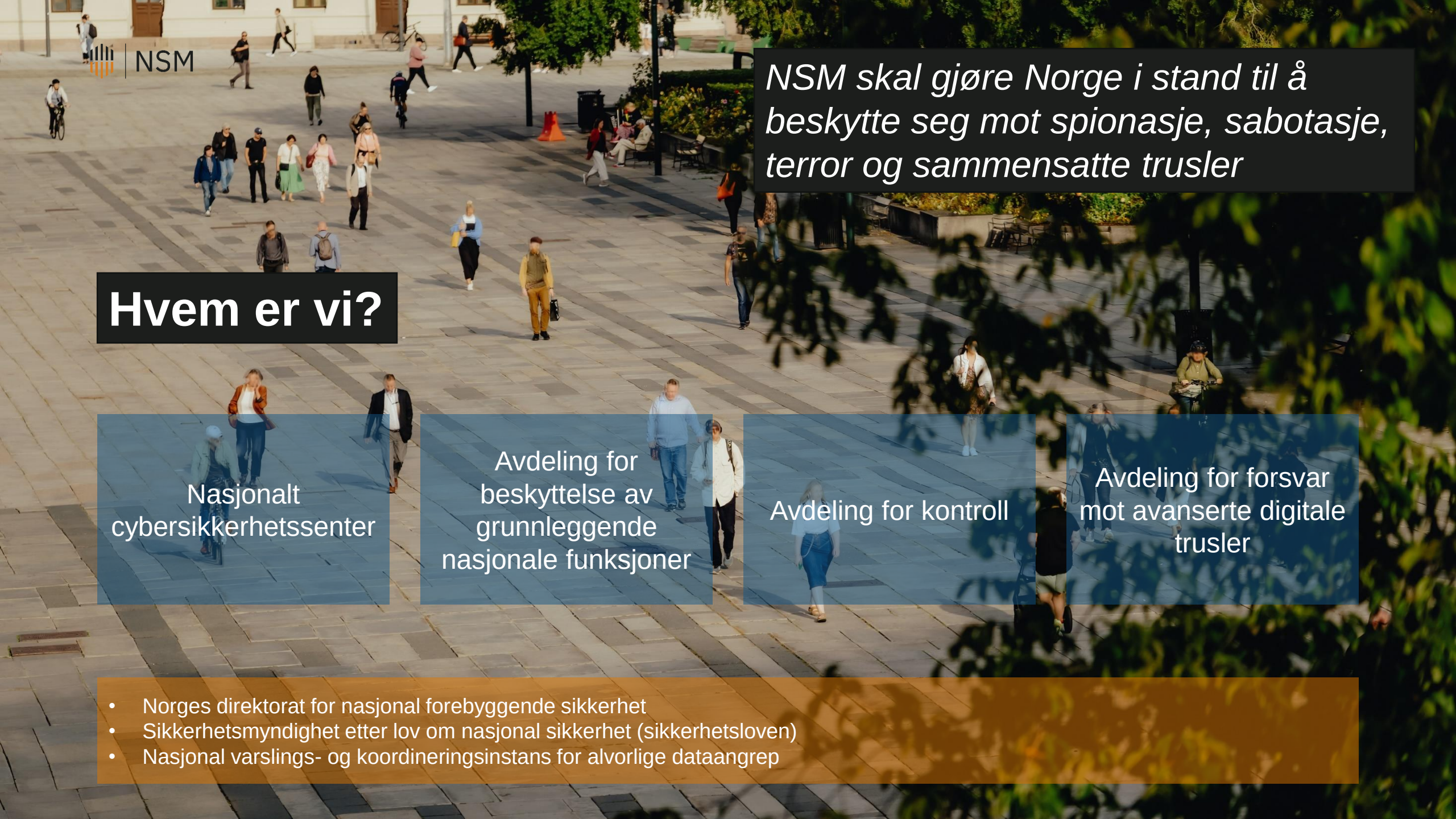
NSM

Cybersikkerhet i en usikker tid

Normonferansen 2023 - 21.11.2023

Per Håvard Pedersen
Nasjonal Sikkerhetsmyndighet, Nasjonalt Cybersikkerhetssenter (NCSC)



NSM

NSM skal gjøre Norge i stand til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler

Hvem er vi?

Nasjonalt cybersikkerhetssenter

Avdeling for beskyttelse av grunnleggende nasjonale funksjoner

Avdeling for kontroll

Avdeling for forsvar mot avanserte digitale trusler

- Norges direktorat for nasjonal forebyggende sikkerhet
- Sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven)
- Nasjonal varslings- og koordineringsinstans for alvorlige dataangrep

NASJONALT
CYBERSIKKERHETSSENTER

Utvikling og tilgjengeliggjøring av tiltak og anbefalinger. Rådgiving

Nasjonal responsfunksjon med deteksjon og hendelseshåndtering

Nasjonale tekniske sikkerhetstjenester

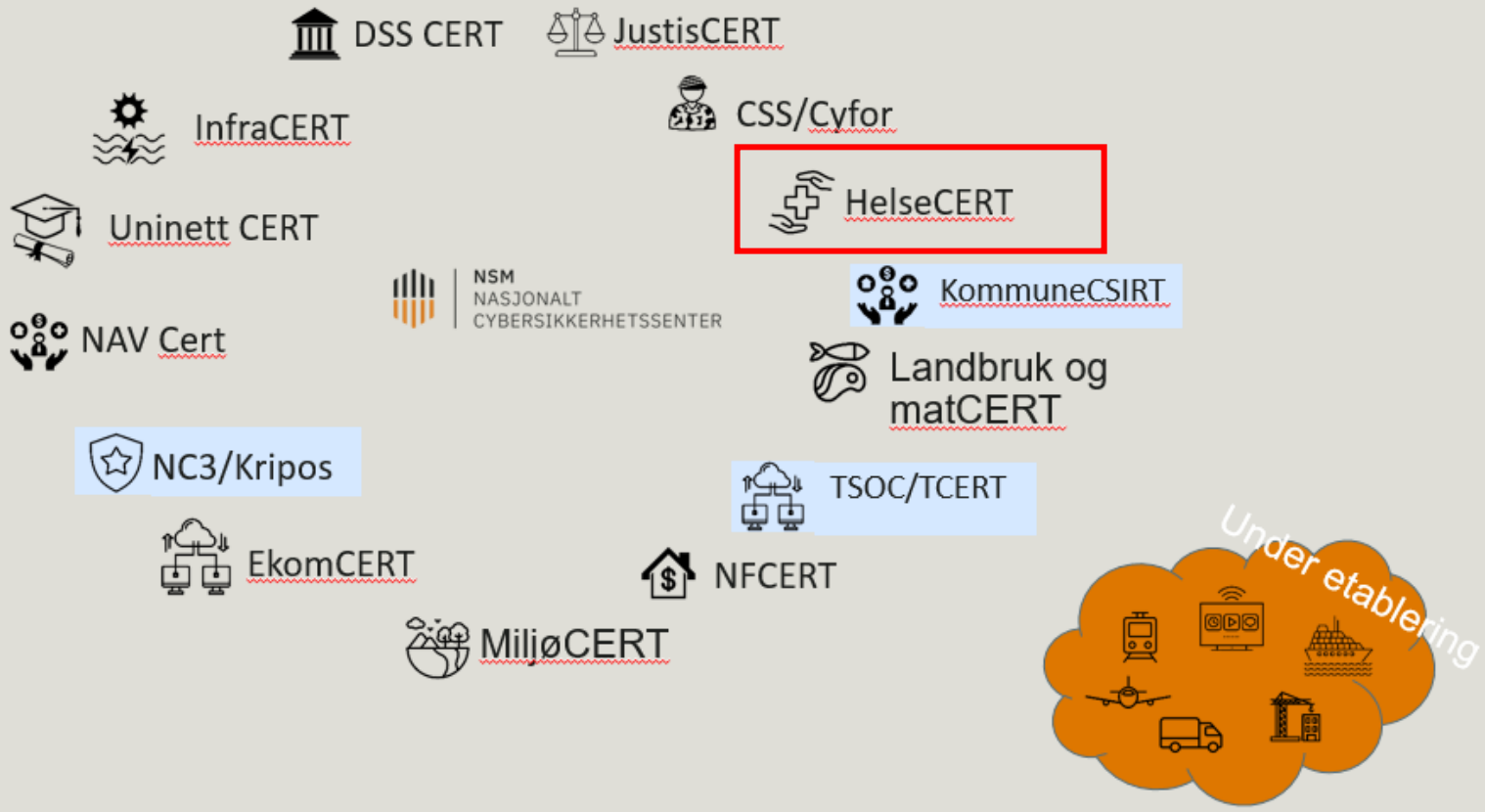
Samlet nasjonal kompetanse der ulike aktører samarbeider basert på felles risikobilde og situasjonsforståelse i felles lokaler og over nett

Partnerprogrammet

- Regelmessige operative briefer og situasjonsrapport
  - Gir overordnet cybersikkerhetsbilde, hendelsesomtale og sårbarheter
- Temamøter månedlig
- Ad hoc-arrangementer
- Diskusjonsmøter/workshops for partnere
  - Brukes i utvikling av tips/veiledere

NSM

Sektorvise Responsmiljøer (SRM)



NSM

Kvalitetsordning for leverandører som håndterer IKT-hendelser

mnemonic
Defendable
sopra steria
Netsecurity
ATEA
Orange Cyberdefense

Formålet med ordningen er at virksomheter som opplever en IKT-sikkerhetshendelse skal kunne velge en leverandør av hendelseshåndteringstjenester der NSM har vurdert at leverandøren tilfredsstiller de kvalitetskrav som NSM har definert til tjenesten.

NSM

- Målrettede
- Svært avanserte
- Stort skadepotensiale

Trusselaktører

- Kortsiktig vinning
- Mindre avansert
- Begrenset skadepotensiale

Krig

- Alle metodene vil kunne benyttes ved en krise/krig
- Ressurskrevende

Sabotasje

- Tilganger kan benyttes til sabotasje
- Skade, ødelegging og forstyrrelser i det fysiske domene
- Tjenestenekt og løsepengevirus kan også være sabotasje

Spionasje

- Statlige og statssponsede aktører
- Industrispionasje og beslutninger
- Ofte overlappende med statens interesse

Økonomisk

- Kortsiktig vinning

Politiske protester

- Informasjonslekkasjer
- Tjenestenekt

«Rampestreker»

- Tjenestenekt
- Testing av metoder
- Vandalisering av nettsider

NSM

Nasjonal Sikkerhetsmyndighet

Rapporter og bakgrunnsmateriale

NSM

Illustrasjon: NSM

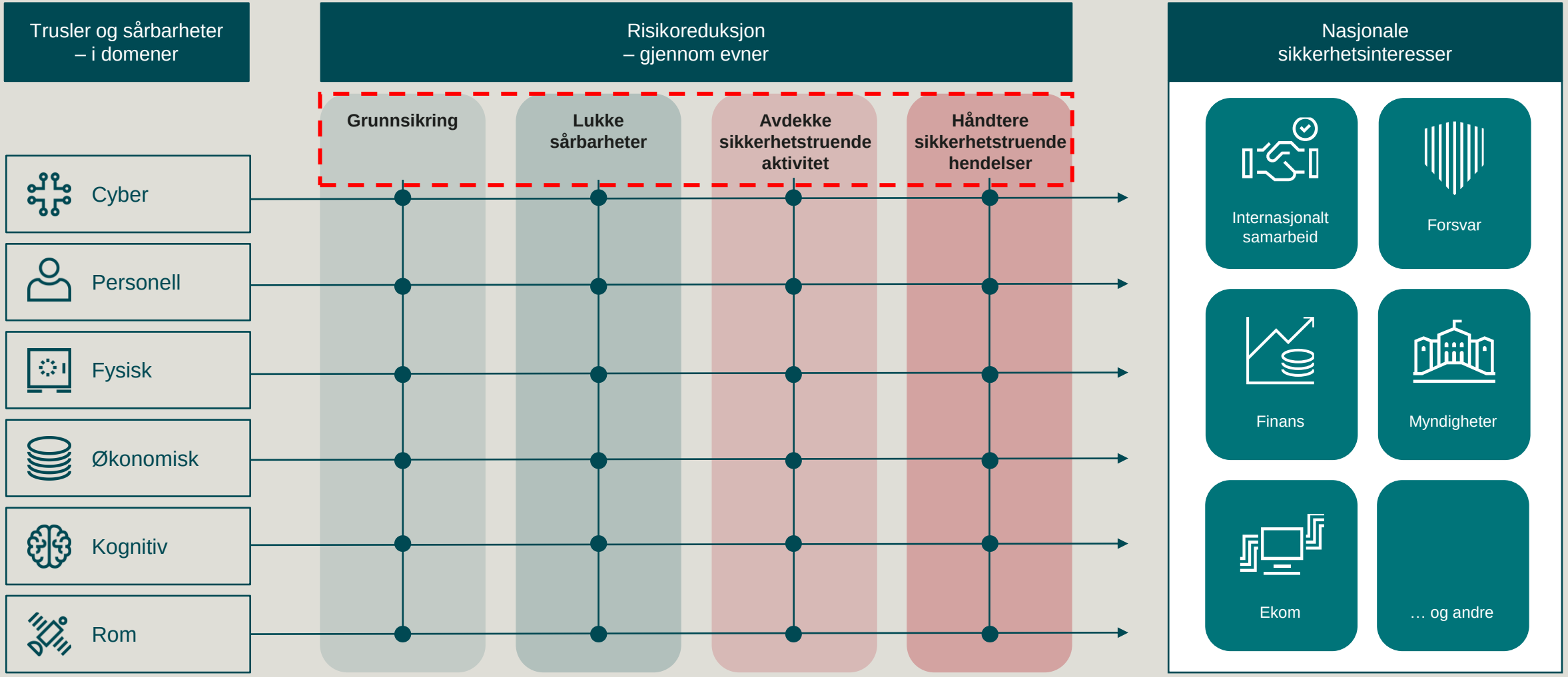
NSM

- «Norge står ovenfor betydelige sikkerhetsutfordringer fram mot 2030. Det norske samfunnet er avhengig av felles innsats og samarbeid mellom norske myndigheter, virksomheter og befolkningen for å oppnå tilstrekkelig motstandsdyktighet.»

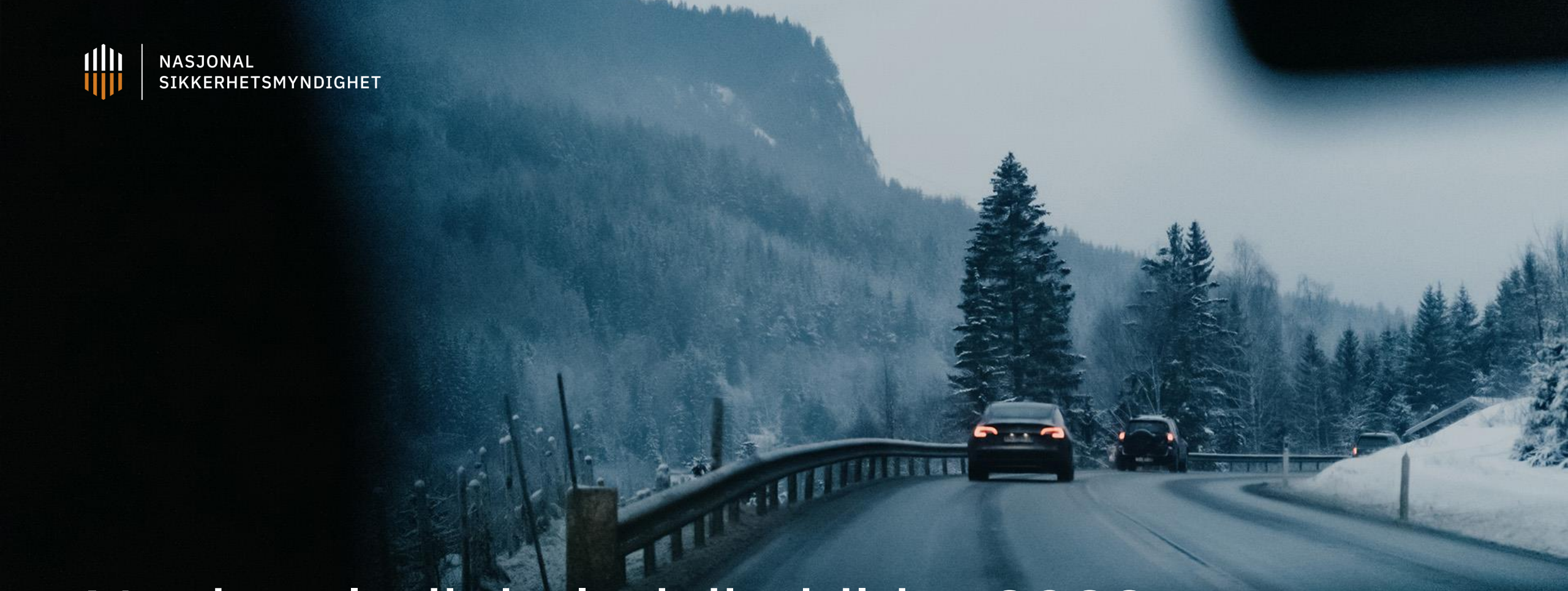
- «Norge er også avhengig av et sterkt internasjonalt samarbeid for å stå imot grenseoverskridende trusler som cyber- og påvirkningsoperasjoner.»

1. Infrastrukturen i Norge må beskyttes bedre
2. Vi må ha en felles situasjonsforståelse av trussel- og risikobildet
3. Den digitale motstandskraften i samfunnet må styrkes

Helhetlig sikring mot trusler



NASJONAL
SIKKERHETSMYNDIGHET



Nasjonalt digitalt risikobilde 2023

Teknologisk utvikling i en uforutsigbar verden

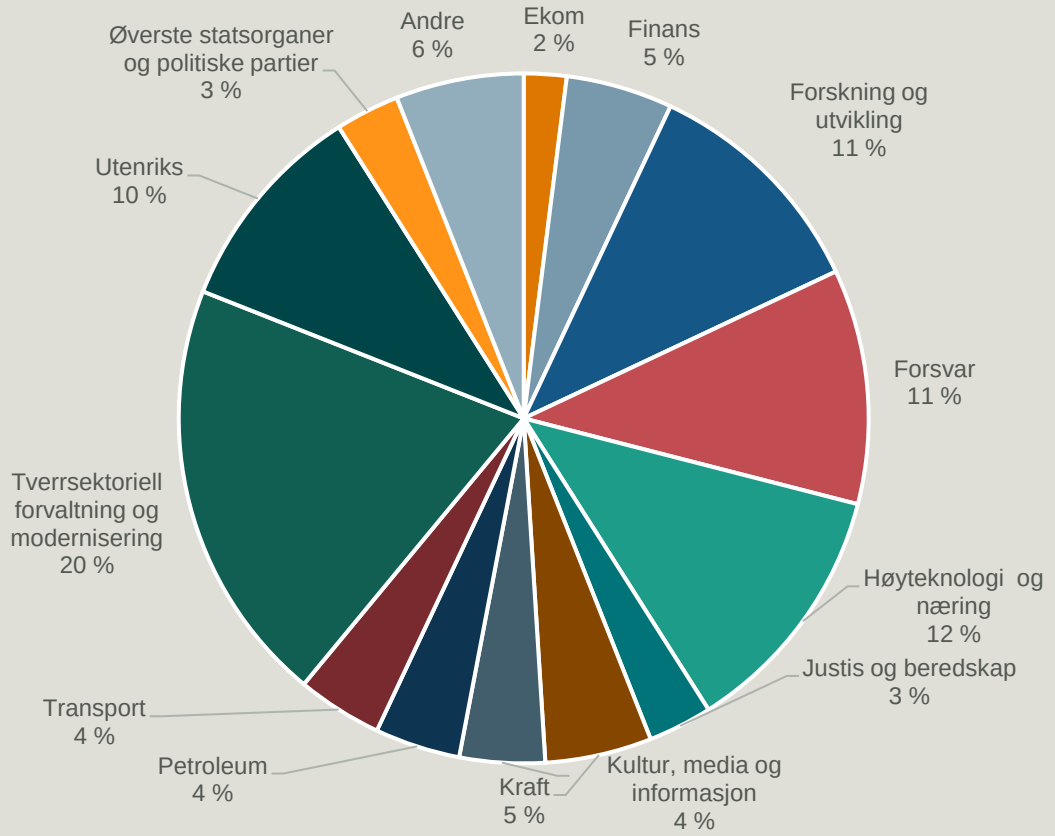
NSM

De store linjene

- **Krig i Europa**
- **Teknologi i rivende utvikling:**
  - Kunstig intelligens
  - Kvanteteknologi
- **Norges geopolitiske betydning forsterket**
  - Mottak av alliert støtte i lys av NATO-utvidelsen i nord
  - Norge en kritisk energileverandør til Europa

NSM

Disse sektorene rammes av cyberangrep



Økt trusselaktivitet	Høyest trusselaktivitet	Redusert trusselaktivitet
• Finans • Helse • Transport • Forsvarssektoren	• Høyteknologi og næring • Tverrsektoriell forvaltning	• Forskning og utvikling

Stadige bølger av tjenestenektangrep

- Antall tjenestenektangrep seksdoblet siden sommeren 2022, målt mot de tre foregående årene – til sammen

- Norges militære støtte til Ukraina oppgis ofte som motivasjon for angrepene

- Ikke fått alvorlige konsekvenser, men
  - angrepsformen er i utvikling
  - mer sofistikerte
  - vanskeligere å oppdage

- Angrepsfrekvensen anses av NSM som **en ny normal**

NSM

Cyberangrep blir stadig mer profesjonelt utført

- Sosial manipulasjon/*spear phishing* langt mer sofistikert enn tidligere

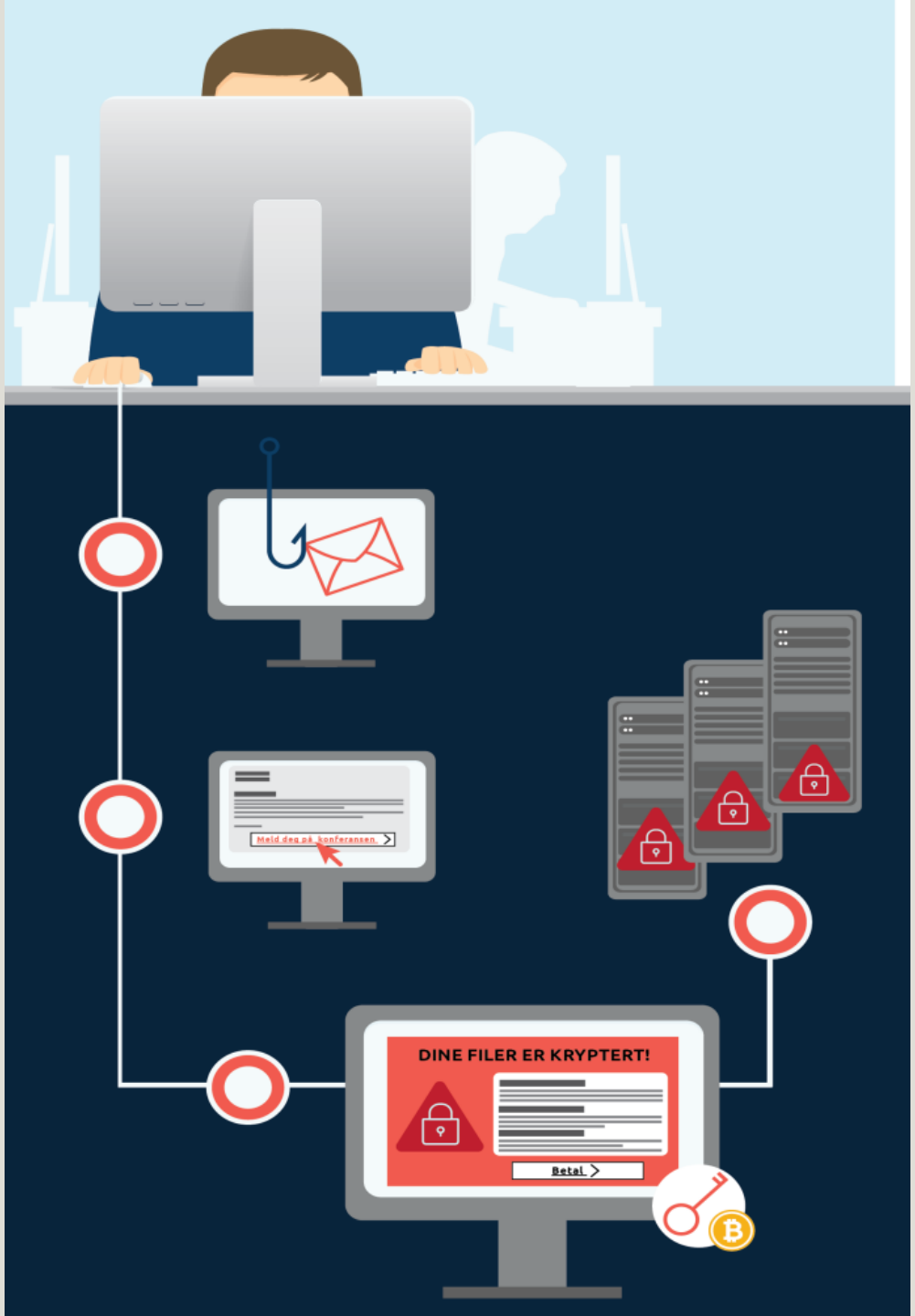
- Alle faser av og typer cyberangrep kan kjøpes, eksempelvis:
  - Sårbarhetsscanning
  - Stjålne brukernavn og passord
  - Løsepengeangrep
  - Tjenestenektangrep

- **Kunstig intelligens** vil ytterligere forsterke og akselerere denne utviklingen det neste året

NSM

Løsepengevirus

- Internasjonalt politisamarbeid om politietterforskning
- Lønnsomheten i løsepengebransjen har gått kraftig ned siden toppårene 2020 og 2021
- NSM har registrert færre løsepengeangrep mot norske virksomheter det siste året
- Dette betyr nødvendigvis ikke at risikoen avtar



NSM

Erfaringer fra NSMs inntrengingstester:

Ti sårbarheter i norske IKT-systemer

Rapporten deler erfaringer fra NSMs inntrengingstester over tre år. Testene avslører ti vanlige sårbarheter. Les hvilke sikkerhetstiltak som anbefales med utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet.

- Utdaterte systemer/programvare
- Dårlige passord
- Slurv med tilganger

Fem effektive tiltak mot dataangrep

1. Installer sikkerhetsoppdateringer så fort som mulig, og mest mulig automatisk
2. Ikke tildel administrasjonsrettigheter til sluttbrukere
3. Ikke tillat bruk av svake passord, og bruk multifaktorautentisering der det er mulig
4. Fas ut eldre IKT produkter
5. Tillat kun programvare som er godkjent av virksomheten eller enhetsleverandøren

nsm.no/5tiltak

Leverandørkjeder og uoversiktlighet

I og utenfor det digitale domenet

- *«Trusselaktører utnytter at funksjoner og infrastruktur i stat og samfunn henger sammen i uoversiktlige verdikjeder. Hendelser som tilsynelatende er rettet mot verdier ett sted i en verdikjede, kan i realiteten være konstruert for å ramme et egentlig mål et annet sted i verdikjeden.»*

  - NSMs sikkerhetsfaglige råd 2023

- Sårbare verdikjeder utnyttes!
  - Leverandører
  - Programvare

- Gjenstår arbeid med å kartlegge viktige samfunnsfunksjoner
  - Uoversiktlige verdikjeder gjør det vanskeligere å beskytte viktige nasjonale verdier

- Trusselaktørene leter etter sårbarheter hos leverandører

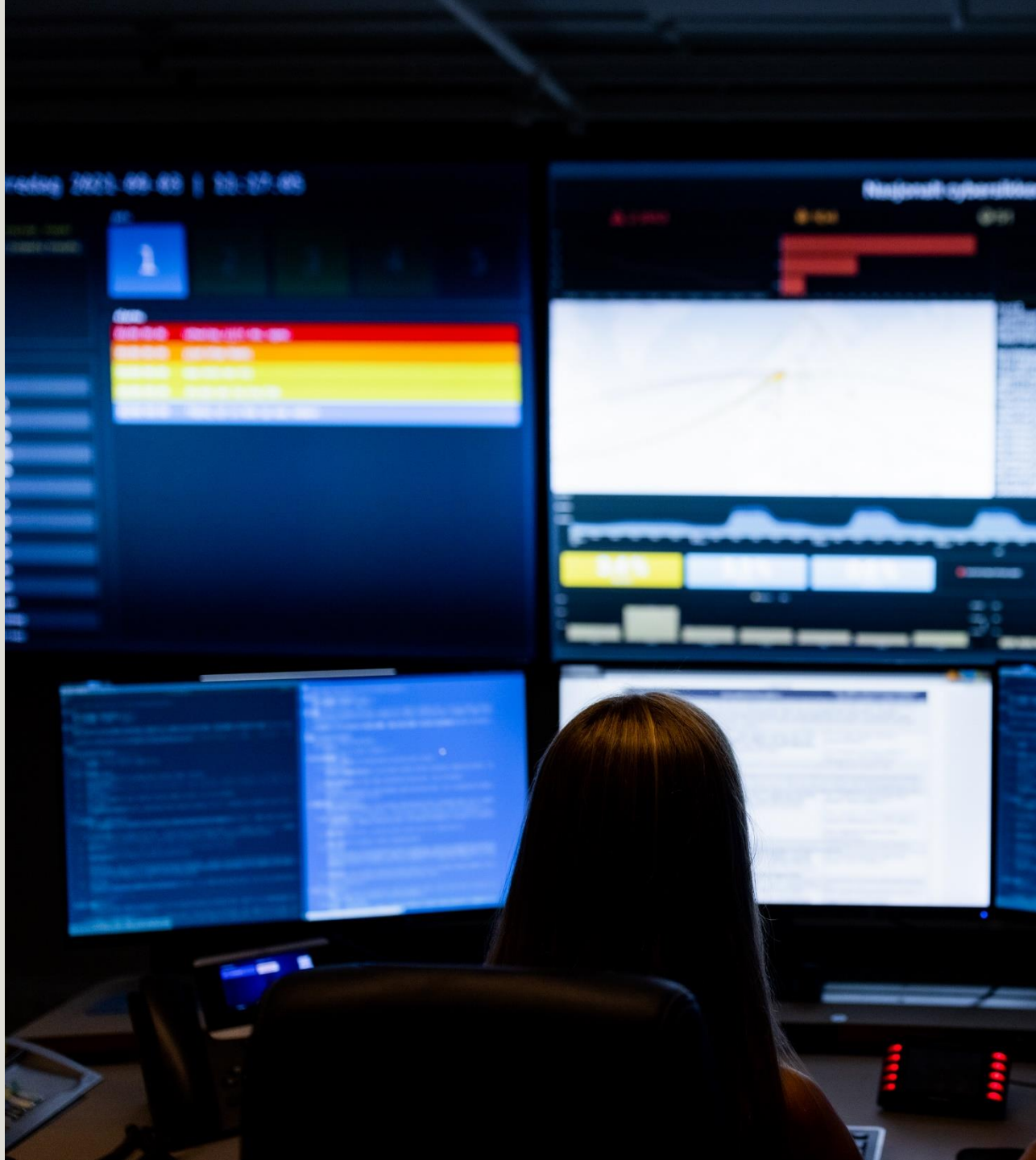
- Innsidetrusselen må tas på alvor

Foto: Ola Sverre Haugli / Forsvaret

NSM

Utvikling fremover

- Teknologi utvikling
  - Generelt: Gir nye muligheter og **nye sårbarheter**
  - Kunstig intelligens
  - Kryptografi - Kvanteakopalypsen
- Cyberverktøy som er tilpasningsdyktige til styring- og kontroll-systemer (OT)
  - Integrasjoner mot andre it systemer
  - Fjerntilganger
- Komplekst sårbarhetsbilde
  - Økende kompleksitet
  - Sårbarheter kan bli mer krevende å oppdage
    - lange digitale verdikjeder
  - Grunnleggende sikringstiltak



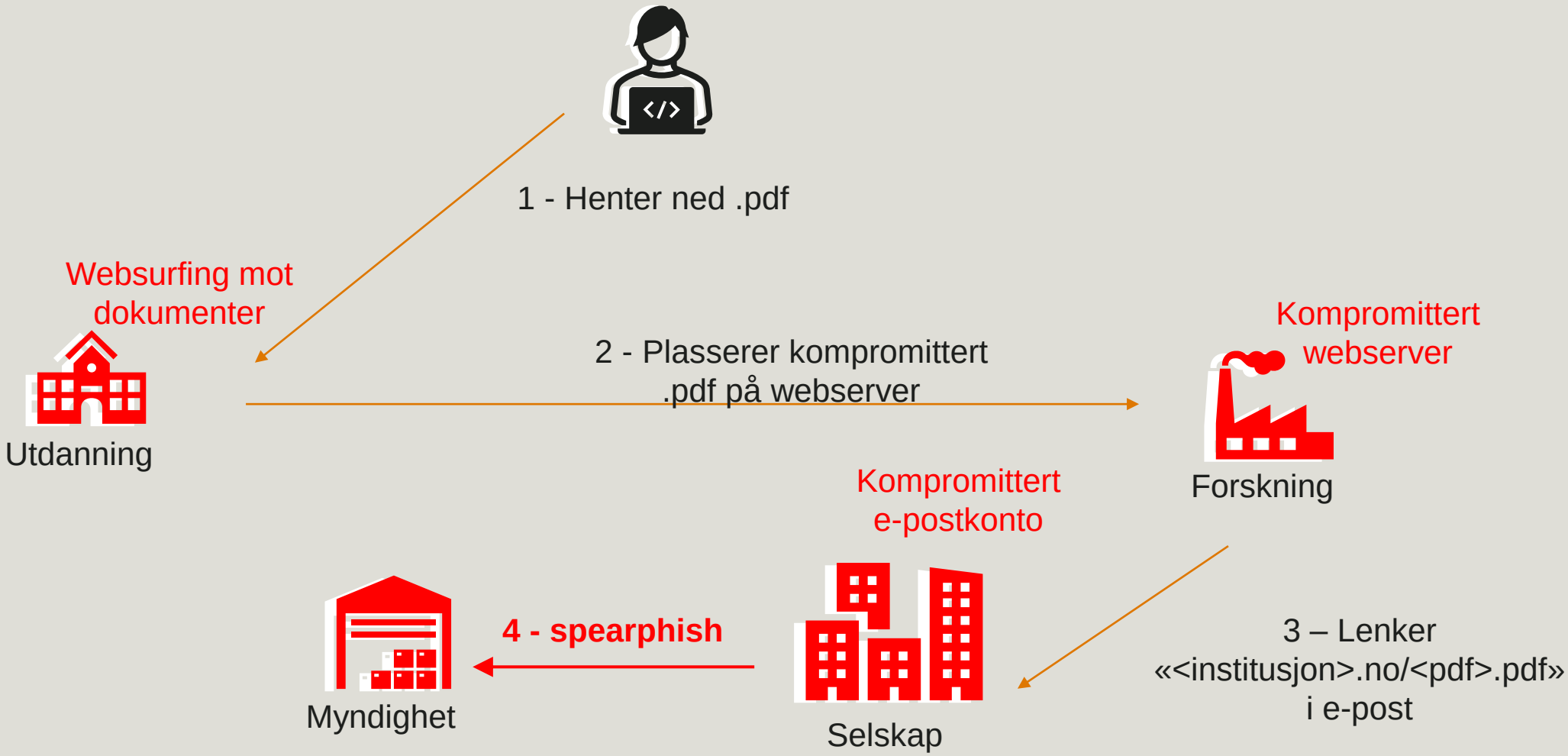
NSM

Et dynamisk situasjonsbilde

- Nye teknologier, sårbarheter og innbruddsmetoder vokser raskt
- Usikkerhet preger sikkerhetspolitikken globalt
- Gapet mellom trusselaktørenes kapabiliteter og demokratiske allierte lands sikkerhetsarbeid øker
- De neste årene vil kreve mer av oss, på statlig nivå, samfunnsnivå - og på individnivå

Slik kan din virksomhet bli rammet av en cyberoperasjon

Et eksempel



Oppsummering

- Taktskifte i internasjonal sikkerhetspolitikk
- Cyberangrep kan ramme alle!
  - Sammensatte trusler
- Behov for høyere beredskap og sikkerhetstiltak over tid
- Varsling
- Akseptabelt sikkerhetsnivå må speile risikobildet

Hjelp oss å bygge et nasjonalt situasjonsbilde

- **Varsler om uønskede hendelser er avgjørende for nasjonal situasjonsforståelse**
- **Lag rutiner for å varsle internt og til myndighetene**

www.nsm.no/varsle

NASJONAL
SIKKERHETSMYNDIGHET

Takk for oppmerksomheten!

Tlf. 67 86 40 00
www.nsm.no