Evaluering af KRISØV 2013

BEREDSKABSSTYRELSEN

RIGSPOLITIET

Udgivet af Beredskabsstyrelsen og Rigspolitiet

Beredskabsstyrelsen
Datavej 16
3460 Birkerød
Telefon: 45 90 60 00
Fax: 45 90 60 60
E-mail: brs@brs.dk
www.brs.dk

Rigspolitiet
Polititorvet 14
1780 København
Telefon: 33 14 88 88
Mail: politi@politi.dk
www.politi.dk

Udgivet: August 2014
ISBN 978-87-91590-75-7

Forsidefoto: Colourbox

Indhold

Øvelseschefernes forord

KRISØV er en tilbagevendende national krisestyringsøvelse, der hvert andet år afprøver om rolle- og ansvarsfordeling, planer, procedurer og samarbejdsrelationer i det nationale krisestyringssystem fungerer efter hensigten.

KRISØV 2013 den 6. – 7. november 2013 var den sjette siden seriens start i 2003, og KRISØV har således været en katalysator for krisestyringssystemets udvikling i over et årti. Gennem årene er øvelseskonceptet gradvist ændret. Hvor tidligere KRISØV'er involverede flere uafhængige "spor", forsøgtes det denne gang at gøre én overordnet hændelsestype – cyberangreb – til omdrejningspunktet for at sikre samspil og koordination ud fra et fælles udgangspunkt. KRISØV 2013 blev dermed den hidtil største danske cyberøvelse, og ord som aktuel, nødvendig og realistisk er blevet brugt af deltagerne til at beskrive forløbet. Temaet blev valgt på baggrund af, at cyberangreb allerede i dag har en central placering i det nationale risikobillede, og at alt tyder på, at beredskabsplanlægning og krisestyringskapacitet på cyberområdet vil spille en stadig stigende rolle for samfundssikkerheden. Samtidig var der fra udgangssituationen et betydeligt læringspotentiale, eftersom mange øvelsestagere ikke i forvejen kunne forventes at have et indgående kendskab til cybertrusler og cybersikkerhed.

Når vi som øvelseschefer skal vurdere KRISØV 2013, er vi imponerede. Det skyldes ikke blot den indsats, som hundredvis af øvelsestagere og en bredt sammensat øvelsesledelse præsterede på de to øvelsesdage, men også den grundighed og det engagement, der blev lagt i at planlægge og forberede sig på øvelsen. Det at gøre forberedende aktiviteter til en mere integreret del af øvelseskonceptet var en særlig prioritet i forbindelse med KRISØV 2013, da vi ved af erfaring, at der er en klar positiv sammenhæng mellem omfanget af forberedelser og udbyttet af øvelser.

Under planlægningen og afviklingen af KRISØV 2013 blev der endvidere lagt særlig vægt på at skabe gode rammer for realistiske mediespil og borgerspil. Det er vores vurdering, at dette også lykkedes, og at bl.a. forsøget med at anvende et Twitter-lignende socialt medie for første gang i KRISØV-serien forløb godt. Befolkningen bruger i stigende grad sociale medier til at søge svar på spørgsmål i krisesituationer, og myndighederne kan både bruge de sociale medier som kilde til information og som middel til proaktiv kommunikation med offentligheden.

Valget af cyberangreb som overordnet øvelsesscenarie betød samtidig, at en række "nye spillere" blev bragt på banen under KRISØV 2013. Det gælder både aktører med et særligt ansvar for håndtering af cyberhændelser, og aktører, som ikke tidligere har deltaget i det nationale krisestyringssystems tværgående fora. Det er vores generelle indtryk, at øvelsen bidrog til at tydeliggøre afgørende snitflader på cyberområdet mellem disse aktører, og at de udviste stor professionalisme i forhold til at indgå i stabsarbejde, dele informationer og viden, koordinere handlinger og ressourcer i opgaveløsningen og samordne ekstern krisekommunikation til offentligheden.

KRISØV 2013 viste, at det nationale krisestyringssystem i sin eksisterende form kan anvendes i en kompleks situation, hvor mange myndigheder samt ejere og operatører af kritisk infrastruktur udsættes for cyberangreb. Som det fremgår af de følgende sider, kan der dog også peges på en række læringspunkter, konklusioner og anbefalinger, som kan bidrage til den fortsatte udvikling af krisestyringssystemet – både den udvikling, der finder sted i de tværgående fora og den udvikling, der sker blandt de deltagende organisationer enkeltvis.

God læselyst.

Mads Ecklon
Øvelseschef
Beredskabsstyrelsen

Bjarne Sørensen
Øvelseschef
Rigspolitiet

1. Sammenfatning

Den overordnede målsætning med KRISØV 2013 og med den efterfølgende tværgående evaluering er læring; dels generel læring om opgavevaretagelsen i det nationale krisestyringssystem, som gælder for alle større hændelses- og indsatsforløb, dels specifik læring på cyberområdet, som var omdrejningspunktet for KRISØV 2013 og dels læring af øvelsesteknisk karakter vedrørende planlægning, gennemførelse og evaluering i KRISØV-serien.

Evalueringen har tre fokusområder, og følgende udgør de overordnede konklusioner og anbefalinger.

Fokusområde 1: Tværgående samarbejde om krisestyringen

- KRISØV 2013 viste, at det eksisterende nationale krisestyringssystem er en velegnet ramme for at håndtere en situation med mange, komplekse og samtidige cyberangreb.
- Samarbejdet om krisestyringen fungerede godt generelt, men øvelsen afdækkede, at deltagelse i det nationale krisestyringssystem ikke er tilstrækkeligt strategisk forankret i alle organisationer, og at fokus i udviklingen af de tværgående stabe i lige så høj grad bør være på ad hoc medlemmer som på faste medlemmer. Observationer, som understøtter denne konklusion vedrører problemstillinger omkring forberedelse af forbindelsesofficerer, graden af parathed i baglandet, utilstrækkeligt kendskab til og begrænset brug af gældende plansæt.
- Det blev ligesom under tidligere KRISØV'er konstateret et særligt forbedringspotentiale vedrørende udarbejdelse og ajourføring af dokumentet Nationalt Situationsbillede (NSB). Samme konklusion gælder generelt for de lokale, myndighedsspecifikke og sektorvise situationsbilleder, som udgør datagrundlaget for NSB.
- I National Operativ Stab (NOST) blev godt indarbejdede procedurer, stram mødeledelse, høj mødedisciplin, effektiv sekretariatsvirksomhed og den generelle stabsdynamik fremhævet som særligt velfungerende. I Det Centrale Operative Kommunikationsberedskab (DCOK) fik samarbejdet om medieovervågning og krisekommunikation et løft sammenlignet med tidligere øvelser, men plansæt for staben blev ikke fulgt i tilstrækkeligt omfang, særligt på øvelsens første dag. I Hovedstadens Lokale Beredskabsstab (LBS11) kunne kvaliteten af stabsvirket også være hævet gennem mere metodisk anvendelse af stabsprocedurer, særligt i forbindelse med opstart og layout af tekniske hjælpemidler i den indledende "kaosfase".
- I de tværgående stabe kunne der generelt konstateres et godt fokus på igangværende hændelser, men ofte begrænset tværgående og proaktivt fokus på hændelsernes mulige udvikling. Tilsvarende var der ikke altid tilstrækkelig struktur i forhold til at holde overblik over status for planlagte, iværksatte og udførte aktiviteter.

Det anbefales:

- At alle statslige myndigheder og andre relevante parter forankrer arbejdet med beredskabsplanlægning og krisestyring på det strategiske ledelsesniveau i de enkelte organisationer, herunder deltagelsen i de nationale krisestyringsøvelser. Formålet med den strategiske forankring er at sikre, at myndigheder m.fl. kan varetage krisestyring inden for eget ansvarsområde i henhold til egen planlægning, bistå andre under større ulykker og katastrofer, der involverer flere sektorer samt indgå i tværgående krisestyringsfora.
- At statslige myndigheder og andre relevante parter opfordres til at udarbejde instrukser for udsendelse af repræsentanter til det nationale krisestyringssystems tværgående stabe som et fast element i deres beredskabsplaner. I denne sammenhæng kan potentielle ad hoc medlemmer også med fordel gøres opmærksomme på de tværgående stabes plansæt og øvrige relevante publikationer, kravet om sikkerhedsgodkendelse for adgang samt mulighederne for uddannelse i stabsdeltagelse via kurser, øvelser, sidemandsoplæring mv.
- At NOST fortsætter arbejdet med at forbedre kvaliteten af Nationalt Situationsbillede. Arbejdet bør tage udgangspunkt i behovet på strategisk niveau i regeringens krisestyringsorganisation og resultere i et nyt, samlet koncept for Nationalt Situationsbillede, hvori der lægges vægt på datagrundlag, prioritering, sammenhæng

og aktualitet. Det anbefales herefter at prioritere træning i NOST-sekretariatet samt blandt sektoransvarlige repræsentanter for at opbygge rutine i at udfærdige lokale, sektorvise og nationale situationsbilleder.

- At DCOK følger op på de udviklingsmuligheder, som blev identificeret under KRISØV 2013, herunder revidere konceptet for stabens procedurer og opgaver som myndighedsfælles kommunikationsberedskab og støttefunktion for NOST. Fokus bør herefter være på at understøtte stabsarbejdet med den struktur og den styring, som plansættet tilbyder samt opbygge rutinering i procedurerne blandt faste og ad hoc medlemmer, så DCOK udvikler større sammenhængskraft og parathed i forbindelse med enhver aktivering.
- At LBS11 inddrager læringspunkterne fra KRISØV 2013 i forbindelse med en videreudvikling af stabens operationsbefaling og generelle plansæt, herunder udvikling af standardprocedurer og vejledninger for medlemmernes opgaver samt layout af fysiske rammer og tekniske hjælpemidler ved aktivering.

Fokusområde 2: Styrkelse af kendskab og viden på cyberområdet

- KRISØV 2013 bidrog til at hæve opmærksomheden og læringen om cybertrusler og cybersikkerhed, men viste også, at man kan tage yderligere initiativer for at inkludere cyberforhold i beredskabsplanlægningen. Øvelsen afdækkede fx begrænset planlægning for og rutine i brugen af alternativ informations- og kommunikationsteknologi (IKT) blandt flere øvelsestagere. Tilbagemeldinger pegede også generelt på behov for bedre koordinering mellem traditionelt beredskabsarbejde og arbejde med it-sikkerhed og kommunikationsforhold.
- Under KRISØV 2013 var rolle- og ansvarsfordelingen i forbindelse med cyberhændelser på plads mellem Rigspolitiet, Politiets Efterretningstjeneste (PET), Forsvarets Efterretningstjeneste (FE) og Center for Cybersikkerhed (CFCS), og afprøvningen under øvelsen demonstrerede, at setuppet virkede. Øvelsen indikerede dog også, at ikke alle øvrige deltagere havde forudgående kendskab til den præcise opgavefordeling mellem disse myndigheder, og at der fortsat er stort behov for målrettet rådgivning og videndeling på cyberområdet blandt "ikke-specialist"-myndigheder.

Det anbefales:

- At brugen af alternative informations- og kommunikationsmidler planlægges og trænes yderligere på centralt og decentralt niveau for at imødekomme situationer, hvor primære digitale kanaler sættes ud af drift. Dette kan fx ske enten via "KOM-øvelser" (også kaldet signaløvelser) eller som element i andre øvelser og uddannelsesaktiviteter. Myndigheder og andre aktører bør endvidere opfordres til at udarbejde enkle instrukser omkring ressourcer og procedurer for brug af alternative IKT-midler som led i egen beredskabsplanlægning.
- At myndigheder med et særligt ansvar for håndtering af cyberhændelser følger op på øvelseserfaringerne via målrettet ekstern rådgivningsvirksomhed og udbreder kendskabet til deres rolle- og ansvarsfordeling.

Fokusområde 3: Øvelsestekniske forhold

- Opfølgningen på fire øvelsestekniske anbefalinger fra KRISØV 2011 evalueringsrapporten skabte en bedre øvelsesteknisk ramme for KRISØV 2013, og fokus på læring i både planlægningen, afviklingen og evalueringen bidrog positivt til resultatet. Den øvelsestekniske styring fungerede generelt godt, og en medvirkende faktor var, at øvelsesledelsens centrale indspil/svar-celle blev drevet som en stab. Væsentlige sårbarheder i relation til krisoev.dk-hjemmesiden tydeliggjorde dog behov for et bedre it-teknisk setup for KRISØV 2015.

Det anbefales:

- At de fire øvelsestekniske anbefalinger, som blev fremsat efter KRISØV 2011 og fulgt i KRISØV 2013 også skal gælde ved forberedelsen og gennemførelsen af KRISØV 2015.
- At der udvikles en mere tidsvarende, robust og brugervenlig øvelses-it-platform til brug for KRISØV 2015.
- At debriefinger og et evalueringsseminar fastholdes som god praksis i KRISØV 2015 evalueringsdesignet.

2. Om øvelsen

2.1 Formål og mål

Øvelsens overordnede formål og mål blev fastlagt i Kriseberedskabsgruppens øvelsesdirektiv af 23. oktober 2012.

Formålet var at øve krisestyringssystemet på det centrale niveau, med særligt fokus på evnen til at håndtere konsekvenserne af et større koordineret cyberangreb mod Danmark. Hovedvægten lå på at øve og afprøve samarbejdet og den tværgående koordination i krisestyringssystemet, herunder i relevant omfang regeringens krisestyringsorganisation, NOST, udvalgte centrale myndigheder, herunder Center For Cybersikkerhed samt andre aktører.

Der blev lagt vægt på, at øvelsen gav anledning til at eksperimentere gennem afprøvning af nye eller ændrede procedurer, tiltag mv.

Målene var, at relevante aktører skulle øve og afprøve fire generelle færdigheder og kompetencer (kerneopgaver i krisestyringen): 1. Etablering og drift af relevante stabe; 2. Informationshåndtering, med særligt fokus på opstilling og ajourføring af et fælles situationsbillede; 3. Koordination af handlinger og ressourcer; samt 4. Udsendelse af samordnet, ekstern krisekommunikation til befolkningen og medierne.

Med udgangspunkt i kerneopgaverne skulle øvelsestagerne øve og afprøve evnen til at opretholde og videreføre kritiske samfundsfunktioner i en situation, hvor cyberangreb truede, svækkede eller ødelagde kritisk infrastruktur.

2.2 Afgrænsning

KRISØV 2013 var alene designet til at øve og afprøve samarbejdet om krisestyringens generelle kerneopgaver på det strategisk og operationelle ledelsesniveau i de deltagende organisationer og stabe. Øvelsen omhandlede således ikke den rent it-tekniske håndtering af cyberangrebenes konsekvenser på taktisk niveau.

2.3 Proceduremæssigt grundlag

KRISØV 2013 blev planlagt og gennemført med udgangspunkt i, at øvelsestagerne skulle anvende og følge de beredskabsplaner, som fastlægger procedurerne i det nationale krisestyringssystem. National Beredskabsplan (6. udgave i høringsversion af 30. oktober 2013) udgjorde den overordnede ramme med sit overblik over krisestyringssystemets opbygning og ansvars- og kompetenceforhold på centrale områder samt beskrivelse af procedurerne i forbindelse med alvorlige risici og trusler mod samfundet. Den overordnede ramme blev fyldt ud og konkretiseret af plansættene for de tværgående stabe og aktørernes egne beredskabsplaner, delplaner, instrukser mv.

2.4 Deltagere

KRISØV 2013 involverede flere hundrede personer fra 39 organisationer, herunder myndigheder på centralt, regionalt og lokalt niveau, virksomheder med kritiske samfundsfunktioner, nyhedsmedier og ambassader. De fleste organisationer deltog både med øvelsestagere og medlemmer af øvelsesledelsen. Udover organisationerne enkeltvis var alle det nationale krisestyringssystems niveauer repræsenteret i fem tværgående fora: National Operativ Stab (NOST), Det Centrale Operative Kommunikationsberedskab (DCOK), Hovedstadens Lokale Beredskabsstab (LBS11), Embedsmandsudvalget for Sikkerhedsspørgsmål (E-SIK) og Regeringens Sikkerhedsudvalg (R-SIK).

Øvelsesledelsen bestod af ca. 30 medlemmer fra de organisationer, som var mest centrale i forhold til hovedscenariet - cyberangreb. Den overordnede styring af aktiviteterne i øvelsesledelsen blev varetaget af to øvel-

seschefer assisteret af øvrige centrale øvelsesplanlæggere fra Beredskabsstyrelsen og Rigspolitiet. På de to øvelsesdage var størstedelen af øvelsesledelsen placeret i en central indspil/svar-celle i Beredskabsstyrelsen, hvor der også var oprettet en mediecelle samt en borgercelle til at bringe sociale medier og tæt borgerkontakt ind i øvelsen. Endelig var der decentralt tilknyttet lokale indspillere i flere af de deltagende organisationer og stabe.

2.5 Varighed og forløb

KRISØV 2013 blev gennemført over to dage fra kl. 08:51 den 6. november til kl. 15:43 den 7. november 2013. Øvelsen fandt sted i realtid, men var ikke en døgnøvelse, og deltagerne besluttede selv, hvornår de lukkede ned for egen del af øvelsen mellem dag 1 og 2. Øvelsen begyndte med et "STARTEX" signal fra øvelsesledelsen, hvoraf det fremgik, at indspillene ville starte. Flere stabe var på dette tidspunkt allerede aktiveret, da der ikke var tale om en alarmeringsøvelse, men herudover svarede udgangssituationen til virkeligheden den 6. november.

Eftersom KRISØV er en læringsøvelse, opfordrede øvelsesledelsen til at afholde korte "timeouts" om aftenen på dag 1 for at samle op på og om, der var noget, der med fordel kunne ændres, og på dag 2 blev øvelsen afsluttet med en opfordring til at afholde debriefinger med foreløbig erfaringsopsamling, hvorefter det endelige "ENDEX" signal indeholdende øvelseschefernes førsteindtryk blev udsendt.

2.6 Overordnet scenarie, delscenarier og indspil

Øvelsens overordnede scenarie var et større cyberangreb rettet mod en række af samfundets kritiske funktioner. Angrebene medførte omfattende simulerede afledte konsekvenser, men tab af menneskeliv indgik ikke som led i øvelsens design. Forskellige delscenarier med i alt op mod 700 indspil var beskrevet i flere separate drejebøger.

Ved øvelsens start var den store internetforbindelse "Greenland Connect" mellem Canada, Grønland, Island og Danmark blevet afbrudt. Kort efter satte cyberangreb i flere tempi ind mod en lang række myndigheders hjemmesider, internetportaler og tjenester, som styrer offentlige serviceydelser. Der blev bl.a. opdaget fejl i NemID, digital signatur, CPR-registeret, Kortforsyningen (GST). I sundhedssektoren medførte angrebene bl.a., at data på sundhed.dk var frit tilgængelige, at Fælles medicinkort og Tilskudsregisteret gik ned, og at scannere på hospitaler ikke kunne bruges. Fødevaresektoren blev bl.a. påvirket af angreb på Eksportportalen, og Søfartsstyrelsen erfarede, at oplysninger om ejerforhold i Skibsregisteret var blevet ændret. Politiet blev også ramt, og oplevede angreb på interne arbejdssystemer samt et hack af politiets Twitterprofil med falske meddelelser om, at København skulle evakueres.

Herudover var der forlydender om, at tyske atomkraftværker var lukket ned efter at være blevet inficeret med en virus. Der var ikke risiko for radioaktivt udslip og ingen påvirkning af den danske energiforsyning, men hændelsen skabte bekymring i offentligheden, hvilket blev forværret af, at det europæiske nukleare målesystem og Beredskabsstyrelsens landsdækkende net af faste målestationer fejlagtigt meldte om øget radioaktivitet.

Hackerangreb resulterede fx også i driftstop for den københavnske metro, så togene standsede i rørsystemerne. Blandt passagererne var bl.a. mange kørestolsbrugere pga. en stor handicapkonference og mange udenlandske statsborgere, hvilket gav rig mulighed for at øve samarbejdet med udenlandske repræsentationer i København.

Konsekvenserne blev forstærket af, at store dele af det indre København fra øvelsens start var ramt af strømafbrydelse, som dog viste sig at skyldes overbelastning pga. mekaniske fejl frem for cyberangreb. Energisektoren iværksatte rullende aflastning via ind- og udkobling i to-timers intervaller for prioriterede områder. Det skabte udfordringer for kunder, som enten ikke var eller frygtede ikke at være tilstrækkeligt sikrede med nødstrøm, og indtil reparationsarbejdet i elnettet var tilendebragt ved øvelsens afslutning, fik el-sektoren henvendelser fra en lang række aktører, som forsøgte at få indflydelse på prioriteringerne ved at påberåbe sig særlige behov.

Under hele øvelsen var mobiltelefonnettet ustabilt og kørte på nødstrøm pga. cyberangreb og strømudfald. Samtidig brød e-mail og telefoni ned hos et stort antal organisationer, hvilket blev simuleret ved, at øvelsesledelsen sendte øvelsestagere besked om, at de ikke kunne anvende mobiltelefoner eller e-mail, indtil de fik besked igen.

Endvidere skulle flere øvelsestagere forholde sig til mistanke om eller reelle tilfælde af industrispionage. Fortrolige kommercielle oplysninger om olie og gas på dansk område blev fx stjålet via hackerangreb og sat til salg, hvilket fik Statens IT til at lukke ned for Energistyrelsens og Nordsøfondens IKT.

Efterretnings- og efterforskningsmæssigt foregik der et større arbejde med henblik på at afklare, hvem der udførte angrebene og hvorfra, om der var tale om koordinerede angreb, om det i så fald var en fremmed magt, en gruppe eller et løsere netværk, der stod bag. Dette medførte drøftelser om emner som folkeretten og muligheder for modsvar, hvis det kunne bevises, at en fremmed magt havde organiseret et koordineret cyberangreb mod Danmark.

Endelig skulle øvelsestagerne under store dele af øvelsen forholde sig til indspil, der ikke direkte relaterede sig til cyberangreb, men som bl.a. gav anledning til at teste disponerings- og prioriteringsevnerne samt håndtere bekymring og rygtedannelse i offentligheden, herunder evakuering af hospitalspatienter pga. strømsvigt, fund af forhøjede koncentrationer af bly i komælk, et muligt allergiudbrud pga. et parti forurenede hovedpinepiller, en silobrand på Aarhus Havn mv. Atter andre situationer opstod uforudset som resultater af "players action".

3. Om evalueringen

3.1 Formål, mål og fokusområder

Evalueringens formål og mål er afledt af øvelsesdirektivets beskrivelse af øvelsens formål og mål, jf. afsnit 2.1.

Formålet er at forbedre krisestyringssystemet i Danmark gennem læring. Evalueringen skal både afdække, hvad der fungerede godt og mindre godt under øvelsen for at opnå viden om, hvad der bør fastholdes, udbredes, videreudvikles eller ændres. For at optimere læringspotentialet vil mindre velfungerende forhold dog få mest plads.

Målene udgøres af tre punkter i øvelsesdirektivet, som fastslår, at KRISØV 2013 skal give grundlag for at: i) Styrke varetagelsen af kerneopgaverne i krisestyringen, herunder at vurdere om rolle- og ansvarsfordeling, planer, procedurer og samarbejdsrelationer fungerer efter hensigten; ii) Komme med anbefalinger vedrørende eventuelle ændringer, der kan styrke den samlede krisestyring; samt iii) Styrke bevidstheden om cybertrusler samt viden om sårbarheder og indbyrdes afhængigheder i kritiske samfundsfunktioner i forbindelse med større cyberangreb.

På denne baggrund blev der formuleret følgende tre fokusområder i KRISØV 2013 evalueringsdirektivet af 6. september 2013, som blev godkendt i øvelsesledelsen og fungerede som opdrag for evalueringens tilrettelæggelse.

1. Det tværgående samarbejde om krisestyringens fire generelle kerneopgaver for at håndtere konsekvenserne af et større, koordineret cyberangreb mod Danmark.
2. Udbyttet på strategisk og operationelt krisestyringsniveau med hensyn til at styrke bevidsthed om cybertrusler og viden om sårbarheder og indbyrdes afhængigheder mellem kritiske samfundsfunktioner i forbindelse med større cyberangreb.
3. Opfølgningen på øvelsestekniske anbefalinger fra KRISØV 2011, herunder konklusioner og læringspunkter vedrørende det resulterende udbytte for planlægningen og gennemførelsen af KRISØV 2013 samt anbefalinger til KRISØV 2015.

3.2 Afgrænsning

Den tværgående evaluering fokuserer på NOST, DCOK og LBS11 og vurderer ikke, hvordan de enkelte deltagende organisationer varetog krisestyringen internt under øvelsen. Øvelsestagerne er selv ansvarlige for at evaluere interne forhold.

3.3 Evalueringsmæssigt grundlag

Rammerne for evalueringen udgøres af Beredskabsstyrelsens vejledning "Helhedsorienteret beredskabsplanlægning", herunder særligt beskrivelserne af praksis i forhold til krisestyringens fire generelle kerneopgaver samt Rigspolitiets "Vejledning til evaluering af politioperative øvelser og indsatser". Principperne herfra er benyttet ved opstilling af evalueringsspørgsmål, analyse af indsamlede data samt formulering af konklusioner og anbefalinger.

Herudover udgøres vurderingsgrundlaget af en række planer, som var gældende på øvelsestidspunktet, herunder "National Beredskabsplan" (6. udgave i høringsversion af 30. oktober 2013 til brug for KRISØV 2013), "NOST Hovedplan for Stabens Virke" af 1. februar 2012, "DCOK Hovedplan for Stabens Virke" af 13. maj 2013 samt "Operationsbefaling B212 for iværksættelse af Hovedstadens Beredskabsstab (LBS11)" af 31. januar 2012.

3.4 Organisering, design og datagrundlag

KRISØV 2013 evalueringen blev, ligesom den overordnede øvelsesplanlægning, varetaget af Beredskabsstyrelsen og Rigspolitiet i fællesskab, og evalueringsgruppen indgik i øvelsesledelsen med reference til øvelsescheferne. Før øvelsen deltog evalueringsgruppen i øvelsesledelsens møder og andre forberedende aktiviteter med henblik på at kunne tilpasse evalueringsdesignet bedst muligt til øvelsen. Under øvelsen placerede evalueringsgruppens tre medlemmer sig sammen med tre yderligere ressourcepersoner som observatører i NOST, DCOK og LBS11.

Ligesom ved tidligere KRISØV'er inkluderede evalueringsdesignet et spørgeskema, hvor modtagerne blev anmodet om at udfylde én samlet besvarelse på vegne af hele deres organisation, herunder både øvelsestagere og øvelsesplanlæggere. Som supplement hertil indeholdt KRISØV 2013 evalueringsdesignet to nyskabelser i form af debriefinger i direkte forlængelse af øvelsen den 7. november og et evalueringsseminar den 12. december 2013.

Det samlede datagrundlag for evalueringen bestod af følgende kilder:

- Realtidsobservationer foretaget af observatører under øvelsen i NOST, DCOK og LBS11.
- Iagttagelser foretaget af øvelsescheferne og øvrige centrale øvelsesplanlæggere i øvelsesledelsen.
- Skriftligt materiale sendt cc til øvelsesledelsen under øvelsen, herunder diverse mødereferater, situationsbilleder samt e-mail korrespondance mellem øvelsestagerne.
- Lyd- og billedmateriale fra pressemøder, fiktive radioaviser og anden nyhedsdækning under øvelsen.
- Øvelseschefernes "ENDEX signal" med førstehåndsindtryk.
- 51 afrapporteringsskemaer fra debriefingerne i øvelsesledelsen, NOST og DCOK.
- Et notat med observationer og feedback fra debriefingen i LBS11.
- To afrapporteringer fra deltagende organisationers interne debriefinger.
- Et notat indeholdende erfaringsopsamling fra borgercellen og mediecellen i øvelsesledelsen.
- 24 besvarelser af KRISØV 2013-spørgeskemaet.
- Et udskrift med resultater fra 57 deltageres gruppearbejde på evalueringsseminaret.
- Udtalelser fra øvelsesplanlæggere og øvelsestagere i medieartikler udgivet før, under og efter øvelsen.
- Svar fra høringen over udkastet til evalueringsrapporten.

4. Tværgående samarbejde om krisestyringen

I de nedenstående afsnit gennemgås observationer, analyse, læringspunkter, konklusioner og anbefalinger vedrørende evalueringens fokusområde 1: *"Det tværgående samarbejde om krisestyringens fire generelle kerneopgaver for at håndtere konsekvenserne af et større, koordineret cyberangreb mod Danmark"*.

4.1 Samarbejdet i National Operativ Stab (NOST)

4.1.1 Kerneopgave 1 – Etablering og drift af staben

Af øvelsestekniske grunde var NOST etableret i operationsberedskab (trin 3) før øvelsens start. Staben var sammensat af de syv faste medlemmer – Rigspolitiet (som formandskab og som almindeligt medlem), Beredskabsstyrelsen, FE ved Center for Cybersikkerhed (CFCS), Forsvarskommandoen, PET, Sundhedsstyrelsen og Udenrigsministeriet – samt fem ad hoc medlemmer: Energistyrelsen, Fødevarestyrelsen, Statens IT, Søfartsstyrelsen og Trafikstyrelsen (repræsenteret ved BaneDanmark). Herudover deltog DCOK's stabschef, da DCOK er en stab under NOST, og Geodatastyrelsen deltog under Rigspolitiets ledelse i støttefunktionen Geodata-staben.

Med hensyn til bemandingen vurderes det generelt, at der var tilstrækkeligt personel i NOST. Flere myndigheder stillede med mere end én repræsentant, og disse kunne, når der afholdtes stabsmøder, enten sidde med ved stabsbordet, overvære møderne fra sidelinjen eller arbejde i separat allokerede arbejdsrum. Blandt de myndigheder, som stillede med én repræsentant, har flere efterfølgende tilkendegivet, at to personer havde været mere optimalt for både at holde tilstrækkeligt øje med udviklingen i eget bagland og bidrage aktivt i staben.

Undervejs i øvelsen blev rollen som stabschef for NOST skiftevis varetaget af to af Rigspolitiets ledere, hvilket virkede realistisk i lyset af det overordnede øvelsesscenarie med tegn på et længerevarende hændelses- og indsatsforløb. I enkelte tilfælde blev repræsentanter fra andre myndigheder afløst af kollegaer, men det er generelt ikke indtrykket, at stabsmedlemmerne planlagde for afløsning.

Mødeaktiviteten startede på dag 1 med et 10-minutters velkomstmøde, hvor der blev givet praktisk information om arbejdspladser, forplejning, maillister mv. Formandskabet understregede endvidere vigtigheden af, at sektorvise situationsbilleder skulle udarbejdes i en fælles skabelon som input til Nationalt Situationsbillede (NSB), som blev betegnet som NOST's "hovedleverance". Frem til det første stabsmøde kl. 11:00 foregik forberedelserne generelt afdæmpet og systematisk, og signalerede dermed en kontrolleret "kaosfase". Der blev efterfølgende afholdt stabsmøder kl. 13:00, 15:30 og 17:30. På dag 2 blev der afholdt stabsmøder kl. 9:00, 11:00 og 13:00. Et sidste møde kl. 15:00 var ikke et stabsmøde, da stabschefen meddelte, at øvelsen reelt var afsluttet, så der ikke var behov for at gennemgå dagsordenen eller udsende en sidste version af NSB før den fælles debriefing i NOST.

De syv stabsmøder blev gennemført i henhold til samme faste dagsorden, som lå ved alle pladser på stabsbordet fra øvelsens start. Møderne varede typisk mellem en halv time og tre kvarter. Enkelte deltagere har efterfølgende tilkendegivet, at de fandt stabsmøderne for lange, samt at der var for kort tid mellem dem til at koordinere tilstrækkeligt med kolleger i NOST og eget bagland samtidig med, at de skulle levere input til NSB med kort frist.

Driften af NOST var generelt karakteriseret ved en høj grad af mødedisciplin, en stram mødeledelse og en effektiv sekretariatsvirksomhed, hvilket blev fremhævet under den fælles debriefing som forhold, der fungerede særlig godt. Alle var på plads ved hvert mødes start, det skete yderst sjældent, at deltagere forlod et møde pga. telefonopkald, talerækkefølgen blev respekteret, og stabschefen og sekretariatslederen optrådte lyttende, positive og strukturerede. Det samme gjaldt den generelle stabsdynamik, hvor dialogen mellem parterne blev beskrevet under debriefingen med ordene "aldrig været bedre".

En bagvedliggende faktor herfor kunne være, at mange repræsentanter havde tidligere erfaring i NOST og kendte hinanden. Dog blev der fra flere førstegangsdeltagere blandt de nye ad hoc medlemmer fx efterspurgt en indledningsvis orientering og indføring i stabens virke, en præsentationsrunde, navneskilte, en liste med fagtermer, samt mere konkret hjælp og feedback i startfasen. Forskelle i organisationskulturer og arbejdsgange blev også bragt op, fx at "det kunne være svært som civil myndighed at blive integreret i kommandostrukturen".

Evalueringsgruppen betragter ovenstående som vigtige læringspunkter. Formandskabet kan i en lignende situation, hvor flere nye ad hoc-medlemmer indkaldes, med fordel prioritere den indledningsvise orientering mv. Samtidig bør det imidlertid også kunne forventes, at nye repræsentanter har tilegnet sig et godt forudgående kendskab til procedurerne i NOST. Det er en forudsætning, at deltagerne besidder de rette kompetencer og mandat.

De fysiske rammer, det logistiske setup og it-supporten i NOST vurderes generelt hensigtsmæssig. I stabslokalet var der i en passende afstand til stabsbordet placeret to separate arbejdsstationer til sekretariatets referenter og Geodata-staben, og øvrige repræsentanter i både NOST og DCOK kunne overvære møderne fra pladser langs væggene. Nogle deltagere fandt det dog tidskrævende at måtte overføre data mellem egne medbragte pc'er og Rigspolitiets pc'er i de separate arbejdsrum, samt ikke at kunne tilføje printere til medbragte pc'er. Det er på den baggrund bl.a. foreslået at udbygge NOST it-vejledningen med en mere letlæselig og enkel brugerguide.

Enkelte repræsentanter fremhævede desuden et positivt udbytte af at have anvendt video-tele-konference (VTC) funktion på eget medbragt udstyr til at stå i direkte audiovisuel kontakt med egen organisations interne krisestab.

Med hensyn til alternative IKT-midler var NOST-sekretariatet fx hurtige til at stille en faxmaskine til rådighed, da behovet meldte sig hos øvelsestagere, hvis normale kommunikationslinjer var afbrudt som led i øvelsen. Det blev dog påpeget, at backup-udstyr som faxmaskiner og udlånte SINE radioer skal være klargjort. Problematikken om, at ikke alle myndigheder råder over REGNEM-systemet til klassificeret kommunikation, blev ligeledes nævnt.

Udover at vise udkast til NSB og stabsmødereferater blev storskærmene i stabslokalet stort set kun brugt til at vise kort over det område, som var ramt af strømafbrydelse, og disse blev sjældent inddraget i drøftelserne på møderne. Dette var formentligt et resultat af, at cyberhændelserne ikke medførte behov for at fokusere detaljeret på fysiske skadesteder, men det foreslås, at Geodata-stabens arbejde gives en større rolle i KRISØV 2015.

4.1.2 Kerneopgave 2 – Informationshåndtering

Informationshåndteringen under den mundtlige behandling på stabsmøderne syntes overordnet set at have fungeret ukompliceret. Som anført ovenfor, var der tale om en stram mødeledelse og høj mødedisciplin, hvilket var med til at understøtte informationsudvekslingen og videndelingen. Alle kunne komme til orde, og der blev stillet spørgsmål, hvis noget var uklart. Det er dog evalueringsgruppens opfattelse, at det – ikke mindst for nye deltagere – til tider var vanskeligt at sondre mellem, hvilke informationer der skulle indgå i henholdsvis den mundtlige behandling, i de skriftlige versioner af NSB og i stabsmødereferaterne. Herudover var informationshåndteringen ifølge enkelte deltagere præget af envejskommunikation fra myndigheder til NOST og ikke den modsatte vej.

Specifikt vedrørende Nationalt Situationsbillede

Mens deltagerne overvejende var tilfredse med den mundtlige informationshåndtering, havde de stort set alle kritiske kommentarer i forhold til NSB som skriftligt produkt. Som nævnt, havde formandskabet allerede på velkomstmødet betegnet NSB som "hovedleverancen" og understreget vigtigheden af at følge en ny udarbejdelsesprocedure. Ifølge denne skulle deltagerne først hver især udarbejde sektorvise/myndighedsspecifikke situationsbilleder efter samme skabelon. Disse skulle tilgå NOST-sekretariatet senest 45 minutter før hvert stabsmøde, hvorefter de blev sammenskrevet til samlede NSB-udkast, som deltagerne modtog senest 15 minutter før hvert

stabsmøde. På møderne blev udkastene gennemgået på storskærm for at afkorte tekst og korrigere fejl mv. Efter møderne skulle NOST-sekretariatet tilrette de endelige versioner før udsendelse.

Proceduren var således blevet mere "skriftliggjort" sammenlignet med KRISØV 2011, hvor det var det sagte ord under bordrunder på stabsmøder, som NOST-sekretariatet skulle skrive ind i NSB efterfulgt af en tidskrævende godkendelsesproces blandt stabsmedlemmerne. Da KRISØV 2013 begyndte, var der stor tiltro til, at den nye procedure ville virke, og alle var enige om at følge den konsekvent, hvilket med enkelte undtagelser også skete på øvelsesdag 1. Stabschefen påmindede flere gange om, at al tekst skulle fattes i korthed, og at det ikke var NOST-sekretariatet, men medlemmerne selv, der skulle afkorte tekster efter anmodning, da NOST-sekretariatet ikke forventedes at have den sektorspecifikke ekspertise til at prioritere, hvad der kunne slettes.

Udfordringerne omkring informationshåndteringens omfang og indhold ændrede sig dog efterhånden som antallet af indspil øgedes, og det blev stadig vanskeligere at håndtere de mange aktuelle informationer inden for de rammer, der var udstukket for opdateringen af NSB. Dette blev særlig tydeligt på det sidste stabsmøde på dag 1, hvor det fra formandskabets side blev besluttet, at NOST-sekretariatet i løbet af aftenen skulle arbejde på en optimering af proceduren. Ved øvelsens genoptagelse på dag 2 var sekretariatet klar med ændrede retningslinjer. De blev udsendt på skrift og fremlagt i staben, hvor der i al væsentlighed var opbakning til dem bordet rundt.

Den reviderede procedure betød, at de fleste stabsmedlemmer overvejende skulle koncentrere sig om bidrag til pkt. 2, 5 og 6 i NSB-skabelonen. Pkt. 1 og 3 blev forbeholdt NOST-sekretariatet, pkt. 4 blev forbeholdt efterretningstjenesterne (med mindre andres risikovurderinger var strengt nødvendige), pkt. 7 blev primært forbeholdt Udenrigsministeriet, pkt. 8 blev forbeholdt DCOK, og pkt. 9 og 10 skulle kun udfyldes, hvis indholdet var relevant for alle. Samtidig blev det søgt tydeliggjort, hvilken information der skulle med i mødereferater, men ikke i NSB, som principielt skulle reserveres til regeringens krisestyringsorganisation. Tidsfristerne i proceduren fra dag 1 blev fastholdt.

NSB skabelon anvendt under KRISØV 2013

1. Hændelse i overskriftform
2. Resume af hændelsen/situationen
3. Hvor er det sket?
4. Trusselsvurdering/Risikovurdering
5. Overordnet beskrivelse af iværksatte tiltag
6. Ekstraordinær ressourcetilvejebringelse/-dispositioner
7. Internationale og diplomatiske forhold
8. Mediebillede og krisekommunikation
9. Andre informationer
10. Vurdering af hændelsens mulige konsekvenser

Efter den første NSB-opdatering, blev den nye procedure drøftet og mindre justeringer foretaget på et stabsmøde. På det efterfølgende stabsmøde blev det konstateret, at proceduren grundlæggende fungerede som ønsket.

Evalueringsgruppens nærlæsning af alle udkastene til og de endelige versioner af NSB'er fra øvelsen bekræfter indtrykket af et forbedringspotentiale. Det må i denne forbindelse naturligvis tages i betragtning, at de mange øvelsesindspil næsten uundgåeligt resulterede i komplekse NSB'er, og i debriefingen fremhævede deltagerne, at produktionen gik hurtigere og bedre end i tidligere øvelser. Samlet konkluderedes det dog, at proceduren, selvom den blev forbedret, burde have resulteret i slutprodukter af højere kvalitet. Det blev endvidere tilkendegivet, at der til tider optrådte oplysninger, som var uaktuelle på udsendelsestidspunktet, og dermed blev der efterlyst endnu hurtigere udarbejdelse. Der ses ikke behov for større justeringer i skabelonen for NSB, men derimod optimering af forhold som datagrundlag, prioritering, sammenhæng, aktualitet og rutinering i udfærdigelsen af dokumentet.

Øvrige opgaver som led i informationshåndteringen

Udover arbejdet med NSB varetog NOST-sekretariatet en række andre opgaver i henhold til plansættet, herunder overvågning og fordeling af mail, telefon, fax og sikrede kommunikationssystemer. Blandt de vigtigste af disse opgaver var den løbende logføring i POLDOK. Tilbagemeldinger til evalueringen indikerer, at logføringen blev professionelt udført, men også at det høje aktivitetsniveau gjorde det svært for mange at nå at konsultere indholdet, samt at det primært var de "uniformerede" deltagere, som brugte POLDOK.

En anden vigtig opgave var at udfærdige stabsmødereferater, som fulgte mødedagsordenen gengivet til højre. Referaterne er principielt sammen med POLDOK og NSB de primære kilder til at fastholde overblikket i NOST på skrift. Evalueringsgruppens gennemlæsning af de syv stabsmødereferater og optælling af input fra hver deltager viser imidlertid, at den refererede information ofte var for sparsom, og det var bemærkelsesværdigt, hvor få gange tekst optrådte under de vigtige punkter 4-7. Det vurderes på den baggrund, at de ikke i tilstrækkelig grad fremstod som beslutningsreferater, sådan som det tilstræbes i NOST-planen. Det skal for god ordens skyld nævnes, at stabschefen flere gange opfordrede deltagerne til at vende sig mod referenten og udtale: "Det er følgende, der skal stå i referatet", men det blev sjældent efterlevet. Enkelte deltagere har tilkendegivet, at dagsordenen, og dermed referatskabelonen, bør ændres, så møderne bliver mere præcise.

NOST dagsorden for KRISØV 2013

1. National Status v. formand for NOST
2. Referat fra forrige møde (rettelser)
3. Status for tilstedeværende myndigheder
a) Efterretningsbillede PET
b) Efterretningsbillede FE
c) Risikovurdering andre
Øvrige faste medlemmer
a) Beredskabsstyrelsen
b) Forsvarskommandoen
c) Sundhedsstyrelsen
d) Udenrigsministeriet
e) Rigspolitiet
f) Geodatastyrelsen (rettet til Geodata)
g) DCOK

Øvrige ad hoc myndigheder
a) Statens IT
b) Søfartsstyrelsen
c) Energistyrelsen
d) Digitaliseringsstyrelsen (udgået)
e) Fødevarestyrelsen
f) Trafikstyrelsen
4. Status fra lokale beredskabsstabe
5. Fremadrettede drøftelser
6. Opgaver til næste møde
7. Punkter der skal løftes op til Kriseberedskabsgruppen
8. Næste møde (tidsangivelse)
- Andre informationer
- Vedlagte bilag

Endelig bemærkes det, at der ikke blev udarbejdet en fortløbende aktionsliste i NOST med informationer om, hvilke tiltag, det var besluttet at sætte i værk samt deres status ("gennemført", "under udførelse", "afventer").

4.1.3 Kerneopgave 3 – Koordinering af handlinger og ressourcer

Koordineringen af handlinger og ressourcer syntes generelt at have fungeret godt i NOST. Overfor nævnte faktorer som jævnlige stabsmøder, god stabsdynamik, et flertal af erfarne forbindelsesofficerer samt kompetent mødeledelse og sekretariatsvirksomhed var alle befordrende for koordineringen. Under debriefingen var deltagerne desuden enige om, at koordineringen bl.a. havde været bedre end i tidligere KRISØV'er, fordi deres respektive baglande havde været gode til at tale sammen. Feedback fra spørgeskemabesvarelser bekræfter dette indtryk.

Øvelsen gav fx i særlig grad mulighed for at øve det tætte, direkte samarbejde mellem CFCS, PET's Cybersektion og Rigspolitiet samt til et omfattende bilateralt samarbejde mellem disse og andre deltagende organisationer. Koordineringen i NOST bidrog her til at afklare øvrige øvelsestageres eventuelle manglende eller begrænsede kendskab til den præcise rolle- og ansvarsfordeling på cyberområdet.

Trods dette og talrige andre eksempler på god koordinering kan der dog sættes spørgsmålstegn ved, om NOST til stadighed besad et samlet overblik over nødvendige, tilgængelige og indsatte ressourcer. Et sådant ressourceoverblik blev besværliggjort af øvelsens kompleksitet og af, at cyberangreb som scenarie er så diffust og forskelligt fra andre hændelsestyper (fx med hensyn til fysiske skadesteder), at det for flere af stabsmedlemmerne var vanskeligt at "melde ressourcer ind". Evalueringsgruppen finder imidlertid, at staben skal være mere opmærksom på at få opsummeret de vigtigste handlings- og ressourceprioriteringer ved afslutningen af samtlige stabsmøder.

Herudover synes der, særligt blandt ad hoc-medlemmerne, at have manglet baggrundsviden om, hvilke kapaciteter, de respektive myndigheder råder over i forhold til øvelsens forskellige delscenarier. I en krisesituation vil der ikke være megen tid til at formidle information herom, og på evalueringsseminaret blev det derfor foreslået, at man som supplement til kurser som "Samfundets beredskab" og "Krisestaben i samfundets beredskab" fx kan lade ad hoc-medlemmer præsentere deres opgaver, ansvar mv. på de årlige samlinger i NOST.

Endelig bemærkes det, at det ikke på noget stabsmøde blev drøftet, om beslutninger skulle indstilles til eller anmodes fra regeringens krisestyringsorganisation. Det betød dog ikke, at opmærksomhed på det strategiske niveau var fraværende i NOST's koordinering af handlinger og ressourcer. På et stabsmøde understregede stabschefen fx, at beslutninger fra NOST burde være så friske som muligt før et møde mellem rigspolitichefen og justitsministeren. På et andet stabsmøde blev medlemmerne kraftigt opfordret til at have deres bagland i orden forud for kommunikation til deres departementschefer til brug for videokonferencer med E-SIK og R-SIK.

4.1.4 Kerneopgave 4 – Ekstern krisekommunikation til befolkningen og medierne

Medieovervågning og krisekommunikation på vegne af NOST koordineres i DCOK og beskrives nedenfor i afsnit 4.2. Evalueringsgruppen skal dog her nævne nogle observationer relateret til beslutninger om krisekommunikation i NOST og samspillet med DCOK. Blandt positive eksempler kan nævnes, at man allerede på første stabsmøde besluttede, at forbindelsesofficeren fra CFCS umiddelbart efter mødets afslutning skulle tage kontakt til eget bagland for at fremskynde beslutning om en fælles pressemeddelelse fra CFCS og PET. Et andet eksempel var, at et spørgsmål om proaktiv brug af sociale medier i krisestyringen blev behandlet i staben, hvor et medlem fremhævede, at dette måtte være op til de enkelte myndigheder, og da alle var enige, blev forholdet ført til referat.

Omvendt har evalueringsgruppen kunne observere, at der særligt på dag 1 tilgik NOST forholdsvis begrænset information om medieudviklingen via DCOK-stabschefens talepunkt på dagsordenen og ved, at andre medlemmer sporadisk nævnte oplysninger i mediernes nyhedsdækning. Det blev generelt heller ikke drøftet, om medierne blev anvendt aktivt nok som led i krisestyringen. Tilsvarende vurderes det, at staben ikke var tilstrækkeligt opmærksom på behovet for fyldestgørende tekst under NSB-skabelonens pkt. 8 "Mediebillede og krisekommunikation", til trods for at stabschefen på 3. stabsmøde henledte opmærksomheden herpå som et vigtigt læringspunkt.

Krisekommunikation er en kerneopgave i krisestyringen, og det var derfor uhensigtsmæssigt, at emnet fik så relativt begrænset opmærksomhed i NOST. Dette også set i lyset af tilbagemeldinger, som viser, at øvelsens mediespil generelt blev opfattet som yderst relevant og realistisk. Det foreslås derfor, at input fra DCOK fremover får en mere fremtrædende rolle på NOST-stabsmøder. DCOK er en støttefunktion for NOST, og resultaterne af medieovervågningen, herunder af hvad der skrives, siges og vises om myndighedernes indsats, samt koordineringen af myndighedernes krisekommunikation, bør være solidt integrerede elementer i drøftelserne på NOST-møder.

4.2 Samarbejdet i Det Centrale Operative Kommunikationsberedskab (DCOK)

4.2.1 Kerneopgave 1 – Etablering og drift af staben

DCOK var ligesom NOST allerede aktiveret i operationsberedskab før øvelsens start. Kommunikationsmedarbejdere fra de faste medlemmer (de samme som i NOST) var permanent til stede i DCOK. Derudover deltog repræsentanter fra Statens IT og Trafikstyrelsen som ad hoc-medlemmer.

Tre myndigheder deltog ikke i DCOK, selvom de var repræsenterede i NOST. Dette blev set som en klar udfordring i DCOK, bl.a. fordi disse myndigheders repræsentanter i NOST ikke kunne forventes at have kompetence til at håndtere kommunikations- og pressespørgsmål sideløbende med opgaver i NOST. Det bemærkes, at der tilstræbes spejling af sammensætningen af NOST og DCOK i begge stabes hovedplaner, og at det som udgangspunkt er vigtigt, at kommunikationsmedarbejdere er fysisk tilstede i DCOK, da det giver kortere responstid. Trods dette blev forholdet imidlertid ikke løftet op i NOST-regi. I tilbagemeldinger til evalueringen har de pågældende myndigheder sidenhen identificeret bemanding af DCOK som forbedringspotentiale – eller som minimum forbedret koordinering med DCOK i situationer, hvor fysisk tilstedeværelse ikke vurderes muligt.

Med hensyn til bemandingen blev det på dag 1 konstateret, at der manglede folk fra Rigspolitiet i DCOK, men på dag 2 opnormerede Rigspolitiet, så der udover stabschef og sekretær indgik tre kommunikationsmedarbejdere. To af Rigspolitiets kommunikationsansvarlige varetog skiftevis rollen som stabschef, hvilket virkede realistisk ud fra det overordnede øvelsesscenarie. Ligesom i NOST var det dog generelt ikke indtrykket, at øvrige organisationer havde planlagt for afløsning af personel ved et længerevarende forløb.

Øvelsen startede i DCOK ved, at stabschefen bød velkommen, indledte en introduktionsrunde og informerede om, hvem der ville fungere som stabschefer, og hvem der ville fungere som sekretariatsleder. Stabschefen præsenterede herefter en ny skabelon for DCOK-mediesituationsbilledet med henblik på udfyldelse af NSB i medie- og kommunikationsregi. Dette var med til at give en god start på øvelsen, men flere deltagere har, ligesom det gjaldt i NOST, sidenhen efterspurgt en bedre indledningsvis briefing og praktisk indføring i DCOK's virke. Forholdet skyldtes muligvis, at flere af de tilstedeværende stabsmedlemmer ikke havde forudgående erfaring i DCOK. Meget tydede ligeledes på et begrænset kendskab til DCOK-planen. Evalueringsgruppen konstaterer, at planen indeholdt flere procedurer for stabens drift, som med fordel kunne have været bragt i anvendelse.

På dag 1 blev der ikke afholdt faste stabsmøder efter en fast dagsorden, hvilket var en proceduremæssig afvigelse fra DCOK-planen. I stedet valgte formandskabet en mere ad hoc-tilgang. Det betød, at man typisk tog en "5-minutters bordrunde" på baggrund af det mediemæssige billede og behovet for fælles udspil. På dag 2 gik DCOK over til en mere struktureret mødeaktivitet, bl.a. som følge af en "timeout" ved afslutningen af dag 1, hvor alle blev spurgt om ønsker til justeringer. Man valgte, at alle medlemmer skulle mødes fast i DCOK stabslokalet ca. et kvarter før hvert NOST-stabsmøde for at sikre fælles forståelse af det aktuelle mediebillede og give mundtligt input til DCOK-stabschefen, som denne kunne viderebringe på NOST-møderne. Derudover valgte man at mødes fast i stabslokalet umiddelbart efter hvert NOST-møde for at få en fælles forståelse af det operative situationsbillede, hvad dette kunne medføre af kommunikative opgaver, samt hvem der gjorde hvad i hvilke sektorer. Denne øgede strukturering af mødeaktiviteten medførte tydeligvis et bedre overblik og mindre stress i DCOK på dag 2.

Pladsen i stabslokalet kunne til tider være trang og lydniveauet højt, men det var positivt at se, at flere deltagere fra tid til anden brugte de separate arbejdsrum sammen med NOST-repræsentanter fra egne myndigheder.

4.2.2 Kerneopgave 2 - Informationshåndtering

Ifølge den nye skabelon for DCOK-mediesituationsbilledet, som blev præsenteret umiddelbart før øvelsens start, skulle medlemmerne først udfylde og overlevere blanketter med det aktuelle mediesituationsbillede for egen sektor til DCOK-sekretariatet, som efterfølgende udfyldte NSB-skabelonens pkt. 8 "Mediebillede og krisekommunikation" og videreformidlede resultatet til NOST-sekretariatet før forelæggelse på NOST-stabsmøderne. Blanketsystemet viste sig imidlertid at være for tungt at anvende i forhold til udbyttet. Forbindelsesofficererne fandt generelt blanketterne for bureaukratiske, og det var vanskeligt for DCOK-sekretariatet at sammenskrive de mange input til nogle få linjer tre kvarter før NOST-møderne.

På dag 2 valgte man derfor at overgå til en procedure med flere mundtlige afrapporteringer, som blev dokumenteret af DCOK-sekretariatet og meldt ind til NSB efter samtykke fra de involverede parter. Denne procedure og øvrige tiltag medførte en betydeligt bedre informationshåndtering i DCOK på dag 2, omend evalueringsgruppen hæfter sig ved, at der også på dag 2 tilgik NOST relativt sparsom information fra DCOK på skrift til NSB og via DCOK-stabschefens mundtlige orienteringer på NOST-stabsmøderne.

Som led i informationshåndteringen anvendte politiets medarbejdere i DCOK-sekretariatet flittigt POLDOK, som var projekteret på storskærm i stabslokalet, så alle løbende kunne følge dispositionerne. Dette virkede godt, men det er ikke indtrykket, at de øvrige medlemmer fulgte informationerne i samme grad, hvilket resulterede i, at de

ofte efterspurgte information, som allerede var dokumenteret. Manglende rutinering blandt DCOK-medlemmer i at overvåge POLDOK i tillæg til den eksterne mediedækning blev dermed identificeret som en udfordring.

Der blev ikke som led i informationshåndteringen i DCOK anvendt en fast dagsorden, skrevet korte beslutningsreferater fra møder eller ført en fortløbende aktionsliste med informationer om tiltag og deres status. Dette kunne muligvis have tilført værdi i forbindelse med stabens input til NSB og DCOK-stabschefens talepunkter på NOST-stabsmøderne. Det bemærkes i denne sammenhæng, at der på DCOK's debriefing blev fremsat forslag om fremover løbende at skrive nye emner, opmærksomhedspunkter og en fælles oversigt over kommunikative tiltag op på et whiteboard (fx vedrørende pressemeddelelser, pressemøder, beredskabsmeddelelser, publicerede hjemmesidenyheder mv.). Det blev endvidere foreslået fremover at bruge stabslokalets storskærme mere aktivt til at vise myndigheders hjemmesider, nyhedsmedier mv.

DCOK's overvågning af mediebilledet, herunder de sociale medier, viste sig meget relevant. Ikke kun for at være på forkant med situationen i kommunikationsmæssig sammenhæng, men også rent operativt. Fx spottede medieovervågningen på et tidspunkt en besked på øvelsesmediet "Blokken" om en borger, som sad fast i en hotelelevator pga. strømsvigt. DCOK meldte lynhurtigt dette videre til den relevante myndighed, der straks tog affære.

Som resultat af DCOK's timeout blev det i øvrigt besluttet, at mindst én person fra DCOK-sekretariatet skulle forblive i stabslokalet under NOST-møderne for at sikre konstant bemanding og følge medieudviklingen kontinuerligt. Evalueringsgruppen vurderer, at der her var tale om en hensigtsmæssig tilpasning af stabsprocedurer. Blandt øvrige velfungerende faktorer er bl.a. fremhævet, at det var vigtigt og givtigt, for DCOK-medlemmerne at kunne overvære NOST-møderne.

Endelig skal det bemærkes, at det blev foreslået, at DCOK fremover eventuelt kan udarbejde et "Nationalt Medie- og Kommunikationsbillede" i stil med "Nationalt Situationsbillede". Forslaget går på et selvstændigt dokument som supplement til – ikke erstatning af - DCOK's komprimerede input til pkt. 8 i NSB skabelonen. Evalueringsgruppen vurderer, at forslaget fortjener behandling i stabsudvalget for DCOK, såfremt dette ikke allerede er sket.

4.2.3 Kerneopgave 3 - Koordinering af handlinger og ressourcer

Koordineringen af handlinger og ressourcer i DCOK var generelt præget af godt samarbejde og åben dialog. Kort efter øvelsen var startet, og de indledende scenarier stod klart, foranledigede DCOK-stabschefen fx, at der i plenum blev taget stilling til, hvilken myndighed der under omstændighederne havde det overordnede kommunikative ansvar i forhold til offentligheden. Der var bred enighed om, at det var PET og CFCS i forening, der havde dette overordnede ansvar. Det blev samtidig understreget, at de respektive sektorer selv havde ansvaret for eget bagland og kommunikative udmeldinger derfra, og at DCOK's opgave ikke ville bestå i at producere konkrete kommunikationsprodukter til sektorerne.

Denne ansvarsplacering og præcisering vurderes at have givet en god start på øvelsen og bidrog til, at DCOK i resten af forløbet generelt leverede et højt niveau i forhold til koordineringen af handlinger og ressourcer – både internt i staben og mellem repræsentanternes respektive baglande. Repræsentanterne var således generelt gode til at koordinere, hvad der skulle meldes ud lokalt, og hvad der skulle meldes ud centralt som led i den eksterne tværgående krisekommunikation. Repræsentanterne var villige til at hjælpe hinanden, og der var forståelse for, at de enkelte medlemmer selv havde ansvar for at producere sektorbestemt information samt viderebringe relevant information til DCOK. Det er således det generelle indtryk, at repræsentanterne havde et godt samspil med hinanden, med kollegerne i NOST og med eget bagland gennem hele øvelsen. Der sås fx også et tæt samspil mellem de kommunikationsansvarlige fra Rigspolitiet i DCOK og Københavns Politi i LBS11.

Ikke desto mindre var der flere tilfælde, hvor afgørende informationer ikke eller forsinket tilgik DCOK. På dag 1 afholdt Københavns Politi fx et pressemøde, men dette blev ikke eller kun i meget begrænset omfang kommuni-

keret til DCOK eller NOST. DCOK blev fx heller ikke altid informeret tilstrækkeligt om tilfælde, hvor myndigheder havde nedbrud i mail og telekommunikation, eller hvor deres hjemmesider var nede. Dette tydede på svagheder i informationshåndteringen, som igen betød, at DCOK fik vanskeligt ved at koordinere handlinger og ressourcer.

Ved stabsbordet i DCOK kunne der observeres særlig god koordination mellem Rigspolitiets formandskab og den operative politidel. Flere af de øvrige medlemmer ytrede dog ønske om mere information vedrørende den politioperative del, da politiets dispositioner havde afgørende betydning for koordineringen af de mediemæssige udmeldinger. Flere medlemmer efterlyste desuden en skarpere adskillelse mellem "operativ virkelighed" (hvad er situationen) og "mediemæssig virkelighed" (hvad siger medierne om situationen).

Generelt savnedes proaktiv tænkning i staben i forhold til den fremadrettede situation i stedet for et mere reaktivt virke. Det var imidlertid en særlig kommunikationsmæssig udfordring, at det tog så relativt lang tid for PET og CFCS at lægge sig fast på en fælles udmelding til offentligheden med hensyn til, om der var tale om et cyberangreb, og om det var et koordineret angreb, ligesom det ikke stod klart, hvad mulige scenarier kunne være.

Det blev aftalt med Rigspolitiets strategiske stab (RSS), at DCOK ikke i starten af øvelsen skulle levere et oplæg til en kommunikationsstrategi til regeringens krisestyringsorganisation, men tidligt om morgenen på dag 2 modtog politiet i DCOK en anmodning fra Statsministeriet om et oplæg til statsministeren. Oplægget blev sendt til godkendelse blandt DCOK's øvrige medlemmer inden afsendelsen, og eksemplet illustrerede, at DCOK's organisation og medarbejdere var gearet til at løse akutte ad hoc-opgaver sideløbende med øvrige opgaver.

4.2.4 Kerneopgave 4 – Ekstern krisekommunikation til befolkningen og medierne

Den overordnede ambition var ifølge DCOK formandskabet, at staben skulle være en "speeder" og ikke en "stopklods", når det gjaldt mediemæssige udspil. Dette lykkede generelt godt. Allerede på det første stabsmøde i NOST bad DCOK-stabschefen efterretningstjenesterne tage stilling til, om man kunne udtale sig om årsagen til it-nedbrudene. Stabschefen påmindede også hyppigt om, at han forventede, at myndighederne selv kommunikerede om de tiltag, de informerede om ved "bordrunderne" på dag 1, og nævnte gentagne gange behov for massiv tilstedeværelse af myndighederne i medierne, eftersom cyberangrebene tidligt i forløbet var kendt i medierne.

Stabschefen foreslog også kort efter øvelsens start, at politi.dk (både den landsdækkende side og Københavns Politis side) skulle anvendes som platform for generel information til offentligheden, der vedrørte flere sektorer, hvilket de øvrige stabsmedlemmer tilsluttede sig. Kort tid efter forslog stabschefen at benytte #kriseinfo på øvelsesmediet "Blokken", hvilket medlemmerne ligeledes tilsluttede sig. Omvendt blev et forslag om en fælles Facebook-profil forkastet, da der var bred enighed om, at DCOK ikke skulle informere selvstændigt som organisation, og at der ikke var grund til at oprette nye konti til sociale medier, når der allerede eksisterede mange platforme.

Et andet eksempel var, at DCOK-stabschefen på NOST-stabsmødet kl. 13 på dag 1 foreslog et pressemøde, men NOST-stabschefen fandt dette for tidligt. I stedet blev det aftalt, at pressemødet skulle afholdes af Rigspolitiet med deltagelse af PET og CFCS kl. 15:30. DCOK stod for planlægningen af pressemødet, som kom hurtigt i stand, men desværre blev meldt ud til medierne for sent, hvilket bevirkede, at flere medier, herunder DR, ikke nåede frem. På pressemødets første halvdel var fokus primært på den efterforskningsmæssige indsats og myndighedernes samarbejde, herunder fokus på krisestyringssystemets opbygning, sektoransvaret og efterlevelsen af beredskabsplaner. I sidste halvdel var der fokus på at besvare journalisternes spørgsmål om konsekvenser og forholdsregler for almindelige borgere. DCOK drøftede efterfølgende, at det kunne have været formålstjenstligt at formulere tre hovedbudskaber til talspersonerne, som kunne være prioriteret som afsluttende bemærkninger.

Et eksempel på det strategiske niveaus involvering i krisekommunikationen forekom på dag 2, hvor Rigspolitiets Strategiske Stab bad DCOK om en myndighedsfælles pressemeddelelse om situationen. Denne blev udarbejdet i

samarbejde mellem alle DCOK medlemmer med Rigspolitiet som tovholder og sendt ud med et citat fra rigspolitichefen.

Endelig ydede DCOK en stort indsats med hensyn til at fremme myndighedernes brug af sociale medier, dels til at følge situationens udvikling (reaktivt) og dels til at udsende kriseinformation (proaktivt). Dette er et område, som der i høj grad er fokus på blandt myndighederne efter øvelsen, bl.a. også på baggrund af erfaringer fra stormene Allan og Bodil i 2013. De traditionelle medier er fortsat befolkningens vigtigste kilde til information i krisesituationer, men befolkningen bruger i stigende grad sociale medier, og informationen spredes let og hurtigt blandt brugerne på sociale medier. De traditionelle medier følger desuden myndighedernes sociale medieprofiler og viderebringer relevant information til offentligheden med det samme. På den måde kommer myndighedernes budskaber hurtigt ud til borgerne, selvom det ikke er alle, der følger dem direkte via sociale medier.

4.3 Samarbejdet i Hovedstadens Lokale Beredskabsstab (LBS11)

4.3.1 Kerneopgave 1 – Etablering og drift af staben

LBS11 var sammensat af Københavns Politi (formandskab), Region Hovedstaden, Beredskabsstyrelsen Sjælland, Københavns Brandvæsen, Tårnby Brandvæsen, Frederiksberg Brandvæsen, DONG Energy, Banedanmark, Metroselskabet, Vejdirektoratet, Movia, Øresundsbron, Totalforsvarsregion Sjælland og Hærhjemmeværnsdistrikt København. Ad hoc-medlemmerne var inviteret til at deltage forud for øvelsen, og Københavns Politi havde dermed indtænkt en interessentanalyse med reference til en potentiel skarp situation.

Som et særligt tiltag deltog lederen af Københavns Politis KSN (Kommandostation) også i LBS11-stabsmøderne.

I feedback til evalueringen er det også foreslået, at staben kunne have været suppleret af yderligere ad hoc medlemmer, fx en it-administrator, der on-site bl.a. kunne have beregnet konsekvenser ved nedlukning af essentielle systemer, fx via risiko- og sårbarhedsanalyser for stabens IKT.

Indledningsvis og umiddelbart efter aktiveringen gennemlevede staben en forventet, men relativ lang kaosfase, hvori der ikke indgik en fast struktur for mødevirksomhed. Det vurderes at have haft en afsmittende effekt på det samlede overblik i staben og etableringen af stabsteknik. I takt med at øvelsen skred frem, og strukturen kom på plads, implementerede man dog en fast mødedagsorden og strukturerede møder og referater, ligesom de operative mål blev italesat. Øvelsesteknisk feedback indikerer, at kaosfasens varighed kunne have været reduceret ved at klargøre og starte LBS11 tidligere frem for at bruge uforholdsmæssig megen tid på briefing om øvelsen, øvelsesbestemmelser og anden praktisk information.

Øvelsen afdækkede udviklingsmuligheder i forhold til stabens fysiske rammer og tekniske hjælpemidler. LBS11 indeholder megen IKT, men de teknologiske udfordringer var af et sådant omfang, at det ikke var muligt for én enkelt it-medarbejder at imødekomme det samlede behov for assistance. Ved fraværet af en egentlig "køreplan" for opsætning af stabslokalets IKT forløb de første ca. to timer af øvelsen med et manglende teknisk overblik og dermed en uensartet tilgang til anvendelse af IKT-midlerne. Storskærme kunne fx have været udnyttet mere optimalt via en bedre visualisering af informationer i POLDOK, stabsmedlemmernes egne bidrag og andet af fælles interesse. Tilsvarende blev der identificeret mangel på mere lavpraktisk materiel, fx flere whiteboard tavler. Det var dog opfattelsen, at man mod øvelsens slutning nærmede sig en tilfredsstillende brug af faciliteterne.

Hvert stabsmedlem skulle selv koble sig på og føre POLDOK, og ved hver enkelt operatørplads var der adgang til en folder med vejledning i at logge på. Imidlertid virkede fremgangsmåden kun delvist efter hensigten, idet mange af de fremmødte stabsmedlemmer øjensynlig kun besad meget begrænset eller intet kendskab til de elektro-

niske systemer og ikke var rutinerede i at tilgå og føre politiets POLDOK system. Der opstod derfor megen forvirring og usikkerhed, som indledningsvis forsinkede og begrænsede effektiviteten i stabsvirket.

Der blev undervejs i øvelsen samt mellem øvelsesdag 1 og 2 gennemført timeouts med stabslederne, hvor man fokuserede på umiddelbar erfaringsopsamling. Dette vurderedes efterfølgende at have været en formålstjenlig fremgangsmåde, som alle implicerede udtrykte ønske om at anvende i fremtidige øvelser og eventuelt også ved skarpe hændelser og indsatser, da dette kan facilitere læring og optimering af det videre forløb.

I sin egenskab af politifaglig "peer-review'er" inddrog evalueringsgruppens observatør løbende internt udfærdigede retningslinjer og procedurer for arbejde i en lokal beredskabsstab, herunder bl.a. eksempler på dokumentation af overdragelse/afløsning i en politikreds. Materialet var ment som inspiration, og forslagene var baseret på observatørens mangeårige erfaring med lignende stabsarbejde og relevant uddannelse.

Observatøren inddrog fx overvejelser om den mest hensigtsmæssige indretning af stabslokalet tekniske layout og funktionalitet for at optimere informationsformidling, videndeling og koordination. Der er mange muligheder for at kombinere de forskellige projektorer, fladskærme og PC-arbejdsstationer, så visningerne kan tilpasses forskellige tematiske scenarier. Herudover fremsatte observatøren forslag til procedurer, der kan overvejes som led i en bredere revision af "Operationsbefaling B212 for iværksættelse af Hovedstadens Beredskabsstab (LBS11)". Det kan fx overvejes at producere et bilag, som beskriver, hvad der skal/bør gøres og af hvem fra det øjeblik, man beslutter at aktivere staben, og til myndighedernes forbindelsesofficerer møder fysisk i staben.

Det kan også overvejes at præsentere en strategi i operationsbefalingen, der beskriver hensigten med de operative mål og de opgaver, som skal være styrende for stabens virke med forankring i nærheds-, ligheds- og sektoransvarsprincipperne. Endelig blev det foreslået at overveje, om plansættet med fordel vil kunne struktureres efter kerneopgaver i krisestyringen i lighed med planerne for NOST, DCOK og National Beredskabsplan.

4.3.2 Kerneopgave 2 – Informationshåndtering

Der var under en stor del af øvelsen uklarhed omkring procedurer for informationsformidling og videndeling i staben, herunder for udarbejdelse af fælles LBS11-situationsbilleder og stabsmødereferater samt logføringen.

Hver enkelt myndighed/sektor var ansvarlig for at ajourføre egne "lokale situationsbilleder" i POLDOK, men, som nævnt, kendte kun få af stabsmedlemmerne til Rigspolitiets retningslinjer for anvendelse af POLDOK (version af 6. maj 2013). På baggrund af manglende stabsprocedurer og erfaringsgrundlag var det derfor vanskeligt at sikre den fornødne kvalitet, ensartethed og struktur i de lokale situationsbilleder. Dette påvirkede kvaliteten af de fælles situationsbilleder fra LBS11, med konsekvenser for både informationshåndteringen i staben selv og videre oppe i det nationale krisestyringssystem, eftersom LBS-situationsbilledet udgør et vigtigt input til NSB i NOST. LBS11-situationsbillederne blev dog, efter de indledende manøvrer, løbende ajourført og fordelt såvel horisontalt som vertikalt, idet de indgik som bilag til stabsmødereferaterne, der blev sendt til NOST.

Der var udpeget en funktion til at udarbejde LBS11-situationsbillederne, og man anvendte GIS ved udarbejdelsen. Det var imidlertid ikke klart, om der forelå procedurer for overlevering af oplysninger fra de enkelte stabsmedlemmer til GIS-operatøren. Det indebar endvidere en del udfordringer, at den tekniske løsning ikke tillod at arbejde med opdatering af ét af stabsmedlemmernes lokale situationsbilleder, mens et andet blev vist. Det ene dokument skulle væk, før det andet kunne komme på skærmen.

Stabsmødereferater blev løbende indskrevet i POLDOK, men det var først et stykke inde i øvelsen, at staben arbejdede med tydeliggørelse af strategi og egentlige operative mål mellem møderne. Et stykke ad vejen var der således ikke åbenlys mulighed for at sikre, at alle besad samme opfattelse af trufne beslutninger og de effekter, sådanne kunne have på opgaveløsninger.

Undervejs i øvelsen blev flere tekniske løsninger og kombinationer af visuelle hjælpemidler afprøvet for at forbedre informationshåndteringen, og da man nåede frem til en løsning, som den samlede stab anså for at være optimal, blev denne dokumenteret gennem affotografering med henblik på genanvendelse og yderligere udvikling under øvelser og i skarpe situationer. Løsningen indebar bl.a., at operative mål og GIS-informationer var placeret centralt, og at forskellige aktørers POLDOK-registreringer blev separeret og vist på selvstændige skærme.

Som led i informationshåndteringen blev LBS11-medlemmernes interne problemstillinger mv. skrevet på et whiteboard, og denne praksis vurderes at have været særlig hensigtsmæssig. Pladsen var imidlertid begrænset, og det blev foreslået at etablere en centralt placeret "væg" af whiteboards, hvor elementer i krisehåndteringen løbende kan skitseres, herunder fx visualisering af "Ledestjernen", "5-punkts befalingen" mv. Brugen af whiteboards ses ikke alene som et supplement til brugen digitale IKT midler, men også som et alternativ ved digitale nedbrud – og potentielt eneste alternativ i relation til mulige scenarier, hvori stabens samlede IKT måtte bryde sammen.

4.3.3 Kerneopgave 3 – Koordinering af handlinger og ressourcer

Det vurderes generelt, at LBS11 koordinerede sit arbejde godt i forhold til øvelsens strategiske og operationelle elementer. Stabens fælles situationsbillede blev anvendt ved prioritering af handlinger og ressourcer, og i den sammenhæng inddrog man realistiske vurderinger af risici, scenarier og krisens mulige udvikling. Da først strukturen for stabens drift var på plads, vurderes det, at stabsmedlemmerne var gode til at tænke frem i tid, rum og scenarier. Dette skabte muligheder for, at man kunne planlægge og koordinere godt på tværs af myndigheder og sektorer imellem stabens møder. Stabslederen har endvidere fremhævet værdien af det personlige kendskab blandt deltagerne som særligt befordrende for koordinationen.

Der blev imidlertid ikke ført et samlet ressourceroverblik, og som konsekvens heraf havde staben ikke altid et samlet overblik over nødvendige, tilgængelige og indsatte ressourcer. Endvidere skete der ikke tilstrækkelig videndeling om opgaveløsninger samt til- og fragang af ressourcer. Dette udsprang bl.a. af, at ikke alle forbindelsesofficerer var lige erfarne. Evalueringsgruppens observatør vurderede fx, at et mere fyldestgørende billede af indsatte styrker mv. kunne have været etableret ved målrettet anvendelse af 5-punkts befalingens systematik.

Med hensyn til eksterne relationer kan bl.a. nævnes, at samspillet med Den Administrative Stab (DAS) i Københavns Kommune blev fremhævet som særligt velfungerende under den fælles debriefing i LBS11. Omvendt er der i feedback til evalueringen fra Københavns Kommune tilkendegivet utilstrækkelig kommunikation fra LBS11, herunder at opdateringer og det fælles LBS11-situationsbillede ikke blev modtaget under øvelsen.

KSN-lederens deltagelse på LBS11-stabsmøderne vurderes at have været en god metode til at øge sammenhængen mellem operation og opgaver på tværs af myndigheder og sektorer. Dette var gennem hele øvelsen til stor gavn for koordineringen af handlinger og ressourcer i LBS11 såvel som i KSN, og dermed også for politiets koordinerende ledelse. Samtidig erkendes det dog, at sondringen mellem ansvarsområderne i henholdsvis KSN og LBS, samt disses snitflader, kunne have været mere tydelig.

Endelig viser tilbagemeldinger fra debriefingen tydeligt, at stabens interne uddannelsesstruktur og jævnlige stabsøvelser ønskes fastholdt. Det er i den forbindelse foreslået at iværksætte relevant efteruddannelse og øget træning i stabsledelse, stabsarbejde, stabsdeltagelse og procedurer. Sådanne tiltag kan både målrettes politikredsens formandskab, stabshjælperne og forbindelsesofficerer fra øvrige faste og ad hoc-medlemmer i LBS11. Formandskabet kan i så fald overveje at udvikle et genkendeligt koncept og/eller et sæt praktiske retningslinjer, som aktører med tilknytning til staben kan træne inden for egen organisation. Kompetenceudviklende tiltag kan ligeledes inddrage videreuddannelse via stabskurser udbudt af andre hovedaktører i samfundets beredskab.

4.3.4 Kerneopgave 4 – Ekstern krisekommunikation til befolkningen og medierne

Hver enkelt organisation, som deltog i LBS11 var ansvarlig for egen presse i henhold til sektoransvaret, men der blev udpeget en funktion til koordineringen af krisekommunikation som integreret del af stabens arbejde på og mellem stabsmøderne. I staben havde Københavns Politi således stillet to pressefolk til rådighed. Disses primære opgaver var dels at iagttage og arbejde med sociale medier, herunder i høj grad Twitter (simuleret via "Blokken"), og dels varetage kontakten til de almindelige medier. Der blev samarbejdet med andre aktører om udsendelse af information, og der sås bl.a. et tæt samspil mellem politiets kommunikationsansvarlige i LBS11 og DCOK.

LBS11 tilstræbte proaktivt at rette kommunikationen mod borgere, virksomheder m.fl., men trods disse bestræbelser, må pressearbejdet i staben generelt karakteriseres som reaktivt under øvelsen. Man anvendte ikke medierne aktivt som led i krisestyringen, og der blev først sent i øvelsen arbejdet med en egentlig pressestrategi på skrift, således at strategien fremgik tydeligt for alle i staben. Man havde heller ikke allokeret en separat funktion til medieovervågning, og staben blev derfor ikke serviceret med et samlet overblik over det, der blev skrevet, sagt og vist i medierne. Erfaringerne peger på vigtigheden af, at krisekommunikation indtænkes som fast element i alle de årlige stabsøvelser i LBS11.

4.4 Delkonklusion og anbefalinger

KRISØV 2013 viste, at det eksisterende nationale krisestyringssystem er en velegnet ramme for at håndtere en situation med mange, komplekse og samtidige cyberangreb. Øvelsen sendte samtidig et klart budskab om, at myndighederne tager cybertrusler alvorligt og arbejder med at styrke beredskabet på dette væsentlige område.

I NOST bar samarbejdet præg af, at der er tale om godt indarbejdede procedurer, hvor deltagerne indgår i et respektfuldt samarbejde. Formandskabets stramme mødeledelse og effektive sekretariatsvirksomhed, graden af mødedisciplin og den generelle dynamik i staben fremhæves som særligt velfungerende. Der kunne dog, ligesom under tidligere KRISØV'er, konstateres udviklingsmuligheder i relation til udarbejdelse og ajourføring af NSB. Samme konklusion gælder generelt for de lokale, myndighedsspecifikke og sektorvise situationsbilleder, der fungerer som datagrundlag for NSB. Dette illustrerede et behov for at gennemgå konceptet med henblik på at sikre, at produktet har en kvalitet, som modsvarer behovet på strategisk niveau i regeringens krisestyringsorganisation. Der ses ikke behov for større justeringer i skabelonen for NSB men derimod optimering af forhold som datagrundlag, prioritering, sammenhæng, aktualitet og rutinering i udfærdigelsen af dokumentet.

I DCOK forbedredes samarbejdet om medieovervågning og koordinering af krisekommunikation i forhold til tidligere øvelser. Det skyldtes bl.a. evalueringen af KRISØV 2011, som anbefalede tydeliggørelse af opgaver, rolle- og kompetencefordeling mellem DCOK, DCOK's sekretariat og de involverede myndigheder. Ikke desto mindre lod samarbejdet stadig noget tilbage at ønske, og evalueringsgruppen hæfter sig ved, hvor stor en forskel, der kunne konstateres mellem øvelsens første og anden dag. Fra udgangssituationen burde der således have været bedre struktur og styring, bl.a. via faste stabsmøder. Det altoverskyggende fokus for øvelsen i DCOK var læring, og det findes naturligt, at staben afprøvede forskellige alternativer for at finde den bedste organisering og de mest fordelagtige arbejdsprocesser. Men det må konstateres, at staben burde have forholdt sig eksplicit til flere af de procedurer, som fremgik i DCOK-planen, og som var revideret et halvt år tidligere i maj 2013.

I LBS11 kunne effektiviteten i stabsvirket bl.a. også være hævet gennem mere metodisk anvendelse af stabsprocedurer, særligt i forbindelse med opstart af tekniske hjælpemidler i den indledende "kaosfase", større klarhed omkring procedurerne for informationshåndtering i staben og mere proaktiv ekstern krisekommunikation.

Det bidrog til samarbejdet, at NOST og DCOK faciliteterne er samlet få meter fra hinanden og i umiddelbar nærhed til RKS og RSS i Rigspolitiets hovedkvarter i Ejby. Dette gav rig mulighed for koordination, sparring og ekse-

kveringsevne, og de fysiske rammer vurderes, med enkelte undtagelser, velfungerende. For LBS11 var øvelsen lærerig, idet den afdækkede flere forslag til, hvordan stabslokalets indretning og tekniske layout kan optimeres.

Selvom samarbejdet om krisestyringen generelt fungerede godt i alle tre stabe, afdækkede øvelsen, at deltagelse i det nationale krisestyringssystem ikke er tilstrækkeligt strategisk forankret i alle organisationer. Observationer, som understøtter denne konklusion vedrører bl.a. problemstillinger omkring forberedelse af forbindelsesofficerer fra ad hoc-medlemmer, graden af parathed i baglandet, utilstrækkeligt kendskab til og begrænset fokus på anvendelse af gældende plansæt samt manglende spejling i sammensætningen af NOST og DCOK. Herudover var der et eksempel på, at repræsentanter fra en myndighed, som ifølge øvelsesplanlægningen skulle have deltaget som ad hoc-medlem i NOST og DCOK, ikke kunne få adgang til faciliteterne pga. utilstrækkelig sikkerhedsgodkendelse. Årsagen skal findes i, at den pågældende myndighed ikke var på listen over ad hoc-medlemmer og ikke var bekendt med kravet om sikkerhedsgodkendelse. Myndigheden var i stedet i telefonisk kontakt med NOST og DCOK, men forløbet illustrerede, at krisestyringssystemet er baseret på fysisk tilstedeværelse i de tværgående stabe, og at der er behov for at udbrede kendskabet til kravet om sikkerhedsgodkendelse samt de generelle forventninger til myndighedernes deltagelse i stabene.

I de tværgående stabe kunne der generelt konstateres et godt fokus på igangværende hændelser, men ofte begrænset tværgående og proaktivt fokus i forhold til hændelsernes mulige udvikling. Tilsvarende var der ikke altid tilstrækkelig struktur i forhold til at holde overblik over status for igangværende aktiviteter. Overblikket kunne muligvis have været øget, hvis der – udover logføring, situationsbilleder og stabsmødereferater – var udarbejdet fortløbende aktionslister over aktiviteter samt deres status (”gennemført”, ”under udførelse”, ”afventer”). Opgaven kan fx varetages af en ”plotter” på en tavleoversigt på samme vis, som det fx er god praksis i politiets KSN.

Efter øvelsen tilkendegav flere ad hoc-medlemmer, som ikke tidligere havde deltaget i stabene, at de kunne have ønsket en bedre indledningsvis briefing og praktisk indføring i stabenes virke. Dette illustrerede dog også, at ad hoc-deltagere ikke nødvendigvis på forhånd har tilegnet sig godt kendskab til stabenes respektive plansæt.

Ovenstående problemstillinger indikerer bl.a., at fokus i arbejdet med at udvikle de tværgående stabe fremover i lige så høj grad bør være på forberedelser blandt ad hoc-medlemmer som blandt de faste medlemmer.

Øvelsen viste udviklingsmuligheder i forhold til samordnet ekstern krisekommunikation via traditionelle medier. Brug af sociale medier, som et nyt tiltag i KRISØV-serien, gav et særligt læringsudbytte for mange øvelsestagere.

Evalueringsgruppen er bekendt med at flere stabe siden øvelsen har arbejdet målrettet med forbedringstiltag.

Det anbefales:

- At alle statslige myndigheder og andre relevante parter forankrer arbejdet med beredskabsplanlægning og krisestyring på det strategiske ledelsesniveau i de enkelte organisationer, herunder deltagelsen i de nationale krisestyringsøvelser. Formålet med den strategiske forankring er at sikre, at myndigheder m.fl. kan varetage krisestyring inden for eget ansvarsområde i henhold til egen planlægning, bistå andre under større ulykker og katastrofer, der involverer flere sektorer samt indgå i tværgående krisestyringsfora.
- At statslige myndigheder og andre relevante parter opfordres til at udarbejde instrukser for udsendelse af repræsentanter til det nationale krisestyringssystems tværgående stabe som et fast element i deres beredskabsplaner. I denne sammenhæng kan potentielle ad hoc-medlemmer også med fordel gøres opmærksomme på de tværgående stabes plansæt og øvrige relevante publikationer, kravet om sikkerhedsgodkendelse for adgang samt mulighederne for uddannelse i stabsdeltagelse via kurser, øvelser, sidemandsoplæring mv.
- At NOST fortsætter arbejdet med at forbedre kvaliteten af Nationalt Situationsbillede. Arbejdet bør tage udgangspunkt i behovet på strategisk niveau i regeringens krisestyringsorganisation og resultere i et nyt, samlet

koncept for Nationalt Situationsbillede, hvori der lægges vægt på datagrundlag, prioritering, sammenhæng og aktualitet. Det anbefales herefter at prioritere træning i NOST-sekretariatet samt blandt sektoransvarlige repræsentanter for at opbygge rutine i at udfærdige lokale, sektorvise og nationale situationsbilleder.

- At DCOK følger op på de udviklingsmuligheder, som blev identificeret under KRISØV 2013, herunder revidere konceptet for stabens procedurer og opgaver som myndighedsfælles kommunikationsberedskab og støttefunktion for NOST. Fokus bør herefter være på at understøtte stabsarbejdet med den struktur og den styring, som plansættet tilbyder samt opbygge rutinering i procedurerne blandt faste og ad hoc medlemmer, så DCOK udvikler større sammenhængskraft og parathed i forbindelse med enhver aktivering.
- At LBS11 inddrager læringspunkterne fra KRISØV 2013 i forbindelse med en videreudvikling af stabens operationsbefaling og generelle plansæt, herunder udvikling af standardprocedurer og vejledninger for medlemmernes opgaver samt layout af fysiske rammer og tekniske hjælpemidler ved aktivering.

5. Bevidsthed og viden på cyberområdet

Cyberangreb er ikke et nyt fænomen, men cyberangreb kan i dag få langt større konsekvenser end tidligere, dels fordi samfundet bliver stadig mere afhængigt af IKT, dels fordi IKT-anvendelsen i stigende grad finder sted i komplekse og indbyrdes forbundne netværk med direkte eller indirekte internetopkobling. Samtidig er antallet af cyberangreb stigende, og angribernes fremgangsmåder bliver stadigt mere sofistikerede. Udviklingen peger således på, at man mange steder bør forberede sig bedre på at afværge cyberangreb, hvor det er muligt, og håndtere dem effektivt, når det er nødvendigt. Hertil kræves beredskabsplanlægning og krisestyringskapacitet på cyberområdet – både inden for og på tværs af samfundets sektorer og i det nationale krisestyringssystem.

Dette er årsagen til, at cyberangreb blev valgt som overordnet scenarie for KRISØV 2013 og baggrunden for valget af evalueringens fokusområde 2: "Udbyttet på strategisk-operationelt krisestyringsniveau med hensyn til at *styrke bevidsthed om cybertrusler og viden om sårbarheder og indbyrdes afhængigheder mellem kritiske samfundsfunktioner i forbindelse med større cyberangreb*". I de nedenstående afsnit vurderes omfanget og karakteren af læringsudbyttet, og der afdækkes eksempler på tiltag, som øvelsen har givet eller kan give anledning til.

5.1 Læringspunkter fra spørgeskemaundersøgelsen

For at estimere udbyttet søgte evalueringsgruppen først at sammenligne graden af bevidsthed og viden på cyberområdet blandt de deltagende organisationer henholdsvis før og efter øvelsen. Dette blev gjort gennem KRISØV 2013 spørgeskemaundersøgelsen, hvor der blev modtaget 24 besvarelser.

Svarene viste, at 79 pct. var helt eller overvejende enige i, at bevidstheden om cybertrusler i deres organisation allerede var høj før deltagelse i øvelsen blev besluttet. 80 pct. svarede, at bevidstheden blev øget via deres forberedelser på og deltagelse i øvelsen. Tilsvarende erklærede 79 pct. sig enige i, at deres forudgående viden om sårbarheder i forbindelse med større cyberangreb allerede var høj. Samme antal tilkendegav, at deres viden blev øget via forberedelserne og deltagelsen. Med hensyn til viden om indbyrdes afhængigheder mellem kritiske samfundsfunktioner i forbindelse med større cyberangreb angav 92 pct. både et højt forudgående vidensniveau og en efterfølgende øget viden. 75 pct. var desuden enige i, at øvelsen tilførte deres organisation bevidsthed og viden på cyberområdet, som ellers ikke ville være tilgået det strategiske og operationelle niveau. 17 pct. var uenige i dette, og 8 pct. savnede grundlag for at besvare spørgsmålet.

Tallene indikerer således, at øvelsestagerne generelt fik øget bevidsthed og viden på cyberområdet, særligt hvad angår viden om indbyrdes afhængigheder mellem kritiske samfundsfunktioner, men også, at det forudgående niveau allerede var højt for hovedpartens vedkommende. En gennemgang af de enkelte besvarelser viser desu-

den, at flere af de organisationer, som angav et højt forudgående niveau, var uenige i, at de fik øget deres viden og kendskab. Forklaringen herpå skal delvist findes i, at nogle af de pågældende organisationer i dagligdagen har særligt ansvar for beredskab og sikkerhed på cyberområdet. For nogle organisationer skyldes det endvidere konkrete erfaringer fra alvorlige nyere sager, hvor cyberangreb i en kortere periode har forstyrret eller hindret anvendelsen af dansk it- og teleinfrastruktur, eller hvor informationssikkerheden er blevet kompromitteret.

Med hensyn til det mere specifikke udbytte af øvelsen, var hovedparten af respondenterne enige i, at øvelsen skabte øget opmærksomhed på faktorer som: karakteristika ved cybertrusler (92 pct.), aktører bag cyberangreb (75 pct.), potentielle mål for cyberangreb (83 pct.), tendenser på området (92 pct.); særlige udfordringer ved at håndtere cyberangreb (92 pct.); vigtigheden af at være på forkant (92 pct.) og egne sårbarheder (83 pct.) i en situation med omfattende, koordinerede cyberangreb; behovet for IKT-robusthed og -redundans (79 pct.) samt behovet for innovation i tilfælde, hvor vigtige IKT-systemer sættes ud af drift pga. cyberangreb (75 pct.).

Bemærkninger i spørgeskemabesvarelserne viser endvidere, at det specifikke udbytte langt fra begrænsede sig til disse faktorer. Følgende tjener som et godt eksempel:

> *"Energistyrelsen var inden øvelsen fuldt bevidst om betydningen for energiområdet af cybertrusler og om sårbarheder vedrørende sådanne trusler. Øvelsens planlægning og gennemførelse har øget denne bevidsthed, har konkretiseret og detaljeret den i forhold til udvalgte arbejdsområder, har udbygget den med et erfaringsgrundlag, og har formidlet denne viden, erfaring og forståelse bredere i organisationen. Denne forståelse er dermed i dag bedre forankret i Energistyrelsen end tidligere, således at det fremadrettede arbejde med at beskytte sig mod cyberangreb og med at forberede sig på at kunne håndtere sådanne situationer i dag har et væsentligt bedre grundlag end uden øvelsen.*
>
> *Konkret har øvelsen vist betydningen af at have planlagt for, at Energistyrelsen afbrydes fra internettet. Øvelsen har vist, at en sådan afbrydelse ikke kun kan forekomme som resultat af et forsyningsnedbrud, dvs. kortvarigt indtil genetablering, men også – og formentlig mere realistisk – kan forekomme som en sikkerhedsforanstaltning, der i den konkrete situation besluttes af Statens IT eller Energistyrelsen, og som kan have en længere varighed, målt i dage, der ikke vil kunne forudses fra starten."*

Andre eksempler på specifikt udbytte nævnt i spørgeskemabesvarelserne inkluderer bl.a.:

- Statsministeriets øgede bevidsthed om hovedaktørerne i forbindelse med cyberangreb sammenlignet med andre hændelser.
- Forsvarsministeriets øgede opmærksomhed på snitfladen mellem ansvar for FE og PET samt folkeretlige aspekter i forbindelse med cyberangreb.
- Beredskabsstyrelsens udarbejdelse af et bilag til styrelsens generelle beredskabsplan vedrørende cyberhændelser samt et bilag med oversigt over alternative kommunikationsveje.
- Sundhedsstyrelsens øgede erkendelse af NemID's og sundhed.dk's betydning for mange funktioner i sundhedsvæsenet.
- Fødevarestyrelsens øgede bevidsthed om hvordan it-afhængige funktioner og ydelser hostes; erkendelse af behov for at kortlægge it-afhængige selvbetjeningsydelser, som kunder regelmæssigt benytter sig af; erkendelse af behov for at kortlægge sårbarheder for hver afdeling; samt en ledelsesbeslutning om at udarbejde en nedskrevet prioritering af it-afhængige ydelser, når der kun er begrænset kapacitet til rådighed.
- Københavns Politis udarbejdelse af action cards, forberedelse af lavteknologiske hjælpemidler og igangsættelse af en sårbarhedsanalyse for fortsat drift af LBS11.
- DONG Energys styrkelse af sit kommunikationsberedskab og robusthed til at imødegå cyberangreb.

5.2 Læringspunkter fra evalueringsseminaret

Via gruppearbejdet på evalueringsseminaret den 12. december 2013 identificerede de 57 deltagere en lang række læringspunkter fra øvelsen, som understøtter eller uddyber spørgeskemabesvarelserne. Disse inkluderer:

- At der i dag er mindre overblik end tidligere med hensyn til alternative kommunikationsmidler (fx beredskabernes fælles radionet SINE, VHF radioer, analog telefoni, satellittelefoner, prioriterede mobilnet, REGNEM, fax mv.). For at imødegå dette, blev det foreslået, at der bør udarbejdes en "national plan vedrørende ressourcer og procedurer for alternativ kommunikation ved nedbrud på primær (digital) kommunikation". Lignende forslag var en "national plan for alternative tværfaglige kommunikationsveje" eller en "landsdækkende kommunikationsplan, der som minimum giver overblik over forskellige alternative kommunikationsmidler".
- At KRISØV 2013 for mange demonstrerede manglende indøvelse eller rutine i brug af alternative kommunikationsmidler. Dette gjaldt bl.a. SINE-radioer, og i en gruppe blev der fremsat ønske om at teste en "SINE-nødplan". SINE-radionettet fungerer uafhængigt af alle andre kommunikationssystemer og har i modsætning til mobilnettet nødstrøm til mange timer, hvilket er afgørende i en situation, hvor internettet og mobilnettet går ned. Øvelsen medførte også læring vedrørende satellittelefoner. Efter øvelsen planlagde en organisation fx uden varsel at afprøve satellittelefoner fra taget af organisationens bygning, herunder hardwarens effektivitet og brugeres kendskab til materiellet. En anden organisation identificerede god læring ved, at man til sidst i øvelsen var nød til at bruge ordonnans pga. utilgængelig IKT. En velkendt problematik om, at ikke alle myndigheder råder over REGNEM blev nævnt i samme forbindelse. På baggrund af disse og andre eksempler blev der identificeret behov for flere øvelser for at træne brugen af alternative kommunikationsmidler.
- At stærke og enkle manuelle procedurer ved IKT-nedbrud er påkrævede, men ofte ikke fandtes hos de deltagende organisationer trods øvelsesforberedelserne. Med stærke og enkle manuelle procedurer refereredes her til "noget på skrift, som man kan hænge op på døren".
- At fokus bør bevares og øges på at udarbejde og revidere risikovurderinger med opfølgende handlingsplaner for kritisk IKT-infrastruktur. Disse skal udarbejdes lokalt af de enkelte organisationer, da sektoransvaret gælder på cyberområdet som generelt i beredskabsarbejdet. Det blev identificeret som god praksis at fokusere på at sætte de rette personer og kompetencer sammen i en bred deltagerkreds for at udføre de bagvedliggende analyser, bl.a. for at afdække gensidige afhængigheder på IKT-området.
- At det ofte kræver samspil på tværs af organisationer hurtigt at identificere, hvor kompromitteret dataintegritet er opstået og adskille de netværk og sektioner, som virker fra de, som ikke virker.
- At håndtering af svigt i mindre kritiske offentlige it-systemer er mindre presserende i tilfælde med alvorligere forsyningsproblemer, fx ved strømafbrydelser.
- At få de mest kritiske samfundsfunktioner op at køre igen først kræver strategi og løbende lokal prioritering ud fra en behovspyramide og en liv-først-tankegang.
- At der fortsat hersker nogen tvivl om, hvilken myndighed cyberhændelser skal indrapporteres eller anmeldes til. Det blev foreslået at synliggøre dette og eventuelt oprette et "single point of contact", fx et centralt telefonnummer til brug for myndigheder i forbindelse med cyberhændelser.
- At strafferetlig efterforskning kan besværliggøres, hvis angrebne systemer repareres, inden der er gennemført en sikring af beviser. Der efterspørges information til it-afdelinger omkring, hvordan de skal bevissikre og underrette de myndigheder, der har ansvaret for efterforskningen.
- At karakteristika ved cyberangreb kan medføre lange kommunikationsveje i efterretningstjenesterne med hensyn til at cleare og videregive oplysninger, og at dette også kan medføre et fragmenteret mediebillede.

5.3 Delkonklusion og anbefalinger

På baggrund af input fra spørgeskemaundersøgelsen og evalueringsseminaret konkluderes det, at KRISØV 2013 levede op til målet om at styrke bevidsthed og viden på cyberområdet. Generelt gav både de forberedende aktiviteter og øvelsesdeltagelsen god læring, særligt vedrørende afhængigheder mellem kritiske samfundsfunktioner i situationer, hvor internetbaseret IKT sættes ud af drift. Dette gav tydeligvis stof til eftertanke og i flere tilfælde konkret handling – bl.a. i erkendelse af, at de simulerede angreb kunne have mere vidtrækkende konsekvenser i en virkelig situation. Udbyttet var ikke blot tilfredsstillende for de deltagende organisationer enkeltvis, men bidrog også til øget bevidsthed og viden på tværs af sektorer og i det nationale krisestyringssystems tværgående fora.

KRISØV 2013-deltagerne synes desuden generelt at have fundet øvelsen nyttig, fordi den understregede, hvor afhængige alle er af teknologi, og hvor svært det bliver at løse pålagte opgaver, hvis de normale kommunikationsmidler ikke fungerer eller er ustabile. Øvelsen afdækkede, at der blandt mange deltagere var manglende eller begrænset planlægning for brugen af alternative IKT-midler. Det indikerer behov for yderligere kompetenceudvikling og øvelser – dels for at opbygge og styrke medarbejderes rutine i at anvende alternative IKT-midler, dels for at afdække, om organisationer og tværgående stabe er tilstrækkeligt udstyret med resilient IKT og backupløsninger, herunder eventuelt også ældre og mere simpel teknologi. Tilbagemeldingerne peger endvidere på, at mange deltagere tydeligere end før KRISØV 2013 ser et behov for stærkere koordinering mellem organisationers "traditionelle beredskabsarbejde" og det interne arbejde med it-sikkerhed og kommunikationsforhold mv.

Endelig kunne der under KRISØV 2013 konstateres en god snitfladeopdeling mellem myndigheder med særligt ansvar for håndtering af cyberhændelser. Rolle- og ansvarsforhold var på plads mellem Rigspolitiet, PET, FE og CFCS, og afprøvningen under øvelsen demonstrerede, at setuppet virkede. Øvelsen indikerede dog også, at ikke alle de øvrige deltagende organisationer havde forudgående kendskab til den præcise opgavefordeling mellem disse fire myndigheder samt øvrige aktører som fx Statens IT. Tilbagemeldinger viser endvidere, at "cybermyndighederne" fortsat må forholde sig til et stort behov for målrettet rådgivning blandt "ikke-specialist"-myndigheder samt behov for videndeling i bredere forstand, bl.a. via publikationer.

Det anbefales:

- At brugen af alternative informations- og kommunikationsmidler planlægges og trænes yderligere på centralt og decentralt niveau for at imødekomme situationer, hvor primære digitale kanaler sættes ud af drift. Dette kan fx ske enten via "KOM-øvelser" (også kaldet signaløvelser) eller som element i andre øvelser og uddannelsesaktiviteter. Myndigheder og andre aktører bør endvidere opfordres til at udarbejde enkle instrukser omkring ressourcer og procedurer for brug af alternative IKT-midler som led i egen beredskabsplanlægning.
- At myndigheder med et særligt ansvar for håndtering af cyberhændelser følger op på øvelseserfaringerne via målrettet ekstern rådgivningsvirksomhed og udbreder kendskabet til deres rolle- og ansvarsfordeling.

6. Opfølgning på øvelsestekniske anbefalinger fra KRISØV 2011

I de følgende afsnit ses der på evalueringens fokusområde 3 om, hvordan fire øvelsestekniske anbefalinger fra evalueringen af KRISØV 2011 blev fulgt op, og hvilket udbytte det gav for planlægningen og gennemførelsen af KRISØV 2013. Der opstilles endvidere nogle nye øvelsestekniske forslag, som forhåbentligt vil kunne guide den næste øvelsesledelses forberedelser af den 7. nationale krisestyringsøvelse, KRISØV 2015.

6.1 Forberedende aktiviteter som integreret del af øvelseskonceptet

KRISØV 2011 evalueringen viste, at forberedende aktiviteter generelt havde stor betydning for øvelsestagernes udbytte af øvelsen. Tendensen var, at jo flere aktiviteter de foretog før øvelsen, jo større var udbyttet. Samme

tendens synes at have gjort sig gældende med hensyn til øvelsesplanlæggernes deltagelse i forberedende aktiviteter. Det blev på den baggrund anbefalet at: "*Det bør overvejes at gøre myndighedernes forberedende aktiviteter til en integreret del af øvelseskonceptet.*"

Som opfølgning på denne anbefaling blev der før KRISØV 2013 gennemført et væsentligt større antal forberedende aktiviteter end tidligere i KRISØV-serien. Det inkluderede bl.a. følgende arrangementer med et generelt højt fremmøde: Temadag om cybertrusler og cybersikkerhed, Workshop om kommunikation under cyberangreb, Bliv-klar-til-KRISØV-dagen, Konference om krisekommunikation og sociale medier, Formøde om KRISØV 2013 i DCOK, Orienteringsmøde for øvelsestagere, Briefing for presseansvarlige samt KRISØV 2013 generalprøven.

Oplæggene ved CFCS om, hvordan man kan forberede sig på at imødegå cyberangreb, og hvordan CFCS kan bidrage til beskyttelsen af myndigheder og virksomheder, er blevet fremhævet som særligt hensigtsmæssige i forbindelse med de forberedende aktiviteter. Det samme gælder for den "Dilemmaøvelse om cybersikkerhed", som Beredskabsstyrelsen udviklede som optakt til KRISØV 2013. Evalueringsgruppen er bekendt med, at mindst ni organisationer afprøvede cyberdilemmaøvelsen, og tilbagemeldinger viser, at denne virkede godt som indføring i hovedscenariet for KRISØV 2013 og var god til at afdække sårbarheder inden øvelsen.

Herudover gennemførte de deltagende organisationer ofte mange interne forberedende aktiviteter på eget initiativ og/eller på opfordring fra øvelsesledelsen. For flertallet af de 24 respondenter i spørgeskemaundersøgelsen involverede disse aktiviteter fx skriftlig orientering og/eller et informationsmøde om øvelsen i eget hus; lister med kontaktinformationer, vagtplaner, instrukser mv.; gennemgang af procedurer for alarmering og drift af egen krisestyringsorganisation; forberedelse af krisestyringsfaciliteter; udarbejdelse, revision eller ajourføring af beredskabsplaner; anmodning om at øvelsestagere gennemgik relevante interne planer mv.; samt opfordring til at læse relevante trusselsvurderinger og lignende fra fx CFCS. Omvendt var det tilsyneladende mindre udbredt at anmode egne øvelsestagere om at gennemgå National Beredskabsplan og plansættene for NOST, DCOK og LBS11 (37,5 pct.) eller at gennemgå planer tilhørende relevante samarbejdspartnere (8,3 pct.).

Det vurderes, at summen af de forberedende aktiviteter udgjorde et stort bidrag til at forbedre øvelseskonceptet og deltagernes udbytte af KRISØV 2013. Af spørgeskemaundersøgelsens respondenter angav 50 pct., at dette var tilfældet "i høj grad" og 42 pct. "i nogen grad". Konklusionen peger dermed entydigt i samme retning som efter KRISØV 2011: Jo flere og jo mere omfattende forberedende aktiviteter øvelsestagerne deltager i eller selv gennemfører, jo større er effekten. Forberedende aktiviteter som en integreret del af øvelseskonceptet bør derfor fastholdes i KRISØV-serien – og kan eventuelt også udbredes som god praksis i forbindelse med andre øvelser.

6.2 Færre, men større og dynamiske scenarier med sammenhæng mellem indspil

KRISØV 2011 indeholdt fem meget forskellige spor. Formålet var dengang, og som i tidligere KRISØV'er, at øve så mange forskellige organisationer som muligt. Erfaringerne viste dog, at antallet af spor, og det deraf resulterende antal scenarier og indspil i uforholdsmæssig grad, gjorde KRISØV 2011 til en "stress-øvelse". Det blev derfor anbefalet: *"Der bør fokuseres på færre, men større scenarier. Scenarierne bør være dynamiske, dvs. der bør være vægt på, at de udvikler sig under øvelsen. De enkelte indspil i hvert scenarie bør bygge på hinanden, så indspillene ikke fremstår som enkeltstående hændelser uden større indbyrdes sammenhæng."*

I KRISØV 2013 øvelsesledelsen blev der gjort en stor indsats for at sikre, at ovenstående blev implementeret. Det blev på et tidligt tidspunkt fastlagt, at der kun skulle være et overordnet scenarie (cyberangreb), og efterhånden som arbejdet med drejebøgerne skred frem, blev der udviklet en oversigt over delscenarier og fixpunkter, hvoraf det fremgik, hvilke hændelser, der forventedes at berøre hvilke organisationer og hvornår.

Tilbagemeldingerne fra øvelsestagerne indikerer, at øvelsen overordnet set formåede at bevare fokus på det overordnede scenarie, og at delscenarierne udviklede sig dynamisk og realistisk i løbet af øvelsen. Der er dog

også blevet påpeget, at der ikke altid var den tilstræbte sammenhæng og overensstemmelse mellem delscenarierne. Nogle af disse var desuden ikke forårsaget af cyberangreb, og dermed ikke eller kun indirekte relateret til det overordnede scenarie. Som resultat heraf – og pga. indspillenes antal og frekvens– oplevede nogle deltagere, at KRISØV 2013 trods øvelsesledelsens intentioner alligevel udviklede sig til en "stressøvelse", særligt på dag 1.

Efter evalueringsgruppens vurdering indikerer dette, at der til KRISØV 2015 igen bør udvælges én hændelsestype som overordnet scenarie, og at der i drejebogsarbejdet kan gøres endnu mere for at sikre, at der ikke opstår usammenhængende delscenarier i øvelsen. En overordnet "storyline" kan med fordel udarbejdes tidligt i forløbet, og antallet af indspil med enkeltstående hændelser kan reduceres med henblik på, at øvelsestagerne kan komme bedre rundt om alle aspekter af hovedscenariet.

6.3 Relevante indspil til alle deltagende organisationer

Under KRISØV 2011 viste det sig problematisk, at flere organisationer ikke blev aktiveret til trods for, at de var med på øvelsesledelsens kontaktliste. Det blev på den baggrund konkluderet, at problemstillingen krævede afvejning af et ønske om flere deltagere i KRISØV og, på den anden side, et mere udbredt ønske om færre scenarier. Resultatet var en anbefaling i KRISØV 2011 evalueringen om, at *" Øvelsesledelsen skal ved tilrettelæggelsen af øvelsen sikre, at alle relevante øvelsestagere modtager indspil, der er relevante i forhold til scenariet."*

Som opfølgning blev denne anbefalings ordlyd skrevet direkte ind i KRISØV 2013 øvelsesdirektivet, og evalueringsgruppen har via observationer i øvelsesledelsen kunnet konstatere, at der blev gjort store bestræbelser på at sikre relevante indspil til alle. Spørgeskemabesvarelserne viser desuden, at 19 ud af de 24 respondenter var overvejende eller meget tilfredse med dokumenter med story-line, fixpunkter og indspil til drejebøgerne. 22 af respondenterne var helt eller overvejende enige i, at deres organisationer modtog relevante indspil. Til trods herfor kan det dog konstateres, at nogle få organisationer har tilkendegivet, at de ikke fandt øvelsen tilstrækkeligt udfordrende eller ikke blev aktiveret tilstrækkeligt set i lyset af de ressourcer, de havde afsat til øvelsesdeltagelsen. For disse organisationer vurderes det imidlertid, at årsagen primært skal findes i manglende indspil i de myndigheds- og sektorspecifikke drejebøger, som de pågældende organisationer forventedes at udvikle via egne repræsentanter i øvelsesledelsen.

Evalueringsgruppen betragter det, som en af de væsentligste styrker ved KRISØV-serien, at de deltagende organisationer bidrager aktivt til planlægningen ved at indgå i øvelsesledelsen og formulere egne indspil i drejebøgerne. Evalueringsgruppen skal derfor alene opfordre til, at der i arbejdet med drejebogsudkast til KRISØV 2015 gøres en forstærket indsats for at identificere tilfælde, hvor indspil til konkrete øvelsestagere ikke er tilstrækkelige i antal, frekvens og/eller kompleksitet. Der er vurderingen, at der i forbindelse med planlægningen og gennemførelsen af KRISØV 2015 skal være en bedre strategisk forankring af de enkelte organisationers deltagelse.

6.4 Videreudvikling af mediespillet og indspil fra borgere

I evalueringen af KRISØV 2011 fandt flertallet af øvelsestagerne, at niveauet for mediespillet burde bibeholdes i nationale krisestyringsøvelser, og ca. en tredjedel ønskede mediespillet opprioriteret. Der blev endvidere foreslået at udbygge borgerhenvendelser og eventuelt inddrage sociale medier. I evalueringsrapporten blev det derfor anbefalet, at "*Øvelsesledelsen bør se på mulighederne for at videreudvikle mediespillet og indspil fra borgere."*

Som opfølgning på anbefalingen blev særligt borgerspillet opprioriteret i KRISØV 2013. For første gang i KRISØV sammenhæng, blev der anvendt et Twitter-lignende fiktivt socialt medie kaldet "Blokken". Blokken blev styret fra øvelsesledelsens borgercelle, hvorfra "almindelige danskere" og "bekymrede borgere" kom med indspil eller reagerede på indspil ved at skrive indlæg og ved at ringe rundt til myndighederne for at få oplysninger.

Brugen af Blokken bevirkede, at flere af de deltagende myndigheder skulle forholde sig til at bruge sociale medier. Af de i alt 3.265 indlæg på Blokken stod myndighederne således for 12,3 pct., mens medierne stod for 8,7 pct., og de resterende 79 pct. var skrevet af "øvelsesborgerne". I kombination med telefonopkald og e-mails gav dette et meget realistisk indblik i, hvad borgere kan bekymre sig om i en skarp situation, og gav myndighederne mulighed for at dementere rygter og falske historier. Samtidig gav det myndighederne en direkte kanal til at kommunikere med borgere udover egen hjemmeside, samt i tilfælde, hvor hjemmesider var ud af drift. I en periode hvor politi.dk var nede, kommunikerede politiet fx kun direkte med borgere via Blokken under #kriseinfo.

Mediespillet var også videreudviklet i KRISØV 2013. I øvelsesledelsen var der etableret en mediecelle, som havde ansvar for at publicere artikler på det fiktive øvelsesmedie Ajour24´s hjemmeside. Tilbagemeldinger fra mediecellens personel har generelt været positive. De var fx glade for, at de selv havde ansvar for at bearbejde informationer og selv kunne generere ideer og vinkler på de artikler, som blev produceret under øvelsen. Mediecellen fandt dog, at drejebøgernes på forhånd planlagte medie-indspil i en del tilfælde ikke var udførlige nok. Endelig kunne mediecellen have ønsket, at øvelseshjemmesiderne havde givet flere muligheder kendt fra virkelighedens elektroniske medier, fx en "RSS-feed" eller en "Alert me" funktion, når myndigheder lagde nyheder på hjemmesider (simuleret på myndighedsinfo.dk), samt at kunne skrive læser-kommentarer til artikler publiceret på Ajour24.

Sideløbende med Mediecellens virke på øvelsesledelsens vegne, gjorde DR, Version2 og Computerworld en stor indsats som øvelsestagere. Deres dækning fremstod meget virkelighedsnær, og det havde stor betydning for alle øvelsestageres oplevelse af situationen, påvirkede afviklingen af hele øvelsen i en positiv retning, og medvirkede således til at opfylde målsætningen om et forbedret medie- og borgerspil. DR deltog fx med et hold på 12-14 journalistiske medarbejdere, som bragte fiktive nyheder på egen øvelseshjemmeside og producerede fiktive radioaviser hver time. Samtidig prøvede de via interviews at vriste så mange oplysninger som muligt ud af de øvrige deltagende organisationer, for at kunne informere befolkningen ordentligt i kraft af rollen som public service-mediekanal. DR indkaldte bl.a. også eksperter i studiet for at få realistiske vurderinger af situationen.

Endelig viste erfaringerne betydningen af, at medie- og borgercellerne fastholdes tæt på den centrale øvelsesledelse under øvelsen. Som mulige forbedringstiltag kan nævnes, at medie- og borgercellerne med fordel kan gives bedre kendskab til drejebøger og indspil tidligere i planlægningsfasen samt få demonstreret, hvordan den anvendte teknologi virker i god tid før øvelsesstart. Endvidere kan øvelsesledelsen vælge at bruge Borgercellen mere aktivt, hvis der undervejs i øvelsen ønskes en speciel vinkel på borgerhenvendelserne.

Sammenfattende konkluderes det, at målsætningen om at videreudvikle medie- og borgerspillet blev nået. Tilbagemeldinger fra stort set samtlige medlemmer af øvelsesledelsen og øvelsestagerne, herunder de medie- og kommunikationsansvarlige medarbejdere i DCOK og LBS11, indikerer, at medie- og borgerspillet virkede relevant og realistisk. Førstegangsforsøget med brug af sociale medier i KRISØV 2013 var en succes, og al erfaring viser, at brugen af virkelige medier i KRISØV-serien er en tradition, der bør fastholdes og gerne styrkes yderligere.

6.5 Øvrige øvelsestekniske læringspunkter

KRISØV 2013 deltagernes tilbagemeldinger viser generel tilfredshed med øvelsens format og elementer. Blandt spørgeskemaundersøgelsens 24 respondenter angav omkring 80 pct. fx, at de fandt deres ressourceforbrug i forbindelse med planlægningen og gennemførelsen passende. Ca. samme procentdel fandt mængden af information op til øvelsen, øvelsens varighed, antal scenarier, tempo og antal deltagende organisationer passende.

Blandt øvrige positive erfaringer kan nævnes, at den centrale indspil/svar-celle for første gang i KRISØV-serien blev drevet som en stab, herunder med stabsledelse, stabsmøder og en fortløbende aktionsliste (tavleoversigt), som blev ført af en dedikeret "plotter" foranstaltet af Rigspolitiet. Dette vurderes som en vigtig medvirkende faktor til, at de øvelsesteknikske aspekter generelt fungerede godt på øvelsesdagene.

Omvendt kunne der konstateres væsentlige sårbarheder ved den teknologiske platform for KRISØV 2013. Krisoev.dk hjemmesiden indeholdt en række undersider med forskellige funktioner, bl.a. som myndighedernes egne hjemmesider, øvelsesmediernes hjemmesider og Blokken. Disse fungerede, men langt fra optimalt, og flere problemer måtte rettes akut og meddeles øvelsestagerne efter øvelsesstart. Herudover havde forbindelsen kapacitetsproblemer, der var problemer med at tilgå siderne for ikke-Windows baserede operativsystemer, og urene på siderne gik forkert. Det er desuden bemærket, at opsætningen ikke virkede betryggende, idet man efter login på krisoev.dk blev videreført til et privat domæne. Det er vurderingen, at den anvendte platform er teknisk og sikkerhedsmæssigt uanvendelig til fremtidige øvelser.

6.6 Evalueringstekniske læringspunkter

Med KRISØV 2013 evalueringsdesignet, som var det hidtil mest omfattende i KRISØV-serien, ønskede Beredskabsstyrelsen og Rigspolitiet at gøre erfaringsopsamling til en mere integreret del af øvelseskonceptet. Øvelsesplanlæggerne og øvelsestagerne tog generelt positivt imod dette, og der var særlig tilfredshed med de nye tiltag i form af debriefingerne og evalueringsseminaret. Debriefingerne gjorde det muligt at fastholde umiddelbare indtryk på skrift, mens de stadig var friske i erindringen. Evalueringsseminaret gav mulighed for feedback, efter at deltagerne havde haft godt en måned til at reflektere over individuelle og organisatoriske øvelseserfaringer.

I de 24 spørgeskemabesvarelser angav to tredjedele af respondenterne, at de finder deres ressourceforbrug i forbindelse med øvelsens evaluering passende, og 17 pct. svarede, at ressourceforbruget bør øges. Herudover har et stort antal deltagere tilkendegivet, at de, udover deres bidrag til den tværgående evaluering, gennemfører interne evalueringsaktiviteter som fx seminarer, evalueringsrapporter og/eller implementeringsplaner. Dette betragtes som yderligere anerkendelse af, at det er vigtigt at fastholde og udnytte den viden og læring, som opnås.

6.7 Delkonklusion og anbefalinger til KRISØV 2015

Opfølgning på de fire øvelsestekniske anbefalinger fra KRISØV 2011 evalueringsrapporten skabte en bedre øvelsesteknisk ramme for KRISØV 2013, og fokus på læring i både planlægningen, afviklingen og evalueringen bidrog positivt til resultatet. Udbyttet inkluderede bl.a. det største antal forberedende aktiviteter hidtil i KRISØV-serien og et veltilrettelagt medie- og borgerspil, herunder udpræget tilfredshed med inklusionen af sociale medier.

Øvelsen formåede at bevare fokus på cyberangreb som overordnet scenarie, men der var ikke altid den tilstræbte sammenhæng mellem de enkelte delscenarier. Som resultat af dette, samt det store antal indspil, oplevede nogle deltagere, fx i DCOK, at KRISØV 2013 udviklede sig til en "stressøvelse". Enkelte andre blev derimod ikke aktiveret tilstrækkeligt trods målsætningen om, at drejebøgerne skulle sikre relevante indspil til alle deltagere.

Den øvelsestekniske styring fungerede generelt godt på øvelsesdagene. En medvirkende faktor hertil var, at øvelsesledelsens centrale indspil/svar-celle, som et nyt initiativ, blev drevet som en stab. Der kunne dog konstateres væsentlige svagheder ved krisoev.dk, hvilket tydeliggjorde behov for et bedre it-teknisk setup for KRISØV 2015.

De deltagende organisationer tog generelt godt imod det udvidede evalueringsdesign for KRISØV 2013.

Det anbefales:

- At de fire øvelsestekniske anbefalinger, som blev fremsat efter KRISØV 2011 og fulgt i KRISØV 2013, også skal gælde ved forberedelsen og gennemførelsen af KRISØV 2015.
- At der udvikles en mere tidssvarende, robust og brugervenlig øvelses-it-platform til brug for KRISØV 2015.
- At debriefinger og et evalueringsseminar fastholdes som god praksis i KRISØV 2015 evalueringsdesignet.

7. Efterskrift: Fra læring til implementering

Evalueringen har vist stor tilfredshed blandt deltagerne i KRISØV 2013 med øvelsen samt det opnåede udbytte. Der er dog fortsat mulighed for dynamisk at videreudvikle det overordnede øvelseskoncept, og det er vigtigt, at KRISØV-serien fortsat indgår som vigtigt bidrag til udviklingen af det nationale krisestyringssystem og de dertilhørende kompetencer, herunder både den udvikling, som finder sted i de tværgående fora, og den udvikling, der sker internt i de deltagende organisationer.

Øvelseserfaringerne fortjener opfølgning, og som hovedansvarlige for tilrettelæggelsen af KRISØV ønsker Beredskabsstyrelsen og Rigspolitiet at spille en central rolle i denne proces. KRISØV 2013 evalueringsrapporten skal derfor afsluttes med en opfordring til alle organisationer, som deltog i planlægningen, afviklingen og evalueringen af øvelsen, om også at støtte op om de tværgående opfølgningsaktiviteter og iværksætte interne initiativer, som udnytter læringen fra KRISØV 2013 og derigennem styrker samfundets samlede krisestyringskompetencer.

Der vil – i lighed med tidligere nationale krisestyringsøvelser – blive fulgt op på evalueringsrapportens anbefalinger i regi af Kriseberedskabsgruppen. Herudover vil Beredskabsstyrelsen i løbet af 2014 iværksætte en undersøgelse af, hvorledes der følges op på anbefalingerne blandt relevante aktører i beredskabet.