Policynotat

Digital sikkerhet i drift og produksjon

Et samarbeid mellom:

NHO | Norsk Industri | NHO Elektro | abelia | Næringslivets sikkerhets-råd | Finans Norge

Innhold

Forord

Norge står i dag overfor et mer sammensatt og alvorlig digitalt trusselbilde enn på mange år. Digitaliseringen av drift og produksjon har styrket effektivitet og verdiskaping, men samtidig gjort virksomheter og samfunnskritiske funksjoner mer sårbare. Når IT og operasjonell teknologi (OT) smelter sammen, kan digitale hendelser få direkte konsekvenser for drift, leveranser og sikkerhet.

Dette policynotatet belyser disse utfordringene og peker på tiltak for å styrke digital robusthet i norsk næringsliv. Målet er å bidra til en mer helhetlig tilnærming til sikkerhet, hvor teknologi, kompetanse, regelverk og samarbeid ses i sammenheng.

Notatet retter seg mot både myndigheter og næringsliv, og tar utgangspunkt i behovet for økt koordinering, bedre informasjonsdeling og en tydeligere satsing på digital sikkerhet i hele verdikjeden. Et styrket samarbeid på tvers av sektorer vil være avgjørende for å møte et trusselbilde i rask endring.

Med vennlig hilsen

Ole Erik Almlid
Administrerende direktør,
NHO

Ove Guttormsen
Administrerende direktør,
NHO Elektro

Harald Solberg
Administrerende direktør,
Norsk Industri

Odin Johannessen
Direktør,
Næringslivets sikkerhetsråd (NSR)

Øystein Søreide
Administrerende direktør,
Abelia

Kari Olrud Moen
Administrerende direktør,
Finans Norge

Sammendrag

Det digitale trusselbildet er blitt mer alvorlig og komplekst. Skillet mellom digitale og fysiske systemer viskes i økende grad ut, og angrep kan få direkte konsekvenser for drift, produksjon og kritisk infrastruktur. Samtidig skaper økt bruk av sky, sensorer og fjernstyring nye sårbarheter, i mange tilfeller forsterket av manglende oversikt, kompetanse og grunnsikring. Fremveksten av avanserte KI-modeller som reduserer tiden fra sårbarhet til angrep, forsterker dette trusselbildet ytterligere, og øker risikoen for hyppigere og mer alvorlige hendelser.

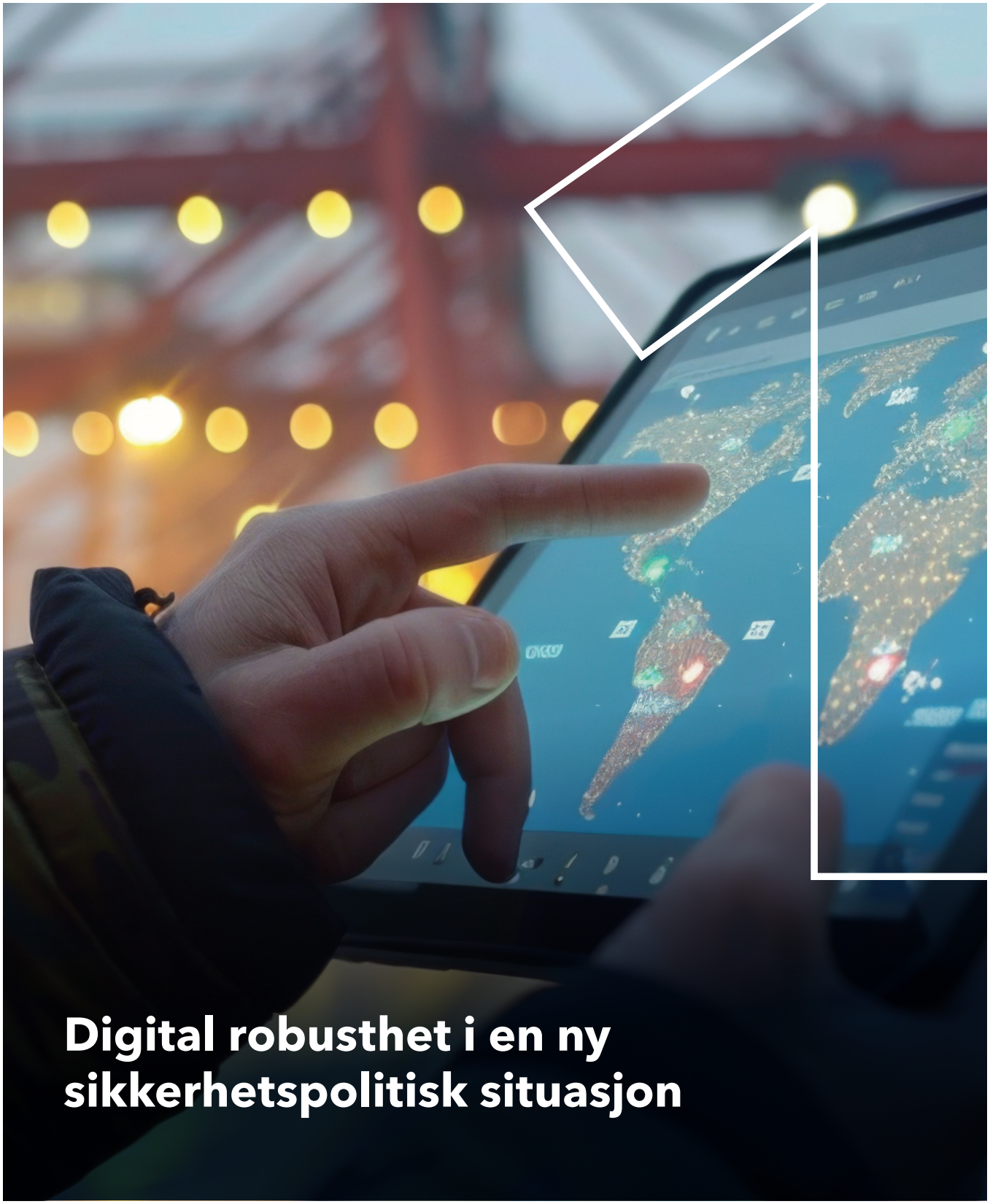
Utfordringsbildet forsterkes også av en for fragmentert samhandling og et komplekst regelverk. Samtidig er det en risiko for at Norge blir hengende etter sammenlignet med EU og andre land, blant annet som følge av et etterslep i implementering av nye regler. Dette kan gi både sikkerhetsmessige svakheter og konkurranseulemper for norsk næringsliv. Samlet svekker dette evnen til å forebygge og håndtere digitale hendelser på tvers av sektorer og verdikjeder.

Samtidig gir digital sikkerhet store muligheter. Virksomheter som bygger robusthet og kan dokumentere sikkerhetsmodenhet, vil stå sterkere både i konkurransen og i møte med økende krav fra marked og myndigheter. Dette handler også om å sikre vilkårene for innovasjon som gjør det mulig å utvikle hele verdikjeder og utløse nødvendige investeringer, samt unngå at Norge sakker akterut i et stadig mer konkurransepreget landskap.

Med dette som bakteppe drøfter dette notatet sentrale utfordringer og trusler, og peker på behovet for et koordinert løft for å styrke digital robusthet gjennom følgende tiltak:

- Bedre informasjonsdeling gjennom mer konkret og målrettet utveksling av trusselinformasjon, samt bedre arenaer og tryggere mekanismer for samhandling
- Mer samordnede tilsyn, harmonisering av regelverk, tydeligere ansvarsdeling og redusert rapporteringsbyrde
- Styrking av kompetansen gjennom et løft i utdanning, etter- og videreutdanning og praksisnær opplæring, særlig i grensesnittet mellom IT og OT (operasjonell teknologi)
- Økt bruk av offentlige anskaffelser til å stille tydelige og gjennomførbare krav som driver frem bedre sikkerhet i leverandørkjeder
- Økt satsing på anvendt forskning, testarenaer og samarbeid mellom industri, akademia og forsvar
- Tettere kobling til europapolitikken gjennom å følge opp og påvirke EU-regelverk for å sikre like vilkår og unngå etterslep
- Økt vektlegging av digital sikkerhet i totalberedskapen

Et gjennomgående budskap er at digital sikkerhet ikke kan håndteres isolert, men må integreres i virksomheters kjerneaktiviteter, i verdikjeder og i samspillet mellom sivile og militære aktører. Når trusselaktørene samarbeider og opererer på tvers av grenser, må også innsatsen for å møte dem bygge på et forsterket og forpliktende samarbeid mellom myndigheter og næringsliv.



Digital robusthet i en ny sikkerhetspolitisk situasjon

Vi opererer i dag i et risikobilde som er mer komplekst enn på flere tiår. Skillet mellom krig og fred er blitt mer uklart, og teknologiutviklingen går så raskt at grensene mellom sivil og militær produksjon mer og mer viskes ut. For norsk næringsliv byr dette på utfordringer, samtidig som det skaper muligheter.

Digitaliseringen har koblet sammen systemer som tidligere var isolerte. I dag er det ikke bare IT-systemer som utsettes for digitale trusler, men også samfunnets fysiske infrastruktur og kritiske verdikjeder. Operasjonell teknologi (OT) er nå en del av det digitale domenet og styrer blant annet produksjonslinjer, vannforsyning, energiproduksjon og transport- og telekommunikasjon. Med dette har vi fått en ny og voksende sårbarhetsflate, hvor digitale og fysiske prosesser er tett sammenvevde.

Dette forsterker behovet for en helhetlig tilnærming til digital sikkerhet, hvor informasjonssystemer og operasjonell teknologi håndteres helhetlig. Sikkerhetstiltak må omfatte både digitale og fysiske prosesser, og ta høyde for at kompromittering av ett domene kan få umiddelbare konsekvenser for det andre.

De fleste angrepene er fortsatt rettet mot IT-systemene, men mangelen på oversikt over koblinger og avhengigheter mellom IT og OT skaper utfordringer. Når grensene mellom domenene blir mindre tydelig, øker risikoen for at et tilsynelatende begrenset angrep kan få store følger.

Når de digitale systemene kompromitteres, kan konsekvensene bli produksjonsstans, tap av kontroll og fare for liv og helse i ytterste konsekvens. Et godt eksempel er cyberangrepet som lammet både IT systemer og den operasjonelle teknologien til Jaguar Landrover høsten 2025. Angrepet slo ut produksjonslinjene og stanset fabrikkdriften, noe som påførte selskapet store økonomiske tap og demonstrerte hvordan digitale angrep kan få umiddelbare fysiske konsekvenser for industrien.

NHOs rapport ***Veien til vekst*** peker på sikkerhet og beredskap som avgjørende for norsk konkurransekraft. Trygghet bygger tillit i verdikjeder, og virksomheter som kan dokumentere robusthet står sterkt. Samtidig er denne tilliten sårbar. Mange virksomheter stoler i stor grad på leverandørene sine, men uten alltid å verifisere hvilke sikkerhetsmekanismer som faktisk er på plass. Når enhver aktør kan bli utsatt for angrep og spre konsekvensene videre i verdikjeden, blir manglende kontroll en direkte risiko. Derfor blir det viktig at virksomheter kan dokumentere reell sikkerhetsmodenhet og robusthet.

Digital sikkerhet kan også være et strategisk fortrinn. Etterspørselen vokser raskt etter teknologi, kompetanse og løsninger som styrker forsvar og beredskap. Dette skaper igjen grunnlag for vekst. Digital sikkerhet stryker således ikke bare motstandskraften, men også konkurransekraften som igjen kan gi tilgang til markeder, partnerskap og investeringer.

Samtidig må veksten bygge på realistisk modenhet. Kompetanse, løsninger og teknologi må tilpasses nivået virksomhetene faktisk befinner seg på. Selv når gode sikkerhetsløsninger finnes, blir de ofte ikke tatt i bruk eller de blir satt opp feil som følge av manglende kompetanse.

Mange virksomheter har tilgang til verktøy som:

- Multifaktorautentisering for ekstra bekreftelse ved innlogging
- Segmentering for oppdeling av nettverk for å begrense spredning
- Sikkerhetsoppdateringer som tetter kjente sårbarheter
- Overvåkingssystemer som oppdager og varsler om angrep

Utfordringen er at mange av disse blir stående uaktivert fordi de oppleves som kompliserte eller forstyrrende for drift. I andre tilfeller tas løsningene i bruk, men konfigureres feil, og skaper en falsk trygghet. Feilkonfigurasjoner er i dag en av de vanligste årsakene til sikkerhetshendelser, og viser at teknologi alene ikke er nok. Det krever kompetanse og gode rutiner for at sikkerhetsløsninger faktisk skal virke etter hensikten.

De siste årene har vi sett en søken etter sofistikerte verktøy trigget av digitale angrep, men som ofte ender i piloter og konsepter uten varig effekt fordi grunnsikringen ikke er på plass. Skal digital sikkerhet faktisk gi effekt, må virksomheter først etablere en solid sikkerhetsplattform.

Med dette som utgangspunkt drøfter policynotatet, utarbeidet av NHO, Abelia, NHO Elektro, Norsk Industri, Næringslivets Sikkerhetsråd (NSR) og Finans Norge, sentrale digitale utfordringer og trusler. Notatet peker videre på nødven-dige tiltak for å sikre digital robusthet som en strategisk forutsetning og et mulighetsrom, særlig i møte med nye sårbarheter i grenseflaten mellom IT og OT.

Den sterke sikkerhetskulturen som gjennom mange år er utviklet i Norge, blant annet innen olje- og gassindustrien, kan være til inspirasjon i møte med de økte utfordringene. Olje og gassnæringen har utviklet denne kulturen gjennom mange år, med tydelige rutiner, risikoforståelse og kontinuerlig læring. Erfaringen viser at høy sikkerhet skapes gjennom kultur og ledelse, ikke bare teknologi. Slike prinsipper kan gi et viktig løft også i andre sektorer som nå står overfor økende digitale trusler.

IT og OT: Forskjeller, likheter og felles risiko

Informasjonsteknologi (IT) og operasjonell teknologi (OT) har ulike roller, men må sees i sammenheng. IT handler om informasjon, kontorstøtte og administrative systemer, der konfidensialitet og dataintegritet er viktigst. OT styrer fysiske prosesser som ventiler, motorer, varme, fremdrift og elektrisitet der tilgjengelighet og sikker drift er avgjørende.

I takt med digitaliseringen er det i praksis få avkoblede, «maskinelle» prosesser igjen. IT og OT er tett integrert, og endringer i ett system påvirker ofte det andre. Tradisjonelt har IT-systemer kunnet tåle hyppige oppdateringer og omstarter, mens OT-systemer har vært mer sensitive for avbrudd. I dag er denne forskjellen mindre tydelig, da stadig flere OT-systemer er avhengige av kontinuerlig digital støtte og oppdateringer må planlegges helhetlig for å unngå driftsforstyrrelser og tap av verdier. Samtidig har IT- og OT-personell ofte ulik bakgrunn og ulike prioriteringer, noe som understreker behovet for tverrfaglig samarbeid og felles forståelse for risiko og sikkerhet.

Både IT og OT er sårbare for angrep, og begge er kritiske for virksomhetens drift. Når disse nå er koblet sammen, øker risikoen for at digitale trusler kan få fysiske konsekvenser. Et kompromittert damanlegg og nettstasjon kan kutte strøm til et sykehus, en sabotert komponent kan lamme et fartøy, og fjernstyrte systemer kan sette liv i fare.

Dette viser at digital sikkerhet må tenkes helhetlig fra start. Sikkerhet kan ikke isoleres til IT alene, men må omfatte de fysiske produksjonsmiljøene inkludert OT.

Og begge miljøene må lære av hverandre. IT miljøer har ofte en mer moden informasjonssikkerhetskultur. OT kan hente mye fra disse miljøenes praksis for hendelseshåndtering, tilgangsstyring og sikkerhetsrammeverk. OT miljøer har på sin side tydelig avviksrapportering, god dokumentasjon, streng segmentering og solid fysisk sikkerhet. Når IT og OT smelter sammen, blir denne gjensidige læringen avgjørende for en helhetlig sikkerhetskultur.

Utfordringer og trusselvurderinger

Digitale sikkerhetsutfordringer

En av de største utfordringene for digital sikkerhet i grenseflaten IT og OT er å balansere beskyttelse av systemer med behovet for kontinuerlig drift og høy ytelse. OT-systemene har tradisjonelt vært isolert, designet for autonom drift og med begrenset eksponering. Effektivisering og fjernstyring har imidlertid ført til økende oppkobling mot internett og sky.

På oppdrag fra NVE har SINTEF vist hvordan driftskontrollsystemer i kritisk infrastruktur i økende grad blir avhengige av slike løsninger (SINTEF, 2025). Dette gir muligheter, men også økt sårbarheter, særlig fordi mange OT-systemer ikke er bygget for oppkobling til internett og sky, og mangler grunnleggende sikkerhetsmekanismer som autentisering eller kryptering.

Når styringssystemer og digitale modeller flyttes til sky og kobles tettere til fysisk utstyr skapes gevinster som sanntidsdata og fjernstyring, men også nye inngangspunkter for trusselaktører. Den økte integrasjon gjør det derfor avgjørende å sikre dataflyt og grensesnitt.

Sensorer og tilkobling gjør at stadig flere maskiner og kjøretøy, fra gravemaskiner til autonome systemer, kontinuerlig samler inn og sender data. Dette gir store gevinster for drift og vedlikehold, men betyr også at utstyret fungerer som små datamaskiner med kameraer, mikrofoner og posisjonssporing. Dersom slike enheter ikke sikres godt nok, kan de utsettes for kartlegging og spionasje.

Mange OT-system er dessuten eldre, spesialtilpassede og utviklet for kontinuerlig drift. Frykt for nedetid gjør at virksomheter kvier seg for å oppgraderinger, samtidig som leverandøravhengighet ofte begrenser handlingsrommet. Ekstern bistand kan være kostbart, og fjerntilgang fra leverandører kan introdusere nye sårbarheter, særlig der dette ikke tidligere har vært brukt.

Fjerntilgang er samtidig en sentral angrepsvei i OT miljøer. Industrielle systemer er ofte avhengige av eksterne tilganger via Remote Desktop, VPN eller proprietære løsninger. Disse er ikke alltid tilstrekkelig sikret, med f.eks. multi-faktorautentisering og tidsbegresning, og kan gi direkte tilgang til kritiske kontrollsystemer. Når IT og OT integreres tettere, blir sikker håndtering av slik tilgang avgjørende for å hindre fysiske konsekvenser av digitale angrep.

Nye tjenestemodeller kan også skape uforutsette sårbarheter. Når virksomheter kjøper utstyr som en tjeneste, følger det ofte ferdig oppsatte kommunikasjonsløsninger, som 4G rutere eller leverandørstyrt fjernaksess. Disse kan kobles opp utenfor virksomhetens egne sikkerhetskontroller og etablere skulte innganger til produksjonsmiljø dersom oversikten er mangelfull.

Selv om nytt utstyr løser deler av utfordringene, har mange virksomheter fortsatt omfattende «legacy»-systemer som ikke er tilpasset dagens krav til oppkobling og sikkerhet. Disse mangler ofte mekanismer for oppdatering, logging og segmentering, og er krevende å oppgradere uten risiko for driftsavbrudd eller tap av garantier. Integrasjonen med moderne løsninger øker derfor den samlede angrepsflaten.

Konsekvensene er at digitale angrep i større grad kan få direkte fysiske effekter. Målet kan være å stjele teknologi, drive utpressing, sabotere eller påvirke samfunnsfunksjoner. Trusselaktørene spenner fra kriminelle grupper til statlige støttede aktører, og angrep kan inngå i bredere hybride operasjoner.

Et skjerpet digitalt trusselbilde

Ifølge ENISA (EUs byrå for cybersikkerhet) retter én av fem digitale trusler seg mot virksomheters drift og produksjon (2025). Stadig flere norske virksomheter og institusjoner har de siste årene blitt utsatt for eller forsøkt utsatt for angrep fra fiendtlige aktører. Kripos vurderer det som sannsynlig at angrep på operasjonell teknologi vil inntreffe, med konsekvenser for forsyningskjeder eller kritisk infrastruktur. Nasjonal sikkerhetsmyndighet (NSM) har registrert cyberhendelser mot så å si alle samfunnssektorer.

Norge har betydelige verdier knyttet til fysiske prosesser og infrastruktur. Dette gjelder ikke minst innen energi. Den geopolitiske situasjonen har styrket vår rolle som strategisk leverandør av gass og andre ressurser, er noe som øker eksponering og sårbarheten. Hendelser som kabelbrudd i 2021 (Institute of Marine Research), 2022 (NUPI) og datainnbrudd på damanlegg 2024 (Barents Observer) viser at dette ikke enkeltstående hendelser, men del av et mønster.

En rapport fra cybersikkerhetsselskapet Check Point viser en økning på 44 pst. i cyberangrep (2025), særlig innen løsepengevirus. Slike angrep rammer samfunnskritiske funksjoner som fabrikker, sykehus, matforsyning, vann og energi. Disse systemene er avhengige av OT-komponenter som styrer ventiler, varme, motorer og sensorer.

Skytjenester kan være lokalisert i andre jurisdiksjoner og avhengige av infrastruktur som sjøkabler. Ved brudd kan tilgang til datasentre og styringssystemer som er kritiske for drift og beredskap svekkes. Selv om trafikk kan omdirigeres via alternative kalbelruter, synliggjør dette hvor sårbare og komplekse verdikjedene er. En sensor i et vannverk kan i praksis være koblet til et datasenter på et annet kontinent, noe som illustrerer bredden i dagens sårbarhetsbilde.

Fremveksten av avanserte KI-modeller markerer et tydelig skifte i trusselbildet. Evnen til å identifisere og utnytte sårbarheter i stor skala kan nå automatiseres, noe som reduserer tiden fra sårbarhet til angrep, og øker sannsynligheten for hyppigere og mer alvorlige hendelser.

Kompetanseutfordringer innen digital sikkerhet

Samtidig som det digitale trusselbildet forverres, mangler norsk næringsliv kompetansen som trengs for å håndtere risikoen. I NHOs kompetansebarometer ble bedriftene spurt om innen hvilke områder de har et udekket behov for IKT-kompetanse i dag. Når det gjelder spesialisert IKT-kompetanse, er det høyest andel som har et udekket behov innen digital sikkerhet. Men også når det gjelder generell IKT-kompetanse, er digital sikkerhet blant de områdene med høyest udekket behov (2024).

Norge står overfor betydelige rekrutteringsutfordringer innen realfag, tekniske fag og IKT. Dette skyldes blant annet:

- få søkere til teknologiutdanninger
- lav rekruttering til realfag i videregående skole
- svak rekruttering til lærerutdanninger i realfag
- begrensede insentiver for utenlandske kandidater til å bli i Norge

Dette svekker tilfanget av kompetanse som er kritisk for digital sikkerhet og bidrar til å skape en grunnleggende utfordring for Norges digitale beredskap.

Mange av de mest etterspurte yrkene innen digital sikkerhet, industriell teknologi og programmering krever solid realfagskompetanse. Når få elever velger fordypning i realfag på videregående, blir tilfanget av studenter som kan gå videre til teknologiske utdanninger mindre. Dette forplanter seg videre til arbeidslivet, hvor etterspørselen etter IKT kompetanse, særlig innen sikkerhet og OT, vokser langt raskere enn tilgangen. Resultatet er et vedvarende kompetansegap som gjør det vanskeligere å sikre drift, utvikle ny teknologi og håndtere et mer komplekst trusselbilde.
Denne utfordringen forsterkes av KPMGs topplederrapport for 2026, hvor teknologisk utvikling og sikkerhet trekkes frem som blant annet de mest presserende ledertemaene. Mange toppledere uttrykker bekymring for om virksomhetene har tilstrekkelig kompetanse for å møte både digital omstilling og økende sikkerhetsutfordringer. Halvparten opplever ikke at deres virksomhet er en del av totalberedskapen, og kun 6 pst mener bedriften i stor grad er rustet til å møte digitale trusler.

Tilgangen på kvalifisert arbeidskraft er særlig begrenset innen industriell OT-sikkerhet, hvor det kreves både operasjonell erfaring og dyp sikkerhetskompetanse. Norge har kun et fåtall svært erfarne ingeniører som de siste 5–8 årene har fått nødvendig opplæring innen sikkerhet,

og industrielle virksomheter er i stor grad avhengige av nettopp disse nøkkelpersonene. Samtidig er kompetanse etterspurt internasjonalt, og sektorer som energi, vann og helse konkurrerer om de samme ressursene. Uten konkurransedyktige vilkår og tydelige karriereveier risikerer Norge å miste kritisk kompetanse.

Mangelen på tverrfaglig kompetanse gjør virksomheter mer sårbare. I situasjoner med cyberrisiko er man ofte helt avhengig av spesialister, og utfordringen blir særlig tydelig når disse ikke er tilgjengelige. Selv om det utdannes flere eksperter, tar det tid før de er operative, og tilgangen er fortsatt utilstrekkelig. Dette svekker både evnen til å sikre kritisk infrastruktur og til å ta i bruk ny teknologi på en trygg måte.

Fragmentert samhandling i sikkerhetsarbeidet

I tillegg til kompetansemangel er samhandlingen på digital sikkerhet for fragmentert. Samspillet oppleves ofte som teknisk og vanskelig å navigere, og aktører utvikler i stor grad egne løsninger og beredskapsplaner. Internt preges mange virksomheter av siloer, særlig mellom IT- og OT miljøene, som vurderer risiko og prioriteringer ulikt.

Dette skaper igjen et krevende utgangspunkt for helhetlig sikkerhetsarbeid. Ulik modenhet forsterker utfordringen, særlig for små og mellomstore virksomheter. Selv aktører med avansert beredskap jobber ofte i siloer i det daglige, og tiltak for bedre samhandling begrenses gjerne til øvelser.

Det finnes mange initiativ, men de er ikke alltid godt koordinert. Samarbeid må skje på tvers av flere dimensjoner:

- mellom myndigheter og næringsliv
- mellom store aktører i kritisk infrastruktur
- mellom store og små virksomheter
- på tvers av sektorer

Når aktører har ulike roller, ansvar og modenhet, blir det krevende å etablere en felles retning.

Konsekvensen blir mangelfull deling av trussel- og hendelsesdata, både mellom aktører og internt i virksomheter. Dette svekker situasjonsforståelsen, gjør responsen mindre effektiv og hemmer utviklingen av robuste sikkerhetsløsninger.

Anbefalinger – tiltak for å styrke den digitale robustheten

Når digitale trusler tiltar, vokser behovet for tiltak og løsninger som ivaretar hele verdikjeden. I det følgende skisseres viktige aksjonsområder fremover hvor myndighetene, virkemiddelapparatet og næringslivet har ulike roller, men også har et felles mål om å styrke den digitale robustheten og gjør den til en integrert del av den norske totalberedskapen.

Bedre informasjonsdeling og situasjonsforståelse

Mye av sikkerhetsinformasjon deles i dag for generelt eller holdes tilbake. For å styrke digitale robusthet må informasjon i økende grad avgraderes og punktgraderes der det er mulig, kombinert med gode rutiner for tilgangsstyring. Når informasjon gjøres konkret og tilpasset mottaker, kan virksomheter bruke den direkte i egne risikovurderinger. Dette forutsetter tydeligere føringer fra NSM, DSB og departementene, samt målrettet deling fra sektormyndigheter.

Det er også behov for løsninger og insentiver som senker terskelen for at næringslivet selv kan dele relevant informasjon tilbake til myndigheter og CERT miljøer på en enkel og trygg måte. Dette forutsetter etablerte rutiner for sikker deling og en kultur der virksomheter ikke frykter negative konsekvenser ved å dele.

Myndighetenes kommunikasjon må være tydelig og målrettet. Dette trenger ikke nødvendigvis å være til alle bedrifter direkte, men gjennom sektorvise CERT miljøer, bransjeorganisasjoner og relevante tilsyn som kan formidle konkret og handlingsrettet informasjon til virksomhetene.

Videre må det også etableres bedre løsninger for samhandling på gradert nivå, slik at virksomheter med sikkerhetsklarert personell får tilgang til mer detaljert trussel- og sikkerhetsinformasjon. Klareringsprosessene må samtidig være tilpasset dagens behov, slik at de ikke blir unødvendig tidkrevende eller ekskluderende for kritiske leverandørkjeder. Dette vil gjøre det lettere å koble nasjonale og sektorvise situasjonsbilder, samt gi næringslivet en mer presis forståelse av risiko.

Det er også behov for å styrke nasjonale samhandlingsarenaer. Regjeringen har foreslått økte midler til sikkerhets- og beredskapstiltak som en del av totalberedskapsmeldingen. Dette gir rom for å utvikle møteplasser hvor aktører kan drøfte hva endringer i trusselbildet betyr for ulike verdikjeder i kritisk infrastruktur.

Følgende arenaer bør videreutvikles og gjøres mer tilgjengelige:

- CERT-miljøer som håndterer hendelser og angrep
- sektorspesifikke fora som deler erfaring og koordinerer tiltak
- tverrsektorielle øvelser som tester samhandling og respons

Slike arenaer må fasiliteres i trygge rammer som legger til rette for åpen erfaringsdeling, for eksempel gjennom bruk av etablerte prinsipper som Chatham House regelen. Når dette kombineres med tilgang til gradert informasjon, styrkes både tillit, felles situasjonsforståelse og nasjonal beredskap.

Enklere og bedre samordnet regelverk, tilsyn og rapportering

Myndighetene må tydeliggjøre handlingsrommet i sikkerhetsregelverket og vise hvordan regelverket faktisk åpner for sikker informasjonsdeling. Samtidig må reglene samordnes for å unngå motstridende krav.

Kravene i følgende regelverk[1] må harmoniseres:

- CER om krav til robusthet i kritisk infrastruktur
- NIS1/NIS2 om krav til cybersikkerhet og hendelseshåndtering
- Cyber Resilience Act om sikkerhet i digitale produkter
- Digitalsikkerhetsloven om nasjonale krav til IKT-sikkerhet

Tilsynsmyndighetene må samarbeide tettere og rollene til sektortilsynene må klargjøres, særlig der virksomheter er underlagt flere tilsyn. I dag kan uklarhet om regelverk og ansvar gjøre at virksomheter utsetter nødvendige sikkerhetsinvesteringer.

Virksomheter risikerer også å måtte rapportere til flere organer, som sektortilsyn, NSM, Datatilsynet, NKOM og politiet. Dette er ressurskrevende og øker risikoen for at sensitiv informasjon kommer på avveie.

Den korte varslingsfristen ved alvorlige hendelser er viktig for god håndtering og læring, men forutsetter tydelig og koordinert rapportering. Dersom virksomheter må rapportere til flere instanser parallelt, øker kompleksiteten betydelig. Myndighetene bør derfor redusere rapporteringsbyrden og etablere et koordinert og brukervennlig system som tydeliggjør hvor, hvordan og hva som skal rapporteres.

[1] CER: EU forordning som skal styrke motstandsdyktigheten til kritiske samfunnsfunksjoner. NIS1: det første EU direktivet om nettverk og informasjonssikkerhet (2016) og NIS2: oppdatert og utvidet direktiv (2023) som stiller strengere krav til cybersikkerhet og rapportering. Cyber Resilience Act er et nytt EU-regelverk for cybersikkerhet i produkter med digitale elementer.

EU peker på et felles og kryptert varslingspunkt (single entry point) som effektivt tiltak for bedre beredskap, redusert byrde og bedre koordineringen. Dette vil både styrke beredskapen og forenkle håndteringen av alvorlige hendelser.

Nasjonale sikkerhetsstandarder må samtidig oppdateres løpende. NSMs grunnprinsipper er et godt utgangspunkt, men må tilpasses ny teknologi, nye trusler og OT-miljøer. Standardene må være levende dokumenter, med jevnlig og tydelig kommunikasjon om endring.

I en tid der også angripere bruker KI, handler sikkerhet like mye om samarbeid og handlekraft som teknologi. Med god grunnsikring kan KI bli et kraftfullt verktøy for å styrke sikkerheten.

Kompetanseløft for digital sikkerhet

Kompetanse på digital sikkerhet, særlig i sårbarhetsflatene mellom IT og OT krever mer enn tradisjonell IT-sikkerhet. Det krever en inngående forståelse av både digitale systemer og de fysiske prosessene de styrer.

Det udekkete kompetansebehovet, omtalt i kap. 2, understreker behovet for en målrettet satsing på utdanning, kompetanseutvikling og rekruttering. Uten et slikt løft risikerer både virksomheter og samfunnet å stå svakere i møte med stadig mer komplekse trusler. Dette forsterker behovet for:

- tidlig og praksisnær realfagsrekruttering
- tettere samarbeid mellom skole, næringsliv og UH-sektor
- flere alternative veier inn i ingeniørutdanninger
- tiltak for å beholde avansert kompetanse i landet

Regjeringens arbeid med ny strategi for realfag og teknologi er derfor positivt, men det er avgjørende at den faktisk øker rekrutteringen, både til utdanningene og til arbeidslivet, og utvikles i tett samarbeid med partene i arbeidslivet.

Det er behov for flere studieplasser og fagretninger innen industriell sikkerhet/OT-sikkerhet, med særlig vekt på yrkesfag og praktisk erfaring. Norge kan med fordel hente inspirasjon fra tyske Dual Studies programmer, som kombinerer utdanning med arbeidserfaring. Slike modeller gir bedre forståelse av teknologien i bruk og en raskere overgang fra teori til praksis, noe som er spesielt viktig i fag hvor driftsforståelse er avgjørende.

For å møte behovene må Kunnskapsdepartementet sikre at universiteter og høyskoler prioriterer studieplasser i tråd med arbeidslivets behov for STEM-kompetanse[2] og dokumenterte søkertall. Samtidig må forkurs og realfagskurs finansieres og styrkes slik at flere får en inngang til ingeniørutdanningene.

Et velfungerende system for livslang læring er avgjørende. Etter- og videreutdanning (EVU) innen digital sikkerhet bør være en integrert del av utdanningssektorens grunnoppdrag, i tråd med kompetansebehovsutvalget anbefaling. Det er behov for:

- fleksible EVU-tilbud
- relevante sertifiseringer i sektorer som energi, maritim, helse og industri
- oppdatering av kompetanse på hvordan digitale angrep påvirker operasjonelle systemer

I dag er denne typen videreutdanning ofte svært kostbar. Selv anerkjente kurs og sertifiseringer innen cybersikkerhet som SANS Institute, er derfor ofte utilgjengelige for mange virksomheter. Det er ikke mangel på fagstoff, men veiledning og praksisnær opplæring. Avansert sikkerhetsopplæring, særlig OT, bør derfor gjøres langt mer tilgjengelig, rimeligere og bedre tilpasset virksomheter med operasjonelt ansvaret. Dette kan løses gjennom en delt innsats hvor myndighetene bidrar med støtte til sertifiseringsløp og kursutvikling i kritiske sektorer, mens bransjene utvikler felles CERT-løsninger og praksisnære læringsarenaer.

[2] Science (naturfag) Technology (teknologi og ingeniørfag) Engineering (ingeniørfag og tekniske fag) Mathematics (matematikk og statistikk)

Praksisnære utdannings- og opplæringsløp bør kunne kombineres med arbeid. Det er særlig viktig å styrke tverrfaglige kompetanse hvor IT-sikkerhet kobler med prosesskontroll og automasjon, slik at både studenter og erfarne fagarbeidere kan bygge etterspurt spesialkompetanse. Dette krever samspill mellom myndigheter utdanningsinstitusjoner og næringsliv.

En slik satsing på utdanning, etter- og videreutdanning og praktisk trening vil redusere sårbarheter, styrke IT/OT-sikkerheten og samtidig gi norsk næringsliv et konkurransefortrinn i en verden hvor sikker drift er blitt en strategisk faktor.

Tydelige offentlige anskaffelser med krav til sikkerhet

Offentlige anskaffelser er et viktig virkemiddel for å styrke den digitale sikkerhet. Mange virksomheter etterlyser tydelige sikkerhetskrav fra innkjøpere og at sikkerhet verdsettes som integrert del av leveransen. Når sikkerhet inngår eksplisitt i konkurransegrunnlaget og det settes av midler til robuste løsninger, skapes insentiver for leverandører til å prioritere digital sikkerhet i utvikling og drift.

Den nye loven om offentlige anskaffelser gir økt handlingsrom til å stille krav som fremmer innovasjon der det etterspørres nye eller vesentlig endrede løsninger. Dette gjør det mulig å heve sikkerhetsnivået utover dagens standard, samtidig som markedet stimuleres til å utvikle bedre teknologier og arbeidsformer.

Myndighetene bør utarbeide standardiserte krav, veiledning og maler, slik at sikkerhet blir en naturlig del av kontrakter. I dag mangler mange virksomheter tydelige føringer for hvordan sikkerhetskrav skal formuleres, vurderes og følges opp. Uten slike standarder ender anskaffelser ofte opp med enten for svake krav eller krav som ikke treffer de faktiske behovene. En standardisering vil bidra til å profesjonalisere markedet, redusere risiko i leverandørkjeder og sikre at investeringer i digital sikkerhet faktisk gir effekt.

Det bør også innføres standardiserte sikkerhetsklausuler i offentlige kontrakter der det er relevant. Slike klausuler kan blant annet:

- stille minimumskrav til cybersikkerhet og OT-sikkerhet
- sikre kontinuerlig oppdatering og vedlikehold
- pålegge rapportering ved hendelser

Erfaringene fra NERC CIP standarden[3] i Nord-Amerika viser hvor galt det kan gå når kravene blir for rigide og omfattende, og dermed vanskelig å etterleve i praksis. Norge må starte med det grunnleggende og bygge krav som er både målrettede, gjennomførbare og forankret i reelle risikoer.

Klausulene kan også tydeliggjøre leverandørens ansvar for sikkerhet i hele verdikjeden, inkludert:

- krav til sikkerhetsrevisjoner
- oppdaterte systeminventarer
- responstider ved hendelser
- forpliktelser til å rette sårbarheter innen gitte tidsfrister
- krav til kontinuerlig modenhetsutvikling og kompetanseheving

Effekten av å innarbeide sikkerhetsklausuler i kontrakter vil være betydelig. Hvordan klausulene utformes avhenger blant annet av hvilken sektor det gjelder, samt av størrelse på bedrift og type kontrakt.

For å sikre at klausulene blir treffsikre og praktisk gjennomførbare, bør det offentlige involvere næringslivet i utviklingen av krav og standarder, eksempelvis gjennom dialogkonferanser eller generelle innspillsprosesser. Dette vil gi bedre grunnlag for realistiske krav og et mer forutsigbart rammeverk. Samtidig kan leverandører med høy

[3] NERC CIP er et sett med obligatoriske cybersikkerhets- og fysisk-sikkerhetsstandarder som skal beskytte den nordamerikanske kraftforsyningen som har vist mangel på internkontroll, forsinket tilgangsstyring og siloer.

sikkerhetsstandard oppnå et konkurransefortrinn, både nasjonalt og internasjonalt.

Økt bruk av innovative og førkommersielle anskaffelser er et viktig supplement. Gjennom prosesser som konkurranse med forhandling, innovasjonspartnerskap eller konkurransepreget dialog kan det offentlige utvikle løsninger i samarbeid med næringslivet uten å låse seg til eksisterende teknologi. Dette er særlig relevant innen digital sikkerhet, hvor behovene utvikler seg raskt og ofte ligger foran det kommersielle tilbudet.

Styrking av forskning og testmiljøer

Digital robusthet handler ikke lenger bare om beskyttelse. Den er i økende grad et strategisk fortrinn som kan åpne nye markeder, styrke tilliten hos internasjonale partnere og gjøre norske aktører mer attraktive for investeringer. Virksomheter som kan dokumentere høy sikkerhetsmodenhet, står sterkere i globale verdikjeder med stadig strengere krav.

Norge har samtidig et stort uutnyttet potensial innen dual use -teknologier, KI og autonomi. Mange norske bedrifter utvikler teknologi i verdensklasse, men møter barrierer i samarbeidet med Forsvaret. At droneselskaper avvises nasjonalt, samtidig som de får store kontrakter internasjonalt, illustrerer mangelen på et system som fanger opp, videreutvikler og beskytter denne kapasiteten. Konsekvensen er svekket verdiskaping og beredskap.

For å realisere dette verdiskapingspotensialet må den anvendte forskningen innen cybersikkerhet styrkes, særlig i skjæringspunktet mellom OT og digitale trusselaktører. Det er behov for mer kunnskap om hvordan sårbarheter og manipulasjon påvirker drift og produksjon. Dette forutsetter samarbeid mellom forskningsmiljøer, industri, akademia og forsvarssektoren.

[4] SFI (Sentre for forskningsdrevet innovasjon) finansierer langsiktige forskningssentre der næringsliv og akademia samarbeider om teknologiutvikling. IPN (Innovasjonsprosjekt i næringslivet) støtter bedrifters egne forsknings- og utviklingsprosjekter. KPN (Kompetanseprosjekt for næringslivet) finansierer forskningsprosjekter som bygger kompetanse på områder næringslivet trenger på lengre sikt.

Eksisterende virkemidler som SFI, IPN og KPN[4] bør i større grad rettes mot tematiske utlysninger, omprioritering av midler og sterkere samarbeid mellom industri, akademia og forsvarssektoren innen følgende områder:

- OT sikkerhet
- dual use teknologi
- avansert industriell digitalisering

Samtidig er det behov for nye ordninger, særlig knyttet til operative testmiljøer og deling av gradert informasjon. Operativ testing, dual use-vurderinger og støtte til pilotering og kvalifisering av OT-teknologi bør inngå i Forskningsrådets portefølje for forsvarsevne, sikkerhet og beredskap.

For å styrke kommersialiseringen av nye sikkerhetsløsninger må det etableres tydeligere insentiver som gjør det mer attraktivt for industrien å bidra i forskning, utvikling og testing. I enkelte sektorer, som olje- og gass, finnes allerede ordninger som støtter pilotering og kvalifisering av teknologi. Disse bør videreutvikles og utvides til andre næringer. I tillegg kan SIVAs katapulter og Forsvarets testsentre være aktuelle.

Tilgang til operative testmiljøer er særlig viktig. Slike arenaer gjør det mulig å simulere avanserte cyberangrep, teste respons og trene virksomheter på reelle hendelser. Dette gir praktisk erfaring og legger grunnlag for utvikling, validering og demonstrasjon av nye sikkerhetsløsninger. Samtidig kan gode testfasiliteter bidra til å posisjonere Norge i det voksende markedet for sikker industriell digitalisering.

Samarbeidet mellom forskning, akademia og næringsliv må videre styrkes. Forskningsmiljøene trenger tilgang til OT-data, trusselbilder og reelle hendelser for å utvikle kunnskap som svarer på industriens behov. Dette er avgjørende for innovasjon, utvikling av nye sikkerhetsløsninger og styrket kompetanse.

Det er også behov for nye samarbeidsstrukturer mellom Forsvaret, forskningsmiljøene og næringslivet. Det må etableres rammer for deling av gradert informasjon med sikkerhetsklarerte personer, samtidig som klareringsprosessen forenkles og effektiviseres. Det er viktig at Forskningsrådets portefølje for forsvarsevne, sikkerhet og beredskap får rammer som fremmer tettere sivilt-militært FoU-samarbeid.

Næringslivet er allerede en kritisk del av totalforsvaret. En betydelig andel av militær transport, satellittkommunikasjonen og digital infrastruktur leveres av private aktører. Dette er sivile systemer med avgjørende betydning for militære operasjoner. For å sikre tilgang i krise og krig må virksomheten være økonomisk bærekraftige i fredstid. Strategiske avtaler, industrisamarbeid og målrettet FoU politikk er derfor nødvendig.

Norge må utvikle en forsknings- og innovasjonspolitikk som utnytter teknologier med både sivil og militær verdi, uten å hemme innovasjon eller kompromittere sikkerhet.

Tettere kobling til Europapolitikken

Industrial Accelerator Act (IAA) forventes å bli et sentralt virkemiddel i EUs arbeid for å styrke det indre markedet og øke industriell konkurransekraft. Målet er å utvikle Europas industrielle base gjennom felles rammer for investeringer, produksjon og teknologiutvikling. Dette blir særlig viktig i lys av økende digitalisering av industrien, der stadig flere produkter og tjenester leveres med innebygd programvare og KI. Den økte programvareavhengigheten skaper nye sårbarheter, blant annet knyttet til ondsinnet aktivitet fra tredjeland, og forsterket av behovet for digital suverenitet og kontroll over kritisk teknologi og infrastruktur.

Et sentralt element i IAA er innføringen av European Preference- og Made in Europe kriterier, som skal gi europeisk produksjon fortrinn i offentlige anskaffelser og strategiske verdikjeder. At regelverket vurderes som EØS relevant, og at EØS-land inkluderes i opprinnelsesbestemmelsene, gir et godt utgangspunkt for norske bedrifter. Norsk industri kan dermed i prinsippet konkurrerer på lik linje med EU aktører. Samtidig er det usikkerhet knyttet til hvordan kriteriene utformes i praksis, og hvilke praktiske konsekvenser de vil få for markedsadgang, dokumentasjonskrav og konkurransevilkår for norske bedrifter.

Det er derfor avgjørende å følge utviklingen og sikre en koordinert nasjonal oppfølging. Lykkes Norge med å posisjonere seg i tide, kan norske bedrifter ikke bare kvalifisere under European Preference ordningene, men også styrke sin rolle i europeiske verdikjeder og få bedre tilgang til støtteordninger og partnerskap. Hvis ikke, risikerer vi at regelverket etableres uten norsk påvirkning, med svekket markedsadgang som resultat.

EU har også lansert flere initiativer for å styrke digital suverenitet, blant annet innen kunstig intelligens, kvanteteknologi og digital infrastruktur. For Norge er det viktig å være tett koblet på denne utviklingen gjennom EØS, og sikre bred involvering av næringslivet.

På regelsiden har digitalsikkerhetsloven, som bygger på NIS1 etablert tydelige krav til virksomheter med samfunnsviktige funksjoner. NIS2 vil utvide omfanget, skjerpe ledelsesansvaret og stille strengere krav til verdikjedesikkerhet. Direktivet må også ses i sammenheng med øvrige EU-regelverk som CER, Dora og utfasing av IKT-forskriften[5].

NIS2 vil bidra til tettere europeiske samarbeidet og innebære at norske virksomheter må oppfylle krav som vil gjelder internasjonale leveranser. Europapolitikken blir dermed en sentral del av det nasjonale sikkerhetsarbeidet.

Det er viktig at kravene til digital sikkerhet utformes risikobasert, pragmatisk og proporsjonal. Regelverket må ta hensyn til virksomhetenes ulike forutsetninger, slik at tiltakene gir reell effekt uten å svekke konkurransekraften. Tidlig involvering av næringslivet, god veiledning og tilgang til kompetanse vil være avgjørende for å sikre en balansert implementering.

[5] CER-direktivet angår kritiske enheters motstandsdyktighet. DORA gjelder finanssektoren og setter krav til digital operasjonell motstandskraft. IKT-forskriften, som fases ut, men med enkelte unntak.

For norsk næringsliv er det også viktig å redusere etterslepet i EØS-innlemmelsene. Mange rettsakter innen digitalisering er fortsatt utestående, noe som skaper en konkurranseulempe. NIS2-lovgrunnlaget er under arbeid, med forestående nasjonal høring.

I tillegg må Norge prioritere andre sentrale EU-regelverk, som:

- KI-forordningen for regulering av kunstig intelligens
- eIDAS 2.0 om digital identitet
- Digital Services Act (DSA) om plattformansvar
- Data Act om datadeling
- Chips Act om databrikker

Myndighetene må tidlig avklare nasjonale håndtering i samarbeid med næringslivet, samtidig som koordineringen på tvers av departement styrkes. Økt kapasitet og kompetanse i forvaltningen er nødvendig for å påvirke prosessene og sikre effektiv innlemmelse. Det er også viktig å unngå tredjelandsbehandling, og sikre like vilkår i EU-programmer.

KI-forordningen bygger på prinsippet om teknologi-nøytralitet, hvor risiko vurderes på lik linje med annen teknologi. Virksomheter må derfor løpende oppdatere risikovurderinger og interne retningslinjer i takt med teknologisk utvikling.

Økt vekt på digital sikkerhet i forsvar og totalberedskapen

Ny NATO forpliktelse, det såkalte 5 prosentmålet, innebærer at alle medlemsstater skal bruke minst 5 prosent av BNP på forsvarsrelaterte formål innen 2035. Av dette skal 1,5 prosent gå til sivil sektor som understøtter forsvarsevnen. I den nye langtidsplanen for forsvarssektoren fra mars 2026 fremheves styrket digital sikkerhet og bedre beskyttelse av kritisk infrastruktur som en sentral del av satsingen. For Norge betyr dette at investeringer i sivil beredskap må ses i sammenheng med næringslivets behov, og at det utvikles nasjonale initiativer for å beskytte operasjonell teknologi og kritisk infrastruktur.

Myndighetene må samtidig bidra til at investeringene understøtter bredere mål som styrket digital sikkerhet, mer robuste verdikjeder og økt konkurransekraft.

Etter hvert som forpliktelser fra EU og NATO implementeres i norsk lovverk og politikk, blir det avgjørende med en helhetlig tilnærming som binder sammen forsvar, beredskap og næringsliv.

Dette krever tidlig involvering av næringsliv i utredninger, planlegging og øvelser, slik at krav og løsninger utvikles i fellesskap. Det forutsetter også bedre koordinering på tvers av sektorer, en felles situasjonsforståelse samt tydelige rammer for sikker informasjonsdeling mellom offentlige og private aktører.

Styrket samhandling for økt digital robusthet

Skal vi lykkes med å bedre vår digitale robusthet, herunder redusere sårbarhetene i grensesnittet mellom IT og OT, må dialogen mellom myndigheter og virksomheter forsterkes. Det må bli enklere for virksomhetene å forstå hva som forventes, hva som kan deles og hvordan man kan få hjelp. Vi trenger et samarbeid der næringslivet opplever at det er en reel verdi å delta. Det forutsetter at myndighetene forenkler og tilpasser, samtidig som virksomhetene tar ansvar, deler erfaringer og bygger kompetanse.

Et styrket samarbeid gir økt redundans, bedre tilgang til en større kunnskapsbase og et mer solid beslutningsgrunnlag. Dette gjør det enklere å koordinere tiltak og reagere raskt når det trengs.

Når angriperne samarbeider, må vi gjøre det samme. Dette må skje gjennom et felles løft hvor kjernen er bedre samarbeid.

Et samarbeid mellom:

NHO | Norsk Industri | NHO Elektro | abelia | Næringslivets sikkerhets-råd | Finans Norge

Layout: NHO Design | Foto: Shutterstock, AdobeStock og iStock.