også for arbeidet med sivil-militær krisehåndtering. Utfordringene i jordskjelvkatastrofer er relatert til (i) kommunikasjon (både kommunikasjon på tvers av etater og krisekommunikasjon), (ii) kunnskap og opplæring av redningspersonell før krisen, (iii) logistikk og risikovurdering under selve krisen, og (iv) mangel på gjennomganger, samt gjenoppbygging av lokalsamfunnet etter krisen har funnet sted.[13]

Utfordringene i forbindelse med flom er (i) bevisstgjøring gjennom kampanjer og utdanning, (ii) kommunikasjon til befolkningen både før og under krisen, (iii) planlegging og øvelser som tester planene, (iv) opplæring og klare lover og regler om ansvarsfordeling mellom etater, (v) koordinering og samvirke på tvers av organisasjoner og etater, (vi) holistisk læring på hvordan en kan forbedre håndteringen, (vii) informasjonshåndtering, (viii) utstyr og infrastruktur og (ix) beslutningsprosesser og finansiering.[14]

ELITE-Prosjektet har oppsummert noen erfaringsområder i figur 2.1.

[11] Tonje Grunnan og maren Maal, Lessons learned and best practices from crisis management of selected natural disasters – elicit to learn crucial post-crisis lessons, FFI-rapport 2014/01993.
[12] Maren Maal og Tonje Grunnan, Lessons learned from crisis management of forest fires – elicit to learn crucial post-crisis lessons, FFI-rapport 2014/01969.
[13] Maren Maal, Tonje Grunnan, Maria Rosaria Gallipoli, Sabatino Piscitelli, Angelo Masi and Marco Mucciarelli, Lessons learned from crisis management of earthquakes – elicit to learn crucial post-crisis lessons, FFI-rapport 2014/01972.
[14] Maren Maal og Tonje Grunnan, Lessons learned from crisis management of floods – elicit to learn crucial post-crisis lessons, FFI-rapport 2014/01973.



Figur 2.1 Problemområder i ulike faser av en krise

I denne figuren er krisekommunikasjon avgrenset til kommunikasjon overfor befolkningen. Figuren illustrerer problemområder som teknologi og informasjonstilgang kan bidra til å løse.

FFI har gjennom mange års forskning på beskyttelse av samfunnet identifisert lignende utfordringer i kriser som er av sikkerhetspolitisk karakter der sabotasjeaksjoner inngår som en del av motpartens virkemiddelbruk.[15] Erfaringene fra denne forskningen er til dels sammenfallende med de erfaringene som også er pekt på i ELITE-prosjektet.

3 Totalforsvaret og sivilt-militært samarbeid

3.1 Totalforsvaret og prinsippene for sivil beredskap

Totalforsvarskonseptet ble skapt i etterkant av 2. verdenskrig, da Norge som stat erfarte at man ikke klarte å forsvare landet med militære styrker alene. Hele samfunnets ressursbase måtte kunne utnyttes, både offentlige og private, militære og sivile, og ressursene måtte kunne skaleres. Dette krevde et tett sivilt-militært samarbeid, spredt over hele landet. Det krevde at staten hadde lover og forskrifter som ga nødvendige fullmakter og et beredskapsplanverk på sivil og militær side. Et slikt beredskapsplanverk finnes også den dag i dag, og planverket er gjenstand for regelmessige revisjoner og øvelser. På sivil side har vi Sivilt beredskapssystem (SBS) som Justis og beredskapsdepartementet er ansvarlig for, og på militær side finnes et tilsvarende planverk, beredskapsplan for Forsvaret (FBS). Begge planene er harmonert med North Atlantic Treaty Organization (Nato) sitt planverk. Som en del av beredskapen har Norge en rekke lover som gir Staten utvidede fullmakter ved behov, eksempelvis Rekvisisjonsloven.[16]

[15] Endregaard et. al., 2015; Hagen, 2015 Endregaard, M., Brattekås, K., Nystuen, K.O., Sandrup, T. og W. Gerhardsen (Ed.)., Beskyttelse av samfunnet i en ny tid, Kjeller: Viten, Forskningsfaglig rapport 1, 2015, og Hagen, J. M., Beskyttelse av samfunnet og digital sårbarhet: BAS-prosjektenes bidrag til samfunnssikkerhetsarbeidet i Norge over 20 år – kompendium for undervisning ved Universitetet i Nordland, Kjeller: FFI-Notat 2015/02111.

[16] Rekvisisjonsloven, https://lovdata.no/dokument/NL/lov/1951-06-29-19?q=rekvisisjon, nedlastet 22.1.2015 og Meld. St. 23 (2012-2013) Digital agenda for Norge – IKT for vekst og verdiskaping.

Nasjonal sivil beredskap bygger videre på fire prinsipper:

- *Nærhetsprinsippet*, som betyr at krisen skal håndteres der den geografisk oppstår, for eksempel skal en flom i Østerdalen håndteres av virksomhetene og kommunen som er rammet, og dersom den går over flere kommuner, kan fylkesmannen samordne på tvers av kommuner.
- *Ansvarsprinsippet*, som betyr at den som har ansvar i fred skal også ha ansvaret i en krise. Dette gjelder de aller fleste tilfeller, men i visse situasjoner, eksempelvis ved krig, kan Forsvaret blant annet ta over driften av luftrommet.
- *Likhetsprinsippet*, som betyr at man skal ha samme organisasjon i fred som i krise/krig. Samme organisasjon skal ha ansvar i normalsituasjoner som i krisesituasjoner. I praksis foregår det likevel en viss omorganisering internt i virksomheter i det tidspunktet beredskapsorganisasjonen i virksomheter, eksempelvis i kommuner, trer i kraft. Beredskapsorganisasjonen trer i kraft først når krisen oppstår, og avsluttes når krisen er avsluttet. Det er viktig her at ansvaret uansett ikke endres.
- *Samvirkeprinsippet*, som fikk styrket oppmerksomhet og betydning etter 22. juli 2011 innebærer en plikt til å samarbeide. Samvirkeprinsippet er ikke noe nytt og har fungert mellom nødetatene i årevis.

Selv om intensjonen med prinsippene er gode, har historien vist at prinsipper blir utfordret ved kriser som oppstår hurtig og overraskende, og de blir også utfordret når hendelsene involverer mange aktører, ulike sektorer og geografiske områder utover kommunegrensen. Alle omorganiseringene i staten på både militær og sivil side representerer imidlertid utfordringer. Forsvaret er for eksempel gjennom en omstilling hvert fjerde år. På sivil side er bildet litt mer sammensatt. Hver omorganisering betyr en endring i teknologi, organisasjon eller begge deler, og relasjoner en er avhengig av i krisehåndteringsarbeidet må etableres og øves på nytt. Justisdepartementet kjører sin prosess innenfor samfunnssikkerhet med meldinger som de siste årene har vært samkjørt mot Forsvarets langtidsplanlegging. Men det er viktig å peke på at under dette overordnede bildet ligger mange initiativer til omorganisering i de enkelte sektorene. Vi kan nevne Brannstudien som så på organisering av brannvesenet, Politistudien og arbeidet med sammenslåing av kommunene (kommunereformen). I tillegg kjører også Kommunal- og moderniseringsdepartementet (KMD) en prosess på digitalisering av offentlig forvaltning gjennom Digital Agenda for Norge og rundskriv fra KMD til alle statlige etatene.[17] Slike initiativer er med på å endre rammebetingelsene for praktisk samhandling i totalforsvaret og for sivilt militært samarbeid ved at ansatte flyttes og formelle organisasjoner og beslutningsstrukturer endres.

3.2 «Silosystemer» i offentlig sektor vanskeliggjør god informasjonsdeling

Virksomhetsinterne IT-systemer i offentlig sektor må forstås utfra de konstitusjonelle betingelsene sektoren operer under. Hver minister er ansvarlig for sitt departement. Hvert

[17] Se Meld. St. 23 (2012-2013) Digital agenda for Norge – IKT for vekst og verdiskaping, og *Digitaliseringsrundskrivet*, 26. august 2014

departements fullmakter er gitt av de lover som departementet forvalter og er underlagt. Olje- og energidepartementet (OED) er for eksempel forvalter av Energiloven, men er underlagt Personopplysningsloven, Forvaltningsloven og Sikkerhetsloven, som gjelder alle offentlige etater. Lovtekster er videre spesifisert og detaljert i forskrifter. Ulike lover henviser til hverandre, og unntak fra loven gis i visse tilfeller, for eksempel kan en annen lov komme til anvendelse i visse situasjoner. Eksempel på unntak kan være at i Offentleglova, skal informasjon være offentlig tilgjengelig, men unntak gis for forhold av betydning for rikets sikkerhet. Det siste er videre regulert i Sikkerhetsloven, som også stiller sterke krav til separasjon av IT-systemer og at deling av informasjon skal skje kun til autoriserte personer og etter prinsippet om behovsprøving. Sikkerhetsloven er for tiden under revisjon av et regjeringsoppnevnt utvalg,[18] og utfallet av denne revisjonen kan også påvirke samhandlingsrommet for sivilt-militært samarbeid. Disse rammene gir regler for IT-systemer som inneholder klassifisert informasjon. Resultatet er adskilte systemer med begrensninger på tilgang. Dette omtaler vi som «silosystemer».

Organisasjoner som er underlagt Sikkerhetsloven og håndterer mye gradert informasjon, typisk Forsvaret, har en behovsprøvd tilnærming til informasjonsdeling, mens organisasjoner som i liten grad har sikkerhetsgradert informasjon, kan ha en annen tradisjon for deling av informasjon og åpenhet ut mot publikum. Forskjeller i kultur, normer og oppfatninger hos ansatte i ulike etater og virksomheter vil kunne påvirke tillit, informasjonsdeling og samhandling på tvers av de samme virksomhetene.

«Silo-utfordringer» skyldes ikke bare institusjonelt grunnlag, organisering og kultur. Noe av problemet er at over tid har staten tatt i bruk ulike informasjonssystemer. En rapport fra Metier[19] illustrerer dette. Rapporten peker på at det er seks ugraderte IKT-løsninger i departements-felleskapet. Et av dem er en felles plattform som driftes av Departementenes service senter (DSS) som 13 departementer benytter. Forsvarsdepartementet, Utenriksdepartementet, Justis- og beredskapsdepartementet, Finansdepartementet og Statsministerens kontor står imidlertid utenfor dette fellesskapet. De som står utenfor har samfunnskritiske funksjoner slik at nedetid må unngås, og de har også ansvar for mange små og store fagsystem med ulike graderingsnivå. I et samhandlingsperspektiv kan imidlertid dette medføre betydelig utfordringer i form av begrensninger eller forsinkelser i informasjonsdeling. Behovet for å bygge ned de tekniske barrierene er tilstede også på operativt nivå for eksempel mellom helsevesenet og politiet, der ulike lover og forskrifter regulerer beskyttelse av informasjon og deling av informasjon.

Det er en økende bevissthet omkring behovet for å redusere barrierene for samhandling på tvers. Et initiativ som tar sikte på å løse opp i dette problemet er Barents Watch samarbeidet. I dette tilfellet blir det arbeidet for en felles løsning mellom syv etater som tillater deling av sensitiv informasjon. Det skal bli etablert et Barents Watch lukket nett som gjør det mulig for Kystverket,

[18]Regjeringen oppnevner sikkerhetsutvalg, Pressemelding 27.3.2015, https://www.regjeringen.no/no/aktuelt/regjeringen-oppnevner-sikkerhetsutvalg/id2403919/

[19] Høie, Ø, Emblemsvåg, N. A., Melsether, T. Berg, L.S., Johansen, S., Kofoed, E. og I. Hagen, *KS2 (kvalitetssikring fase 2) av ny IKT-løsning for departementene*. Rapport til Finansdepartementet og Kommunal og moderniseringsdepartementet, 30. mai 2014.

Forsvaret, Politidirektoratet, Fiskeridirektoratet, Tolldirektoratet, m.fl. å dele sensitiv informasjon. Kystverket har prosjektledelsen og det er allerede utviklet et åpent nett som er satt i drift, se www.barentswatch.no. Systemet er et interessant eksperiment som vil kunne effektivisere samhandlingen sivilt-militært og på tvers av etatene innen miljø, kriminalitets- og fiskeri-overvåkning, for å nevne noen områder. Også Digital Agenda for Norge, som vi har omtalt tidligere, peker nettopp på å bygge ned barrierene mellom ulike etater ved hjelp av IKT: Brukernes kontakt med staten skal foregå primært digitalt, og ved å kople data fra ulike registre kan enkelte søknader eller rapporteringer gjøres automatisk uten brukerens medvirkning.

4 Krisekommunikasjon

4.1 Mobilkommunikasjon og smarttelefoner som bærebjelke i krisehåndteringen

Innenfor totalforsvaret har Forsvaret sin egen kommunikasjonsinfrastruktur, der bare noen få sentrale aktører i totalforsvaret har tilknytning. Forsvarets kommunikasjonsinfrastruktur er derfor primært et militært nett, og siden de fleste sivile samarbeidspartnerne ikke er tilknyttet dette nettet, vil det ha begrenset nytte for samhandling og informasjonsdeling sivilt-militært.

Sivile aktører kjøper sine kommunikasjonstjenester fra en eller flere sivile elektronisk kommunikasjon (EKOM)-tilbydere, og mobilt bredbånd er svært godt utbygd i Norge målt opp mot andel av befolkningen som har dekning. Det er noen få store transmisjonsleverandører i Norge, og Telenor er den viktigste. På radio-aksess nivå og på kommunikasjonstjenestenivå er det flere leverandører i markedet. Staten selv investerer tungt i Digitalt Nødnett, men dette er ikke tilgjengelig for alle offentlige etater. I dag er Digitalt Nødnett et system (et radio-aksess nett) som primært nødetatene bruker, men også andre virksomheter, herunder Røde Kors og kraftbransjen, er aktuelle brukere.

Gitt denne kompleksiteten på EKOM-infrastruktursiden, hvilken teknologi ender så ansatte i offentlige virksomheter med å bruke i sin samhandling sivilt-militært? FFI har tidligere pekt på at menneskene ender opp med å bruke mobiltelefonen[20] som kriseverktøy. Smarttelefoner og tilknytning til Internett via en nettleser gir tilgang til en rikdom av informasjon også for dem som skal håndtere en krisesituasjon. Digitale tjenester som tilbys av Google og andre aktører kan derfor være viktige ressurser for å finne fram til informasjon, for eksempel om bygninger og områder der hendelsen skjer, eller kommunisere med hverandre.

I EUs forskningsprogrammer blir det satset stort på forskning om hvordan IT-baserte samhandlingsverktøy for blant annet nødetatene skal utvikles. Prosjektene blir gjennomført som samarbeid mellom ulike akademiske institusjoner, industri og brukere i en rekke land. I mange tilfeller tar denne forskningen ikke inn over seg at disse systemene bygger på en sårbar kommunikasjonsinfrastruktur som kan svikte pga. uvær, overbelastning, menneskelige feil eller målrettede angrep. I stormene «Dagmar» og «Ivar» sviktet både kraftforsyning og EKOM, noe

[20] *Må ha mer enn mobil i kriser*, FFI Forum, weboppslag 27.11.2014.

som ga negative ringvirkninger for samhandlingen. Problemet er at det i mange sammenhenger "blir lagt alle egg i samme kurv", slik at en svikt i et system forplanter seg til mange systemer og brukere.

Selv om mobilnettet er sårbart, som dokumentert i NOU 2015:13 Digital sårbarhet – sikkert samfunn, viser erfaring fra større internasjonale kriser at kreativiteten er stor, selv i tilfeller der mye av kommunikasjonsinfrastrukturen er ødelagt. Smarttelefoner kan koples sammen og danne nettverk, og bruke hverandre som basestasjoner i et begrenset område. Dette omtales som mesh-nettverk. I internasjonale katastrofer arbeider digitale hjelpearbeidere fra hele verden på dugnad. De plotter informasjon sendt via short message system (SMS) eller epost fra lokalbefolkningen i katastrofeområder inn i åpne Google-kart. Slik bidrar frivillige både i og utenfor katastrofeområdet til bedre situasjonsforståelse og mer effektiv nødhjelp hos de mange bistandsarbeiderne.[21]

4.2 Informasjon på nett

Sosiale medier er blitt en integrert del av livet på nett og innenfor forretningslivet brukes sosiale medier til målrettet markedsføring. Sosiale medier har hatt en formidabel utvikling i antall brukere. Det er hevdet at 72 prosent av alle internettbrukere benytter seg av sosiale medier og 71 prosent kopler seg til via mobile enheter.[22] Sosiale medier gir dermed en rik tilgang til informasjon. Også innenfor norsk offentlig forvaltning og innenfor totalforsvaret har sosiale medier fått økt betydning som kommunikasjonskanal. I statens kommunikasjonspolitikk blir det slått fast at staten skal være tilstede på de samme kanalene som brukerne, og staten skal også ha dialog med brukerne – det skal ikke være bare enveiskommunikasjon. I praksis betyr dette at staten også skal være tilstede på sosiale medier. Statlig bruk av sosiale medier er vist i Tabell 4.1.

Tabell 4.1 Norske statlige virksomheters bruk av sosiale medier i prosent (kilde Statistisk Sentralbyrå)[23].

Type sosiale medier	2013	2014	2015
Nettsamfunn (Facebook o.a.)	68,8	75,4	75,5
Mikroblogger (Twitter o.a.)	61,5	66,5	67,2
Internettjenester for innholdsdeling (YouTube o.a.)	41	44,9	47,6
Digitale dugnadsarena (wikier o.a.)	13,7	21,2	19,2
Blogg på virksomhetens nettsider	35	33,5	35,4

Men kan vi stole på informasjon i sosiale medier? Informasjon som finnes på internettet vil kunne inngå som rådata i mobilapper som igjen leverer tjenester som skal brukes i krisehåndtering. Internett gir en rikholdig tilgang til informasjon og det pågår stadig utvikling av nye tjenester for å analysere og sammenstille informasjon som er tilgjengelig på nettet.

[21] Se Hagen og Pham, 2014.
[22] Cnaan Liphshiz, Israel Recruits 'army of Bloggers' to Combat anti-Zionist Web Sites, 19. Januar 2009.
[23] Statistisk sentralbyrå (SSB), Statistikkbanken, https://www.ssb.no/statistikkbanken/ nedlastet 03.02.2016.

Der er skjær i sjøen. Informasjonskvaliteten og påliteligheten varierer, og det er også en dualitet i måten informasjon blir brukt på. Strand og Hagen (2015)[24] peker på trusselen fra propaganda i det digitale samfunnet. I det 21. århundret har bruken av propaganda akselerert kraftig i takt med samfunnets digitalisering. Fremveksten av sosiale medier kan spre sann og usann informasjon til tusener og millioner av personer på brøkdelen av et sekund. Propaganda mot norske målgrupper, spesielt i potensielle eller faktiske konfliktsituasjoner, er derfor en faktor som Forsvaret og totalforsvaret i stadig større grad må forholde seg til. Studien viser hvordan propaganda dukker opp i «nye klær», gitt av den teknologiske utviklingen vi har opplevd i etterkant av internettets fødsel.

Internettet gir mulighet til å nå mange, samtidig som elektroniske systemer og logikk gir rom for manipulering. Det er for eksempel kjent at antall «Likes» kan manipuleres, kjøpes[25] eller til og med fås gratis. Å få «Likes» kan si noe om hvilken støtte en part har i en konflikt, men falske «Likes» kan bidra til å påvirke hva en kan se. Det er også tilfeller der bloggere er betalt og opererer for stater, som blant annet The Guardian har beskrevet i sin artikkel om russiske «nettroll»[26]. Men Russland er neppe alene om å utnytte mulighetsrommet som digitalisert informasjon på internett gir. Et annet eksempel er Israel, som også har engasjert flerspråklige bloggere for å kjempe sin sak på nettet. Hvor omfattende tvilsom bruk av nettet kan være framgår av en undersøkelse av Fortune 100 virksomhetene. Denne viser at 40 prosent av virksomhetene har falske Facebook-kontoer tilknyttet sin virksomhet, at 20 prosent av Twitter-kontoene er falske og spam på sosiale medier har økt med 658 prosent siden midten av 2013. I følge den refererte studien er hovedmålet til trussel-aktørene å stjele informasjon fra kunder, skade omdømmet, manipulere markedet eller drive ulike former for internettsvindel. Selv om denne analysen ble utført på Fortune 100-virksomheter, så er norske og mindre virksomheter i følge Norsis også utsatt for lignende trusler.[27]

Også myndigheter er villige til å gå langt. Dokumenter lekket av Edward Snowden avdekket at myndighetene overvåker blogger, websider og sosiale medier gjennom infiltrasjon, operasjon under falske flagg og ulike former for forstyrrelse (Greenwald, 2014). Overvåking og informasjonsinnsamling fra internett og annen kommunikasjon setter kildevernet i fare og gjør at den offentlige debatten kan bli «kjølt ned». De kritiske stemmene blir stille. Dette svekker medienes rolle som kritisk kontrollinstans og utarmer skapende og intellektuell kommunikasjon.

Et annet forhold er sentraliseringen av informasjon når mange for eksempel nås vis samme type tjeneste eller nettsamfunn. I en bloggartikkel peker den irakiske bloggeren Hossein Derakhshan[28] på utfordringen som sentralisering av informasjon på nett kan gi. Sosiale medier som eksempelvis Facebook og Twitter gir kun rom for å legge inn én link i teksten, noe som reduserer informasjonsrikdommen for brukeren. Det er algoritmene i sosiale medier, som basert på din

[24] Strand, O M, Hagen, J, *Med Propagandaens århundre unnagjort - hva er propagandatrusselen mot et digitalisert Norge*, FFI-rapport 2015/00811.
[25] Se for eksempel siden «Get your likes», https://www.getyourlikes.co.uk/ nedlastet 07.8.2015.
[26] Walker, S., "Salutin' Putin: inside a Russian troll house", 02.april 2015.
[27] Bakås, T.H., «Sosiale medier – en trussel mot virksomheter», Norsis, 2014.
[28] Derakhshan, H., "The web we have to save", Blog, 14 July 2015.

adferd på nett og hva du liker, bestemmer hva du får lese og se. Det bekymringsfulle er at disse algoritmene setter likhetstegn mellom nyheter, popularitet og viktighet. Når brukeren kan få tilgang til eksempelvis nyheter via Facebook, er det Facebook som bestemmer hvilke nyheter brukeren blir eksponert for. I en krisesituasjon kan dette forholdet være kritisk.

Statistisk sentralbyrå (SSB) (2015) har kartlagt bruk av sosiale medier i alle næringer i staten, og statistikken viser at bruken øker fra år til år. I 2015 rapporterte 87 prosent av statens virksomheter at de benytter en eller flere sosiale medier i kontakt med brukerne. 62 prosent av disse benyttet mediene til å rekruttere nye ansatte. Blant de største virksomhetene med mer enn 1 000 ansatte, var andelen hele 78 prosent. For 87 prosent av de statlige virksomhetene var formålet å utvikle virksomhetenes omdømme. Sosiale medier benyttes også til å gi brukerne mulighet til å påvirke virksomheten ved å gi tilbakemelding. 27 prosent av virksomhetene involverte brukerne i utvikling av tjenester gjennom sosiale medier. 57 prosent av virksomhetene brukte mediene til å innhente og svare på brukernes meninger og spørsmål. Den omfattende bruken av sosiale medier gir store muligheter for myndighetene på kommunikasjonsområdet, men har som vi har påpekt her, også potensielt noen begrensninger.

I konfliktsituasjoner strammes kampen om sannheten inn.[29] Fra et krisehåndteringsperspektiv er det viktig at aktørene i totalforsvaret er våkne og er kjent med både det brede spekteret av utfordringer og risikoen for å bli lurt. Det er også verdt å reflektere over begrensningene i sosiale medier, selv om de gir god funksjonalitet og også stor nytteverdi. En krisekommunikasjonsapp (demonstrator) for sivilt-militært samarbeid som "crawler" (leter) etter informasjon fra nettet, risikerer å videreformidle informasjon som er manipulert med forsett. Slike svakheter må derfor kompenseres for gjennom andre tiltak og prosedyrer.

4.3 Typer kommunikasjon

Vi velger å dele kommunikasjon inn i følgende kategorier:

- Proaktiv kommunikasjon herunder strategisk kommunikasjon[30]
- Løpende kommunikasjon – dette omfatter daglig presse og informasjonsaktiviteter
- Reaktiv kommunikasjon – dette omfatter informasjon når krisen har oppstått, og er nært koplet mot krisekommunikasjon.

La oss først se på den proaktive kommunikasjonen, strategisk kommunikasjon. Strategisk kommunikasjon gjør bruk av ulike virkemidler, både politiske, diplomatiske, økonomiske og militære. Strategisk kommunikasjon handler vel så mye om strategi som om kommunikasjon. Den er rettet mot ulike målgrupper, og forsøker å påvirke deres holdning og i ytterste konsekvens også atferd. Målgrupper kan utgjøre sivilbefolkningen i operasjonsområdet, alliansepartnere, egen befolkning, fiendtlige styrker, grupper som støtter fienden og nøytrale grupper. Strategisk

[29] Søgaard, H. A. og Hagen, J. M., *Kampen om sannheten*, FFI Fokus 02/2014.
[30] Hagen og Søgaard, Strategisk kommunikasjon som redskap i krisehåndteringen, Kjeller: FFI-Rapport - 2013/03101.

kommunikasjon er, slik Nato har definert det (2009),[31] en koordinerende funksjon innenfor påvirkningsrelaterte disipliner som nevnt ovenfor. Summen av tiltak bidrar til å nå strategiske mål overfor hver enkelt målgruppe; det handler om hvordan ord og handlinger blir oppfattet blant annet ved å forsikre seg om at det er et samsvar mellom det som blir sagt på en side, og det som blir gjort på den andre.

Det løpende kommunikasjonsbildet beskriver daglig presse og informasjonsaktiviteter. I dette ligger virksomhetens egne pressemeldinger og utadrettet virksomhet for å få oppmerksomhet om en sak, samt svar til journalister som henvender seg til virksomheten og vil ha informasjon om dagsaktuelle saker.

Når krisen er et faktum er virkeligheten preget av mangelfull situasjonsoversikt, for dårlig tid og stor grad av usikkerhet. Da vil det være nyttig å stille noen grunnleggende spørsmål slik en praktiker innenfor kommunikasjonsfaget ville gjort det:[32]

- Hva er saken?
- Hva er situasjonen sett fra ulike målgruppers ståsted (og hvem er disse målgruppene)?
- Hva er usikkerheten i vår situasjonsforståelse (informasjonskvalitet)?
- Hva er kommunikasjonsmålene (dvs. endringen en ønsker å oppnå)?
- Hva er veivalgene og hvordan skal vi angripe situasjonen? Her må det systematiseres mht. målgruppe, kommunikasjonskanal og middel.
- Hva er hovedbudskapet?
- Hvordan skal vi helt konkret gjøre arbeidet? Her er det snakk om tiltak som for eksempel å ha utarbeidet spørsmål og svar.

4.4 Utfordringer for krisekommunikasjon

Sviktende krisekommunikasjon kan bidra til å skape en informasjonskrise i kjølvannet av selve krisen. Et eksempel på dette er Deep Water Horizon skandalen i 2010 der topplederen i BP dro på yacht-race ferie, mens ansatte hadde omkommet og miljøkatastrofen vokste i omfang. Ulykken var ille, miljøkatastrofen var stor, men handlingen til lederen og de signalene han sendte ut gjorde at støynivået økte og omdømmet til BP fikk seg enda en knekk.[33] Erfaringer fra flere storulykker viser at med god krisekommunikasjon kan virksomheten komme godt ut omdømmemessig. Et eksempel på god håndtering er Statoils håndtering av In Amenas.[34] Topplederen var i dette tilfelle «på» og til stede, samt viste empati med de forulykkede og ikke minst handlekraft innenfor de rammer Statoil hadde. Statoil gikk kun ut med verifisert informasjon og pårørende fikk alltid

[31] NATO, ACO Strategic Communication, ACO Directive (AD) 95-2. 2009.
[32] Kilde: Henning A. Søgaard, kommunikasjonsrådgiver FFI
[33] Mohr, H. and R. Satter, , "BP CEO Tony Hayward attends glitzy yacht race; Gulf residents infuriated", AP, 19th June 2010.
[34] *The In Amenas Attack*, Report of the investigation in to the terrorist attack on In Amenas. Prepared for Statoil ASA's Board of Directors, 8. September 2013.

tilgang til informasjonen først. Informasjon ble koordinert med norske myndigheter og BP. I løpet av seks dager førte hendelsen til at det i norske medier alene ble publisert 9000 artikler! Dette illustrerer hvilket press som oppstår på virksomheter når det oppstår krisesituasjoner.

En annen sentral utfordring er hvordan budskapet blir oppfattet. I 2015 opplevde Europa en stor tilstrømning av flyktninger fra Syria spesielt og masseimmigrasjon til Europa ble et tema i alle norske og internasjonale medier. Ungarn stengte grensen, Tyskland åpnet opp, og diskusjoner på nett dreide seg om menneskeverd, omsorg og frykt for at Europas egne velferdssystem skulle bli overbelastet og kollapse. I tillegg ble det spekulert i om terrorister kunne gjemme seg blant flyktningene. Krisen illustrerer blant annet effekten av Tysklands kommunikasjon utad med budskapet om at Tyskland skal ta i mot 800 000 flyktninger. Det sendte signaler om åpne grenser, og forbundskansler Angela Merkel ble et symbol på håp, samtidig som stadig flere ønsket seg til Tyskland: Men håpet ble vendt til skuffelse når det enorme presset i neste instans førte til at landet måtte stramme inn.[35]

Eksemplet viser hvordan krisekommunikasjon i praksis møter en rekke utfordringer og dilemmaer. Særlig ved store internasjonale kriser er dette en utfordring, og Forsvaret blir ofte en del av dette gjennom Nato eller Forente nasjoner (FN). Nyhetssyklusen blir stadig raskere, noe som medfører en «spinning» av nyhetsbildet. Det pågår en vekselvirkning mellom sosiale medier og tradisjonelle medier ved at mediene fanger opp nyheter på sosiale medier og vise versa. Utilstrekkelig kvalitetssikring av informasjon kan føre til at desinformasjon og usikkerhet sprer seg. I denne situasjonen blir alle sitt eget mediehus, privatpersoner så vel som offentlige etater, og informasjonsflyten blir tilsvarende vanskelig å begrense[36]. Samtidig oppstår nye globale medieaktører med ulike budskap på forskjellige språk for forskjellige målgrupper. Eksempler er Russia Today og Al Jazeera. Dermed kan nordmenn få ulik oppfatning av situasjonen dersom de leser nyhetsbildet på norsk, engelsk, eller på sitt eget morsmål. Dette byr på nye utfordringer all den tid krisekommunikasjon i Norge må formidles til ulike nasjonaliteter på ulike språk.

En annen mulighet er talevarsling eller varsling på SMS. I Sverige har det pågått et arbeid med talevarsling over mobiltelefon. Tjenesten varsler mobiler i et gitt område, og iverksettes av redningsleder fra for eksempel politiet. En lovendring må på plass for å kunne geografisk lokalisere (GEO-lokalisere) mobiltelefonene. Under forutsetning av at mobilnettet er tilgjengelig vil derfor befolkningen i et gitt område kunne motta varsel (talemelding) om hendelser og evakuering.[37] GEO-lokalisering kan imidlertid også være problematisk av personvernhensyn og retten til å bevege seg fritt.

4.5 DSBs veileder for krisekommunikasjon

Krisekommunikasjon er en viktig del av krisehåndteringen. DSB har utviklet en veileder for krisekommunikasjon. Denne sier følgende om kommunikasjon av risiko (s 11):[38] «Et viktig trekk

[35] Strømmen, K-, «Vi er to land som ikke lukker øynene», NRK, 8.9.2015
[36] Søgaard og Hagen, *Kampen om sannheten*, 2014.
[37] Se SOS Alarm, http://www.sosalarm.se/nytt-system-for-vma, nedlastet 7.1.2015.
[38] Tema. Risiko- og krisekommunikasjon. September 2014, DSB.

ved kommunikasjon om risiko er balansegangen mellom å beskrive en situasjon som så farlig at det fordrer handling, og samtidig unngå panikk». Dette betyr at en må avveie budskapets formulering mot forventet reaksjon og situasjonens alvorlighet. Hvis det for eksempel brenner om bord på et skip, er det viktig å evakuere raskt, men samtidig å unngå å skape panikk og kaos da dette kan forverre situasjonen.

DSB anbefaler at alle virksomheter utarbeider egne scenarioer og basere mye av sin planlegging for krisehåndtering og krisekommunikasjon på disse. DSB anbefaler å tenke både stort og internasjonalt, men også ta høyde for at kriser kan oppstå som følge av tekniske feil eller dødsfall blant egne medarbeidere.

En plan for krisekommunikasjon må i følge DSB beskrive hvordan planen er koblet til virksomhetens øvrige kriseplanverk, samt en oversikt over roller og ansvar til viktige bidragsytere. Alle planer bør dessuten beskrive hvordan og hvor ofte planen skal revideres, samt hvem som er formelt ansvarlig. Planen bør inneholde:

- Mål og prinsipper for virksomhetens krisekommunikasjon.
- Ansvar, roller, funksjoner og oppgavefordeling for alle som skal jobbe med krisekommunikasjon og viktige bidragsytere, eks. sentralbord og personalavdeling.
- Kommunikasjonsstabens organisering sett opp mot resten av kriseorganisasjonen.
- Hvem som skal være talspersoner overfor media.
- Definerte målgrupper og kanaler for å nå disse.
- Hvilke andre virksomheter man bør samordne og koordinere med vedrørende kommunikasjonsprodukter.
- Teknisk utstyr, stabslokale og alternative møtesteder.
- Vaktplaner og turnus, samt hvem som har kompetanse og opplæring til eventuelt å kunne bistå kommunikasjonsstaben i deres oppgaver.

Det finnes en rekke egnede kommunikasjonskanaler. Nettportalene «Regjeringen.no» og «kriseinfo.no» er viktige arenaer. I tillegg kommer medier som avsier, radio og TV og sosiale medier, SMS, analoge kanaler mm. Hva ulike medier skriver om en sak bør overvåkes dersom en vil følge med hvordan ulike gruppers holdning til en sak utvikler seg. Det er mulig å drive overvåking av sosiale medier selv, for eksempel via programmer som Tweetdeck[39] og Hootsuite,[40] og det er også firmaer som spesialiserer seg i dette segmentet. Aktuelle kanaler bør i følge DSB beskrives nærmere i virksomhetens egen krisekommunikasjonsplan, helst med kontaktinformasjon for de mest sentrale kanalene.

DSBs veileder inneholder også en sjekkliste om hva som bør gjøres etter krisen:

[39] Se Tweetdeck, https://about.twitter.com/products/tweetdeck
[40] Se Hootsuite, https://hootsuite.com/products/social-media-analytics/core-analytics

- Forberede eventuelle gjennomganger, evalueringer eller granskinger.
- Gjennomføre egenevaluering.
- Diskutere hendelsen og læringspunkter i strukturerte og systematiske former.
- Samle og analysere medieomtale.
- Revidere planverk og rutiner.
- Klargjøre loggen.
- Være forberedt på kritisk presse, eks. spørsmål om «Når fikk dere beskjed?», «Når ble ledelsen varslet?».
- Oppfølging av egne ansatte.
- Samarbeid med eventuelle støttegrupper.

5 Mobilapplikasjoner for krisekommunikasjon

5.1 Byggesett for mobilapplikasjoner

Samhandlingsutfordringer på tvers av etater er vel kjent gjennom øvelser og i reelle kriser der informasjon må flyte raskt mellom ulike aktører. Det betyr konkret at brannmannen eller Heimevernet (HV)-soldaten må kunne bli nådd på parkeringsplassen utenfor kjøpesenteret eller når han eller hun er på vei hjem fra jobb. Det er her muligheten i mobilapplikasjoner som understøtter krisehåndteringen ligger.

Som beskrevet av Hagen og Pham (2014) er flere mobilapplikasjoner utviklet og brukt i større internasjonale katastrofer, og det er interessant å observere at slike enkle verktøy bryter ned barrierer og bedrer samarbeid og krisehåndtering. Publikum er svært viktig i så måte. Det viste blant annet erfaringene fra 22. juli 2011, da campingturister bistod i redningsarbeidet. Teknologirådet peker i sin rapport på at aldri før har publikum vært bedre rustet til å bistå med viktig informasjon. De anbefaler at det utvikles en nød-app for smarttelefoner i Norge som gjør det enkelt og trygt for befolkningen å rapportere hendelser til nødetatene. De sier at det må være mulig å dele stedsinformasjon via tale, tekst, direktemeldinger og video, og det bør også vurderes om applikasjonen også automatisk skal kunne sende inn profildata til mobileieren. Teknologien gir muligheter for kortere responstid, bedre situasjonsforståelse, responskvalitet, samhandling og koordinering og ikke minst bedre kontakt med publikum.[41]

Det finnes ulike app-byggesett tilgjengelig på internett som gjør det mulig for brukerne selv å designe og publisere egne apper. Tabell 5.1 viser et utvalg slike app-byggesett med noen kommentarer knyttet til byggesettets funksjonalitet.

[41] På nett med publikum. Hvordan smarttelefonen og sosiale medier gir nye muligheter for norsk politi, Oslo: Teknologirådet, Rapport 02, 2014.

Tabell 5.1 Oversikt over app-byggesett[42]

App-byggesett	Pris	Egenskaper
App factory	$99-999	For Android, iOS og Blackberry
Appery IO		Skybasert med visuelle utviklingsverktøy, trenger ikke programmeringskunnskaper
App Machine	$499 per app	Prekodede byggesteiner, online-butikk med avanserte tjenester
App Makr	Gratis, eller månedavgift 1-9$	For Andriod og iOS, gir full autonomi over appen
Appsbar	Gratis	Tilbyr rammeverk, ulike app-typer
Appsme	Gratis eller 8-40$ per mnd	Trenger ikke teknologikunnskaper men gir også avanserte muligheter for teknologer
Appy Pie	Gratis eller 7$ per mnd	«Klikk og dra»-plattform
Bizness Apps	24$ per mnd	Tilbyr mange design-rammeverk
BuildFire		Tilbyr å omforme webside til mobilapp
Canvas Business Apps & Forms	13$ eller gratis en måned	«Klikk og dra»-app-bygger
Google Tools for building app	Gratis	Rammeverk, krever programmeringsforståelse
Como	Gratis for inntil fire nedlastinger, 41$ for ubegrenset	Partnerskap med Amazon App-store
EachScape	Gratis prøveversjon	Tilbyr templates
GameSalad	Gratis eller 299$ per mnd	«Klikk og dra» og adferdsbibilotek
Mobile Roadie	1499$ per mnd	Kan lage avanserte apper med GEO-målrettet utsending av melding mm
PhoneGap	Gratis	Åpen kildekode-rammeverk
Salesforce1 Platform	25$ til 150 $ per mnd	Enkelt å lage for ulike digitale enheter
Taplytics	Gratis prøve og fra 40-300$ per mnd	Tilbyr funksjonalitet for oppdatering av apper for hele teamet som utvikler appen
Zengine	Gratis for HTML app, eller 39$+ per mnd	
Zoho Creator	Gratis for 15 dager, ellers 5$+ per mnd	Trenger ikke teknologikompetanse i det hele tatt

App-byggeverktøy kan ha sine fordeler i stedet for at teknologer som kanskje ikke kjenner bruksområdet like godt skal designe verktøyene. Slike byggeverktøy finnes både i gratis form og er da gjerne reklamebasert, eller som betalbare produkter med en månedsavgift som igjen er avhengig av ulike faktorer. De ulike verktøyene tilbyr ulike utviklingsmuligheter og funksjoner, og de dekker i ulik grad ulike operativsystemer. Mange av verktøyene markedsfører seg med at teknisk kompetanse ikke er nødvendig i det hele tatt, og det finnes enkle introduksjonsvideoer på YouTube. Et eksempel på dette er introduksjonsvideoen til tjenesten Appsbar[43] som gjør det mulig å lage og publisere en egen app helt gratis.

[42] Angeles, S.,"18 Best App Makers", Business News Daily, December 8, 2015.
[43] Se: appsbar.com - How to Build a Free Android, iPhone, Windows, Blackberry, Facebook and HTML5 App. https://www.youtube.com/watch?v=Oatucw4hoO0

Det er allerede utviklet mange apper innenfor området krisehåndtering og krisekommunikasjon. Det finnes en egen app crawler-tjeneste http://appcrawlr.com/app/ som kan brukes for å søke opp mobilapplikasjoner. Vi har brukt denne for å finne fram til noen apper som allerede dekker området krisekommunikasjon. Disse er imidlertid ikke utformet for totalforsvaret og Forsvaret, men gir en ide om hva slike apper kan inneholde.

5.2 Eksempel på mobilapper for krisekommunikasjon og omdømmestyring

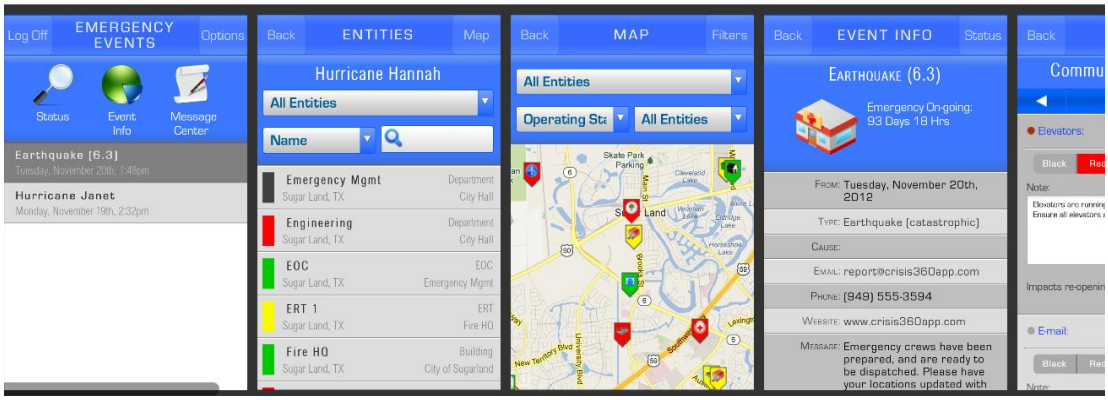
Ved å bruke app crawler (en tjeneste som søker opp apper) og søke på «crisis communication» fant vi følgende apper for krisekommunikasjon som illustrerer hva andre har tenkt på før oss, og hva som kan være potensialet i denne type tjenester.

«Crisis360 Emergency Management Communications for Business Continuity and Situational Awareness» for iPhone og iPad er i følge produsenten laget for profesjonelle (nødetatene): Appen reklamerer med sømløs sporing, spredning av informasjon og kommunikasjon gjennom en krise. Den passer for virksomheter med lokasjoner spredt geografisk. Av den grunn kan idéen den bygger på være av interesse også for Forsvaret og sivilt-militært samarbeid. Kort beskrevet samler appen sammen informasjon, rapporterer og kommuniserer informasjon relatert til krisens utvikling og til krisehåndtering. Appen kan også passe for selskaper som er lokalisert på ulike steder. Operativt personell kan ta bilder i feltet og gjøre disse tilgjengelige i et kommandosenter umiddelbart. Appen plasserer berørte anlegg på et kart og logger hendelser til senere bruk i forbindelse med erstatningsutbetalinger fra forsikringsselskap. Appen bygger på web og sky-teknologi.[44]

Den tilbyr spesifikt:

- Umiddelbar tilgang for å kunne se hendelsesdetaljer, skadeomfang, bilder og oppdateres raskt.
- Situasjonsforståelse: Samlet oversikt over hendelse og hjelpeinitiativer som i tur kan bidra til å ta bedre beslutninger.
- Sanntidsoppdatering: Oppdateringer er reflektert i appen og tilgjengelig for andre i sanntid.
- Behovsbasert brukertilpasning.
- Skrivebord og kart som gir muligheter for både sammendrag og detaljer.
- Sentraliserte oppdateringer som logges for å gi mulighet for å analysere hendelsen i ettertid.
- Historisk oversikt: Fullstendig historie av alle oppdateringer av gitt person og tid.

[44]Se: http://appcrawlr.com/app/show/1181298 nedlastet 04.01.2015.



Figur 5.1 Crisis 360 Emergency Management Communication for Business and Situational Awareness (for Iphone)

Omdømme- appen vil også kunne være av interesse i denne sammenheng. I følge produsenten sporer denne Google, Yahoo, Bing, YouTube, Twitter, blogger og nyheter, slik at man kan vite hva folk ser når de søker opp ditt navn, din merkevare eller din virksomhet. Appen gir muligheter til å se forandringer i sanntid slik at du umiddelbart kan forsøke å ta tilbake kontroll over ditt «digitale omdømme» som kan finnes ved å søke på google, yahoo etc. Appen tilbyr følgende tjenester:

- Spre navn, merkevarenavn i Google, Yahoo og Bing Search Engines.
- Den markerer resultatene med tommel opp eller ned og lager slik sett en score på ditt digitale omdømme.
- Skaffer deg regulære oppdateringer og omtaler om dine tema i blogger og nyheter, på Twitter og på YouTube.

Figur 5.2 Your own online reputation - Iphone App[45]

Google har en dominerende markedsposisjon på søk på nettet. I Norge er denne andelen på mer enn 90 prosent. Tjenesten Google Alerts[46] [47] gjør det mulig fortløpende å bli varslet om aktivitet og registreringer på angitte tema. Gjennom Google Analytics blir det også tilbudt en rekke

[45] Se: http://appcrawlr.com/ios/reputation
[46] Se: https://www.google.com/alerts, nedlastet 4.1.2015.
[47] Se: https://support.google.com/alerts/, nedlastet 5.1.2015.

tjenester det er mulig å bygge videre på for apper og nettsider som brukeren har utviklet selv. En av disse er kontroll av applikasjonen en bruker, eksempelvis krisekommunikasjons-appen. Det er mulig å finne ut hvor mange som bruker den, hvor brukerne er og hva de bruker av tjenester. Oppskrift med kode på hvordan bruke Google Analytics ligger tilgjengelig på nett.[48]

Disse få eksemplene gir en liten indikasjon på hvordan app-teknologi kan brukes for å lage krisekommunikasjonsverktøy for håndholdte enheter. Det økende omfanget i tilbudet av apper, viser at dette er blitt en industri og et marked med produsenter og kjøpere. De kommersielle appene, som er omtalt her, kan gi inspirasjon for utvikling av en krisekommunikasjons-app for Forsvaret og sivile samarbeidspartnere.

5.3 Verktøy for opinionsanalyse

Opinionsanalyse (sentimentanalyse) er enkelt forklart analyse følelser og meninger og holdninger. Opinionsanalyse kan være nyttig for å følge med på hvordan et narrativ eller et omdømme utvikler seg.

En definisjon av sentimentanalyse er: "a linguistic analysis technique where a body of text is examined to characterise the tonality of the document".[49] Senitmentanalysen ser bak antallet likes, retweets og kommentarer som blir gitt til en kampanje, bloggartikkel eller video på nett. Den bistår til å forstå dypere hvordan folk reagerer på det budskapet som blir publisert. Det finnes mange ulike verktøy på nett som kan være nyttige for å forstå hvordan en når ut til målgrupper med et budskap. På en blogg av iprospect kan en få en oversikt over ti praktiske verktøy som kan hjelpe til med å forstå målgruppene[50]. Tabellen under gir en oversikt over 12 mulige verktøy, noen betalingstjenester og noen gratisversjoner.

Tabell 5.2 Ulike verktøy for opinionsanalyse

Verktøy	**Innhold**	**Kostnad**
Meltwater	Automatiserer markedsovervåkning i sann tid, kan filtrere på dato, geografi, språk og sentiment, markedsføres også som verktøy i krisesituasjoner, http://www.meltwater.com/no/products/understand/	Betalingstjeneste
Google Alerts	Et godt startpunkt for å følge trender og konkurrenter, https://www.google.com/alerts	Gratis
People Browser	People Browser er finansiert av Darpa for å bygge neste generasjons nettverk. Det gjør det mulig å lage ditt eget sosiale nettverk og utnytter muligheten til å lage egne toppdomenenavn (gLTD), http://www.peoplebrowsr.com/	Gratisversjon småskala finnes, ellers betalingstjeneste
Google analytics	Analyseverktøy for å følge med på brukere av ens websider, apper etc. og utarbeider ulike typer rapporter, http://www.google.com/intl/no_ALL/analytics/features/index.html	Gratis og betalingstjeneste

[48] For mer informasjon om oppsett av Google Analytics og analyse av for eksempel din app, se her: https://developers.google.com/analytics/devguides/platform/ nedlastet 1.2.2016.
[49] "Definition of sentiment analysis", Financial Times, ft.com/lexicon.
[50] iProspect, 10 sentiment analysis tools track social marketing success, Blog.

Verktøy	Innhold	Kostnad
Hotsuite	Måler og analyserer effekten av kampanjer på sosiale medier, sporer engasjement og konversasjon med innsikt fra Facebook, LinkedIn, Google+mm https://hootsuite.com/plans/free	Gratisversjon og betalingstjeneste
tweetstats	Lager graf over din twitterstatistikk, veldig enkel tjeneste, http://www.tweetstats.com/	Gratis
Facebook insights	Gjør det mulig å lage egne annonser og se totalt antall likes, antall fans, active brukere, Likekilder, damografikk, medieforbruk mm., https://www.facebook.com/help/search/?q=insights	Gratisversjon og betalingstjeneste
Pagelever	Tilbyr både markedsanalysetjenester og reklamekampanjer, inklusive måling av kampanjenes effekt langs ulike sosiale mediekanaler, http://www.unifiedsocial.com/platform/intelligence/#~pAMGjlU2mW18ay	Betalingstjenestefri demo
Social mention	Sporer og måler hva folk uttaler om deg, bedriften eller et nytt produkt eller tema i realtid, ved å overvåke sosiale medier inklusive Twitter, Facebook, FriendFeed, YouTube, Digg, Google, http://socialmention.com/	Betalingstjeneste
Marketing grader	Måler din aktivitet på blogger, twitter etc, enkel tjeneste som crawler nettet, https://marketing.grader.com/	Gratis
Retriever	Nordens største leverandør av medieovervåkning inkl sosiale medier, verktøy for redaksjonell research og medieanalyse, medieeksponering over tid, per kilde, kildekategori og geografisk nedslag, http://www.retriever-info.com/no/om-oss/	Betalingstjeneste
	Mediaovervåkning og analyse, overvåker realtid TV og radio, http://www.opoint.com/	Betalingstjeneste Gratis prøveversjon

6 Begrensninger og muligheter for bruk av mobilapper i krisekommunikasjon

6.1 Kommunikasjonsinfrastrukturen

Norge ligger langt framme når det gjelder bruk av IKT og digital modning, faktisk som nr. 1 i Europa og nr. 5 på verdensbasis i følge *Global Cybersecurity Index & Cyberwellness Profiles*. Trenden er at datatrafikken fortsatt vil øke, blant annet som følge av økning i maskin til maskin kommunikasjon og bruk av Skype og lignende tjenester, mens taletrafikken går ned i følge NKOM (2014). Samtidig kan smarttelefoner brukes til stadig flere tjenester, betaling, kart, speil, meldingsutveksling og sikkerhet. Vi går dermed rundt med små datamaskiner i lommene som blir stadig viktigere og mer avanserte verktøy.

De digitale tjenestene som er tilgjengelige via apper er videre avhengig av en informasjons-infrastruktur som fører med seg med både kjente og ukjente sårbarheter (jf. NOU 2015:13). Vi skal ikke diskutere sårbarheter spesifikt her - utover å peke på at digitale sårbarheter akkumuleres på tvers av EKOM-tilbydere. Bildet er relativt komplekst, og en komplett oversikt er umulig, selv med gode risikoanalyser, sikkerhetsarbeid og tilsyn/revisjon. Derfor forekommer det tidvis også hendelser som gjør at EKOM-nettet ramler ut. Som European Union Agency for Network and Information Security (ENISA) har påpekt i sin rapport er programvarefeil, maskinvarefeil,

menneskelige feil og overbelastning i nettet noen av grunnene til store utfall i Europa.[51] I Norge har vi dessuten tilfeller med ekstremvær som gir strømbortfall og utfall av EKOM, i tillegg har sårbarheten i EKOM også en geografisk side der visse områder er mer utsatte enn andre for utfall.[52] Å garantere seg 100 prosent mot alle mulige feilhendelser og utfall er dermed umulig.

Totalt sett er imidlertid både oppetid og dekning (målt i prosent av befolkningen med dekning) veldig bra, men i krisesituasjoner kan man risikere at infrastrukturen svikter. 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.[53] Denne erfaringen fikk man for eksempel i Lærdal da brannen etter hvert tok Telenors sentral og trafostasjonene til E-verket, og med det forsvant kommunikasjonen også.[54] Vi vil her referere til fjellvettreglene der DNT også har gode råd om mobilbruk i fjellheimen[55] som også er relevante i krisesituasjoner. Vi har i tekstboksen tillatt oss en modifisert utgave:

- Mobiltelefonen kan være et nyttig hjelpemiddel, men du kan ikke stole på den i alle situasjoner eller områder.
- Mange steder er det dårlig dekning. Telenor og Netcom har egne dekningskart.
- Ikke avtal ringetider. Du kan befinne deg i områder uten dekning når du skulle ringe.
- Lad opp batteriet når du kan. Spar på batteriet, du kan få bruk for det. Ta med lader eller batteri-backup.
- Oppbevar mobiltelefonen og eventuelt ekstrabatteri varmest mulig. Kulde reduserer batterikapasiteten kraftig.
- Oppbevar mobiltelefonen i vanntett innpakning.
- Hvis du ikke har dekning, søk opp i høyden. Prøv andre kommunikasjonsmidler som radio.
- Hvis du ikke kan ringe, prøv å sende en tekstmelding. Den kommer mye lettere gjennom.
- Husk at en mobiltelefon aldri kan erstatte din egen sunne vurdering.

I rene sivile kriser der uhell og natur er rot-årsak, for eksempel teknisk svikt, flom og storm, er for eksempel ikke behovet for avlyttingssikring så prekær. Det vil likevel være nyttig uansett å tenke igjennom også de scenarier der sikkerhet er et tema. Dette fordi en god applikasjon med høy grad av brukervennlighet kan bli fristende å bruke også i situasjoner der slike applikasjoner ikke burde bli benyttet. Noen retningslinjer for bruk kan derfor være fornuftig å bygge inn.

6.2 Lagring av data

En annen sentral problemstilling er hvor data blir lagret og hvor lenge. I de appene som kan lastes ned gratis eller kjøpes fra Android, Apple eller Google, vil data bli lagret på servere utenfor Norges grenser. En rapport overlevert til Kommunal og moderniseringsdepartementet peker på at det er restriksjoner på å lagre for eksempel personopplysninger utenfor Norges grenser og at Arkivloven og Sikkerhetsloven begrenser bruk av skytjenesters lagring av visse typer sensitive

[51] Mattioli, R. and M. Dekker, National Roaming for Resilience. National roaming for mitigating mobile network outages. ENISA, November 2013.
[52] Hagen og Pham, 2014.
[53] Hagen, J. *Robust kommunikasjonsinfrastruktur for samhandling i krise*, FFI-Fakta, november 2014.
[54] Se «Slik jaget ildstormen gjennom sentrum», webpresentasjon, VG, 1. februar 2015.
[55] Se «10 råd om mobilbruk på tur», Den Norske Turistforening.

data (Interdepartemental arbeidsgruppe, 2015). Også tilsynspraksisen utfordres – det er mildt sagt krevende å få gjort stedlig tilsyn og revisjon hos store globale skyleverandører. En tredje faktor er regelverket om anbud. I starten betaler man lite for skytjenesten, men ettersom skybruken øker, noe som kan skje i løpet av en krisesituasjon, øker kostnadene. Da kan kravene om offentlig anbud tre i kraft.

Det norske regelverket på lagring av personopplysninger er så langt harmonisert med EUs regelverk. EU Kommisjonen jobber med kontraktsforhold mellom brukere og skyleverandører og om disse er gode nok.[56] Dessuten er datastrømmen mellom brukernes klienter og servere heller ikke transparent og en har som bruker liten kontroll over dataflyten. I en sikkerhetspolitisk eller kriminalitetshåndteringskontekst kan dette bli en utfordring. Derfor kan Sinetts tilnærming med Mlab og CEI-demonstratoren med server hos FFI, alternativt en privat skyløsning for Forsvaret, være en interessant case for totalforsvaret i Norge, i alle fall opp til et visst trusselnivå. En større brukermasse reiser på en annen side spørsmål om framtidig kapasitet til å vedlikeholde og videreutvikle systemet. Å ha kapasitet til dette er i seg selv et viktig sikkerhetstiltak.

6.3 Avveining mellom sikkerhet og funksjonalitet

Cyber er definert av Forsvaret selv som et eget domene i Forsvaret på linje med land, sjø og luft.[57] Truslene i framtidens konflikter vil kunne omfatte elektronisk krigføring mot kommunikasjons-infrastruktur, cyberangrep mot nasjonale datasystemer og psykologiske virkemidler som villedning gjennom bruk av både tradisjonelle og sosiale medier, eventuelt i kombinasjon med fysiske angrep. Målet vil kunne være påvirkning av utvalgte personer og grupper gjennom desinformasjon, undergraving og manipulasjon.[58] Angrep kan rette seg mot sivile så vel som militære aktører.

De kriminelle nettverkene blir i økende grad også profesjonalisert, og de bruker ulike typer virkemidler i sine kampanjer. Kriminaliteten kan være rettet mot IKT-systemer eller IKT-systemer kan brukes som støtte i kriminelle kampanjer og operasjoner.[59] Libicki et al. (2015) ved forskningsinstitusjonen RAND anslår at det svarte kriminelle cybermarkedet vil fortsette å vokse og at det er en reell fare for at de kriminelle vinner over de lovlydige. RANDs studie av markedet for skadevare viser at markedet er modent, og både profesjonelle og amatører handler her.[60] Dette, sammen med forhøyet avlyttings- og sabotasjetrusselen i enkelte scenarier, setter krav til sikkerhet når det gjelder bruk av sivil mobil teknologi til krisehåndteringen.

I det nederlandske eksperimentelle K2-systemet PROMISE (Promise, 2015), utviklet for det nederlandske forsvaret, utnyttes nettopp smarttelefoner og apper for mer effektiv og billig

[56] "Expert Group on Cloud Computing Contracts", weboppslag, EU-kommisjonen.
[57] Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren, «FDs Cyberretningslinjer».
[58] Se Søgaard og Hagen, Kampen om sannheten, FFI Fokus 2014.
[59] *Datakrimstrategien*, Politidirektoratet, 12. mai 2015.
[60] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar, Rand 2014.

samhandling. De tester ut nedgradering av informasjon, som sammen med sikkerhetsmekanismer kan gjøre det mulig å bruke smarttelefoner og apper i operasjoner. Aktuelle sikkerhetstiltak som er til vurdering inkluderer sterk autentisering av enhetene, kryptert lagring av informasjon på enhetene, VPN, herding av OS, separering av apper, sikkerhetsstyring og sikring av grensesnitt mot andre systemer. Imidlertid må sikkerhet også vurderes opp mot prossesseringshastighet, brukervennlighet og batteriets utladningstid.

6.4 Organisatoriske og kulturelle forhold

Som omtalt innledningsvis er totalforsvaret hierarkisk oppbygd og sektorisert. Det finnes likevel mekanismer som skal bidra til koordinering. Nasjonal beredskap bygger på fire viktige prinsipper, hvorav samvirkeprinsippet er viktig for å gi bedre situasjonsforståelse og sivil-militær samhandling. Men også nærhetsprinsippet, som innebærer at kriser organisatorisk skal håndteres på lavest mulig nivå, blir relevant i denne sammenheng. Teknologiske løsninger som åpner for informasjonsutveksling mellom aktører helt ned på enkeltmannsnivå og beslutningstaker vil kunne styrke nærhetsprinsippet ved at man på "aller laveste nivå" blir i bedre stand til å kunne utføre en økende mengde av oppgaver på stedet der man enhver tid er mer effektivt og i sann tid.

Totalforsvaret er en stor samvirkeorganisasjon, men den er ikke statisk. Det har vært og vil komme store omorganiseringer i ulike sektorer. Organiseringer og struktur i viktige samhandlingsaktører som brannvesen, politi og kommuner er utredet eller skal utredes. Med hver omorganisering endres kontaktpunkter innad i Totalforsvaret. Spørsmålet er hvor godt organisasjonsendringene er ivaretatt i totalforsvaret og om totalforsvaret i seg selv har gode nok styringssystemer til å foreta fortløpende endringer i sine prosedyrer. Forsvaret har for eksempel mistet mange av sine sivile kontaktpunkter i egen omlegging på 2000-tallet og i kombinasjon med omleggingen av den sivile beredskapen. Det er krevende å oppdatere alle kontakter og rutiner, samt ha øvd rutinene. Et spørsmål er om teknologi og infrastruktur, som for eksempel CEI-appen og bakenforliggende system eller lignende, kan bidra til å redusere noen av de organisatoriske barrierene, bygge tillit på tvers av sivile og militære aktører, bedre situasjonsforståelse og beslutninger også i perioder med omorganisering. Dersom dette skal lykkes, må en også ha et fokus på organisatoriske prosesser og rutiner for oppdatering av elektronisk informasjon.

Neste kapittel beskriver hvordan et konsept for krisekommunikasjon basert på mobilapplikasjoner kan se ut.

7 Ideskisse til et rammeverk for krisekommunikasjon basert på mobilapplikasjoner

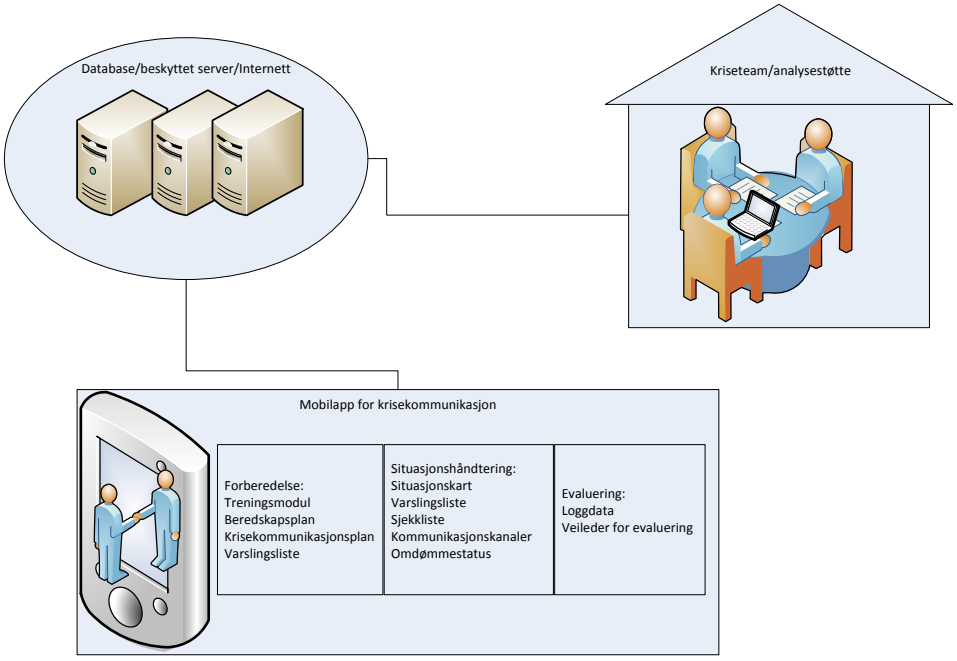
7.1 Grunnleggende konsept

Figur 7.1viser en skisse av en idé til et konsept for mobilapplikasjon for krisekommunikasjon for totalforsvaret.

Idéen består av tre deler:

1. Selve appen,
2. informasjonskilder, som kan være databaser, data på en beskyttet eller sikret server, eller data tilgjengelig på internett, og
3. menneskelige ressurser i form av kriseteam og/eller analysestøtte.

I figur 7.1 er ideskissen eksemplifisert med én krisekommunikasjons-app for å illustrere et grunnleggende tankesett i den videre diskusjonen. Det er dog nødvendigvis ikke en "universal-app" for krisekommunikasjon man er ute etter som sådan, men at man også kan tenke seg mulighetene for å utvikle flere apper knyttet til de samme serverne og informasjonskildene. I tillegg må det også være en bakenforliggende infrastruktur for å få appen eller appene ut til brukeren. Hvordan denne infrastrukturen bør være har vi ikke i denne rapporten gått nærmere inn på, men her er det nærliggende å tenke seg at det for eksempel kan etableres en felles app-store for ulike krisekommunikasjons-apper som man kan laste opp avhengig av situasjonen. Enten ved å utnytte distribusjonsmekanismer som allerede eksisterer, eller å bygge egen parallellstruktur som tilbyr disse.



Figur 7.1 Forenklet idéskisse for krisekommunikasjonsapp for Totalforsvaret

I figuren kommuniserer appen mot informasjonskildene, for eksempel en beskyttet server, leser data lagret på denne og skriver tilbake til serveren. Det kan for eksempel være lokaliseringsdata på mobiltelefonen som bruker appen. Kriseteam og/eller analysestøtteteam henter informasjon fra samme informasjonskilder, for eksempel den beskyttede serveren, analyserer data, tar beslutninger, og skriver/oppdaterer informasjon på serveren, slik at brukerne av appen også får tilgang til et oppdatert informasjonsbilde.

Brukere av appen er alle samvirkeaktører, militære så vel som sivile, som er involvert i å håndtere en konkret krisesituasjon og har en rolle innen krisekommunikasjon. Dette vil kunne inkludere personell på taktisk, operasjonelt og strategisk nivå. Appen kopler sammen samvirkeaktørene virtuelt og bidrar til at alle får et felles mest mulig oppdatert informasjonsbilde.

Som de andre appene vi har vist til i denne rapporten, må det være mest mulig med sanntidsendring. Appen må derfor kunne kople seg opp mot en eller flere servere og databaser, samt internett.

Vi ser for oss en app med tilbud om forskjellige funksjoner/tjenester før, under og etter krisen. Dette omtales nærmere i de neste avsnittene.

7.2 Forberedelse

Første fase oppstår før krisen inntreffer. Alle samvirkeaktører vil ha et grunnleggende informasjonsbehov for å kjenne til den felles beredskapsplanen og krisekommunikasjonsplanen, samt ha en oppdatert kontaktliste og varslingsliste tilgjengelig. Dette er informasjon en app kan hente fra en sentral server.

For å være best mulig forberedt, kan et enkelt øvingsprogram, eller en quiz, være en mulig tilleggsfunksjon. Målet bør være at brukeren kan trene og øve på viktige trinn i krisekommunikasjonsprosessen, bli kjent med krisekommunikasjonsplanen, trene på hva brukeren skal gjøre rent praktisk i en tenkt situasjon, herunder hvem brukeren skal varsle. Et treningsprogram kan også inneholde introduksjon til viktige dilemmaer som brukeren må ta hensyn til i utarbeidelse av budskap, for eksempel hvordan samme budskap kan bli oppfattet ulikt av ulike målgrupper. Et annet dilemma er hensynet til egen operasjonssikkerhet i forhold til risiko for andre grupper. Et eksempel på dette dilemmaet er da de allierte under 2. verdenskrig knekte krypteringen til tyskerne, men ikke kunne varsle egne konvoier da deres bevegelser kunne avsløre at krypteringen nok var knekt. Det er godt illustrert i filmen om Alan Turing som ble regissert av Morten Tyldum.

7.3 Situasjonshåndtering

Mens situasjonshåndtering pågår, vil funksjoner som eksempelvis situasjonskart med plotting av ressurser og hendelser kunne være svært nyttig. Dette er en funksjon som er i bruk i andre apper også, herunder i internasjonalt nødhjelpsarbeid.

Andre funksjoner er varslingslisten og sjekklisten for krisekommunikasjon. Dessuten vil tilgang til ulike kommunikasjonskanaler – eksempelvis Twitter, Facebook, SMS mv. være nyttig, avhengig av hvilken målgruppe en skal gi informasjon til.

For å kunne følge historien og hvordan den utvikler seg, kan en fortløpende omdømmestatus være nyttig. Her kan en se for seg en tjeneste som crawler nettet for informasjon om den aktuelle saken og så presenterer et statusbilde. Omdømmeappen, omtalt i kapittel 0, er et eksempel. Det finnes

også ulike digitale verktøy for opinionsanalyse og markedsføring, som også er omtalt i kapittel 5.3. Verktøyene har ulik brukervennlighet, og kan være til hjelp for å følge med på hvordan narrativet og omdømmet utvikler seg.

En oppsummering av risikobildet slik Nasjonal sikkerhetsmyndighet (NSM) NorCERT, DSB, Politiets sikkerhetstjeneste (PST), Etterretningstjenesten eller andre myndigheter ser det til enhver tid er også nyttig. Dersom en skal få til noe slikt, kreves det samarbeid på tvers av organisatoriske grenser. En enkel løsning kan være en abonnementsordning på nyhets-feeds, eventuelt i kombinasjon med bearbeiding av analyseteamet. Det er likevel viktig at nyheter når raskt ut til brukerne.

Til sist vil logging være viktig slik at dette kan brukes i neste fase til evaluering.

Konseptet er bygget rundt tre deler (jfr. kapittel 7.1): Appen og dens brukere, databaser og kriseteam/analysestøtte. Både brukere og kriseteamet/analysestøtten må kunne oppdatere informasjon (data) i databasen og også hente informasjon (data) fra denne. Da vil alle parter kunne ha tilgang til samme oppdaterte informasjons-bilde.

Tilleggsfunksjoner er presentert i underkapittel 7.5.

7.4 Evaluering

Når en fase av krisen er over, kan en modul som tilbyr verktøy for å evaluere og lære være av verdi. Typisk vil dette kunne være logg og quiz.

Det kan også være en veileder for evaluering av hendelsen med en gjennomgang av sentrale problemstillinger som er felles for alle typer kriser. Eksempler kan være: Var forberedelsen god nok? Hvilke hendelser var vanskeligst å håndtere og hvorfor? Var informasjonsbildet tilstrekkelig, og eventuelt hvorfor ikke? Hensikten er at dette kan bidra til bedre tjenester i framtida.

7.5 Mulige tilleggsfunksjoner

Mennesker involvert i krisehåndtering og hendelshåndtering vil også kunne ha nytte av en «Jeg er OK-knapp» eller «Jeg trenger hjelp-knapp» der det sendes GEO-lokasjonsdata til mottaker. Slike knapper har Norsk Luftambulanse implementert i sin app.[61]

Det er også mulig å se for seg ulike tilleggsfunksjoner slik som:

- Værvarsel for området, oppkopling mot yr.no.
- Scenariospesifikke situasjonsbilder: For eksempel vil et scenario med fiskeriovervåkning og hendelse til sjøs kreve annen type informasjon enn en kjemikaliehendelse på et

[61] Hagen, J og Q. Pham, *Brannvesenets behov for robust informasjonsinfrastruktur for samhandling i krisesituasjoner*, Kjeller: FFI-Rapport 2014/01704.

industrianlegg. Kjemikalieulykker krever informasjon om farlige stoffers helsevirkninger. Mens fiskeriovervåkning og tyvfiske vil kunne ha nytte av tilgang til informasjon om skipstrafikken, vil en kjemikaliedatabase være nyttig i det andre tilfellet.

- I tillegg kan en tenke seg en tjeneste eller funksjon der informasjonskvaliteten som finnes på internett blir fortløpende vurdert og formidlet. Det kan for eksempel være viktig å varsle dersom det pågår for eksempel propagandakampanjer eller cyberangrep som forfalsker informasjon på internett, eller viktige norske sider er nede. Det er her mulig å tenke seg kopling mot en analysetjeneste som jobber og lagrer fortløpende resultater på eksempelvis en beskyttet server, som appen igjen er koplet opp mot. Dette gir muligheter for verifikasjon av informasjon og mennesker inn i loopen. Rent praktisk kan det ivaretas gjennom en analysestøttefunksjon.
- Videre kan appen tenkes å kople seg opp mot ulike servere og hente informasjon fra disse, for eksempel server som gir et ugradert sanntidssituasjonsbilde på cybertrusler. Eksempler på denne type informasjon kan være situasjonsbilde på distribuerte nektelsesangrep slik Arbor networks presenterer bildet digitalattackmap.com.[62] eller det kan være koplet mot en server der NSM/NorCERT og PST legger ut fortløpende statusinformasjon angående risikoen i Norge.
- Det er mulig å se for seg ytterligere «produkter», maler eller apper, som kan lastes ned fra en server, avhengig av klassifiseringsnivå og behov. Her er det imidlertid nødvendig med mer forskning på hvilke type produkter eller apper dette kan være. Ulike maler for krisehåndtering og krisekommunikasjon, basert på type scenario, er en mulighet. I dette ligger også en idé om å tilby fleksibilitet slik at brukeren selv kan utvikle egne apper som dekker det spesifikke behovet i den enkelte situasjonen. Dette er noe av det Sinett utvikler gjennom app-byggeverktøyet Mlab.

7.6 Avveining mellom sikkerhet og funksjonalitet

Sikkerhet blir ofte framhevet som en utfordring og noe som kan hemme god funksjonalitet. Men god sikkerhetspraksis vil også kunne spille en positiv rolle. Det finnes mange tiltak og mekanismer som kan tas i bruk, jf. tidligere omtale av PROMISE-prosjektet, se kapittel 6.3.

På den ene siden har Forsvaret et strengt sikkerhetsregelverk og et behovsprøvd informasjons-delingsregime. På den andre siden er det i mange sammenhenger nødvendig å dele informasjon. Disse to hensynene må kunne balanseres for at samhandling skal være mulig. Hvor denne balansen skal være er ikke avklart. Utfordringen blir tydelig i sivilt-militært samarbeid. Her blir tillit viktig. Kanskje vil Forsvaret være nødt til å nedgradere noe informasjon, mens de sivile aktørene må styrke sikkerheten i sine systemer og prosedyrer for at tilstrekkelig tillit kan gi grunnlag for bedre informasjonsdeling og samhandling? Men så lenge Forsvaret lagrer

[62]Digital Attack Map, Top daily DDoS attacks worldwide, web streaming, http://www.digitalattackmap.com/?imm_mid=0b2597&cmp=em-strata-na-na-newsltr_20131030_elist#anim=1&color=0&country=ALL&time=16000&view=map nedlastet 8.8.2015.

informasjon (gradert eller ugradert) på graderte systemer vil det være vanskelig å dele den med andre (Manchini, 2016).

Innledningsvis ser vi noen muligheter: Konseptet vi har presentert fordrer at dataene ikke er tilgjengelig for hvem som helst, men at de kan lastes ned til godkjente brukere av appen. Til dette kreves det autentiseringsmekanismer og mulighet til å fjernslette appen. Slike mekanismer eksisterer allerede og er mulig å implementere ved behov.

Et annet forhold er at grensesnittene mellom de ulike samarbeidende partnerne kan kreve ulike sikkerhetsmekanismer og ulik tilgang til informasjon. I sin enkleste form kan en tenke seg en flat sikkerhetsmodell som bygger på at det er like stor grad av tillit mellom alle samhandlende aktører som får tilgang til appen, mens i en mer avansert modell kan en tenke seg at brukerne deles inn i ulike grupper med varierende tilgang til informasjon fra den sentraliserte serveren. For eksempel kan det tenkes at HV og Forsvarets Operative Hovedkvarter (FOH) deler mer informasjon enn FOH og Røde kors. Den enkleste løsningen vil likevel være å ha en brukergruppe og basere alt på helt åpen informasjon, eventuelt nedgradert informasjon. Da vil alle samvirkeaktørene ha samme tilgang til informasjon.

7.7 Personopplysninger

Hvilke personopplysninger skal appen lagre? I en ideell situasjon, kunne en tenkt seg at brukeren registrerte viktig medisinsk informasjon, slik som eksempelvis helseappen på Iphone gir mulighet for. I en nødsituasjon kan dette redde liv. Dilemmaet er at samme informasjon kan misbrukes dersom en motpart får tilgang til informasjonen. Dette er spesielt aktuelt i krig og konflikt.

Hvordan og hvor lenge personopplysninger skal lagres er en annen problemstilling som må avklares. Hvis noen trykker på nødknappen og profildata blir overført, bør det være regler for hvor lenge dette kan lagres. Brukeren må også i henhold til Personopplysningsloven være informert om eventuell bruk og lagring av personopplysninger, herunder GEO-lokaliseringstjenester. Det er også viktig å være klar over at signaleringsdata kommuniserer hele tiden og legger spor, mens trafikkdata er koplet til den direkte bruken av appen og mobiltelefonen. I begge tilfeller kan dataene bidra til å profilere mobilbrukeren, altså er det snakk om personopplysninger.

8 Konklusjon og veien videre

Innledningsvis stilte vi spørsmålet: *Hva er mulighetsrommet for bruk av mobilapplikasjoner i sivil-militær krisehåndtering?*

Som denne rapporten viser, mener vi det finnes både spennende og høyst relevante muligheter for Forsvaret og totalforsvaret i å utnytte det potensialet som mobilteknologi etter hvert representerer til bruk i krisekommunikasjon og sivil-militær samhandling. Dette gjelder både på nettverks- og applikasjonsnivå. Generelt er teknologiske løsninger som er datasentriske, og som vektlegger

åpenhet, høy tilgjengelighet, enkelhet i bruk og som virker på mobile plattformer, et viktig element for å få informasjonen nærmere brukeren og de oppgavene som skal løses. Behovet for tilgang og deling av relevant informasjon der man til enhver tid er, samt behovet for sikkerhetsløsninger som gir større fleksibilitet, blir stadig mer påtrengende i krisehåndtering.

I kriser kan beslutningstakere typisk oppleve underskudd av relevant informasjon «der og da», for dårlig tid til beslutninger og generelt stor usikkerhet. Usikkerheten er knyttet til både situasjonen og til informasjonen som blir presentert. En mobilapplikasjon som gir mulighet for deling av sanntidsinformasjon og en felles krisekommunikasjonsstrategi kan teoretisk sett bidra til å redusere disse samvirkeutfordringene på tvers av sektorer og samvirkeaktører. Å tilrettelegge for teknologiske løsninger som åpner for informasjonsutveksling mellom aktører helt ned på enkeltmannsnivå og beslutningstaker vil i denne sammenheng også kunne styrke nærhetsprinsippet ved at man blir i bedre stand til å kunne utføre og ferdigstille en økende mengde av oppgaver på stedet, der man er mer effektivt og i sann tid. Rapporten skisserer derfor en ide til et konsept for å gjøre informasjon og funksjonalitet tilgjengelig i form av mobilapplikasjoner. I konseptet beskrives noen sentrale elementer, og forholdet mellom disse elementene, for å illustrere hvordan dette kan settes sammen til en "større helhet" som fungerer godt sammen, og som kan være relevante for informasjonsutveksling og samhandling i krisehåndtering.

Vi stilte også noen tilleggsspørsmål:

- Hva finnes av gratis og kommersielle mobilapplikasjoner for krisekommunikasjon og hvilke behov dekker disse løsningene? Svaret er at finnes en rekke løsninger, både gratis og kommersielle. Det eksisterer også flere app-byggesett der noen krever programmeringskompetanse og andre ikke.

- Hva vil være de største mulighetene og utfordringene for å ta i bruk slik teknologi? Utfordringene ved å ta i bruk andres apper er at man ikke har kontroll med hvor data lagres, appens funksjonalitet, sikkerhet og oppdateringer. Appene er ikke designet spesielt for det behovet som totalforsvaret vil ha for krisekommunikasjon i utfordrende situasjoner. Disse utfordringene kan reduseres gjennom eget utviklingsarbeid. App-teknologien gir muligheter for effektivisering, gitt utfordringene vi kjenner i dag med informasjonsdeling på tvers av domener og felles situasjonsbilde. Det finnes også en rekke verktøy for opinionsanalyse som gjør det mulig å følge med på utviklingen i folks holdninger til en sak.

- Hvilke informasjonsbehov kan dekkes av mobilapper? Internettet utgjør et hav av informasjon, noe som erfaring fra internasjonale humanitære kriser viser. Mobilapper kan hente informasjon fra nettet ved å crawle nettet og ved å kople seg opp mot ulike tjenester. Det finnes enorme mengder informasjon, men det er viktig å være klar over at kvaliteten på informasjonen lagret på nett kan være svært varierende, og i alvorlige sikkerhetspolitiske kriser direkte misvisende og et ledd i propagandakampanjer. Dessuten er kommunikasjonsinfrastrukturen i bunnen sårbar, særlig i sikkerhetspolitiske kriser og større

naturkatastrofer. Det vil derfor være viktig med alternative prosedyrer dersom internettet går ned i et område og en mister tilgang til informasjon.

Det er flere forhold som taler i mot at man ukritisk tar i bruk ferdigutviklede kommersielle eller gratis apper, jf. krisekommunikasjonsappene, som er omtalt i denne rapporten. Noe av grunnen er hensynet til behov hos norske aktører, datalagring og transparens, samt sikkerhet. Det er også organisatoriske utfordringer og barrierer når ulike virksomheter skal samarbeide, men samtidig gir samvirkeprinsippet et pålegg om samarbeid som er en dytt i riktig retning.

Selv om fremtidig bruk av smarttelefoni for militære applikasjoner forventes å øke er selvsagt ikke løsningen på «alle utfordringer» i det sivil-militære domenet bare å ta i bruk eller å lage en app. Men som rapporten beskriver er det et stort mulighetsrom for å utnytte mobilteknologi i forhold til å oppnå mer fleksible løsninger og for å tilgjengeliggjøre informasjon helt ned på enkeltmannsnivå. Dette vil styrke nærhetsprinsippet, forutsatt at den bakenforliggende infrastruktur sørger for at informasjonen når frem til brukeren.

I det videre forskningsarbeidet vil det derfor være naturlig å se på muligheten for å utvikle en eller flere teknologidemonstratorer som kan bidra til å øke kunnskapen på dette området og for å videreutvikle konseptet. Demonstratorer vil kunne bidra til å belyse potensiell nytteverdi mer konkret, samt å gi bedre dybdekunnskap og innsikt i noen av problemstillingene knyttet til hvilke muligheter man har for bruk av mobilapplikasjoner i sivil-militær krisehåndtering, også på infrastruktursiden og bakenforliggende systemer. Dette vil kunne bidra til å øke kunnskapen ikke bare innenfor temaer som informasjonsdeling, situasjonsforståelse og samhandlingsevne internt i totalforsvaret, men også innenfor området strategisk kommunikasjon som eksempelvis informasjon til offentligheten.

9 Referanser

Ablon, L., Libicki, M.C and A.A. Golay, *Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar*, Santa Monica: RAND Corporation 2014, http://www.rand.org/pubs/research_reports/RR610.html, nedlastet 7.8.2015.

Angeles, S., «18 Best App Makers», *Business News Daily*, 2015, http://www.businessnewsdaily.com/4901-best-app-makers-creators.html nedlastet 6.8.2015.

appsbar.com - How to Build a Free Android, iPhone, Windows, Blackberry, Facebook and HTML5 App, YouTube, https://www.youtube.com/watch?v=Oatucw4hoO0 nedlastet 3.2.2016.

Bergh A., *From the death grip of PowerPoint to mobile freedom – the Mobile Learning App Builder (MLAB)*, Kjeller: FFI-notat 2014/01452, 2014.

Bergh, A., "Distributing the disruption", *International Conference on Military Communications and Information Systems (ICMCIS)*, Published in IEEE *Xplore*® Digital Library , 2015: 1 - 6, DOI: 10.1109/ICMCIS.2015.7158688, 2015a.

Bergh, A. "The Final Destination: Building Test Bed Apps for DIL Environments", *Vehicular Technology Conference (VTC Spring)*, 2015 IEEE 81st, Published in IEEE *Xplore*® Digital Library, 2015: 1 - 5, DOI: 10.1109/VTCSpring.2015.7146128, 2015b.

Bakås, T.H., *Sosiale medier – en trussel mot virksomheter*, Norsis, publisert 12.12.2014, https://norsis.no/2014/12/sosiale-medier-en-trussel-mot-virksomheter/, nedlastet 3.1.2015.

Bjørnstad, A. L., og Elstad, A-K., *Utvikling og evaluering av spørreskjema med fokus på organisasjon og bruk av samhandlingsteknologi*, Kjeller: FFI-rapport 2015/00046, 2015.

CYFOR, *Mulighetsstudie - Militær anvendelse av LTE mobilnett*, CYFOR CKT-studierapport 2015 (Begrenset), 2015.

Liphshiz, C., "Israel Recruits 'army of Bloggers' to Combat anti-Zionist Web Sites", Haaretz, 19. Januar 2009, http://www.haaretz.com/print-edition/news/israel-recruits-army-of-bloggers-to-combat-anti-zionist-web-sites-1.268393, nedlastet 23.10.2015.

Digital Attack Map, webside, http://www.digitalattackmap.com/?imm_mid=0b2597&cmp=em-strata-na-na-newsltr_20131030_elist#anim=1&color=0&country=ALL&time=16000&view=map nedlastet 8.8.2015.

Derakhshan, H., "The web we have to save", Blog, 14. July 2015, https://medium.com,/matter/the-web-we-have-to-save-2eb1fe15a42#.7cg7eol0s, nedlastet 26.1.2016.

Datakrimstrategien, Politidirektoratet, 12. mai 2015, http://www.nsr-org.no/getfile.php/Dokumenter/Eksterne%20publikasjoner/Datakrimstrategi_2015.pdf, nedlastet 7.8.2015.

Digitaliseringsrundskrivet, 26. august 2014, https://www.regjeringen.no/globalassets/upload/kmd/aif/dokumenter/digitaliseringsrundskrivet_2014.pdf, nedlastet 23.10.2015.

Digital agenda for Norge — IKT for vekst og verdiskaping, Meld. St. 23 (2012–2013), https://www.regjeringen.no/no/dokumenter/meld-st-23-20122013/id718084/?ch=1, nedlastet 23.10.2015.

"Definition of sentiment analysis", Financial Times, ft.com/lexicon, https://lexicon.ft.com/Term?term=sentiment-analysis, nedlastet 1.2.2016.

Et forsvar i endring, Forsvarssjefens fagmilitære råd, Forsvaret 2015, https://forsvaret.no/fakta_/ForsvaretDocuments/EtForsvariEndring-Nett.pdf, nedlastet 23.10.2015.

Elstad A-K., Reitan B. K, "Mobile information platforms in the military domain", *NOKOBIT Vol.23 (Proceedings 2015),* 2015. http://ojs.bibsys.no/index.php/Nokobit/article/view/269/233, nedlastet 3.2.2016.

Elstad, A-K., Bjørnstad A. L., Hafnor, H., *Erfaringsrapport – analysestøtte knyttet til organisasjon og samhandling under Gram-øvelsene 2011–2013*, Kjeller: FFI-rapport 2015/00045, 2015.

Endregaard, M., Brattekås, K., Nystuen, K. O., Sandrup, T. og Gerhardsen, W. (Ed.)., *Beskyttelse av samfunnet i en ny tid*, Kjeller: Viten, Forskningsfaglig rapport 1, 2015.

"Expert Group on Cloud Computing Contracts", weboppslag, EU-kommisjonen, http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm, nedlastet 1.2.2015.

Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren, «FDs Cyberretningslinjer», Oslo: Forsvarsdepartementet, 1. mars 2014, https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf, nedlastet 3.2.2016.

«Get your likes», https://www.getyourlikes.co.uk/ nedlastet 7.8.2015

Global Cybersecurity Index & Cyberwellness Profiles, Report, Geneve: International Telecommunication Union, April 2015, http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf , nedlastet 26.8.2015.

Greenwald, G., *Overvåket. Snowden, NSA og overvåkningsstaten*, Oslo: Cappelen Damm, 2014.

Grunnan T, Maal M, Lessons learned and best practices from crisis management of selected natural disasters – elicit to learn crucial post-crisis lessons, FFI-rapport 2014/01993, 2014.

Hagen og Søgaard, *Strategisk kommunikasjon som redskap i krisehåndteringen*, Kjeller: FFI-Rapport -2013/03101, 2013.

Hagen, J. M., *Beskyttelse av samfunnet og digital sårbarhet: BAS-prosjektenes bidrag til samfunnssikkerhetsarbeidet i Norge over 20 år – kompendium for undervisning ved Universitetet i Nordland*, Kjeller: FFI-Notat 2015/02111, 2015.

Hagen, J. *Robust kommunikasjonsinfrastruktur for samhandling i krise*, FFI-Fakta, november 2014, http://www.ffi.no/no/Publikasjoner/Documents/FFIFakta_RUTIL%20%282%29.pdf nedlastet 1.2.2015.

Hagen, J.M. og V.Q, Pham, *Brannvesenets behov for robust informasjonsinfrastruktur for samhandling i krisesituasjoner*, Kjeller: FFI-Rapport 2014/01704, 2014.

Høie, Ø, Emblemsvåg, N. A., Melsether, T. Berg, L.S., Johansen, S., Kofoed, E. og I. Hagen, *KS2 (kvalitetssikring fase 2) av Ny IKT-løsning for departementene*. Oslo: Rapport til Finansdepartementet og Kommunal og moderniseringsdepartementet, 30. mai 2014, Metier.

Interdepartemental arbeidsgruppe, *Kartlegging av hindringer i regelverk for bruk av skytjenester. Overlevert kommunal- og moderniseringsdepartementet 13. mai 2015.* Oslo: Rapport fra interdepartemental arbeidsgruppe med deltakelse fra Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Kommunal- og moderniseringsdepartementet (KMD), Kunnskapsdepartementet (KD), Kulturdepartementet (KUD), Nærings- og fiskeridepartementet (NFD) og Samferdselsdepartementet (SD). https://www.regjeringen.no/contentassets/d48b5b5895e54d679fef76e0860140a8/skytjenester_arbeidsgrupperapport.pdf, nedlastet 15.8.2015

iProspect, 10 sentiment analysis tools track social marketing success, Blog, http://www.iprospect.com/en/ca/blog/10-sentiment-analysis-tools-track-social-marketing-success/, nedlastet 21.1.2016.

Johnsen, F. T., *Purple Nectar 2015*, Kjeller: FFI-reiserapport 2016/00184, Unntatt offentlighet, 2016.

Karlsen, L. H., Reitan B. K., *CEI - et sosialt taktisk rapporteringssystem - teknisk beskrivelse av Android klient for smarttelefon og nettbrettstøtte til CEI-systemet*, Kjeller: FFI-notat 2014/00526, 2014.

«Lag din egen app», Oslo: *Forsvarets forum* nr. 6, 2015, http://www.fofo.no/Lag+din+egen+app.b7C_xdfYWN.ips?template=master, nedlastet 23.10.2015.

Mattioli, R. and M. Dekker, *National Roaming for Resilience. National roaming for mitigating mobile network outages*. Heraklion (Hellas): ENISA-rapport. November 2013.

Maal, M., Grunnan, T., *Lessons learned from crisis management of forest fires – elicit to learn crucial post-crisis lessons*, Kjeller: FFI-rapport 2014/01969, 2014.

Maal, M., Grunnan, T., *Lessons learned from crisis management of floods – elicit to learn crucial post-crisis lessons*, Kjeller: FFI-rapport 2014/01973, 2014.

Maal M., Grunnan T, Maria Rosaria Gallipoli, Sabatino Piscitelli, Angelo Masi and Marco Mucciarelli, Lessons learned from crisis management of earthquakes – elicit to learn crucial post-crisis lessons, FFI-rapport 2014/01972, 2014.

Meld. St. 23 (2012-2013) *Digital agenda for Norge – IKT for vekst og verdiskaping*, Oslo: Kommunal og -moderniseringsdepartementet.

Manchini, F., *Modern mobile plattforms from a security perspective*, Kjeller: FFI-rapport 2016/00319, 2016.

Mohr, H. and R. Satter, "BP CEO Tony Hayward attends glitzy yacht race; Gulf residents infuriated", AP, 19th June 2010, http://www.csmonitor.com/From-the-news-wires/2010/0619/BP-CEO-Tony-Hayward-attends-glitzy-yacht-race-Gulf-residents-infuriated, nedlastet 9.9.2015.

Må ha mer enn mobil i kriser, FFI Forum, FFI nyhetsoppslag på nett 27.11.2014, http://www.ffi.no/no/Aktuelle-tema/Sider/Må-ha-mer-enn-mobil-i-kriser.aspx, nedlastet 7.1.2015.

NATO, *ACO Strategic Communication*, ACO Directive (AD) 95-2. 2009.

NKOM, *Det norske markedet for elektroniske kommunikasjonstjenester*, 20. mai 2015 Revidert 2. september 2015, http://www.nkom.no/marked/ekomtjenester/statistikk/det-norske-ekommarkedet-rapporter/_attachment/18155?_ts=14f8d082dd5 , nedlastet 3.2.2016.

NOU 2015:13 Digital sårbarhet – sikkert samfunn, Beskytte enkeltmennesker og samfunn i en digitalisert verden, https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/?ch=1&q= , nedlastet 2.3.2016.

Mørketallsundersøkelsen, Informasjonssikkerhet, personvern og datakriminalitet, Oslo: Næringslivets sikkerhetsråd (NSR), Rapport, http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014_WEB.pdf, nedlastet 18.12.2014.

Promise 1.0 Final report, Defence Material Organisation, [Dutch] Ministry of Defence, Final version 1.3, 30. April 2015.

På nett med publikum. Hvordan smarttelefonen og sosiale medier gir nye muligheter for norsk politi, Oslo: Teknologirådet, Rapport 02, 2014.

Reitan, B., K., *Information Management i det nye informasjonslandskapet*, Kjeller: Forsvarets forskningsinstitutt, Kjeller, FFI-rapport 2010/01732, 2010.

Reitan, B. K., Darisiro, R., Elstad, A-K., Gran, C. J., «Bringing New Arrangements to C2 - Experiments with Social Information», In: *20th International Command & Control Research & Technology Symposium (ICCRTS): The International Command and Control Institute*, 2015a.

Reitan, B. K., Elstad A-K., Gran C. J., *En ny klasse kommando og kontroll informasjonssystemer (K2IS) – eksperimenter med smarttelefoner og samhandling*, Kjeller: FFI-rapport 2015/02298, 2015b.

«Regjeringen oppnevner sikkerhetsutvalg», Pressemelding publisert på nett 27.3.2015, https://www.regjeringen.no/no/aktuelt/regjeringen-oppnevner-sikkerhetsutvalg/id2403919/ nedlastet 3.2.2016.

Rekvisisjonsloven, Lovdata, https://lovdata.no/dokument/NL/lov/1951-06-29-19?q=rekvisisjon, nedlastet 22.1.2015.

Robust kommunikasjonsinfrastruktur for samhandling i krise, Kjeller: FFI-Fakta, november 2014, http://www.ffi.no/no/Publikasjoner/Documents/FFIFakta_RUTIL%20(2).pdf nedlastet 15.8.2015.

«Slik jaget ildstormen gjennom sentrum», webpresentasjon, VG, http://www.vg.no/spesial/2015/laerdal/brannen.php, nedlastet 1.2.2015.

SOS Alarm, webside, http://www.sosalarm.se/nytt-system-for-vma, nedlastet 7.1.2015.

SSB, Statistikkbanken, https://www.ssb.no/statistikkbanken/ nedlastet 3.2.2016.

Strand, O. M, og Hagen J., *Med Propagandaens århundre unnagjort - hva er propagandatrusselen mot et digitalisert Norge*, Kjeller: FFI-rapport 2015/00811, 2015.

Strømmen, K., «Vi er to land som ikke lukker øynene», NRK, 08.09.2015, http://www.nrk.no/verden/_-vi-er-to-land-som-ikke-lukker-oynene-1.12541045, nedlastet 9.9.2015

Søgaard, H.A., Hagen, J. M., *Kampen om sannheten*, Kjeller: FFI-FOKUS, nr. 2 2014, http://www.ffi.no/no/Publikasjoner/Documents/FFI-Fokus_Kampen%20om%20sannheten_single-side.pdf, nedlastet 15.8.2015.

Søreide, I.E., *Ny Langtidsplan for Forsvarssektoren, Anmodning om Forsvarssjefen tilråding om den videre utviklingen av Forsvaret*, Brev datert 1. oktober 2014, https://www.regjeringen.no/globalassets/upload/fd/dokumenter/rammeskriv.pdf, nedlastet 18.12.2014.

«10 råd om mobilbruk på tur», weboppslag, Den Norske Turistforening, https://www.dnt.no/mobilvett/ nedlastet 3.2.2016.

Tema. Risiko- og krisekommunikasjon. DSB, september 2014, Tønsberg: DSB, http://www.dsb.no/Global/Publikasjoner/2014/Tema/risiko_og_krisekommunikasjon.pdf, nedlastet 23.10.2015.

The In Amenas Attack, Report of the investigation in to the terrorist attack on In Amenas. Prepared for Statoil ASA's Board of Directors, 8. September 2013, http://www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf, nedlastet 9.9.2015

«Vil legge til rette for bruk av skytjenester», Kommunal og moderniseringsdepartementet, publisert 5.6.2015, https://www.regjeringen.no/no/aktuelt/vil-legge-til-rette-for-bruk-av-skytenester/id2425281/ nedlastet 5.8.2015

Walker, S., "Salutin' Putin: inside a Russian troll house", 2. April 2015, http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house nedlastet 7.8.2015.