

A large circular graphic on the left side of the slide. It features a blue-toned digital cityscape with glowing lines and binary code (0s and 1s) at the bottom, suggesting a high-tech or cyber environment.

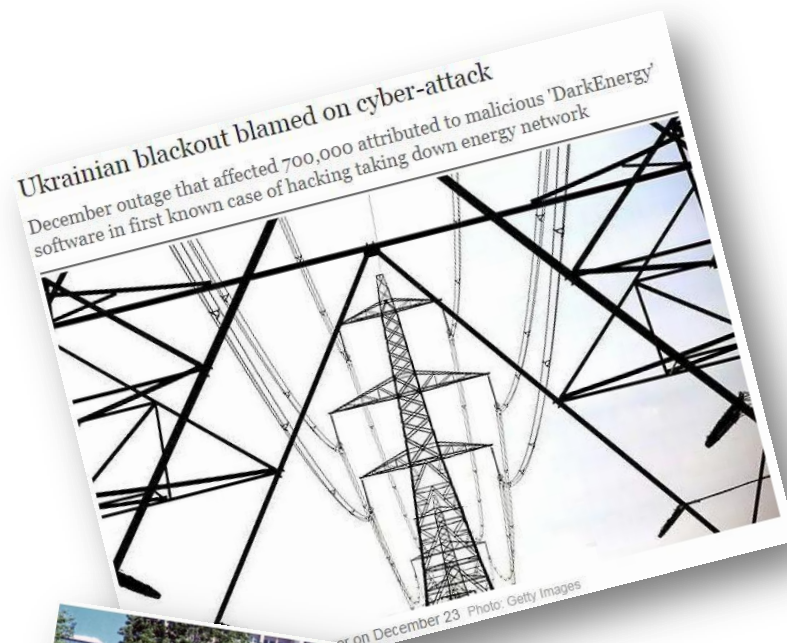
DIGITALISERING AV OFFENTLIG SEKTOR - KAN DET VÆRE SIKKERT?

Bente Hoff
Leder Strategisk IKT-sikkerhet
NSM



Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet.

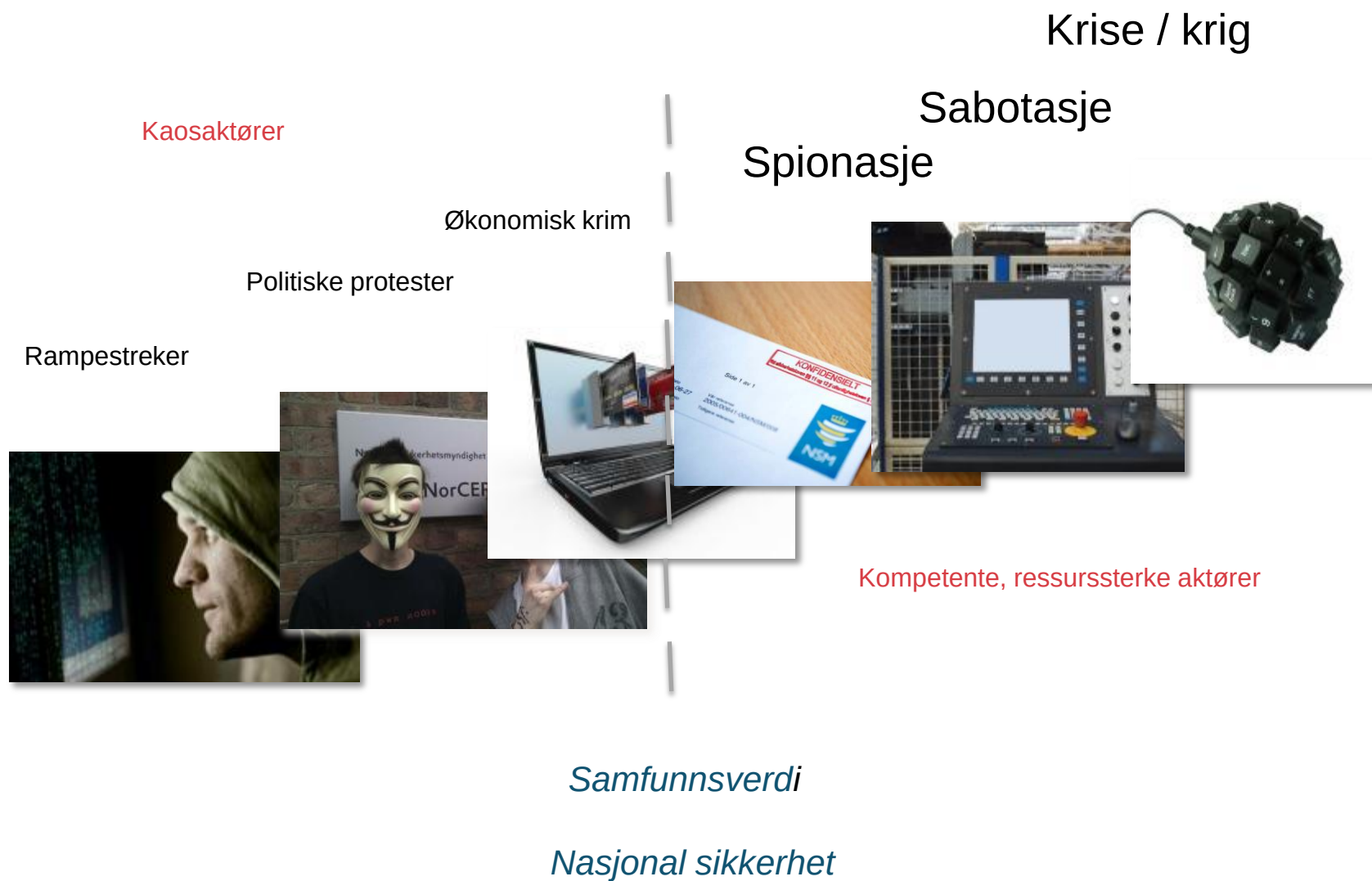
Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser.



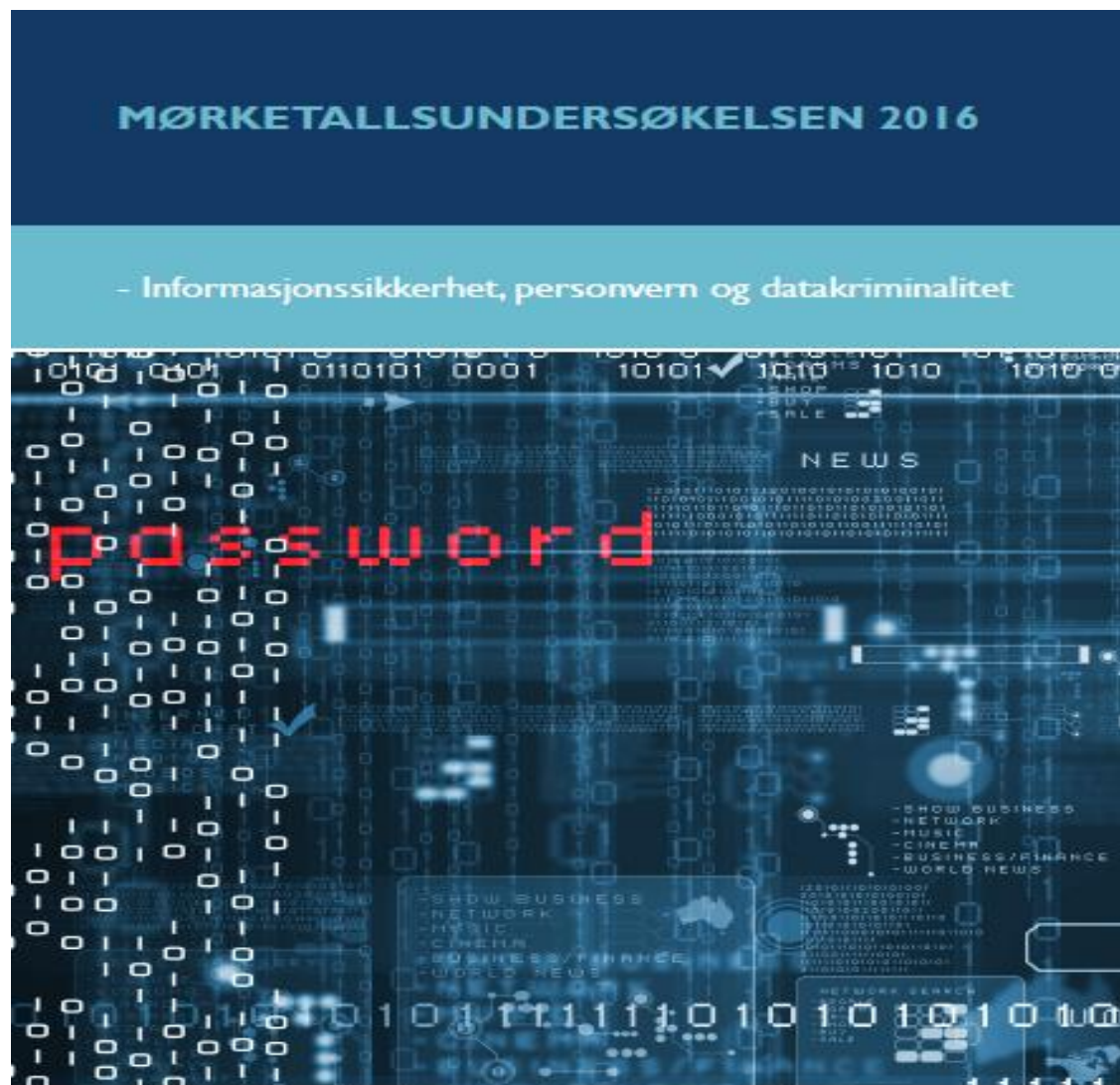
- ➔ Antall hendelser øker
- ➔ Alvorlige angrep blir mer komplekse
- ➔ Angripere utnytter i større grad leverandører uten tilstrekkelig sikkerhet
- ➔ Epost er fortsatt vanligste angrepsmetode



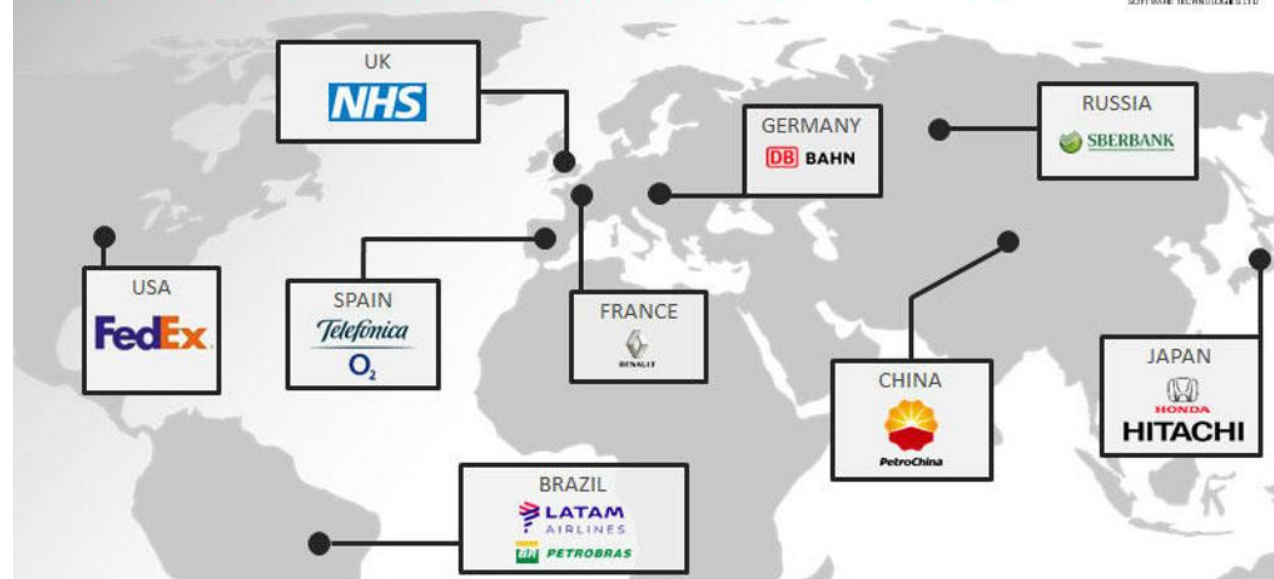
TRUSSELAKTØRENE



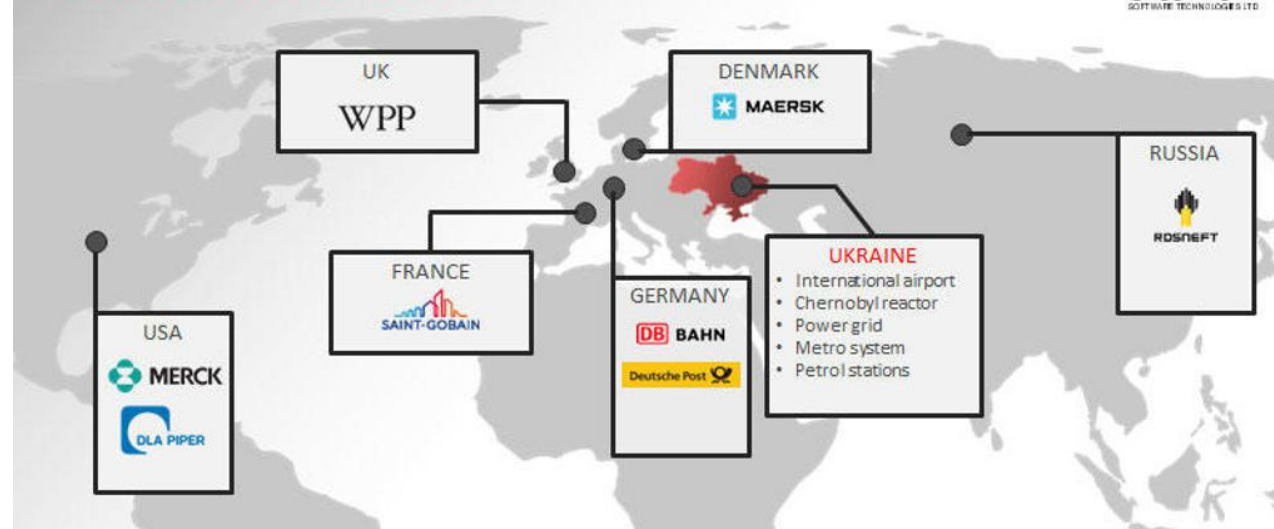
KONSEKVENSER?

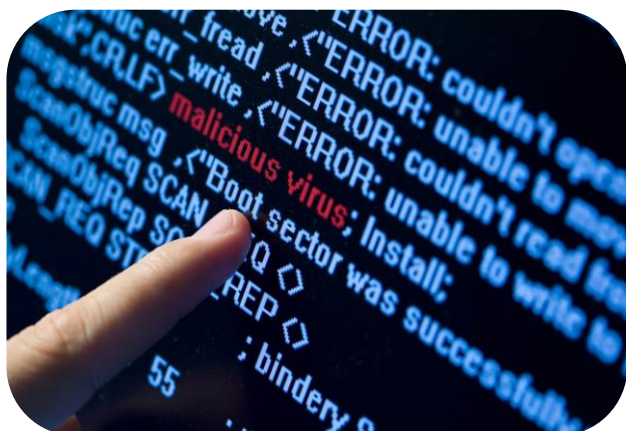


MAY 2017: WANNACRY GLOBAL ATTACKS



A MONTH LATER: PETYA OUTBREAK





IT-systemer som kan
forsvares



Sikkerhetskompentanse



Tjenesteutsetting uten
å øke risikoen

4

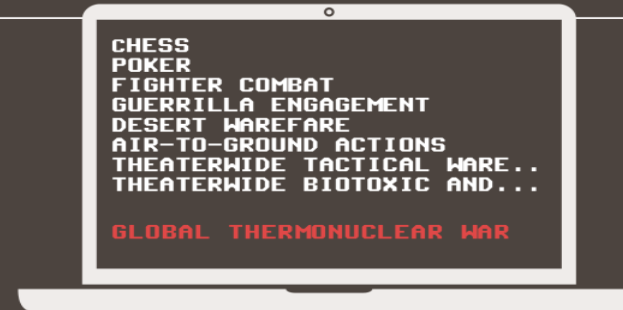
EFFEKTIVE TILTAK MOT DATAANGREP

1 Oppgrader program- og maskinvare



2 Installer sikkerhetsoppdateringer så fort som mulig

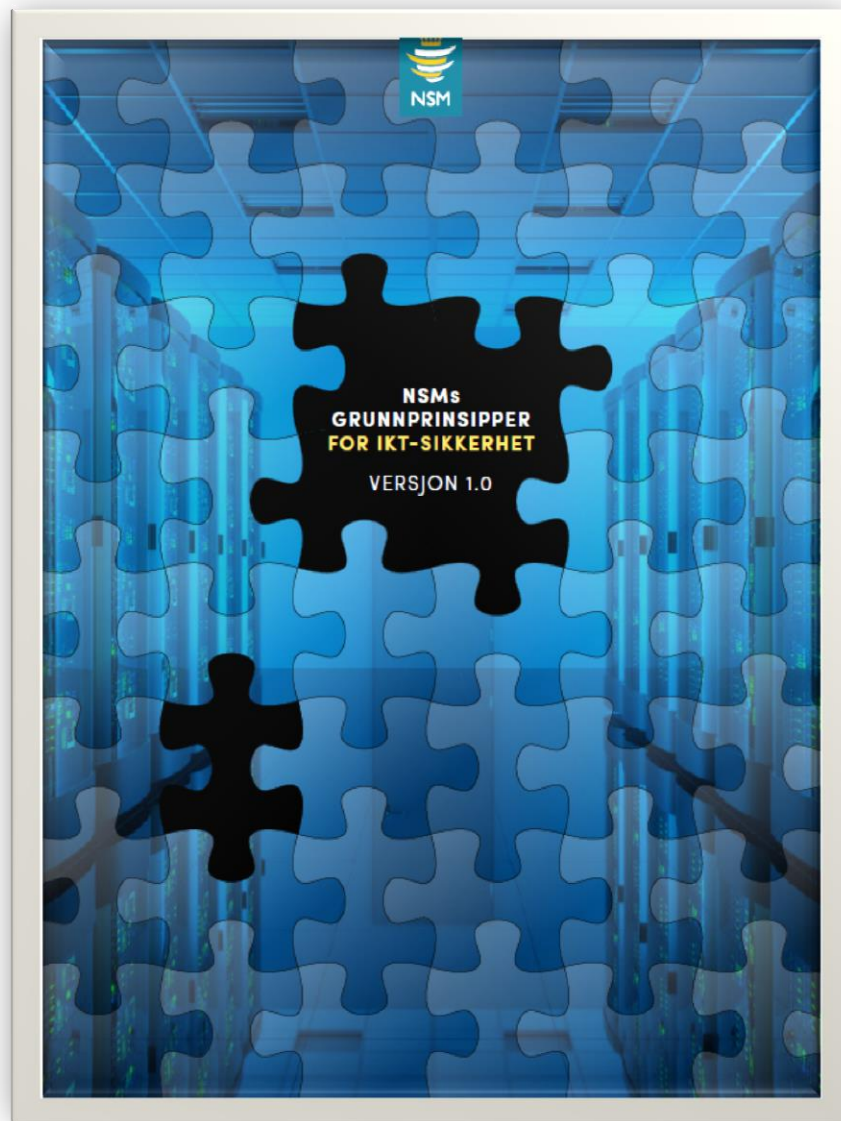
3 Ikke tildel sluttbrukere administratorrettigheter



4 Blokker kjøring av ikke-autoriserte programmer

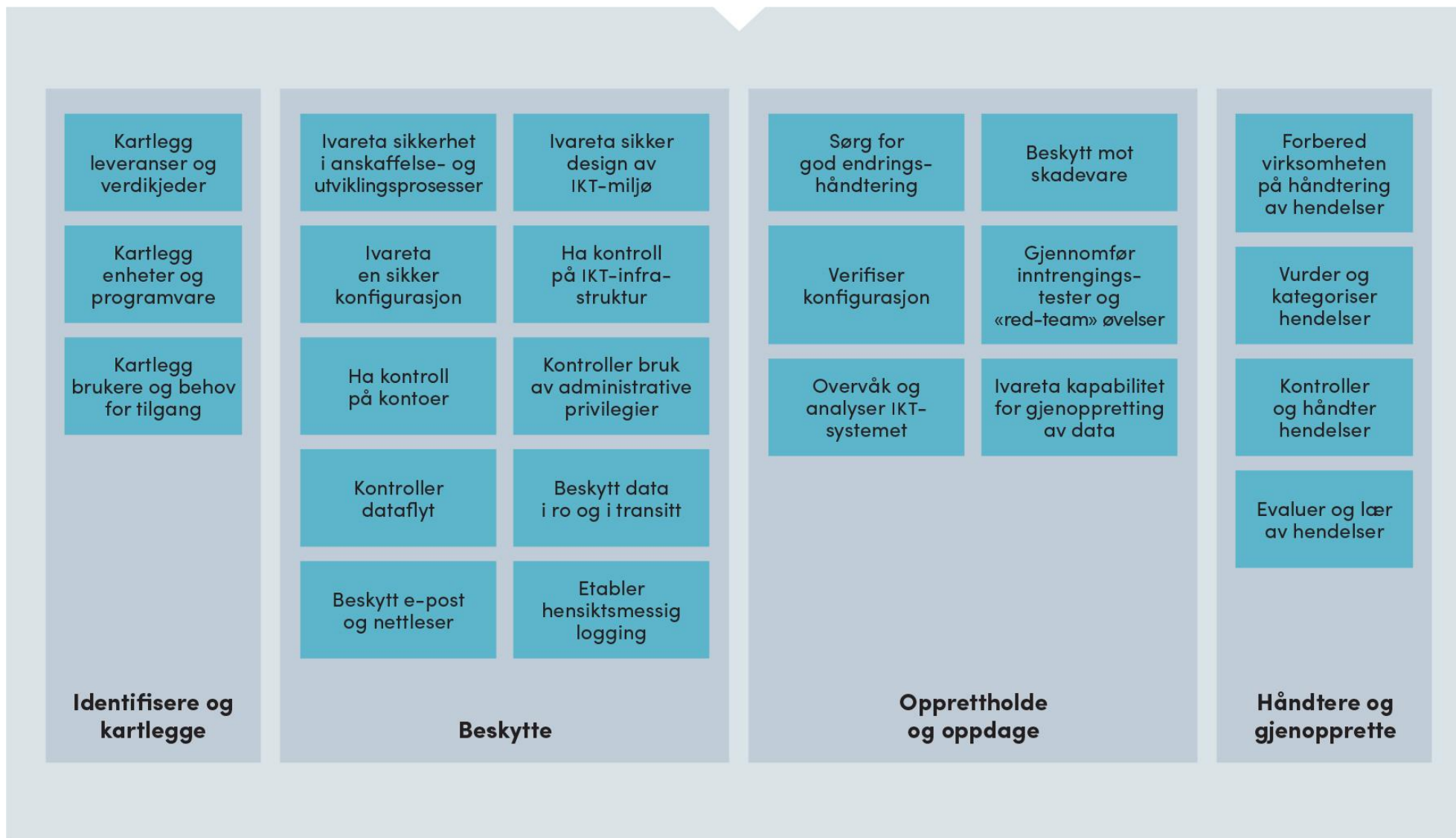
NSMS GRUNNPRINSIPPER FOR IKT-SIKKERHET

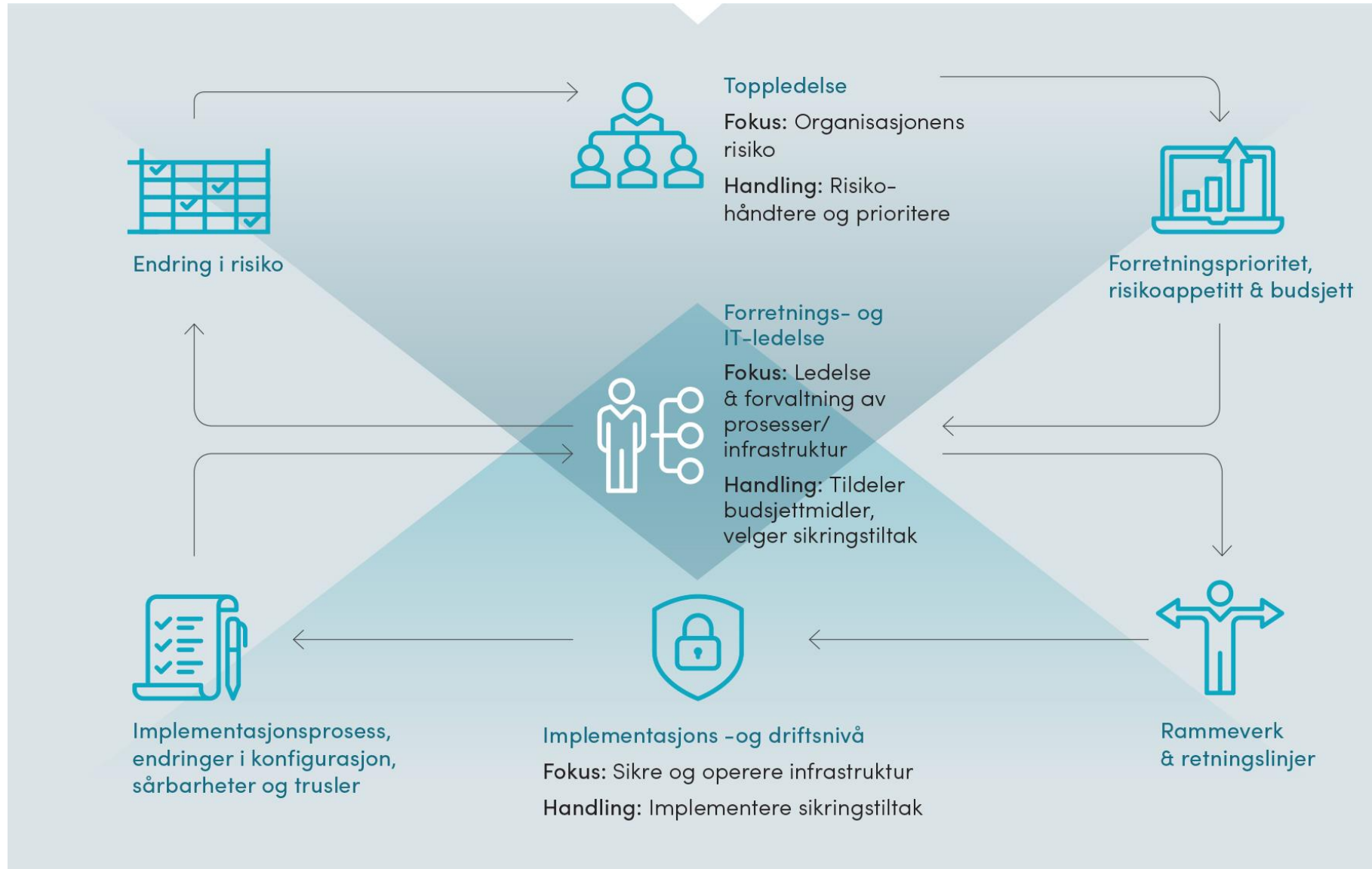
- EN MINIMUMSBASELINE SOM BØR IVARETAS FOR ALLE IKT-SYSTEMER



* I tillegg gjelder sikringskrav beskrevet i relevante lovverk og regelverk

NSMs GRUNNPRINSIPPER FOR IKT-SIKKERHET





«Sikkerhet er for viktig til å overlates til sikkerhetsekspertene»

IKT-kompetanse er en begrenset ressurs i Norge, og enda færre har kompetanse knyttet til hvordan man beskytter IKT-systemer både mot utilsiktede og tilsiktede hendelser

Dette betyr at det hersker konkurranse om knappe ressurser



Større, mer kompetente miljøer reduserer
sårbarhetene

Det er for mange små IT-avdelinger

Særlig i offentlig sektor



GOD SIKKERHET KREVER KOMPETANSE OG KAPASITET

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester

Virksomheten må sørge for at sikkerhetsnivået opprettholdes eller forbedres i forbindelse med tjenesteutsetting



TJENESTEUTSETTING MEDFØRER ØKT SIKKERHETSRISIKO

Tjenesteutsetting medfører økt sikkerhetsrisiko på grunn av **redusert kontroll på stadig mer komplekse verdikjeder**

Virksomheter må aktivt etablere organisatoriske, prosessuelle, tekniske og juridiske sikringstiltak



Statoil henter hjem sikkerhetskritiske IT-oppgaver fra India

Statoil konkluderer med at det er høy risiko å drifte IKT-infrastruktur fra India. Nå henter de hjem alle sikkerhetskritiske IT-oppgaver mot anlegg etter NRKs avsløringer.



MODERNISERING MEDFØRER OFTE AT IKT-LØSNINGER FÅR ØKT NASJONAL BETYDNING OG ØKT BESKYTTTELSESBEHOV

NSM er bekymret for....

... datasikkerheten når virksomheter setter ut tjenestene

... at økt kritikalitet ikke blir risikovurdert og identifisert

... tilgjengelig bestillerkompetanse

... nasjonal kontroll på kritisk infrastruktur

... om sikkerhetsvurderinger oppdateres med digitaliseringstakten



Nasjonal sikkerhetsmyndighet (NSM) er bekymret for at tjenesteutsetting gjøres uten at virksomheter vurderer sikkerhetsaspektet godt nok Foto: Istockphoto/Getty Images

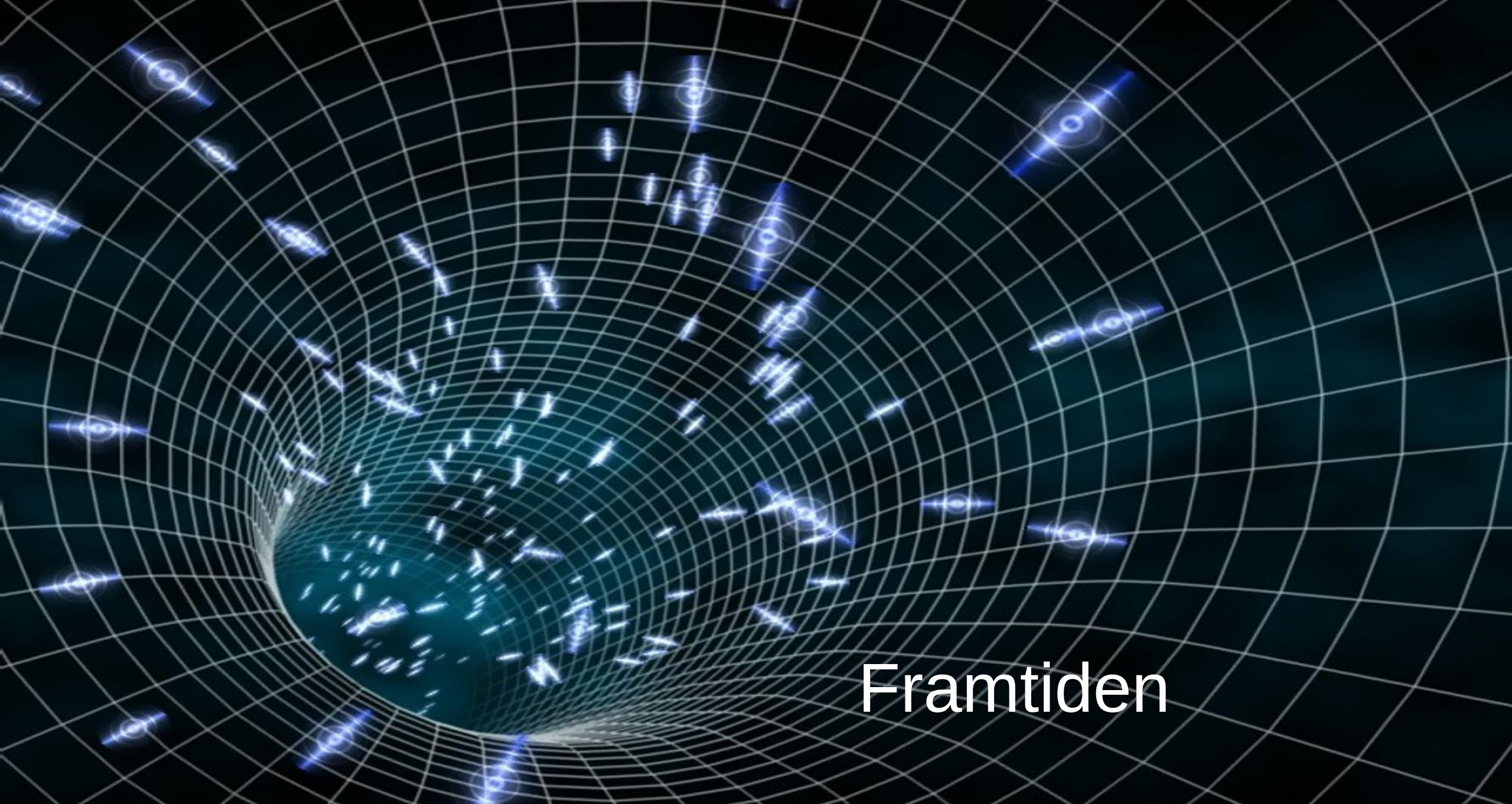
Meninger Innlegg



Bekymret over at tjenester settes ut

Vi er bekymret for datasikkerheten når virksomheter setter ut tjenestene. Datalagring og -prosessering utenfor landets grenser krever særlig aktsomhet.

Kjetil Nilsen, direktør, Nasjonal sikkerhetsmyndighet



Framtiden



Spørsmål?

NSM sikrer samfunnsverdier

