
GlobalConnect

Vi gjør for lite for å sikre oss mot cybertrusler

Per Morten Torvildsen

EVP NetCo, GlobalConnect

GlobalConnect

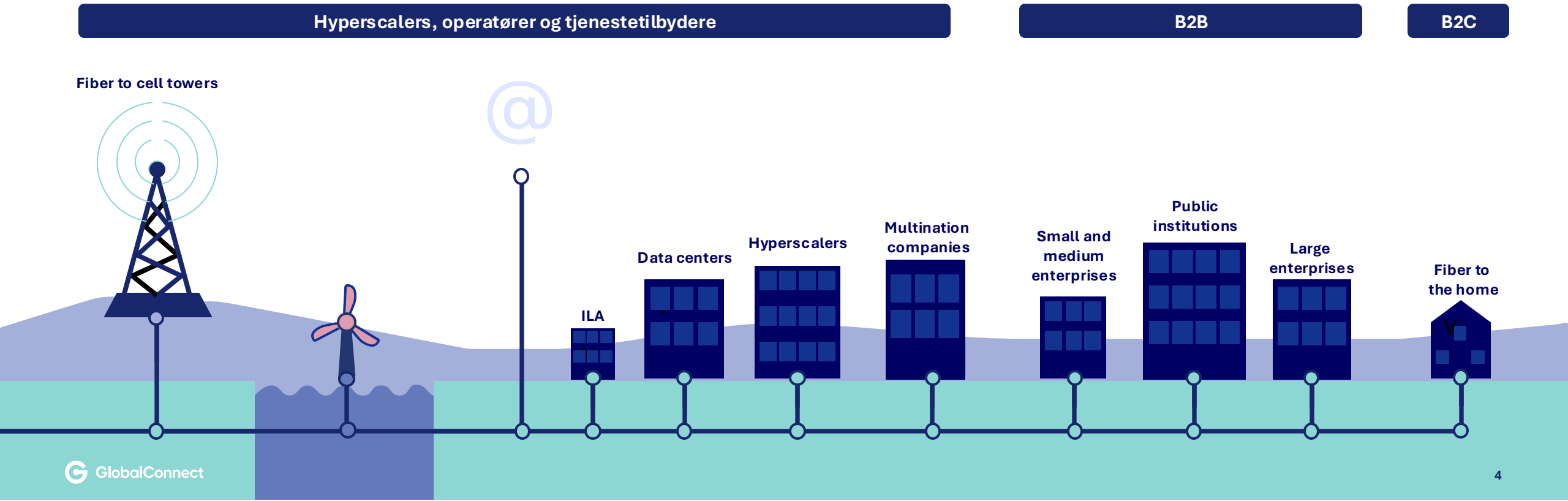
Norges digitale infrastruktur er vår livsnerve

– vi bærer 50 % av dataen inn og ut av regionen

~50%	data håndtert inn og ut av regionen
30.000	bedrifts- og offentlige kunder
>1.1 million	private kunder
> 245.000	km med fiber
40.000	m2 datasenter på 24 lokasjoner i Norden

Fibernettverk er ryggraden i våre digitale samfunn

Fiberinfrastruktur er fundamentet for moderne internett, mobilnett, skytransport (cloud computing) og IoT. Trådløs teknologi muliggjøres av data som transporteres via fiberkabler, noe som sikrer høy hastighet, lav forsinkelse og høy kapasitet.



Norges digitale infrastruktur er vår livsnerve

– og det gjør oss sårbare

DEN DIGITALE VERDIEN

DEN DIGITALE SÅRBARHETEN

Vi er et av de mest digitaliserte landene. Vår utfordring er ikke å være digitalt best, men digitalt *robust*.

DEN DIGITALE VERDIEN

DEN DIGITALE SÅRBARHETEN

4 viktige varsler i det norske trusselbildet

1. To tredjedeler av norske ledere i bransjer som regnes som de mest samfunnskritiske, rapporterer om en økning i dataangrep, samtidig som truslene blir stadig mer sofistikerte.

2. Russisk etterretning kan se seg tjent med å utføre sabotasjeaksjoner mot mål i Norge i 2026. Sivil infrastruktur kan rammes. Hensikten vil være å skape uro i samfunnet.

3. Både NSM og PST forventer at norske virksomheter i løpet av 2026 blir utsatt for cyberoperasjoner hvor KI-verktøy spiller en viktig rolle.

4. NSMs inntrengingstester i 2025 avdekket kritiske og gjennomgående sårbarheter i statlige virksomheter, hvor de i de fleste tilfeller fikk full kontroll over systemene på grunn av svak passordsikkerhet og mangelfull tilgangsstyring.

Et lands digitale blackout er ikke lenger utenkelig

Når digital infrastruktur feiler, feiler mange samfunnskritiske områder

Den nye analysen avdekker landets sårbarhet– basert på data og innsikt

De norske strukturelle sårbarhetene, samt hvilke økonomiske og samfunnsmessige konsekvenser det kan få dersom landets digitale infrastruktur faller ut i flere dager.

Analysen bygger på infrastrukturdata, politiske rammevilkår, casestudier og innsikt fra eksperter, operatører og offentlig-private initiativer

Et lands digitale blackout er ikke lenger utenkelig
Når digital infrastruktur feiler, feiler mange

Helse

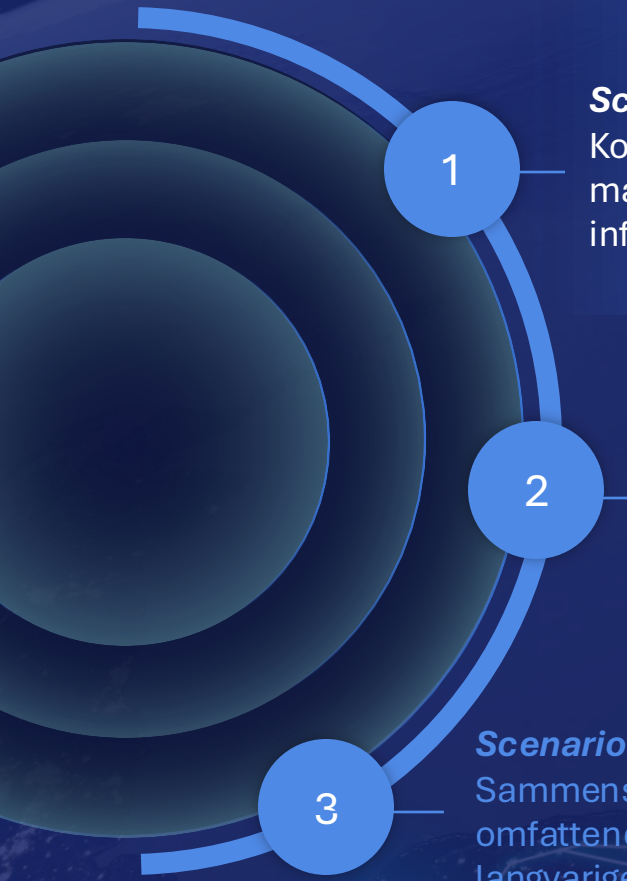
Finans

Transport

Energi

Et lands digitale blackout er ikke lenger utenkelig

Når digital infrastruktur feiler, feiler mange



1

Scenario 1
Korte avbrudd forårsaket av lokale maskinvarefeil, problemer med delt infrastruktur eller programvarefeil

Opptil 4 timer
Telefoni- og internetttjenester for innbyggere og bedrifter påvirkes umiddelbart, men operatørene gjenoppretter driften raskt.

2

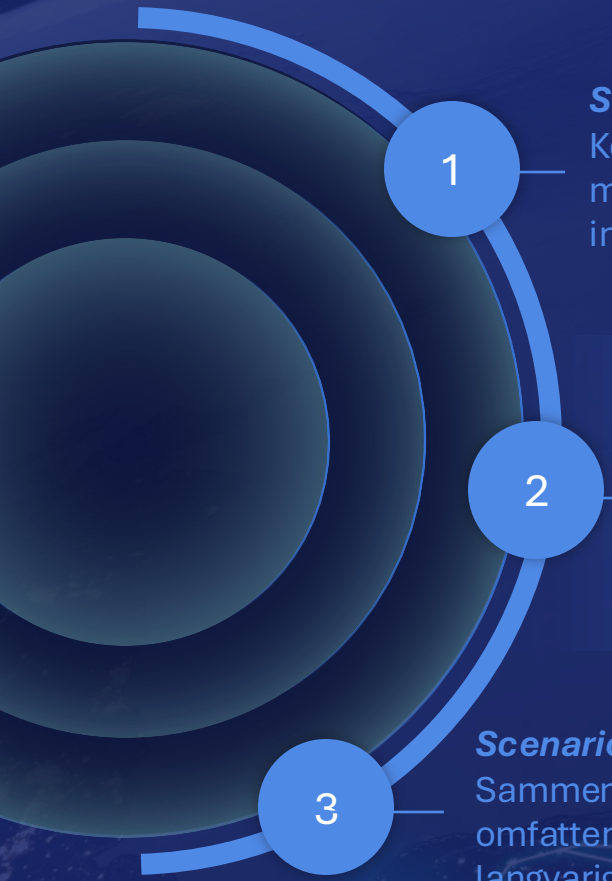
Scenario 2
Sammenfall av faktorer som cyberangrep, delvis ustabilitet i strømnettet eller orkestreringsfeil. Kan utløses som et resultat av fiendtlig statlig aktivitet og utilstrekkelig reservekapasitet

3

Scenario 3
Sammensatte, koordinerte cyberangrep og omfattende sabotasje av fysisk infrastruktur eller langvarige strømbrudd – utført som hybrid krigføring

Et lands digitale blackout er ikke lenger utenkelig

Når digital infrastruktur feiler, feiler mange



1

Scenario 1
Korte avbrudd forårsaket av lokale maskinvarefeil, problemer med delt infrastruktur eller programvarefeil

Opptil 4 timer
Telefoni- og internetttjenester for innbyggere og bedrifter påvirkes umiddelbart, men operatørene gjenoppretter driften raskt.

2

Scenario 2
Sammenfall av faktorer som cyberangrep, delvis ustabilitet i strømnettet eller orkestreringsfeil. Kan utløses som et resultat av fiendtlig statlig aktivitet og utilstrekkelig reservekapasitet

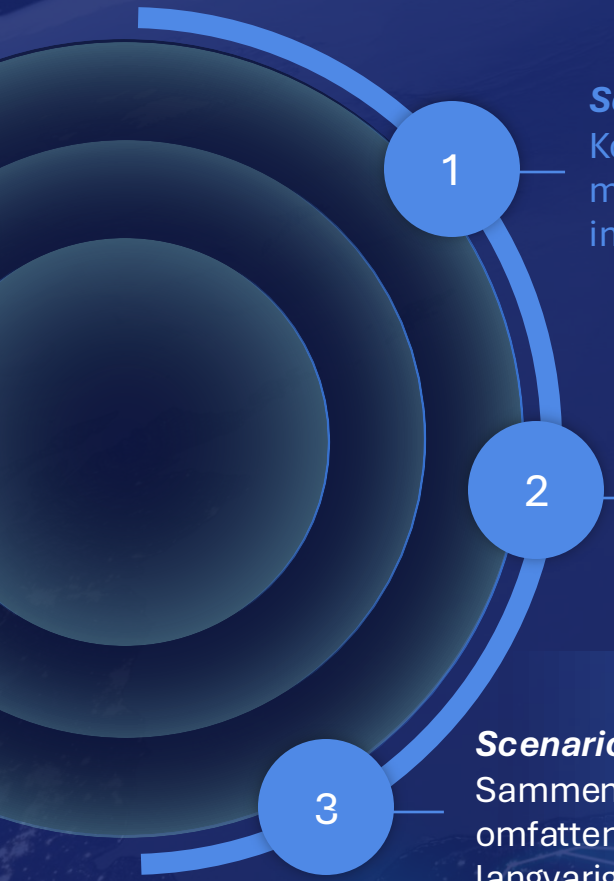
8 – 16 timer
Flere sektorer opplever driftsforstyrrelser, og koordineringen mellom myndigheter og bedrifter blir vanskelig. Backup-systemer begynner å svikte, og kritiske funksjoner blir påvirket.

3

Scenario 3
Sammensatte, koordinerte cyberangrep og omfattende sabotasje av fysisk infrastruktur eller langvarige strømbrudd – utført som hybrid krigføring

Et lands digitale blackout er ikke lenger utenkelig

Når digital infrastruktur feiler, feiler mange



Scenario 1
Korte avbrudd forårsaket av lokale maskinvarefeil, problemer med delt infrastruktur eller programvarefeil

Opptil 4 timer
Telefoni- og internetttjenester for innbyggere og bedrifter påvirkes umiddelbart, men operatørene gjenoppretter driften raskt.

Scenario 2
Sammenfall av faktorer som cyberangrep, delvis ustabilitet i strømnettet eller orkestreringsfeil. Kan utløses som et resultat av fiendtlig statlig aktivitet og utilstrekkelig reservekapasitet

8 – 16 timer
Flere sektorer opplever driftsforstyrrelser, og koordineringen mellom myndigheter og bedrifter blir vanskelig. Backup-systemer begynner å svikte, og kritiske funksjoner blir påvirket.

Scenario 3
Sammensatte, koordinerte cyberangrep og omfattende sabotasje av fysisk infrastruktur eller langvarige strømbrudd – utført som hybrid krigføring

1 – 7 dager
Samfunnet rammes av omfattende systemsvikt på tvers av infrastruktur og tjenester. Kommunikasjon, energi, transport og finansielle tjenester lammes.

Kostnaden ved et angrep

Ifølge Copenhagen Economics kan et **omfattende landsdekkende brudd** i konnektiviteten i Danmark koste mellom **€500 millioner og €1 milliard** per time, avhengig av omfang og sektoreksponering.

Scenarioanalysene viser at den mest presserende risikoen ikke lenger er et enkelt angrep, men en ‘perfekt storm’

	Regionalt	**Nasjonalt**
Sektorielt	*Sannsynlighet: Moderat* Forstyrrelse av et lokalt system eller en prosess innenfor én enkelt sektor	*Sannsynlighet: Moderat – Lav* Krever svikt i en sentralt styrt tjeneste
Tverrsektorielt	*Sannsynlighet: Moderat – Lav* Samtidige forstyrrelser på tvers av sektorer innenfor en region på grunn av delte avhengigheter	*Sannsynlighet: Lav* Koordinert fler-sektor forstyrrelse som påvirker nasjonal kontinuitet

Den mest presserende risikoen i dag er ikke lenger et enkelt angrep,
men en perfekt storm – samtidige, flernivåangrep på sammenkoblede systemer.

Norge er ikke klar til å unngå eller håndtere scenario 3

scenarioanalysen viser hvordan et bortfall raskt kan utvikle seg til en samfunnskrise.

Den digitale livsnerven

Et vesentlig fellestrekk ved scenariene er at tap av forbindelse ikke påvirker systemer isolert. De avledede effektene sprer seg som ringer i vannet, og mange sektorer – både offentlige og private – vil oppleve direkte eller indirekte konsekvenser.

Den digitale infrastrukturen er kommet under press

Angrep på fiberforbindelser

Programvare med økt kompleksitet og sårbarhet

For mye legges i ett datasenter

Fire prinsipper for en styrket digital beredskap

1) Digital infrastruktur må behandles som en grunnpilar i nasjonal sikkerhet

Cyber- og telekommunikasjonssystemer er anerkjent som kritiske, men må nå integreres fullt ut i nasjonale krisebudsjetter, risikovurderinger og forsvarsplanlegging..

2) Robusthetsstrategien må gå utover kabler – og omfatte programvare og kontrollsystemer

Sårbarheter i distriktene, flaskehalser ved landingspunkter og overavhengighet av bestemte programvareplattformer kan utløse kjedereaksjoner.

3) Krisehåndtering må koordineres i sanntid og stresstestes på tvers av sektorer

Teleberedskapsrådet bør forankres i nasjonale kriseplaner og operativt beredskapsarbeid.

4) Robusthet må være regional av design – ikke nasjonal av antakelse

Norges geografiske forhold gjør landet mer sårbart enn sine nordiske naboer. Regional reservekapasitet, felles reparasjonsteam og koordinerte rutingsprotokoller er avgjørende.

Vi skal ikke vente på krisen – vi må forberede oss på den

3 anbefalinger

1

En digital robusthetssertifisering for kritiske operatører, som validerer deres evne til å motstå systemisk press på tvers av cyber-, fysiske- og AI-domener.

2

Et nordisk digitalt robusthetsskjold, som muliggjør grenseoverskridende koordinering, felles reserve-systemer og felles beskyttelse av den sentrale digitale infrastrukturen — samtidig som nasjonal suverenitet og krav til datalagring ivaretas.

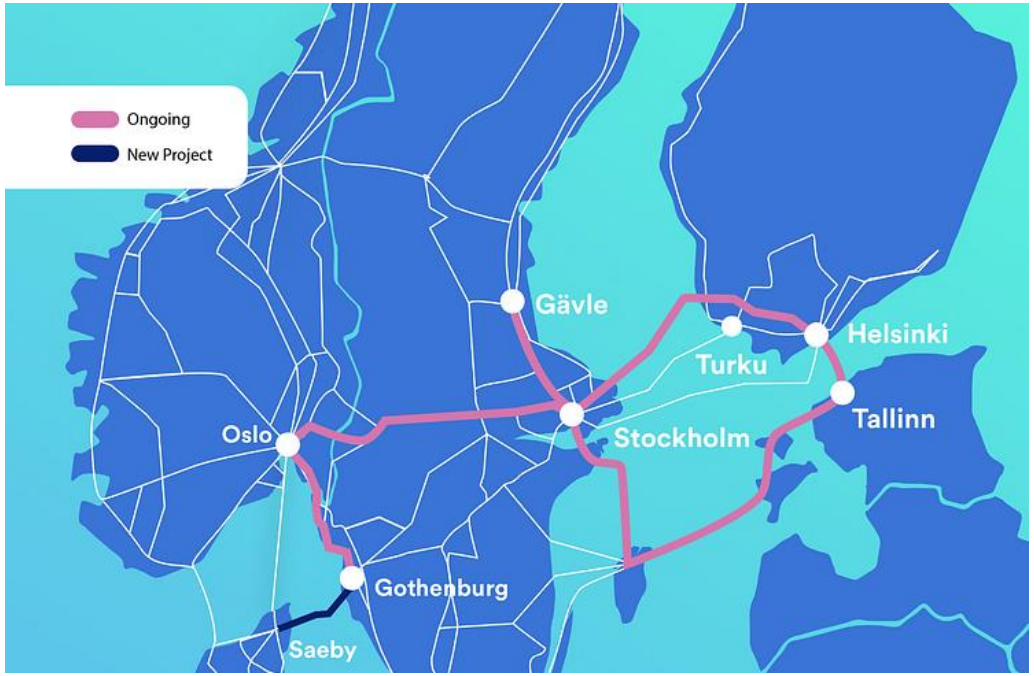
3

En tilbakevendende "Black Sky"-øvelsesrekke for å teste flerdagers, tverrsektorielle reaksjoner på forstyrrelser — som går utover simuleringer og inn i reell operasjonell validering.

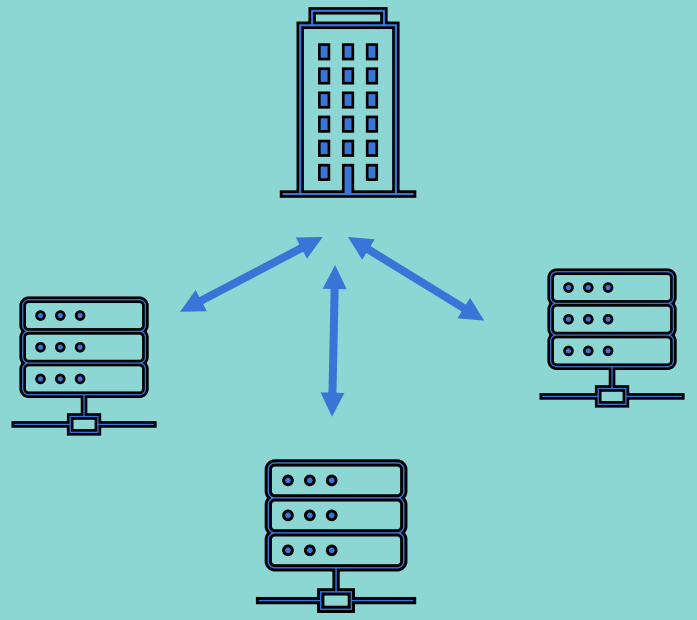
Robusthet er et spørsmål om redundans

Det er behov for diversitet på fiber …

Et tett og forgreinet nettverk med mange alternative hovedruter – både på land og under vann – sikrer redundans og gode muligheter for omdirigering.



… og på data og plattformer i mange datasentre



Vi må beskytte fiberkablene våre – på land og under vann

Finnish police don't suspect criminal activity regarding dar in south of country

DIGI Ledige stillinger Nyhetsbrev Nyhetsstudio Tips oss

SIKKERHET

MDG ber regjeringen trykke på alarmknappen for å hindre sabotasje

Flere skader på undersjøiske kabler i Østersjøen får fram sabotasjefrykt hos Miljøpartiet De Grønne. De ber om strengere sikkerhetstiltak på norsk sokkel.

Nyheder

Ny teknologi skal reducere risiko sabotage på telekabler

Nordisk telegigant eksperimenterer med telekabler

Magnus Norberg, affärsområdeschef för stadsnätet, berättar att sabotaget påverkar stora delar av Eskilstuna och Strängnäs och kan ta dagar att reparera. Foto: TT/SVT

Stort internetsabotage i Eskilstuna och Strängnäs

UPPDATERAD 5 SEPTEMBER 2025 PUBLICERAD 3 SEPTEMBER 2025

Flera kabelskåp med fiberkablar saboterades under tisdagskvällen i Eskilstuna kommun. Nästan 2 000 kunder drabbades i Eskilstuna och Kvicksund, och flera vårdcentraler i Strängnäs.

– Det är allvarligt, säger Magnus Nordberg, affärsområdeschef för stadsnätet på Eskilstuna energi och miljö.

Störningen påverkade både internet och tv-tjänster, samt 5G- och 4G-näten.

graveuheld? Hele Norden er i alarmberedskab

ødelagte kabler i Finland. Kabelbrud havde næppe skabt påstyr sikkerhedsforsker.

Bohlin, Sveriges civilt försvar. Ekströmer/TT

Grävskopor kapade internetkablar

Två internetkablar på finsk mark gick sönder på måndagen. I båda fallen rör det sig om olyckor och på tisdagen reparerades kablarna.

Nätägaren Global Connect uppträckte driftstörningar på kablarna vid två olika tidpunkter på måndagskvällen.

– De påverkade 100 av våra företagskunder och 6 000 finska hushåll, säger Niklas Ekström, kommunikationschef på Global Connect.

Den ena kabeln ligger på land i finska staden Esbo utanför Helsingfors och den andra ligger tre–fyra mil bort i Vihti, norr om staden. På tisdagseftermiddagen hade företaget reparerat båda kablarna.

"Vi kan bekräfta att båda kablarna gick sönder på grund av grävarbete, och därför bedömer vi dessa incidenter som ett sammanträffande av olyckliga omständigheter", skriver Niklas Ekström i ett mejl till SVD.

Sveriges Radios Ekot, som först rapporterade om kabelbrotten, uppgav under morgonen att finsk polis misstänkte brott, något även Sveriges minister för civilt försvar Carl-Oskar Bohlin (M) gav uttryck för.

"Vi ser allvarligt på detta. Finsk polis utreder vad som har hänt och på grund av omständigheterna kring det inträffade misstänks sabotage", skrev ministern i en kommentar till TT.

Senare tydliggjorde ministern att han återgav information från svenska Polismyndigheten om att man med hänsyn till omständigheterna misstänkte sabotage.

Även Finlands regering sa initialt att de såg allvarligt på händelsen. Det skrev Finlands transport- och kommunikationsminister Lulu Ranne på X. Senare dementerades det misstänkta sabotaget av finländsk polis.

"Polisen har för närvarande ingen brottsutredning på gång gällande kabelbrottet mellan Finland och Sverige", skriver man i ett uttalande på sin sajt.

I november framkom det att två undervattenskablar skadats i Östersjön, den ena mellan Finland och Tyskland, den andra mellan Sverige och Litauen. Polisen utreder den händelsen som misstänkt sabotage.

Det kinesiska fartyget Yi Peng 3 har pekats ut för inblandning i den händelsen. Fartyget har de senaste veckorna legat still på internationellt vatten i Kattegatt, där det bevakas av dansk kustbevakning.

Annica Ögren
annica.ogren@swd.se

SVERIGE

Nya kabelbrott mellan Finland och Sverige

Uppdaterad i går 14:56 Publicerad i går 08:58

Två nya kabelbrott upptäcktes på en internetledning mellan Sverige och Finland

Båda tros ha orsakats av byg finska Trafik- och kommuni

Lou Mikko

Spara Dela

Kabelbrotten inträffade måndag i ligger i Helsingforsområdet. Enlig Connect handlade det om interne Sverige och Finland. Flera svensk Post- och telestyrelsen (PTS), info

– Vi känner till att de håller på att

Jyllands-Posten

Netværksudbyder: Datakabler blev ødelagt ved gravearbejde i Finland

brud på kabler i Finland. Men kablerne blev ødelagt ved gravearbejde.

Udland

Skadede kabler i Østersøen skyldes formentlig sabotage, siger tysk forsvarsminister

To datakabler blev revet over inden for kort tid.

13.12.24 • DI Digital • Nyheder

Lippert og Espersen med fælles melding: Søkabler skal beskyttes meget bedre

landenes sikkerhed og den kritiske infrastruktur er i kudlinjen, når søkabler skæres over. Derfor skal forsvaret nod den form for hybrid krigsførelse prioriteres langt mere nd nu.

Verden

Sabotasje i to undersjøiske kabler i Østersjøen

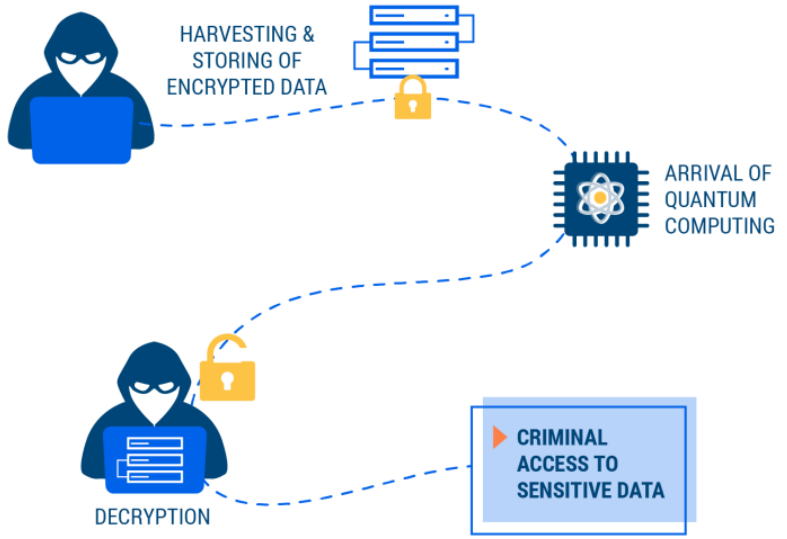
(AGDER PRESS): En internettkabel fra Litauen til Sverige ble først ødelagt. Deretter gikk det 18 timer senere da en kabel fra Finland til Tyskland.

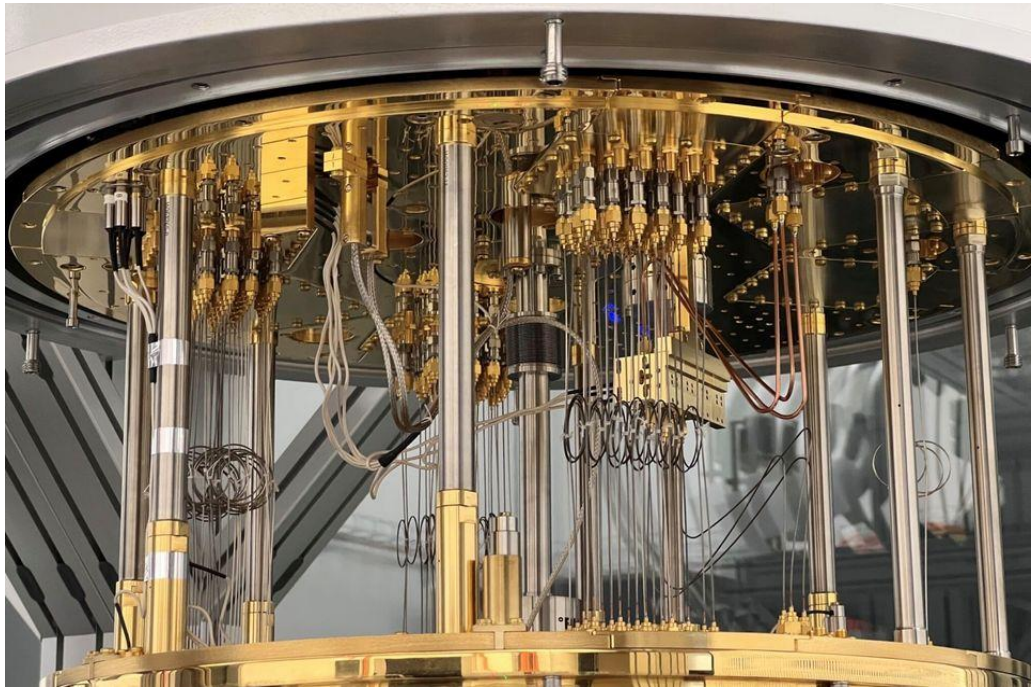
Svensk politi etterforsker sabotasje mot mer enn 30 mobilmaster

Om lag 30 uforklarlige tilfeller av sabotasje rettet mot mobilmaster blir nå etterforsket av svensk politi. De fleste ligger på landets østkyst.

Fremtidens trussel er her allerede i dag

Harvest-now-decrypt-later

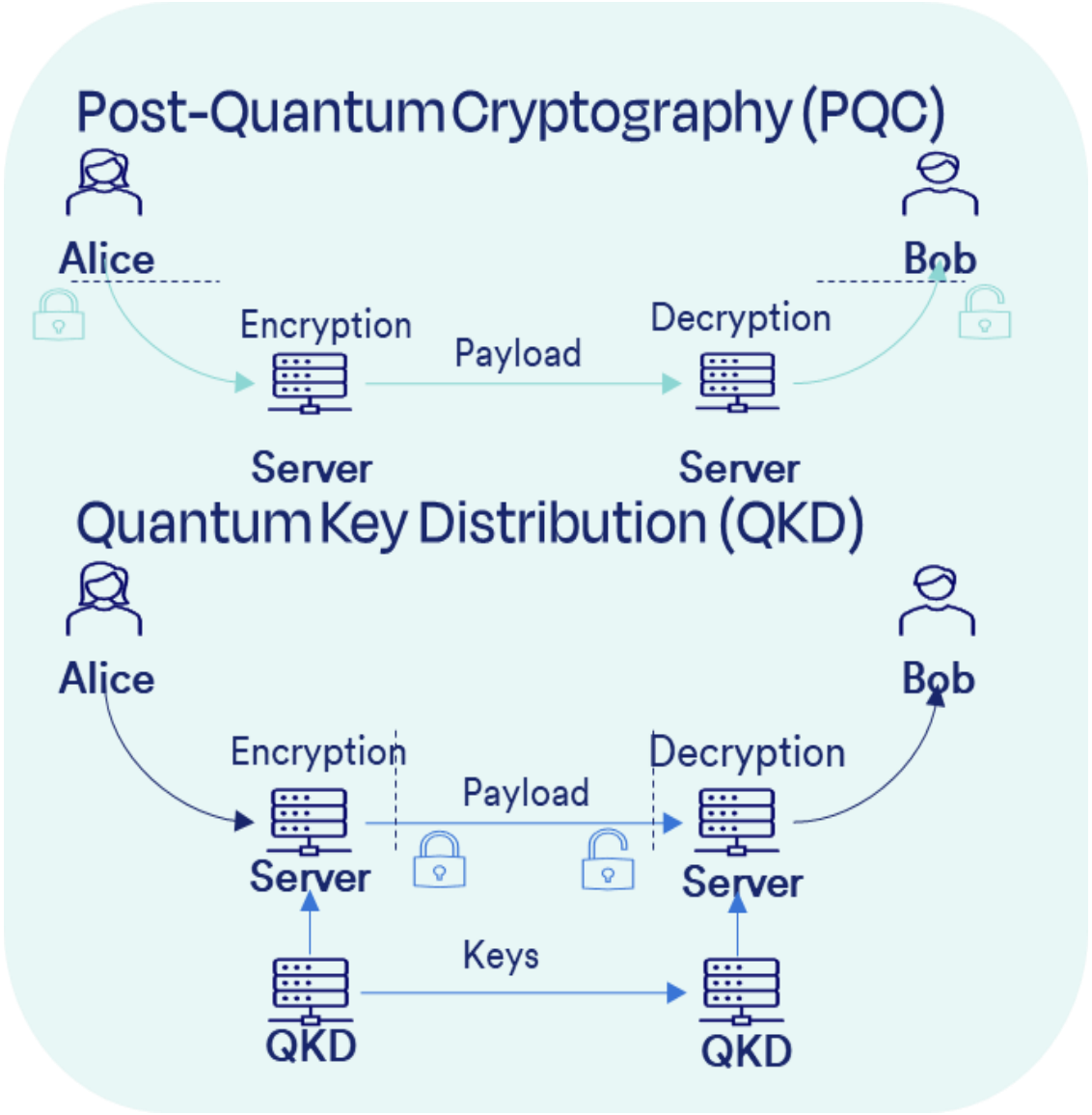




Løsningene: PQC og QKD

PQC – Anvendelse av nye krypteringsalgoritmer som ikke kan brytes av kvantedatamaskiner

QKD – Anvendelse av kvantemekanikk for å utveksle nøkler mellom to kommunikasjonsparter. Disse nøklene brukes etterfølgende av en eksisterende kvantesikker symmetrisk krypteringsalgoritme



Organisasjoner må allerede begynne å forberede seg

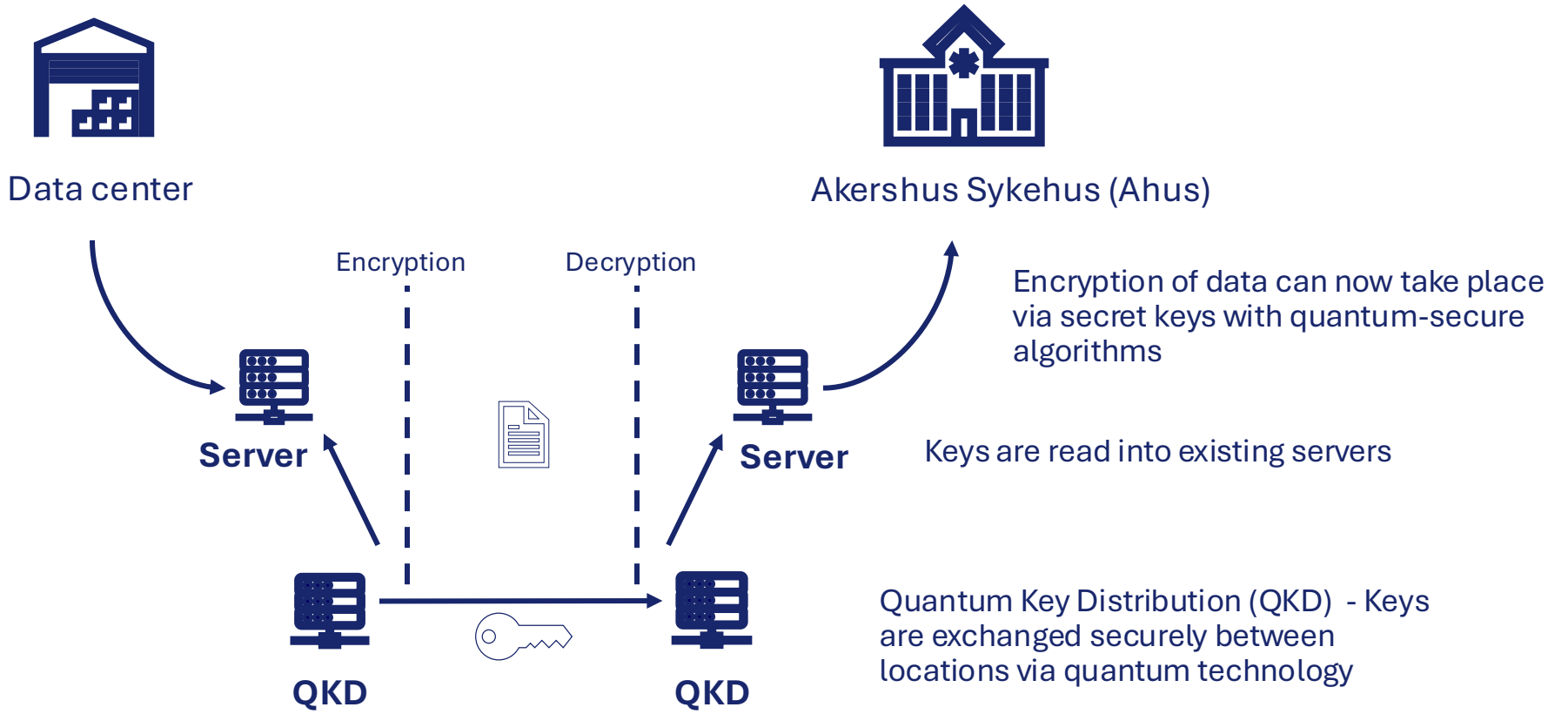
Kvantecomputere kan i fremtiden bryte dagens kryptering. Høst nå. Dekrypter senere.

Sikringen byr på en kombination av kvantesikker kryptografi (PQC) og Kvantekryptering (QKD).

Nasjonal sikkerhetsmyndighet (NSM): Virksomheter og organisasjoner må allerede nå begynne å forberede seg og høste erfaringer med kvanteteknologi:

- Lag en plan for en vellykket migrering til kvanteresistent kryptografi
- Bruk sikre algoritmer og protokoller
- Vær forberedt på å bytte kryptografiske algoritmer

Kvantesikkert nettverk som legger til et ekstra lag med sikkerhet




GlobalConnect