



Nasjonal  
kommunikasjons-  
myndighet

# EkomROS 2016

**Torstein Olsen**  
**direktør**

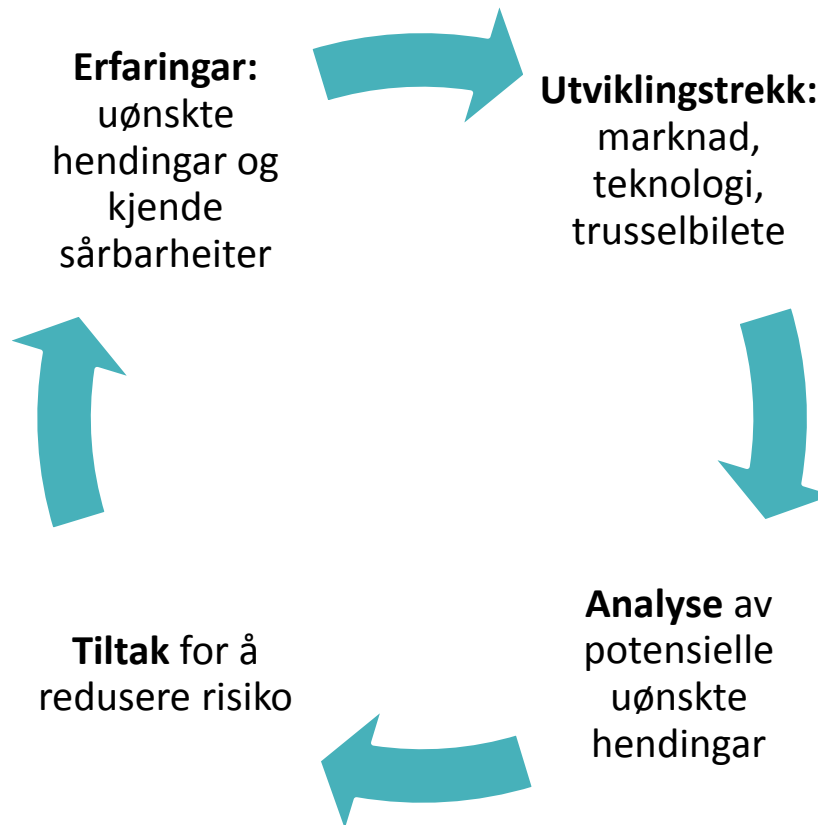
Overlevering av rapport til Samferdselsdepartementet 28. april 2016

# Risiko og sårbarheit i ekomsektoren



- Arbeide systematisk, målretta og sporbart med samfunnssikkerheit
- Oversikt over risiko og sårbarheit innan eget ansvarsområde
- Sett i verk førebyggjande tiltak og beredskapstiltak på bakgrunn av eit godt utgreia kunnskapsgrunnlag

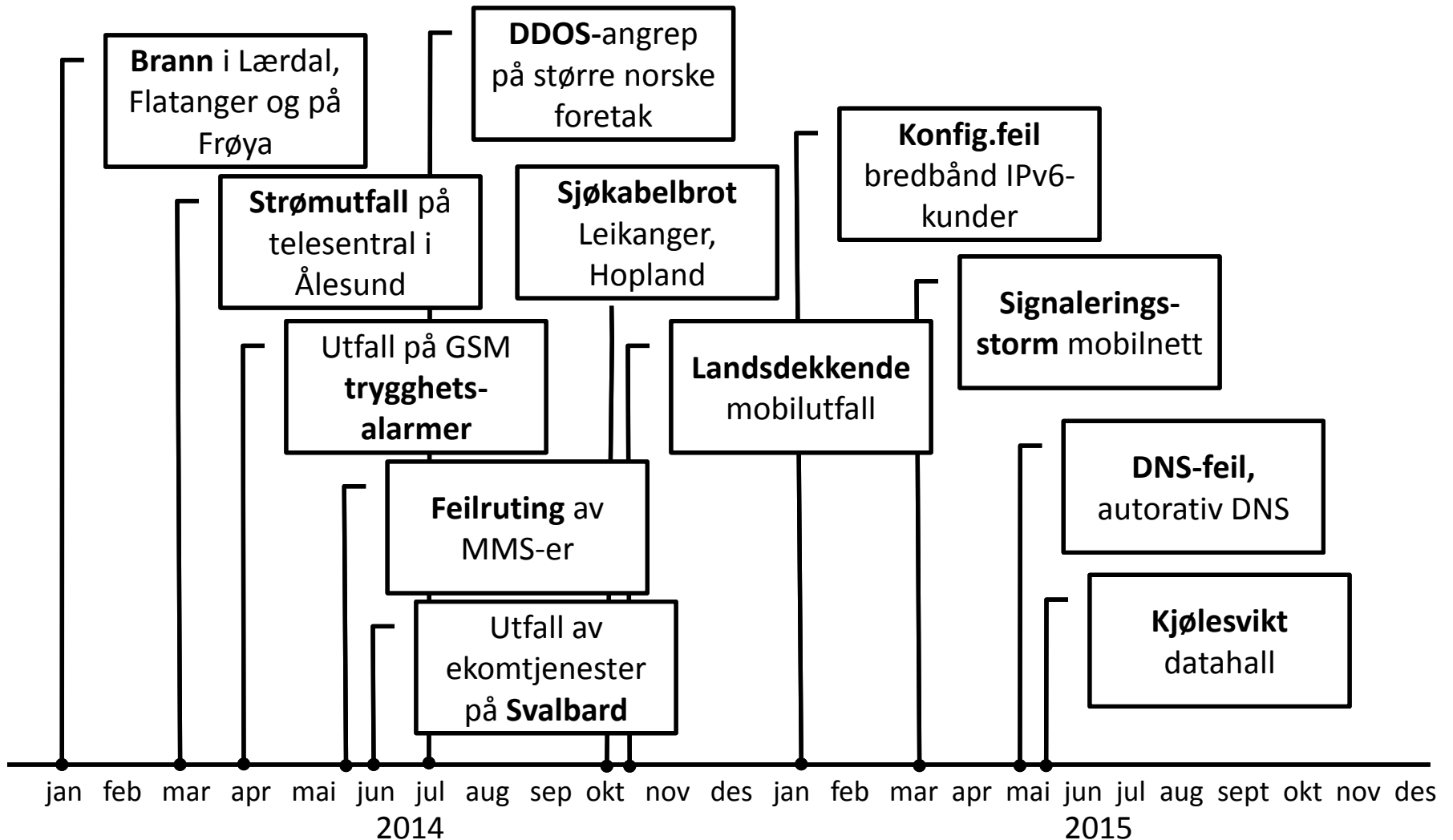
# EkomROS: Overordna risikoanalyse av sektoren



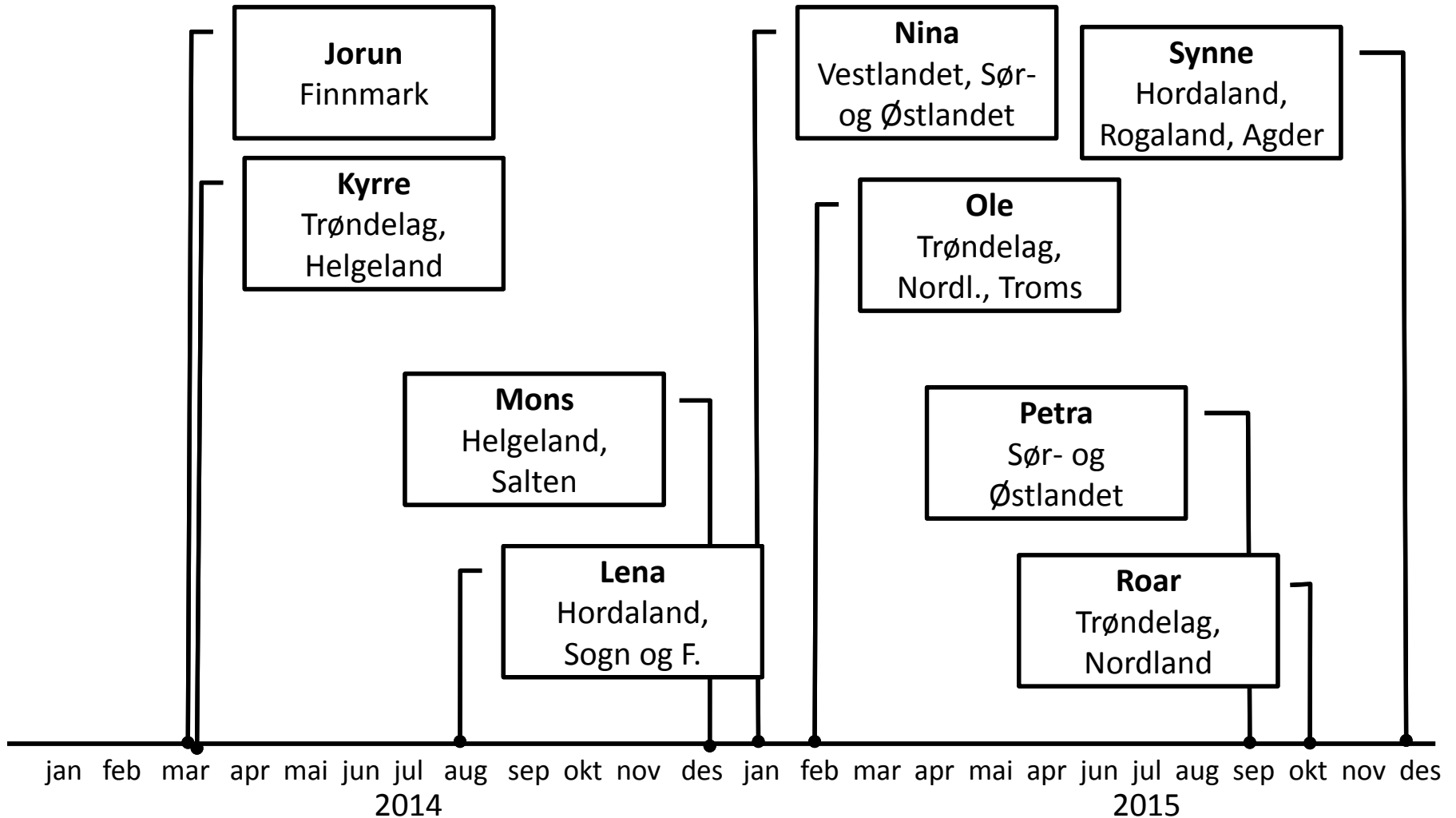
The background features two large, smooth, curved lines. One is a thin blue line that starts high on the left and curves down towards the bottom center. The other is a thicker orange line that starts lower on the left, peaks in the upper left quadrant, and then curves down towards the bottom right.

## 2014 og 2015

# 2014 og 2015 – utvalg av hendinger i Noreg



# 2014 og 2015 – ekstremvêr



# 2014 og 2015 – «bugged, tracked, hacked»

**PÅ SPORET AV DN.** Den tyske hackeren Karsten Nohl kaster følge DNS bevegelse i Oslo med utgangspunkt i mobilnummeret. DN testet ut overvågningsmetoden som nå selges kommersielt, i en månad.

**Magasinet Teknologi**  
**Sirklet inn fra utlandet**  
 Nå kan hackere finne ut eksakt hvor du er til enhver tid, fra et hvilket som helst sted i verden, bare ved å kjenne mobilnummeret. Og du kan ikke gjøre noe med det. DN testet ut den nye overvåkningsmetoden – som allerede er til salgs

**BILLIG MIDDAG HVER DAG**

**Gemalto: – NSA klarte ikke å stjele SIM-nøklene**

Gemalto ble trolig hacket i 2010 og 2011 av NSA og britiske Government Communications Headquarters (GCHQ), men følge sikkerhet kaste ikke de to satsige sikkerhetsorganisasjonene å hente ut verdifulle informasjon. (B. Simon Yeo/Flickr)

Av Trend Bli, 25. januar 2015 kl 08:59  
 Hverder at de usansett ikke kan spionere på 3G og 4G-nett.

**SIKKERHETSHULL:** Det er avdekket sikkerhetshull i det svenske og danske telenettet til Telesnor og Tello.

**Lekker ditt mobilnummer når du surfer**

## Stortinget og statsministeren OVERVÅKES

Utenfor Stortinget, regjeringskontorene og boligen til statsminister Erna Solberg befinner det seg avansert spionutstyr som kan overvåke alle mobiltelefoner i området. Spørsmålet er: Hvem står bak?

The background features two overlapping sine waves. A blue wave starts at a high point on the left, descends to a low point in the middle, and then rises. An orange wave starts at a low point on the left, rises to a high point in the middle, and then descends. The text '2016-2020?' is positioned in the middle-right area of the slide, between the two waves.

**2016-2020?**



# Viktige utviklingstrekk (1)

## Teknologi

- Felles IP-basert sambandsinfrastruktur
- VoLTE
- Network function virtualization
- Over-the-top (OTT) tenester

## Organisasjon

- Utkontraktering
- Internasjonalisering
- Managed services



# Viktige utviklingstrekk (2)

## Brukarane

- Mobile tenester
- Samfunnskritiske brukarar
- Internet of Things



Telenor har nådd «tingenes Internett»-milepæl  
Norge ligger langt fremme når det gjelder nettikoblede enheter, ifølge telegartneren.



Til tross for en pris på 6 milliarder er ikke det digitale nødnettet bygget for normal datatrafikk. Nå skal de vanlige mobilnettene tas i bruk.



### Meld. St. 27 (2015–2016) Melding til Stortinget

Digital agenda for Norge  
IKT for en enklere hverdag og økt produktivitet

#### Regjeringen vil:

- At ekommyndigheten, sammen med berørte departementer, skal legge til rette for gode kommunikasjonsløsninger for nød- og beredskapsstatene.
- Arbeide for at de offentlige ekomnettene i størst mulig grad skal kunne bære framtidige tjenester for nød- og beredskapsstatene.



FREMTIDENS KOMMUNIKASJON I DET NORSKE FORSVARET  
**Forsvaret vil bli mobiloperatør. Militært samband på nettene til Telenor, Netcom og Ice**  
Derfor frister 4G/LTE langt mer enn det sterkt kritiserte Nødnettet.

The background features two wavy lines: a thin blue line and a thicker orange line, both curving across the page.

# Analysen

# Datagrunnlag

.....

Resultat frå tilsyn

Nkoms utgreiingar om falske basestasjonar, SS7, nasjonal autonomi,...

Nordisk NIS-samarbeidet



Trusselvurderingar  
NSM, PST, E-tenesten

Nkoms topologi-  
kartlegging

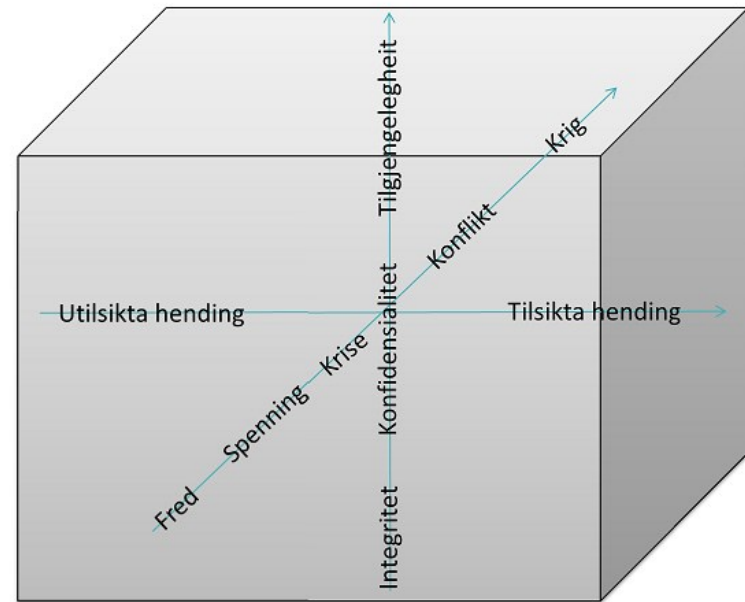
Nasjonalt  
risikobilde, DSB

ENISA  
trendrapportar

Hendingsrapportar,  
ENISA, NSM,  
ekomtilbydarane

# Metodisk tilnærming

- Definere mulegheitsrommet
- Grovanalyse (identifisere risikoområder)
- Analyse av potensielle uønskete hendingar
- Identifisere tiltak



# Grovanalyse: Identifiserte risikoområde



**Den nasjonal sambandsinfrastrukturen og sentraliseringa av tenesteproduksjon** fører til at enkeltfeil kan få store konsekvensar



**Kompleks verdikjede og omfattande utstyrsportefølje** gjer det vanskeleg å kjenne heile sårbarheitsbiletet, aukar avhengiga til leverandørane



**Utkontraktering og internasjonalisering** utfordrar kompetanse, ansvar, læring, og kontroll på nye måtar

# Risiko for potensielle uønskede hendinger

ID	Uønsket hendelse	Risiko	Usikkerhet
H2	Konfigurasjonsfeil i landsdekkende IP-nett	Moderat/høy	Høy
H3	Utpressing av nøkkelressurs – sabotasje transportnett	Moderat/høy	Høy
H8	Utpressingsforsøk mot ISP - skadevare	Moderat/høy	Høy
H12	Kartlegging av norsk kritisk infrastruktur	Moderat/høy	Høy
H1	Multippel transmisjonsfeil i transportnett	Moderat	Høy
H4	Fiberbrudd Svalbard og Finnmark	Moderat	Moderat
H5	Strømsvikt på kritiske anlegg i Oslo	Moderat	Moderat
H6	Signaleringsstorm i landsdekkende mobilnett	Moderat	Lav
H7	Sikkerhetshull i VoLTE	Moderat	Høy
H13	Ressursproblemer - entreprenør	Moderat	Høy
H14	Ressursproblemer - leverandør	Moderat	Moderat
H15	Overvåkning via nett i utlandet	Moderat	Høy
H9	DNS-angrep	Lav/moderat	Lav
H10	Kompromittering av sertifikatutsteder	Lav/moderat	Lav
H11	Bortfall av GPS	Lav/moderat	Lav

# Høgst risiko: Kartlegging av/etterretning mot kritisk ekinfrastruktur (H12)

## Mål

- Kartlegging av/etterretning mot kritisk personell
- Kartlegging av/etterretning mot kritisk ekinfrastruktur

## Dette bidrar til risikoen

- Kritisk infrastruktur: høgverdig mål for utlandsk etterretning
- Aktører har evne og vilje til (avansert) kartlegging
- Vanskeleg å oppdage, m.a. p.g.a. utkontraktering og internasjonalisering
- Vanskeleg å oppdage; får lett mindre merksemd
- Kan utnyttast til å «lamme» samfunnet i ein konflikt-/krigssituasjon






# Høgst risiko: Logiske feil i transportnett og kjernenett (H2, H3, H8)

## Dette kan utløyse feilen

- Utsikta hending (konfigurasjonsfeil, programvarefeil etc.)
- Tilsikta hending (utpressing, sabotasje, etc.)

## Dette bidrar til risikoen

- Systemkompleksitet skjuler logiske sårbarheter
- Logiske feil går «på tvers» av den fysiske redundansen
- Kan løysast ut av ein enkelt programvarefeil, eller enkeltperson
- Avhengig av mange ressursar (interne/eksterne) for feilsøking
- Berar av store samfunnsverdiar



The image shows a screenshot of a webpage from digi.no. At the top, there is a navigation bar with the site name 'digi.no' and a search bar. Below this is a large advertisement for a Microsoft Surface Pro 4, featuring the text 'INNOVASJON.' and a price tag of '11 499,-'. The ad includes an image of the device and a 'Dustin' logo. Below the advertisement is a news article with a photo of a woman and the headline 'SS7 SIGNALERING Forsøkte å kartlegge Telenor for sårbarheter, så knelte mobilnettet'. The article text is partially visible, mentioning 'Et internasjonalt sikkerhetselskap var kilden. Telenor nekter å si hvem...'.

The background features two large, smooth, wavy lines. One is a thin blue line that starts high on the left and curves down to a minimum before rising again. The other is a thicker orange line that starts lower on the left, peaks, and then curves down to a minimum before rising again. The word 'Tiltak' is centered between these two curves.

# Tiltak

# Risikoreduserende tiltak

	Tiltak	Risikoreduserende effekt														
		H 2	H 3	H 8	H 12	H 1	H 4	H 5	H 6	H 7	H 9	H 14	H 15	H 10	H 11	H 13
T1	Redundans og swapping					X	X									X
T2	Risikovurderinger og tiltak - planlagt arbeid i nett	X				X			X							X
T3	Utveksling av trusselbilde		X	X	X		X			X	X		X	X		
T4	Awareness - etterretning				X		X						X			
T5	Vedlikehold av reservestrom							X								
T6	Risikovurderinger og tiltak – teknologiske/ organisatoriske endringer								X	X						
T7	Sikringstiltak mot logiske sårbarheter og skadevare	X	X	X	X				X	X	X		X	X		
T8	DNSSEC og BCP										X					
T9	Implementering av forordning (EU) 910/2014													X		
T10	Øke operativ krisehåndteringsevne	X	X	X		X	X	X	X		X	X		X	X	X
T11	Risikovurderinger og tiltak – avhengighet til underleverandører											X	X			X
T12	Videreutvikle regelverk – utkontraktering/ internasjonalisering											X	X			X

Tabell 5. Forslag til tiltak sammen med en angivelse av hvilke hendelser tiltakene har risikoreduserende effekt på.

# Tiltak med brei risikoreduserande effekt

## Utveksling av trusselbilette

- Informasjonsutveksling i Ekomsikkerhetsforum (sikkerhetsmyndighetene, Nkom, tilbydarane)
- Informasjonsutveksling mellom NorCERT, NkomCSIRT og tilbydarane sine CERT/sikkerhetsmiljø

## Sikringstiltak mot logiske sårbarheiter og skadevare

- Autorisasjon og logisk tilgangskontroll
- Logging og sporing

## Auka operativ krisehandteringsevne

- Vidareutvikle den proaktiv beredskapen hos tilbydarane og myndighetene
- Samhandlingsløysingar for krisehandtering
- Myndigheitsfinansiert beredskapsutstyr

# Tiltak for å styrke tilbyderane sine egne risikovurderingar

## Planlagt arbeid i nett

- Dokumenterte prosessar for risikovurderingar før planlagt arbeid i nett
- Sette i verk tilpassa skadeførebyggande tiltak
- Kontroll, verifikasjon og beredskap

## Teknologiske og organisatoriske endringar

- Identifisere *nye* sårbarheiter som vil følgje av endringane
- Sette i verk proaktive risikoreduserande tiltak (jf. krav i ekomregelverket)

## Avhenge av underleverandørar

- Identifisere sårbarheiter knytt til avhengiga til underleverandørar (leverandørar, entreprenørar,...)
- Sette i verk risikoreduserande tiltak; førebyggande tiltak og beredskapstiltak

# Tiltak retta mot den fysiske infrastrukturen

## Halde fram arbeidet med bevisstgjerung om etterretningstrusselen i organisasjonane

- Opne kjelder, publisering på nett, konferansar, sosiale medier,...
- Underleverandørar, konsulentar, etc.
- Informasjonssikkerheit/objektsikkerheit/personellsikkerheit

## Redundans i transport- og regionalnett

- Auka diversitet i transportnett (jf. også ekomplanen)
- Styrking av redundans i regionalnett, m.a. gjennom «Forsterket ekom»-programmet.



### Meld. St. 27 (2015–2016) Melding til Stortinget

Digital agenda for Norge  
IKT for en enklere hverdag og økt produktivitet

*Regjeringen vil:*

- At ekommyndigheten skal vurdere virkemidler som legger til rette for etablering av landsdekkende og reelle alternativer for transportnettjenester for å styrke den nasjonale ekominfrastrukturen.
- At ekommyndigheten skal utrede hvordan de ulike landsdekkende nettene på best mulig måte kan utnyttes til å styrke robustheten i den totale nasjonale ekominfrastrukturen.

The background features two large, smooth, wavy lines. One is a thin blue line that starts high on the left and curves down towards the bottom center. The other is a thicker orange line that starts lower on the left, peaks in the upper left quadrant, and then curves down towards the bottom right.

**Takk for  
merksemda**