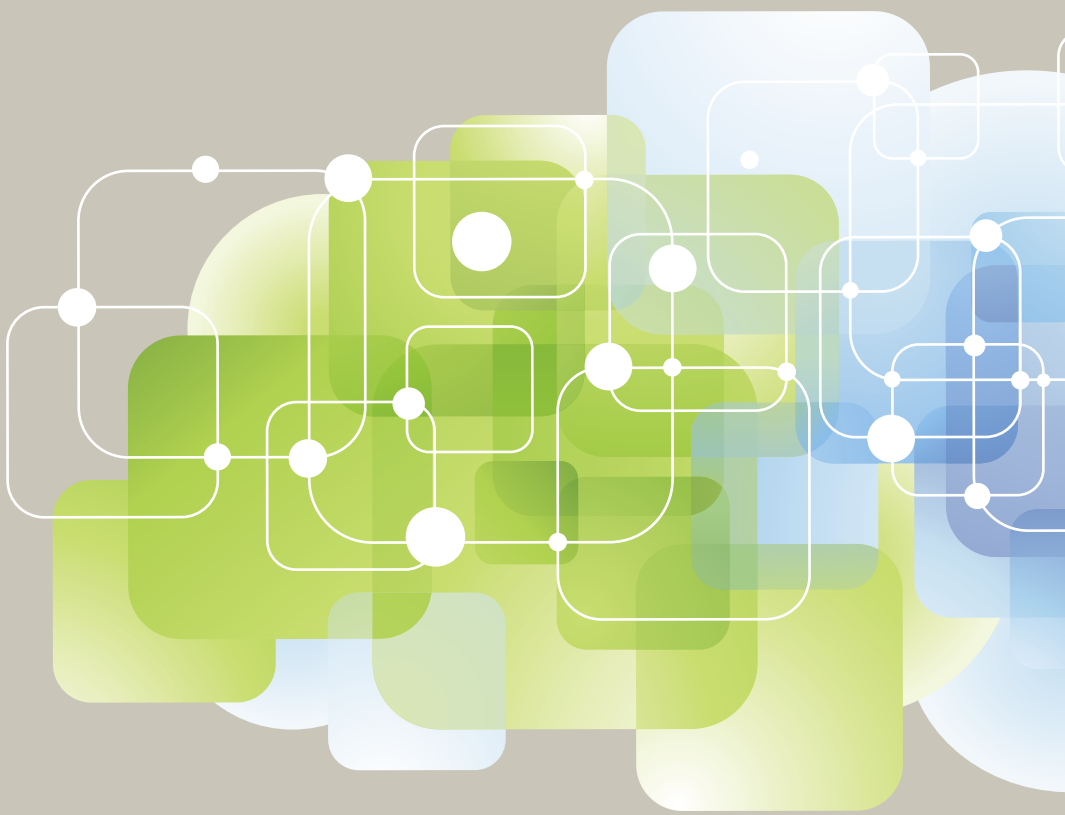
Myndigheten för samhällsskydd och beredskap

NISÖ 2018

Erfarenhetsrapport



NISÖ 2018

Erfarenhetsrapport

NISÖ 2018 – Erfarenhetsrapport

Myndigheten för samhällsskydd och beredskap (MSB)

Produktion: Advant
Tryck: DanagårdLiTHO

Publikationsnummer: MSB1326 - december 2018
ISBN: 978-91-7383-900-6

Förord

Myndigheten för samhällsskydd och beredskaps (MSB) uppgift är att utveckla och stödja samhällets förmåga att hantera olyckor och kriser. I det avseendet spelar MSB:s övningsverksamhet en central roll. MSB:s uppdrag är att främja övningsverksamheten genom främst sektorsövergripande övningar. Målet är att aktörerna med hjälp av övningar ska utveckla en god förmåga att begränsa konsekvenserna av olyckor och kriser, en god förmåga att kunna leda och fatta beslut inom eget ansvarsområde, samt att kunna samverka med andra.

Samtidigt som allt fler samhällsfunktioner digitaliseras och blir uppkopplade, finns brister i informations- och cybersäkerheten hos aktörer i alla samhällssektorer. Att höja lägstanivån på samhällets informations- och cybersäkerhet är avgörande för en säker digitalisering, inte minst ur ett totalförsvarsperspektiv. MSB har ett särskilt mandat att samordna och stödja arbetet med samhällets informations- och cybersäkerhet. I detta ingår även att svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. MSB:s uppgift på informationssäkerhetsområdet riktar sig till allt från andra myndigheter, kommuner och näringslivet till enskilda individer.

Den 14-15 februari 2018 genomförde MSB den nationella informationssäkerhetsövningen NISÖ 2018. Övningen syftade till att stärka samhällets förmåga att hantera nationella it-relaterade kriser, främst genom att utveckla förmågan till samarbete och samordning mellan privata och offentliga aktörer inom utpekade sektorer.

Denna rapport sammanfattar arbetet med NISÖ 2018 och presenterar viktiga lärdomar och utvecklingsbehov för att öka samhällets krisberedskap, särskilt inom informations- och cybersäkerhet.

Stockholm, 2018-11-30

Åke Holmgren
Chef, Avd. för cybersäkerhet och
skydd av samhällsviktig verksamhet

Innehåll

Sammanfattning

För att kunna utveckla den framtida övningsverksamheten och se till att krishanteringssystemet fortsätter att utvecklas är det nödvändigt att ta vara på erfarenheter från de övningar som genomförs. Den här erfarenhetsrapporten beskriver övningen *Nationell informationssäkerhetsövning 2018* (NISÖ 2018), som genomfördes den 14–15 februari 2018. Rapporten redogör även för erfarenheter från planeringen och genomförandet av övningen, samt för de aktörsgemensamma utvecklingsbehov som har identifierats.

NISÖ 2018 planerades, genomfördes och utvärderades av projektet *NISÖ 2018*. Övningen genomfördes som en simuleringsövning med motspel vid Ledningsregementet i Enköping.

NISÖ ska stärka förmågan att hantera större it-relaterade kriser

Övningsverksamhet är en viktig del i arbetet med att stärka förmågan att hantera olika händelser och kriser. Övningar planeras på lång sikt, så att varje enskild övning kan bidra till såväl planerade förmågehöjningar som till att upprätthålla den förmåga som finns. Övningarna i NISÖ-serien syftar till att stärka samhällets förmåga till krishantering och förmåga att hantera större it-relaterade kriser.

Samordning mellan privata och offentliga aktörer i fokus

NISÖ 2018 syftade till att stärka samhällets förmåga att hantera nationella it-relaterade kriser, främst genom att utveckla förmågan till samverkan och samordning mellan privata och offentliga aktörer inom följande sektorer:

- energi
- hälso- och sjukvård
- information och kommunikation
- lokala och regionala myndigheter
- transport.

Två övergripande utvecklingsområden har identifierats

Försvarshögskolans fick i uppdrag att göra en formell utvärdering av hur de aktörsgemensamma målen uppfylldes under övningen. De utvecklingsområden som MSB presenterar i den här rapporten är baserade på resultaten av Centrum för totalförsvar och samhällets säkerhet (CTSS) utvärdering och det erfarenhetsseminarium som genomfördes efter övningen.

MSB har sorterat de identifierade områdena och anpassat dem till det bredare utvecklingsarbete som pågår inom myndigheten. Två huvudsakliga, övergripande områden i behov av utveckling identifierades under NISÖ 2018: *samverkan och systemförståelse samt informationsdelning och lägesbild.*

Samverkan och systemförståelse

Utvärderingen av NISÖ 2018 visar att förmågan till samverkan mellan privat och offentlig sektor under it-relaterade kriser fortsatt behöver utvecklas. Dessutom behöver kunskapen om krishanteringssystemet stärkas. Utifrån de påvisade bristerna i samverkan och systemförståelse identifierades tre konkreta utvecklingsområden inför det fortsatta utvecklingsarbetet:

- privat-offentlig samverkan
- kunskap om samverkansforum
- kunskap om lokala och regionala aktörers behov och förmågor.

Informationsdelning och lägesbild

Utvärderingen visar även att arbetet med informationsdelning och lägesbild behöver stärkas i flera avseenden. De konkreta utvecklingsområden som har identifierats för att stärka förmågan till informationsdelning och lägesbildsarbete är:

- robusta och säkra kommunikationer
- traditionella kommunikationskanaler
- lägesinformation och lägesbild.

Lärdomar och slutsatser efter utvärdering och seminarier

Erfarenhetsrapporten avlutas med en sammanfattning av slutsatser och lärdomar från planeringen, genomförandet och utvärderingen av NISÖ 2018. Dessa slutsatser bygger på utfallet av den processutvärdering som genomfördes i anslutning till NISÖ 2018 och de samtal som fördes under erfarenhetsseminariet i maj 2018.

Inledning

1. Inledning

1.1 Samhällets informationssäkerhet och it-relaterade kriser

Det svenska samhället är beroende av en fungerande it-infrastruktur. Det gäller såväl medborgare som företag och myndigheter. En fungerande it-infrastruktur är dessutom en förutsättning för att de offentliga och privata aktörer som bedriver samhällsviktig verksamhet ska kunna fullgöra sina uppdrag.

Både företag och myndigheter använder sig av it och kommunikationsteknologi i det dagliga arbetet. Sårbarheter i it-system kan alltså få stora konsekvenser för både enskilda individer och för samhället i stort. It-relaterade kriser kan exempelvis drabba sjukvården, medier, energiförsörjningen, statliga myndigheter, kommunala aktörer och transporter. Detta kan i sin tur leda till att samhällsviktig verksamhet destabiliseras: informationssystem sätts ur funktion, traditionella kommunikationsvägar bryts och viktiga transporter försvåras. För att kunna förebygga och hantera it-relaterade kriser behöver det svenska samhället stärka sin förmåga att hantera denna typ av händelser. Förmågan behöver stärkas hos såväl privata som offentliga aktörer som tillhandahåller samhällsviktiga tjänster.

It-relaterade kriser har i regel ett snabbt händelseförlopp, vilket innebär att aktörerna behöver kunna upptäcka avvikelser och hantera situationen redan på ett tidigt stadium. Organisationer som berörs av en it-relaterad kris måste även samordna sina insatser och snabbt skapa en gemensam lägesbild med övriga aktörer i krishanteringssystemet.

1.1.1 Utvecklingen på informations- och cybersäkerhetsområdet

Utvecklingen på informations- och cybersäkerhetsområdet går fort och behovet av ökad it- och informationssäkerhet är påtagligt i hela samhället. Beslutsfattare arbetar kontinuerligt med att utveckla lagar och direktiv för att möta de nya utmaningar som ett allt mer it-beroende samhälle står inför. Policyutvecklingen inom informations- och cybersäkerhetsområdet har gått framåt i ett snabbt tempo sedan den första nationella informationssäkerhetsövningen (NISÖ) hölls 2010.

Utveckling har skett på såväl nationell som internationell nivå. År 2013 antogs EU:s cybersäkerhetsstrategi[1]. Detta var startskottet för

1. Europeiska kommissionen (2013;2009) *Cybersäkerhetsstrategi för EU, (JOIN (2013) 1 final); Om skydd av kritisk informationsinfrastruktur,* KOM(2009)149

arbetet med *NIS-direktivet*[2], som antogs i juli 2016 och implementerades i svensk lagstiftning den 1 augusti 2018. Direktivet syftar till att harmonisera de krav på informationssäkerhet som EU ställer på medlemsstaterna, på leverantörer av samhällsviktiga tjänster och på leverantörer av digitala tjänster. Parallellt med utvecklingen på europeisk nivå har en rad utredningar och styrdokument tagits fram för en svensk kontext. Värda att nämna är till exempel NISU-utredningen[3] som kom 2015 och regeringens strategi på området som kom 2016[4].

Att nya policyer utvecklas är nödvändigt, men den snabba utvecklingen inom it- och informationssäkerhetsområdet ställer höga krav på de aktörer som bedriver samhällsviktig verksamhet. Policyutvecklingens snabba hastighet på internationell och nationell nivå innebär därmed ytterligare prövningar för dessa organisationer, utöver de teknologiska och organisatoriska utmaningar som karakteriserar it- och informationssäkerhetsområdet. Aktörer behöver utbildning och övning för att upprätthålla förmågan att förebygga och hantera framtida it-relaterade krishändelser, och för att kunna följa med i utvecklingen.

1.2 It-relaterade kriser och behovet av övning

Erfarenheter från inträffade it-incidenter och it-relaterade kriser visar att det är viktigt att aktörer är förberedda för de specifika utmaningar som just it-krissituationer ställer dem inför. Regelbundna nationella övningar är en förutsättning för att utveckla och utvärdera aktörernas förmåga att hantera it-relaterade krishändelser.

Särskilt viktiga är de nationella tvärsektoriella övningarna, som syftar till att utveckla samordning och samverkan i samhället. It-relaterade kriser ställer även krav på teknisk kompetens samt förutsätter samarbete mellan tekniska experter och övriga medarbetare i organisationen, exempelvis ledningsgruppen eller kommunikatörer. Övning och utbildning för att hantera de tekniska aspekterna av it-relaterade kriser är därmed också av stor vikt för att bygga upp förmågan.

I Sverige har övningarna i NISÖ-serien varit viktiga delkomponenter i övningsarbetet. Den första NISÖ-övningen genomfördes 2010, och ytterligare en övning i serien hölls 2012. Detta i linje med de nationella och internationella direktiv som syftar till att stärka Sveriges och EU:s förmåga inom it- och informationssäkerhet.

---

2. Europaparlamentet och rådet (2016) *Direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen ("Nis-direktivet")*, (EU) 2016/1148
3. Justitiedepartementet (2015) *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten,* SOU 2015:23
4. Justitiedepartementet och Regeringen (2016) *Nationell strategi för samhällets informations- och cybersäkerhet,* Skr. 2016/17:213

1.2.1 Europeiska och internationella övningar

På internationell nivå uppmanar den Europeiska kommissionen EU:s medlemsstater att anordna regelbundna övningar för insatser under och efter storskaliga it-incidenter. Europeiska kommissionen lyfter också behovet av övningar på europeisk nivå.[5]

Under de senaste åren har ett antal internationella övningar genomförts. I november 2010 ägde den första paneuropeiska övningen rum, *Cyber Europe 2010*. Efter den har sedan Cyber Europe 2012, 2014, 2016 och 2018 följt. Även den amerikanska säkerhetspolisen har hållit i aktiviteter på området, som också har varit öppna för europeiska aktörer. Ett exempel är övningen *Cyber Storm*. Genomförandet och planeringen av NISÖ 2018 har utgått från erfarenheterna från dessa tidigare aktiviteter.

1.3 Övningsserien Nationell informationssäkerhetsövning (NISÖ)

Myndigheten för samhällsskydd och beredskap (MSB) ansvarar för övningsserien NISÖ. NISÖ syftar till att stärka samhällets förmåga till krishantering och samhällets förmåga att hantera it-relaterade kriser. Övningsverksamheten ska även stärka samverkan på bred front i krishanteringssystemet. NISÖ 2018 är den tredje övningen i övningsserien, och nästa övning planeras till 2021.

1.4 Innehållet i denna rapport

Den här rapporten beskriver övningen NISÖ 2018. Rapporten redogör för erfarenheterna från planeringen och genomförandet, samt beskriver de aktörsgemensamma utvecklingsbehov som har identifierats. De deltagande aktörernas enskilda insatser och aktörsspecifika mål ingår inte i rapporten, utan hanteras i stället enskilt av respektive organisation.

Syftet med rapporten är att beskriva de erfarenheter och lärdomar som har genererats under NISÖ 2018, och att redogöra för de utvecklingsbehov i krishanteringssystemet som har identifierats i samband med övningen. Därmed syftar rapporten också till, sett ur ett större perspektiv, att stärka samhällets förmåga att hantera it-relaterade kriser.

Försvarshögskolans *Centrum för totalförsvar och samhällets säkerhet* (CTSS) har haft i uppdrag att göra en formell utvärdering av NISÖ 2018. De utvecklingsområden som MSB presenterar i denna rapport är baserade på resultaten av CTSS utvärdering av NISÖ 2018.

---

5. *Cybersäkerhetsstrategi för EU; Om skydd av kritisk informationsinfrastruktur*

Planering av NISÖ 2018

2. Planering av NISÖ 2018

NISÖ 2018 planerades, genomfördes och utvärderades av ett projekt, även det kallat *NISÖ 2018*. Projektet genomfördes som ett långsiktigt samarbete mellan avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet och enheten för övning vid MSB. Projektet bemannades av personal från MSB och av externt verksamhetsstöd. Det finansierades med 2:4-medel som hade avsatts för projektet. Planeringen, genomförandet och utvärderingen av NISÖ 2018 pågick i två år, från 2016 till och med genomförandet 2018.

2.1 Planeringsstruktur

Projektgruppen planerade NISÖ 2018 utifrån MSB:s planeringsmodell för simuleringsövningar med motspel, med fokus på medverkan från deltagande aktörer. Syftet med planeringsprocessen var att ge alla deltagande aktörer förutsättningar att förbereda genomförandet utifrån sin valda ambitionsnivå och sin tillgängliga kompetens. Dessutom behövde projektet arrangera ett tillräckligt omfattande motspel, med individer som kunde agera omvärld under genomförandet och förse de deltagande aktörerna med inspel under övningens gång.

Planeringen startade formellt i samband med att projektdirektivet beslutades i maj 2016. Projektet genomförde informationstillfällen och arbetsmöten för de deltagande aktörerna i form av startmöte och tre planeringskonferenser. Dessutom genomfördes också skrivarstugor för inspelsarbete. I skrivarstugorna deltog främst lokala övningsledare och utsedda inspelsskapare, som i samverkan skrev de inspel som konstruerades utifrån det övergripande övningsscenariot.

2.1.1 Deltagande aktörer

Aktörerna vid NISÖ 2018 kom från följande samhällssektorer:

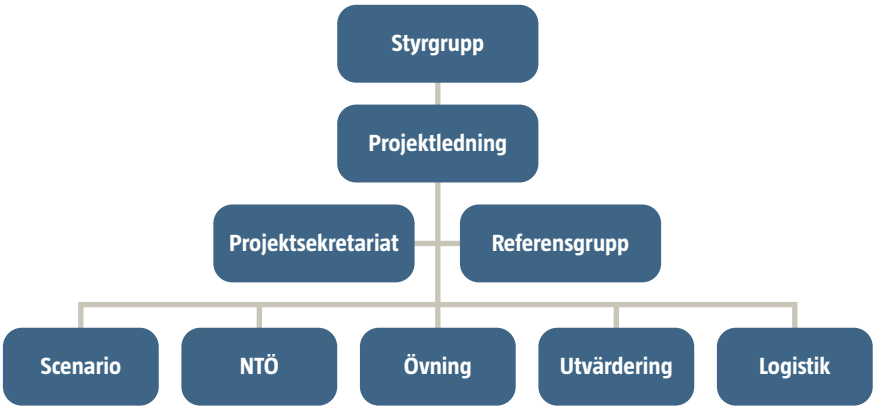
- energi
- hälso- och sjukvård
- information och kommunikation
- lokala och regionala myndigheter
- transport.

Urvalet av de representerade sektorerna vid NISÖ 2018 överensstämmer i stora drag med de prioriterade sektorer som EU beskriver i NIS-direktivet.

Följande aktörer deltog i NISÖ 2018
Affärsverket svenska kraftnät
CGI
Eon
Energimyndigheten
Evry
Försvarsmakten
Gävle hamn
Gävle kommun
Luftfartsverket
Länsstyrelsen i Gävleborgs län
Länsstyrelsen i Stockholms län
Länsstyrelsen i Västra Götalands län
Myndigheten för samhällsskydd och beredskap
Post- och telestyrelsen
SJ
Stockholms läns landsting
Säkerhetspolisen
Tele 2
Telia
Teracom
Tieto
Trafikverket
Transportstyrelsen
Uniper
Vattenfall

2.1.2 Projektorganisation

Projektet leddes av MSB:s utsedda projektledning och organiserades enligt beprövade principer för planering av samverkansövningar. Övningsplaneringen utgick från internationell standard för övningsplanering[6] och från MSB:s metodstöd. Projektets arbetsformer och dokumentation utgick ifrån den projektstyrningsmodell som MSB har valt.



Figur 1. *Planeringsorganisation NISÖ 2018*

Avsikten med detta sätt att utforma projektorganisationen var att skapa förutsättningar för att planera och förbereda övningens olika delar. Projektet bemannades främst av MSB-personal och av inhyrt expertstöd. När övningen väl var genomförd skalades projektorganisationen ned, och endast de delar som arbetade med utvärdering fanns kvar i projektet.

De deltagande aktörernas lokala övningsledare (LÖL) fungerade som referensgrupp i planeringsarbetet, vilket innebar att de vid planeringsmötena bidrog med kunskap och synpunkter inför genomförandet. De granskade också det material som skickades ut inför planeringsmötena. Vidare var de lokala övningsledarna en viktig resurs i skrivandet av inspel, där de bidrog med kunskap från respektive organisation.

6. Swedish standards institute (2013), *Samhällssäkerhet – Vägledning för övningar,* SS-ISO 22398:2013, IDT

2.1.3 Tidsplan

Den tidsplan som användes i projektet följde praxis vid planering av större övningar.

Datum	Händelse
11 maj 2016	Projektdirektivet beslutas
8 mars 2017	Startmöte
18–19 maj 2017	Planeringsmöte 1
30–31 augusti 2017	Planeringsmöte 2
4–5 oktober 2017	Skrivarstuga 1
8–9 november 2017	Skrivarstuga 2
22–23 november 2017	Planeringsmöte 3
23 januari 2018	Skrivarstuga 3
25 januari 2018	Genomförande av tekniktest
14–15 februari 2018	Genomförande av NISÖ 2018
20 mars 2018	Utvärderingsseminarium
24 maj 2018	Erfarenhetsseminarium
30 november 2018	Projektavslut

Tabell 1. *Tidsplan för NISÖ 2018, projektets gemensamma aktiviteter*

2.1.4 Övningsdokumentation

Inför övningen togs ett antal dokument fram, med syftet att beskriva

- hur planeringsprocessen skulle inriktas och genomföras
- hur olika delar av verksamheten under övningen skulle bedrivas
- hur utvärderingen skulle genomföras och vad den skulle fokusera på.

Dessa uppgifter återfinns i följande dokument:

- övningsbestämmelser för planeringsprocessen
- övningsbestämmelser för genomförandet
- logistikplan
- övningsledningsbestämmelser
- utvärderingsplan.[7]

7. Dessa dokument har, med undantag av logistikplan och övningsledningsbestämmelserna, beslutats av projektets styrgrupp. Övningsledningsbestämmelserna och logistikplanen är inga inriktande dokument och fastställdes därför av projektledaren.

Genomförande av NISÖ 2018

3. Genomförande av NISÖ 2018

3.1 Syfte och mål med övningen

NISÖ 2018 syftade till att stärka samhällets förmåga att hantera nationella it-relaterade kriser, främst genom att utveckla förmågan till samarbete och samordning mellan privata och offentliga aktörer inom utpekade sektorer.

Målet med NISÖ 2018 var att stärka samhällets förmåga att hantera större it-relaterade kriser, främst genom att utveckla förmågan till samverkan och samordning mellan privata och offentliga aktörer. Övningens mål baserades på fyra kärnprocesser:

- lägesbildsarbete
- inrapportering av konsekvensbedömningar vid it-incidenter
- hanterandebedömningar vid it-incidenter
- samordning av budskap till medier och allmänhet.

Följande aktörsgemensamma mål fastställdes för övningen:

1. **Skapa en lägesbild med fokus på händelse och konsekvenser** med egenhändigt insamlad information samt information ställd till förfogande av andra, och
   - bidra till samordning av lägesbildsarbetet genom att ställa skapad lägesbild till andras förfogande
   - vid behov ta emot andra aktörers lägesbilder för att skapa en samlad lägesbild.
2. **Ta beslut om hantering och planera åtgärder** utifrån egen lägesbild, andras lägesbilder samt samlade lägesbilder, och
   - dela information om hantering och planerade åtgärder till relevanta (det vill säga berörda och potentiellt berörda) aktörer.
3. **Utföra och vid behov samordna information och kommunikation gentemot allmänhet och medier**, om
   - händelsen och konsekvenserna
   - hanteringen.
4. **Pröva rådande**
   - rutiner för incidentrapportering
   - handlingsplaner
   - arbetssätt.

3.2 Övningens upplägg

NISÖ 2018 genomfördes under två dagar, den 14–15 februari 2018, på Ledningsregementet i Enköping (LedR). Samtliga deltagare, både motspelande och övande, fanns på plats på LedR.

Under övningen kom varje övande aktör att representeras av en kaderorganisation. Anledningen till att man övade i relativt små kaderorganisationer, det vill säga mindre grupper sammansatta av enstaka representanter från de funktioner som skulle ha agerat i liknande, verkliga situationer, är att övningen i första hand syftade till lärande och utveckling ur ett systemperspektiv – inte till att förbereda en faktisk krisledningsorganisation. Respektive organisation valde själv vilka funktioner som skulle vara med i övningen, utifrån de egna aktörsspecifika målen.

Följande avgränsningar gjordes för övningen:

- NISÖ 2018 beaktade endast aspekter som rör informations- och cybersäkerhet (logisk eller elektronisk säkerhet).
- NISÖ 2018 övade inte hanteringen av de fysiska konsekvenser som skapas av it-incidenter.

3.3 Metod och genomförande

NISÖ 2018 genomfördes som en simuleringsövning med motspel.

3.3.1 Simuleringsövning i verklighetsnära miljö

En simuleringsövning är en övning som prövar de deltagande aktörernas krishanteringsförmåga i enlighet med gällande regleringsbrev och principer, såväl enskilt som gemensamt.[8] Allmänt kan sägas att övningsformatet simuleringsövning med motspel i så stor utsträckning som möjligt sker i en miljö och med uppgifter som liknar verkligheten vid en kris. Vidare består en simuleringsövning med motspel av två huvuddelar: övande aktörer och ett aktivt motspel. En deltagande aktör kan dela upp sig så att delar av organisationen deltar i övandet, medan andra delar återfinns i motspelet.[9] De övande aktörerna får enbart kommunicera med varandra eller med motspelet.

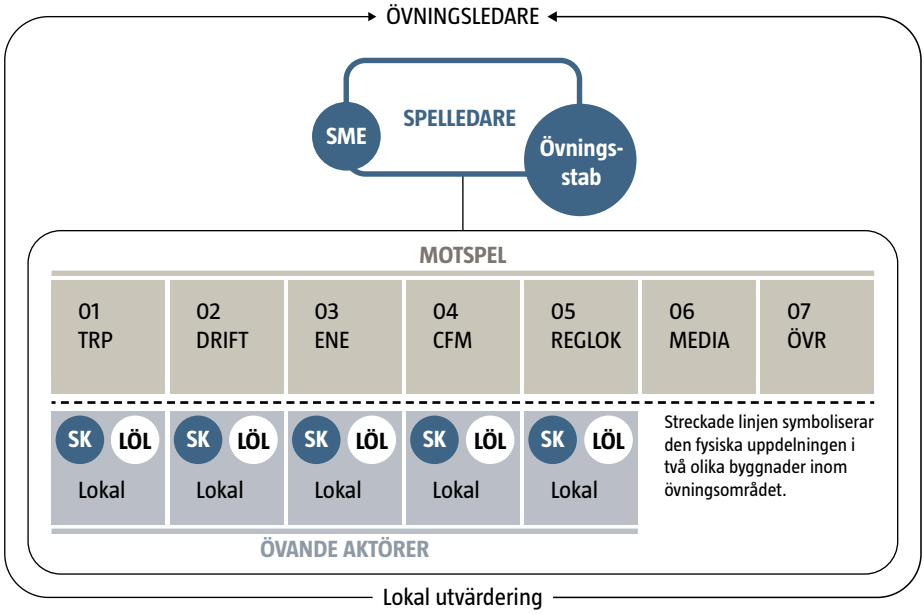
8. MSB (2013) Övningsvägledning: *Metodhäfte – Simuleringsövning med motspel*, MSB604
9. MSB (2016) Övningsvägledning: *Grundbok – Introduktion till och grunder i övningsplanering*, MSB602, s. 45

3.3.2 Genomförande – förutsättningar och spelorganisation

NISÖ 2018 genomfördes i en konstruerad miljö i LedR:s lokaler, och motspelet bestod av representanter från respektive aktör. Under övningen var övningsledningen och motspelet åtskilda från de övande aktörerna, som befann sig i en annan byggnad. Motspelet var uppdelat i olika moduler med en central spelledning i mitten. De övande aktörerna var placerade så att 2–3 aktörer delade rum, men de kunde fysiskt samverka med övriga övande i angränsande rum. Aktörerna tog med egna datorer för att kunna koppla upp sig mot Övningswebben (se nedan), eventuella egna krisledningssystem och mot spelstödssystemet för givare i motspelet. Sambandsverktyget *Webbaserat informationssystem* (WIS) simulerades med hjälp av en katalog på servern.

Utifrån ett övergripande scenario agerade de övande på händelser som spelades in, allt för att skapa förutsättningar som liknar en verklig krishändelse. För att kunna öva så verklighetsnära som möjligt användes också olika tekniska hjälpmedel.

Ett sådant hjälpmedel var Övningswebben, en portalsida som utgjorde de övandes internet. Där publicerades exempelvis en sambandskatalog och scenariots bakgrundshistoria. På Övningswebben fick de övande även tillgång till övningsmedier, såsom tidningar och sociala medier. Med hjälp av Övningswebben kunde de deltagande också publicera sina egna alster i sociala medier och kommunicera internt och externt under övningen. Under hela övningen fanns stabspersonal tillgänglig i två stabsexpeditioner, en hos de övande och en i anslutning till motspelet. Där fanns möjlighet till teknisk och logistisk support.



Figur 2. *Genomförandeorganisation NISÖ 2018 – Sakområdesexperter (SME), transportsektorn (TRP), driftleverantörer inom IT-sektorn (DRIFT), energisektorn (ENE), centrala förvaltningsmyndigheter (CFM), (REGLOK) regionala och lokala aktörer, media (MEDIA), övriga (ÖVR), spelkoordinatorer (SK), lokal övningsledare (LÖL).*

Alla funktioner som beskrivs i figuren förutom de övande tillhörde spelorganisationen (det vill säga spelledningen och motspelet).

Övningsledarens roll under övningen var främst att ansvara för övningens gemensamma inledning och avslutning, samt att avbryta övningen vid behov. Själva simuleringen leddes i stället av spelledaren, som ansvarade för motspelet. Till sin hjälp hade spelledaren en övningsstab, som bland annat bemannade stabsexpeditionerna och skötte tekniska system. Dessutom fanns ett antal sakområdesexperter (SME) till spelledarens hjälp för frågor om informationssäkerhet och kommunikation.

Givarna i motspelet bemannade sex olika moduler, indelade utifrån de berörda samhällssektorerna. Modulen MEDIA bemannades av inhyrda journalister som producerade artiklar i den fingerade Krispressen, tänkt att efterlikna en kvällstidning. De kom också med inspel och kommentarer i Övningswebbens simulerade sociala medier. Journalisterna genomförde även intervjuer med de övande.

I de övande aktörernas lokaler fanns fem spelkoordinatorer (SK), en för varje motspelsmodul förutom MEDIA. Spelkoordinatorerna fungerade som spelledarens ögon och öron hos de övande, tillsammans med en lokal övningsledare för respektive organisation. De lokala övningsledarnas roll under genomförandet var främst att

- hjälpa de övande aktörerna att installera sig och komma igång i lokalerna innan övningen började
- meddela motspelet hur de övande reagerade på inspelet under övningen, och om tempot behövde öka eller minska.

De lokala övningsledarna hade även i uppgift att samverka med spelkoordinatorerna och de lokala utvärderarna.

Utvärdering

4. Utvärdering

Försvarshögskolans *Centrum för totalförsvar och samhällets säkerhet* (CTSS) hade i uppdrag att stödja MSB i arbetet med att utvärdera övningens måluppfyllnad. CTSS uppdrag bestod i att vara sammanhållande för delprojektet Utvärdering, samt att vara utvärderingsledare under övningens genomförande. Uppdraget avslutades i maj 2018 när CTSS överlämnade en utvärderingsrapport till MSB. Resultatet från CTSS utvärdering har sedan legat till grund för de utvecklingsområden som MSB presenterar i denna rapport.

4.1 Utvärderingens syfte

Utvärderingen syftade till att ta vara på de erfarenheter och lärdomar som övningen genererade, och till att identifiera eventuella utvecklingsbehov. En bedömning om huruvida målen för övningen uppnåddes planerades till ett senare skede.

De erfarenheter som samlades upp under utvärderingen ligger till grund för ett långsiktigt arbete med att formulera och på sikt implementera åtgärdsplaner i de medverkande sektorerna. Utvärderingens syfte var alltså inte att formulera några utvecklingsplaner i sig, utan att ge en generell bild av vilka utvecklingsområden övningen aktualiserade. Utvärderingen syftade också till att ge tentativa rekommendationer om vad som skulle kunna vara i fokus för framtida förmågehöjande åtgärder.

Eftersom övningen inte var prövande syftade utvärderingens inte till att kvalitetsbedöma de analyser, bedömningar och beslut som producerades och rapporterades in under övningen. I stället låg tyngdpunkten på att bedöma samverkansförmågan, genom att studera de aspekter av samverkan som aktualiseras genom NIS-direktivet. Dessutom utvärderades samverkan mellan de myndigheter[10] som enligt NIS-direktivet är tillsynsansvariga.

10. Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket och Post- och telestyrelsen.

4.2 Utvärderingsprocessen

Materialet till den aktörsgemensamma utvärderingen av NISÖ 2018 samlades in via deltagande observation och enkäter som de övande aktörerna fick svara på.

Dessutom medverkade ett antal observatörer vid LedR i Enköping under övningen. Observatörerna ansvarade för att följa olika frågor och sektorer. Observationerna överlämnades sedan i rapportform till utvärderingsledaren. Vidare fick de övande svara på uppföljningsfrågor efter övningen, om vilka behov de upplevde att de hade haft och om de upplevde att den information som delades ut under övningen var användbar. Dessa frågor skickades som en enkät till de övande organisationerna i direkt anslutning till övningens avslut.

Resultatet av utvärderingen sammanställdes sedan i en utvärderingsrapport. Utvärderingsrapporten innehöll analyser av respektive mål, slutsatser samt identifierade lärdomar och utvecklingsbehov.

Arbetet med att ta vara på erfarenheterna från utvärderingen har skett i samverkan mellan MSB och de aktörer som deltog i NISÖ 2018. I mars 2018 hölls ett utvärderingsseminarium. Syftet med seminariet var att kvalitetssäkra och förankra utvärderingens slutsatser. I april 2018 skickades utvärderingsrapporten till MSB för kommentar och kvalitetssäkring. Resultaten justerades sedan utifrån slutsatserna från utvärderingsseminariet, och en justerad utvärderingsrapport överlämnades till MSB i april 2018. Därefter hölls ett erfarenhetsseminarium i maj 2018 med representanter från de övande aktörerna. Syftet med seminariet var att återföra erfarenheter aktörerna emellan.

Prioriterade utvecklingsområden

5. Prioriterade utvecklingsområden

CTSS identifierade nio aktörsgemensamma utvecklingsområden i sin utvärdering av NISÖ 2018:

- kunskapshöjning om olika samverkansforum
- säkra och robusta kommunikationer
- användning av traditionella kommunikationskanaler
- användning av traditionella informationsdelningsmetoder
- återrapportering och svar på inlämnat underlag
- kravställning och beställarkompetens (när det gäller information från andra aktörer)
- kunskap om lokala och regionala aktörers behov och förmågor
- kunskap om övriga aktörers informations- och kunskapsbehov
- överbryggande av glappet mellan privat och offentligt.

De första tre områdena uppmärksammades även i samband med utvärderingen av NISÖ 2012. Då identifierades också ett utvecklingsbehov relaterat till lägesbildsfrågor. Även i utvärderingen av NISÖ 2018 finns aspekter av lägesbild och informationsdelning med i ett antal av de ovanstående utvecklingsområdena.

MSB har fördelat om de identifierade områdena för att skapa sammanhängande åtgärder i utvecklingsarbetet och för att anpassa dem till det bredare utvecklingsarbete som pågår, bland annat efter samverkansövningen SAMÖ 2018.

MSB:s indelning av utvecklingsområdena ser ut på följande sätt:

- **Samverkan och systemförståelse**
  - *Utvecklingsområde 1:* Privat-offentlig samverkan under kriser
  - *Utvecklingsområde 2:* Kunskap om samverkansforum
  - *Utvecklingsområde 3:* Kunskap om lokala och regionala aktörers behov och förmågor
- **Informationsdelning och lägesbild**
  - *Utvecklingsområde 4:* Tillgång till robusta och säkra kommunikationer
  - *Utvecklingsområde 5:* Användning av traditionella kommunikationskanaler
  - *Utvecklingsområde 6:* Lägesinformation och lägesbild

Förutom de ovanstående utvecklingsområdena kommer MSB också att fortsätta arbetet med att utveckla en samordnad nationell förmåga att upptäcka, varna för, stödja vid och hantera it-relaterade incidenter och kriser. Ytterligare åtgärder kommer även att presenteras i en nationell handlingsplan för informations- och cybersäkerhet[11] (levereras 1 mars 2019). Utvecklingen av samhällets förmåga att hantera större it-relaterade kriser hänger också nära ihop med den generella utvecklingen av krisberedskapen och totalförsvaret. Ytterligare några utvecklingsområden kommer därför att presenteras i *Nationell risk- och förmågebedömning*.

5.1 Samverkan och systemförståelse

5.1.1 Privat-offentlig samverkan under kriser

Att stärka förmågan till samverkan mellan privata och offentliga aktörer har varit ett syfte även under tidigare övningar i övningsserien NISÖ. Anledningen till detta är att förmågan till samverkan är avgörande för att säkerställa att Sverige har en god krisberedskap. Utvärderingen av NISÖ 2018 visar att förmågan till samverkan mellan privat och offentlig sektor under it-relaterade kriser fortsatt behöver utvecklas.

Utvärderingen påvisar utmaningar som visserligen inte är nya, men som blir allt tydligare när fler och fler aktörer från en allt bredare skärning av samhället deltar i den här typen av övningar. NISÖ 2018 visade hur krisberedskapssystemet i huvudsak är uppbyggt mellan myndigheter. De privata aktörer som allt oftare äger de system och anläggningar som drabbas av, eller som behöver användas vid, en it-relaterad kris hamnar i skymundan i de strukturer som har konstruerats. Detta bidrar till de kunskapsluckor som har uppmärksammats i föregående avsnitt av den här rapporten. Den myndighetsorienterade strukturen skapar även brister i hur information som skulle vara av vikt vid samverkan i kris kan spridas, exempelvis för att skapa lägesbilder. Bristerna observerades hos såväl privata som offentliga aktörer under övningen. En annan observation som behöver bemötas i det framtida utvecklingsarbetet är att privat verksamhet ofta är transnationell med viktiga funktioner i andra länder än Sverige, vilket påverkar förutsättningarna för samverkan under en it-relaterad kris.

11. Regeringen till MSB (2018) *Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*, Ju2018/03737/SSK

UTVECKLINGSOMRÅDE 1

Den privat-offentliga samverkan behöver fortsatt stärkas, genom utveckling av naturliga ingångar till krisberedskapsstrukturerna och de tilltänkta rapporteringsvägarna.

De offentliga krisberedskapsstrukturerna och de sektorsöverskridande tjänster som privata aktörer tillhandahåller behöver harmoniseras i större omfattning. Förutsättningarna för samverkan kan även stärkas genom att de berörda aktörernas informationsdelningsprocesser formaliseras och förstärks.

MSB avser att fortsätta det löpande arbetet med att utveckla den privat-offentliga samverkan inom området, i enlighet med vad som beskrivs i svar på regeringsuppdrag om privat-offentlig samverkan på informations- och cybersäkerhetsområdet[12]. Ytterligare åtgärder kopplade till privat-offentlig samverkan kan även komma att ingå i den nationella handlingsplan som levereras 1 mars 2019. Arbetet med privat-offentlig samverkan är centralt även inom det utvecklingsarbete som sker inom totalförsvarsområdet.

5.1.2 Kunskap om samverkansforum

Samverkan är centralt i svensk krishantering, eftersom det inte finns någon aktör med krisledande ansvar. Alla aktörer som är berörda måste kunna samverka kring nödvändiga beslut och insatser vid en it-relaterad kris.

Samverkan i svensk krishantering utgår från *ansvarsprincipen*. Ansvarsprincipen innebär att den som bedriver den berörda samhällsverksamheten under normala förhållanden har motsvarande ansvar att upprätthålla verksamheten under krissituationer. I ansvarsprincipen ingår därmed att starta och bedriva samverkan. För att möjliggöra samverkan under kriser finns en rad samverkansforum och -nätverk i samhället.

Utvärderingen av NISÖ 2018 visade att det finns ett fortsatt behov av att öka de berörda aktörernas kunskap om vilka samverkansforum som finns och om forumens funktion. Kunskapen om olika samverkansforum bedöms vara alltför personberoende. Utöver de observationer som gjordes under 2012 års övning visar NISÖ 2018 även på att privata aktörer behöver känna till många av de forum som existerar på myndighetsnivå inom deras sakfrågeområden, även om de själva inte nödvändigtvis deltar i forumen.

12. MSB (2018) *Privat-offentlig samverkan på informations- och cybersäkerhetsområdet*, 2017-7117

UTVECKLINGSOMRÅDE 2

Kunskapen om olika samverkansforum behöver spridas till en större skara medarbetare hos de berörda aktörerna.

Det behöver finnas tydliga instruktioner för hur och i vilka former berörda aktörer ska samverka i olika forum. Samtidigt behöver alla som arbetar inom krisberedskapssystemet ha god kännedom om vilka samverkansforum som finns och vilken funktion de har.

MSB avser att fortsätta att sprida kunskap om de samverkansforum som finns inom området, som en del av myndighetens arbete med nationell samverkan kring informations- och cybersäkerhet (se även ovan om privat-offentlig samverkan). Detta arbete kommer även att kunna stärkas av den pågående utvecklingen av totalförsvaret.

5.1.3 Lokala och regionala aktörers behov och förmågor

Samspelet mellan nationell, regional och lokal nivå är avgörande vid en kris. Detta gäller även it-relaterade kriser. För första gången i övningsserien NISÖ deltog 2018 även regionala och lokala aktörer. Under övningen var det på just lokal och regional nivå som scenariohändelserna resulterade i den sorts samhällsstörningar som skapar det samverkansbehov som övningen fokuserade på. Det innebar även att det var på lokal och regional nivå det uppstod behov av att planera de mer praktiska aspekterna av krishantering, och att det lokalt och regionalt finns en god kunskap och förmåga att få till den hantering som behövdes. Centrala myndigheter behöver mer kunskap om lokala och regionala aktörers verksamhet i händelse av en it-relaterad kris.

UTVECKLINGSOMRÅDE 3

Centrala myndigheter behöver förbättra sina kunskaper om, och skapa rätt förväntningar på, lokala och regionala aktörer. Detta är ett grundkrav för att få till stånd en god förmåga att (åter)rapportera till och samverka med regionala aktörer.

MSB avser att fortsätta arbetet med att sprida kunskap om lokala och regionala aktörers behov och förmågor. Detta dels som en del av myndighetens breda arbete med informations- och cybersäkerhet, dels som en del av arbetet med att planera och genomföra totalförsvarsövningen TFÖ 2020.

5.2 Informationsdelning och lägesbild

5.2.1 Tillgången till säkra och robusta kommunikationer

Att berörda aktörer i samhället har tillgång till säkra och robusta kommunikationer är en förutsättning för god krishantering vid en allvarlig it-relaterad kris.

Arbetet med att utveckla och tillgängliggöra säkra och robusta kommunikationer fortgår, till exempel när det gäller signalskyddssystem. Utvärderingen visar att arbetet behöver intensifieras och få högre prioritet för att utveckla välfungerande, gemensamma kanaler och metoder för säker kommunikation mellan alla berörda aktörer vid en allvarlig it-relaterad kris. Behovet av skyddade kommunikationer och system identifierades redan under NISÖ 2012, men under NISÖ 2018 observerades mer specifikt behovet av att utveckla förmågan att dela information (exempelvis lägesbilder) på ett tillgängligt sätt i säkra och robusta system och kanaler. Säkra och robusta kommunikationer, som även stödjer förmågan att dela hemliga uppgifter, behövs för att förmedla information till andra berörda aktörer, inte bara till allmänheten.

UTVECKLINGSOMRÅDE 4
Förmågan att kommunicera säkert under it-relaterade kriser behöver stärkas.

System som Rakel och WIS är avsiktligt begränsade till de aktörer som är utpekade i lagar och förordningar. System behöver göras tillgängliga för ett större antal aktörer, såväl privata som offentliga. Systemen behöver även dimensioneras för delning av känslig och skyddsvärd information. Vidare behöver användningen av system som Rakel och WIS övas för att bli ett naturligt verktyg hos berörda aktörer. I dagsläget används systemen i olika omfattning i kommunerna. Ett sätt att förenkla användningen av Rakel under kriser är att uppmuntra kommunerna att använda systemet även i vardagen. Informationsinsatser, utbildningar och övningar i Rakel bör därmed hållas på kommunal nivå.

MSB avser att fortsätta arbetet med att öka tillgången till och kännedomen om säkra och robusta kommunikationer. I detta ligger även ett fortsatt utvecklingsarbete kopplat till Rakel, *Swedish Government Secure Intranet* (SGSI) och WIS. MSB kommer också att ge ut en vägledning om säker och robust samverkan under slutet av 2018, som ett steg i arbetet med att öka kännedomen om säkra och robusta kommunikationer.

5.2.2 Användning av traditionella kommunikationskanaler

Att under en kris kunna sprida information om vad som hänt och fortlöpande ge råd och rekommendationer till det övriga samhället är en central uppgift i krishanteringen för såväl privata som offentliga aktörer.

För att kunna hantera en omfattande it-relaterad kris behöver berörda aktörer ha god kunskap om olika typer av kommunikationsarbete. Kriskommunikation är viktigt och bör präglas av snabbhet, öppenhet och korrekthet.[13] Vidare kan kriskommunikationen i sig påverka själva händelsen.[14] Berörda aktörer behöver kunna kommunicera i digitala kommunikationskanaler, kommunicera via traditionella medier samt upprätta alternativa kommunikationskanaler vid behov.

Utvärderingen av NISÖ 2018 visar att det finns anledning att arbeta vidare med insatser för att säkerställa aktörers förmåga att kommunicera i såväl traditionella som alternativa kommunikationskanaler. I en informations- och cybersäkerhetsövning är det naturligt att de deltagande aktörerna har god insikt och stor vana i att använda digitala kommunikationskanaler. Under NISÖ 2018 visade sig detta genom ett skevt fokus på kriskommunikation i digitala kommunikationskanaler hellre än via mediekontakter och lokala kommunikationsinsatser. Under en större it-relaterad kris är det högst troligt att just de digitala kanalerna inte kommer att fungera fullt ut, vilket gör bred kompetens på kommunikationsområdet till en förutsättning för framgångsrik krishantering. Det är ett viktigt argument för att stärka kommunikationskompetensen hos de berörda aktörerna.

UTVECKLINGSOMRÅDE 5

Berörda aktörer behöver utveckla kunskap och skicklighet i att använda traditionella och alternativa kommunikationskanaler.

Berörda aktörer behöver också höja kunskapen om vilken roll public service har inom krisberedskapen och för att begära Viktigt meddelande till allmänheten (VMA) eller myndighetsmeddelande. Detta är avgörande för att stärka förmågan hos berörda aktörer att kommunicera med allmänheten och andra aktörer under en allvarlig it-relaterad kris.

13. MSB (2014), *Gemensamma grunder för samverkan och ledning vid samhällsstörningar,* MSB777, s.71–73
14. *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*, s.71–73

MSB avser att fortsätta utveckla det nationella arbetet med att förmedla information under allvarliga samhällsstörningar. Det är ett utvecklingsarbete som har bäring både på utvecklingen av krisberedskapen och av totalförsvaret, exempelvis genom totalförsvarsövningen TFÖ 2020.

Vidare fortsätter MSB arbetet med att stötta medieföretagens beredskapsplanering och samverkan, bland annat genom mediernas beredskapsråd. I detta arbete ingår en nära samverkan med public service-bolagen Sveriges Radio och Sveriges Television. MSB är även den myndighet som ansvarar för varningssystemet VMA och utvecklingen av det. Det pågår löpande arbete med att hitta nya metoder och tekniker som kan komplettera dagens VMA-system.

5.2.3 Lägesinformation och lägesbild

Informationsdelning och lägesbild är centrala komponenter i svensk krishantering. Tillgången till en samlad (gemensam) lägesbild är en förutsättning för att hantera alla typer av kriser, även it-relaterade sådana. Vid en kris är det mycket viktigt att snabbt kunna kartlägga och presentera krisens händelseförlopp. När det gäller it-relaterade incidenter och kriser kan det även behövas lägesbilder som fokuserar på informations- och cybersäkerhetsaspekterna av krisen, utöver den bredare, nationella lägesbilden.

Trots att de centrala myndigheterna under NISÖ 2018 lyckades tillgängliggöra den insamlade informationen och sammanställa lägesbild i enlighet med rådande lagstiftning[15] upplevde de övriga aktörerna att informationsdelningsprocessen var ensidig. Den information som de centrala myndigheterna förmedlade plockades inte heller alltid upp av de aktörer som var berörda av informationen. Dagens system för att distribuera lägesbilder till berörda aktörer förutsätter att aktörerna har kännedom om, tillgång till och möjlighet att bevaka och delta i de forum där informationen publiceras. De måste också kunna använda sig av de delningsytor som används. Därför behövs mer kunskap och eventuellt också nya tillvägagångssätt i det framtida lägesbildsarbetet. Vidare behövs ett tydligare kommunicerat syfte med den formulerade lägesbilden: vad den förväntas innehålla och vilken målgrupp som ska ta del av den.

15. I *Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap* (2015:1052) ställs krav på inrapportering av olika aspekter av incidenthantering till centrala myndigheter, men inte på hur informationen ska delas ”nedåt” i systemet. Detta upplägg återfinns även där fokus ligger på att rapportera in till bevakningsansvariga myndigheter och sedan vidare till MSB och Regeringskansliet.

Beställarkompetens och förmågan till kravställning när det gäller lägesinformation är avgörande för att aktörer under tidspress ska kunna skapa sig en korrekt lägesbild och fatta övervägda beslut under en kris. NISÖ 2018 visade en oförmåga hos aktörerna att ställa krav på eller explicit beställa specifik information från övriga aktörer.

CTSS utvärdering visade att rådande förvaltningsprinciper, en konsensuskultur och ansvarsfördelningen gjorde det problematiskt för de övande aktörerna att uttrycka missnöje med den information som delades och med de arbetssätt som användes inom ramen för övningen. I stället för att efterfråga rätt material och snabbare svar löste aktörerna de upplevda problemen med tidskritisk information på egen hand. Detta förhållningsätt hos aktörerna visar på en lösningsinriktad attityd vilket är positivt, men det visar även på brister när det gäller kravställning och beställarkompetens.

UTVECKLINGSOMRÅDE 6

Lägesbildarbetet i samhället behöver fortsatt utvecklas för att berörda aktörer ska uppleva att centrala myndigheter i tillräcklig utsträckning kommunicerar med dem utifrån deras behov.

Utvecklingsarbete behövs med avseende på såväl arbetsprocessen och lägesbilden som produkt som på verktygen för att presentera lägesbilden. Utvecklingsområdet omfattar såväl den offentliga sektorn som privata företag. Privata aktörer kan även behöva en större tydlighet när det gäller vad de kan förvänta sig från centrala myndigheter, samt när det gäller vilken information de ska leverera till nationella myndigheter. Aktörernas arbetsprocesser för att kravställa tidskritisk information behöver också utvecklas. För att skapa förmågan att under tidspress identifiera egna och andras behov av information under en it-relaterad kris behövs ökad kunskap, samt ett utvecklingsarbete som rör roller och funktioner. Det är viktigt att utveckla den ömsesidiga förståelsen mellan berörda aktörer, så att de lättare kan avgöra vilken information och kunskap som är relevant i respektive organisations besluts- och hanteringsprocesser.

MSB avser att fortsätta utveckla arbetet med informations- och cybersäkerhetsrelaterade lägesbilder. Detta är en del av den fortsatta utvecklingen av förmågan att hantera större it-relaterade kriser. När det gäller det generella utvecklingsarbetet kring informationsdelning och samlade lägesbilder fortsätter MSB att erbjuda utbild-

ningar inom ramen för implementeringen av *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*.[16] Även den incidentrapportering som sker från statliga myndigheter och som en del av NIS-regleringen bidrar till att utveckla det löpande utbytet av lägesinformation i samhället.

16. Exempelvis ges kursen "Informationsdelning och samlade lägesbilder – gemensamma grunder för samverkan och ledning" under 2019.

Slutsatser

6. Slutsatser från planering, genomförande och utvärdering av NISÖ 2018

Det här avsnittet presenterar de övergripande slutsatserna och lärdomarna från planeringen, genomförandet och utvärderingen av NISÖ 2018. Slutsatserna bygger på processutvärderingens utfall och de samtal som fördes under erfarenhetsseminariet i maj 2018. Nedan har projektet NISÖ 2018 sammanställt tre kategorier av erfarenheter som bör beaktas vid planeringen av framtida övningar inom informationssäkerhetsområdet.

6.1 Behov av tydlig kommunikation med deltagande aktörer

Den planeringsmetod som användes vid NISÖ 2018 bygger på samarbete mellan alla berörda parter under förhållandevis lång tid. Projektet för övningen behöver kommunicera tydligt med de aktörer som deltar, så att det finns en gemensam vision för hur planeringen bör fortskrida och för vilket arbete de deltagande aktörerna behöver utföra på egen hand. Till exempel behöver projektet kommunicera hur de deltagande aktörerna bör planera sin respektive kompetensförsörjning för att kunna delta i övningsplaneringen på ett givande sätt. Det krävs också löpande kommunikationsaktiviteter för att hålla de deltagande aktörerna uppdaterade och inte minst fortsatt engagerade. Exempel på sådana kommunikationsaktiviteter är utskick om arbetsläget och deadlines.

Vidare är det viktigt att redan tidigt i arbetet skapa rimliga förväntningar på hur mycket tid som krävs för att det ska vara givande att delta i NISÖ. Det efterfrågas också kunskapshöjande kommunikationsåtgärder som kan fungera som förlagor och goda exempel på lösningar i det praktiska arbetet med övningen, exempelvis hur ett ”bra” inspel ser ut. Dessutom behöver den information som projektet kommunicerar göras pedagogisk, så att det är enkelt för de deltagande aktörerna att ta till sig informationen.

6.2 Deltagande aktörers ambitionsnivå, engagemang och kunskapsläge

De deltagande aktörerna behöver ta ansvar för den egna processens kontinuitet genom att närvara under hela planeringsförloppet, och genom att utföra sin del av arbetet mellan planeringskonferenser och skrivarstugor. Eftersom NISÖ är tänkt att identifiera glapp i förmågan på systemnivå är det avgörande att de aktörer som deltar har höga ambitioner och är villiga att öva både för egen skull och för att bidra till de gemensamma målen. Det är också viktigt att aktörerna har grundläggande kunskap om krisberedskapssystemet, om varandra, om övningsformen och om övningsmetoden.

6.3 Övningsdesign

6.3.1 Metod

NISÖ 2018 var en renodlad simuleringsövning på samlad övningsplats, medan NISÖ 2012 genomfördes som en kombinerad seminarie- och simuleringsövning. Det kan konstateras att vilket övningsupplägg som än väljs går fördelarna med det andra upplägget delvis förlorade. Inför framtida övningar bör det föras en bred diskussion mellan alla intressenter som är engagerade i övningen om de för- och nackdelar som finns med olika typer av övningsupplägg. Dessutom bör aktörernas behov i relation till formatet för övningen diskuteras. Detta gäller såväl valet av övningsmetod som övningens praktiska förutsättningar, till exempel att övningen är samlokaliserad.

6.3.2 Utformning

Inför framtida övningar behövs en reflektion kring vilken utformning som är den bästa för övningar i it- och informationssäkerhet. När det gäller processen att utforma scenariot för en storskalig simuleringsövning med många deltagande aktörer är det också viktigt att ta hänsyn till hur aktörerna utvecklar sina inspel. Vid framtida övningar bör de som ansvarar för det övergripande scenariot redan i ett tidigt skede säkerställa att aktörerna samverkar i inspelsarbetet för att undvika missförstånd och onödiga omarbetningar.

Det är även positivt om övningar som samlar många berörda och viktiga aktörer skapar utrymme för att nätverka vid sidan av det scenariobaserade övandet. Det krävs sannolikt mer än två övningsdygn om övningen ska bli tillräckligt lång för att skapa förutsättningar för samverkan, och dessutom lämna tillräckligt med spelfri tid för att de övande ska kunna mötas på ett förtjänstfullt sätt.

6.3.3 Kompetensförsörjning under övningen

Två huvudsakliga erfarenheter kopplade till kompetensförsörjning under övningen och övningens upplägg bör uppmärksammas.

Den första lärdomen är att scenariots utveckling bör beslutas med mandatet hos den personal som skall medverka vid övningen i åtanke. Personalen som övas måste ha de mandat till vardags, i sina organisationer, för att fatta de beslut som krävs för att driva övningens fiktiva scenario framåt. Om aktörerna ska kunna öva lämpliga funktioner och förmågor är det också viktigt att de deltagande aktörerna utser personal på ett sätt som gör det möjligt att nå de aktörsgemensamma målen.

För att övningen ska bli så verklighetstrogen som möjligt bör det ställas tydliga krav på vilka aktörer som behöver delta, och vilka funktioner i scenariospelet aktörerna behöver delta i. Krishanteringssystemet är komplext och består av en rad inbyggda beroendeförhållanden mellan de samhällsviktiga aktörerna. Av naturliga skäl kan inte alla aktörer alltid vara representerade vid själva övningstillfället. Därför är det viktigt att i designen av framtida övningar kartlägga vilka beroendeförhållanden som kan komma att aktualiseras i skarpt läge. Analysen av dessa beroendeförhållanden bör sedan ligga till grund för planeringen av kompetensförsörjning och scenariospelets utformning. Detta innebär inte att övningar inte kan genomföras utan dessa aktörers deltagande, utan snarare att denna aspekt måste hanteras i ett tidigt skede av framtida projekt.

BILAGA 1
Målpreciseringar
NISÖ 2018

Bilaga 1: Målpreciseringar NISÖ 2018

MÅL 1

De övande ska skapa en lägesbild med fokus på händelse och konsekvenser ...

... med egenhändigt insamlad information och information ställd till förfogande av andra ...

... bidra till samordning av lägesbildsarbetet genom att ställa skapad lägesbild till andras förfogande ...

... och vid behov ta emot andras lägesbilder för att skapa en samlad lägesbild.

Detta mål svarar mot NIS-direktivets kapitel II, artikel 10 samt kapitel IV, artikel 14. Observationer som gäller detta mål fokuserar på processerna för upptäckt, verifiering och bevakning av större mönster i händelse av it-incidenter:

- Om och hur deltagande aktörer upptäcker en it-incident
- Om, hur och när deltagande aktörer utbyter information med varandra vid upptäckt av en it-incident
- Om och hur deltagande aktörer verifierar it-incidenter och om de arbetar gemensamt för att skapa en samlad lägesbild
- Om och hur deltagande aktörer arbetar gemensamt för att uppdatera och upprätthålla en samlad lägesbild.

MÅL 2

Deltagande aktörer tar beslut om hantering och planerar åtgärder ...

... utifrån egen, andras och samlade lägesbilder ...

... och delar information om hantering och planerade åtgärder till relevanta (berörda samt potentiellt berörda) aktörer.

Detta mål svarar mot NIS-direktivets kapitel IV, artikel 14 samt kapitel V, artikel 16. Observationer som gäller detta mål fokuserar på processer och metoder för larmning och rapportering av it-incidenter och på de konsekvens- och hanterandebedömningar som bör genomföras när en incident har identifierats:

- Om, när och hur deltagande aktörer analyserar och beskriver konsekvenser, planerade åtgärder och resursbehov, samt om informationen delas med andra organisationer
- Om, hur, när och med vilka deltagande aktörer utbyter information om identifierade problem och behov.

MÅL 3

Deltagande aktörer utför och samordnar vid behov information och kommunikation gentemot allmänhet och medier ...

... om händelse och konsekvenser ...

... om hantering.

Detta mål svarar mot NIS-direktivets kapitel II, artikel 10 samt kapitel IV, artikel 14. Observationer som gäller detta mål fokuserar på processer och metoder för hur de deltagande aktörerna samverkar och samordnar sin information till allmänhet, medier och andra organisationer som finns representerade i övningen, antingen som övande eller som en del av motspelet:

- Om, när och hur kommunikationsarbetet med anledning av it-incidenten inleds
- Vad är fokus för kommunikationsarbetet i de olika faserna (upptäckt, verifiering, hantering) – intern inriktad på egen organisation, inriktad på allmänheten, på medier, eller på andra organisationer?
- Om, hur, när och med vilka de deltagande aktörernas informationsansvariga utbyter information
- Om, hur, när och med vilka de deltagande aktörernas informationsansvariga samarbetar för att samordna sin information till allmänhet och medier.

MÅL 4

De övande har genomfört sitt arbete utifrån rådande ...

... rutiner ...

... arbetssätt ...

... och handlingsplaner.

Detta mål fångar främst upp de övande aktörernas egna behov och önskemål på övningen, och täcks därmed in av de aktörsspecifika målen och organisationernas lokala utvärderingar. De aktörsspecifika målen kan ha flera andra fokusområden och är inte en del av den här utvärderingen.

Samtliga mål svarar även mot NIS-direktivets kapitel III, artikel 11, som rör samverkan vid it-relaterad krishantering. Eftersom samverkan är ett medel snarare än ett mål är samverkan mer en grund för hur observationspunkterna formuleras än något som utvärderas i sig.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1326 - december 2018 ISBN 978-91-7383-900-6