CYBERSIKKERHET – VEIKART FOR ET TRYGGERE NORGE

November 2025

Skrevet av
TEK Norge

Innhold

1. Innledning og strategiske sikkerhetsmål

Norge har de senere årene tatt høyde for en betydelig styrking av cybersikkerheten og totalberedskapen. I 2025 kom en rekke viktige grep på området. Totalberedskapsmeldingen, den første nasjonale sikkerhetsstrategien, en sikkerhetsplan for digital infrastruktur, et historisk forsvarsløft og implementeringen av digitalsikkerhetsloven. Slik har Norge lagt grunnlaget for en mer robust og motstandsdyktig digital infrastruktur.

Men det gjenstår mye, for vi ligger bak våre naboland og truslene øker for hver dag som går. Så tempoet må opp, koordineringen og samordningen mellom privat og offentlig sektor iverksettes, og beslutningene fattes. Vi har nok planer og utredninger – nå må vi handle!

Dette oppdaterte veikartet reflekterer de nye rammebetingelsene og bygger videre på de ti områdene TEK Norge identifiserte i 2023, men tilpasset dagens geopolitiske realiteter og nye regulatoriske landskap.

Norge står nå i en posisjon der vi kan bygge på eksisterende politiske beslutninger og etablerte finansieringsrammer for å bli et ledende land innen cybersikkerhet, med styrket motstandskraft og robusthet i digital infrastruktur.

TEK Norge har i det følgende et antall forslag til tiltak som skal underbygge vår utvikling og motstandskraft. Vi mener det er nødvendig å sette konkrete effektmål for de enkelte tiltak – samt å måle utvikling over tid. I tillegg ønsker vi en kultur med kontinuerlig benchmarking mot andre, slik at vi holder tritt med utviklingen. Teknologisk utvikling og politisk usikkerhet gir behov for en mye mer dynamisk tilnærming enn hva vi har vært vant til hittil når det gjelder både type tiltak, gradering av disse og ny tilnærming.

TEK Norge mener vi bør ha følgende overordnede, strategiske sikkerhetsmål for perioden 2025-2030:

1. Oppdatere nasjonal cybersikkerhetsstrategi innen første halvår 2026, med en økonomisk bindende handlingsplan basert på denne i løpet av 2027.
2. Bygge opp tettere cyber-samarbeid mellom de nordiske landene både operativt og strategisk, gjennom tettere løpende informasjonsdeling, felles øvelser og beredskapsplaner, og utvikling av felles situasjonsbilde.
3. Etablere forpliktende partnerskap og samarbeidsarenaer som gjør totalforsvaret i stand til effektivt å utnytte samlet cyberkompetanse og -kapasiteter på tvers av statlig, kommunal, privat og frivillig sektor.
4. Stimulere til økt innovasjontakt og motstandsdyktighet i næringslivet, eksempelvis gjennom økt antall cybersikkerhetspatenter og økt bruk av cyberforsikring.
5. Forbedret rapportering av sikkerhetshendelser basert på felles standarder, med målsetning om reelt og løpende oppdatert situasjonsbilde på cyberdomenet.
6. Norske bedrifters sikkerhetspraksis skal heves til nordisk gjennomsnitt på alle måleområder innen 2027, og myndigheter, kommuner og næringsliv ha redusert teknisk gjeld.
7. Hendelses- og krisehåndteringskapasitet i Norge forbedres til best i Norden innen 2030.

2. Strategi og nasjonalt lederskap

Til tross for Totalberedskapsmeldingen og digitaliseringsstrategien, viser TEK Norges "Nordisk Benchmark 2025" at Norge rangeres bak de andre nordiske landene. Norge scorer særlig dårlig på helhetlig system i forhold til våre naboland.

TEK Norge mener vi må adressere det dokumenterte etterslepet - det er ingen grunn til at Norge skal ligge bak andre nordiske land på cybersikkerhet. Vår cybersikkerhets-strategi må oppdateres snarest mulig, basert på identifiserte svakheter og det må implementeres en handlingsplan for å lukke gapet til nordiske naboer innen 2027.

Vi mener også at det bør forsterkes et nordisk samarbeid og læring, med systematisk benchmarking mot danske, svenske og finske standarder. Videre at det etableres nordisk kompetanseutveksling innen cybersikkerhets-strategi og -implementering, samtidig som det utvikles felles nordiske standarder som kan bidra til regional sikkerhet.

Det er også nødvendig med målrettet forbedring av svake områder, som å prioritere hendelses- og krisehåndtering der Norge scorer lavest, samt fortsatt styrke grunnleggende infrastruktur. Norge har en sårbar digital infrastruktur det er et langstrakt land med spredt bosetting og for få alternative kommunikasjonsruter, særlig nord for Trondheim. Norge må fortsatt øke bidraget til forskning og utvikling, med mål om for eksempel langt flere cybersikkerhetspatenter.

Nasjonalt er det også behov for tydeliggjøring av ulike aktørers roller og mandat, slik at ansvaret for koordinering og samordning av sivil digital sikkerhet er tydelig plassert på tvers av etater, samtidig som man tilrettelegger for bidrag fra næringslivet.

TEK Norges forslag til konkrete tiltak:

2.1 Revidert nasjonal cybersikkerhetsstrategi

- Norges nåværende overordnede strategi på cybersikkerhetsområdet er Nasjonal strategi for digital sikkerhet fra 2019. Etter den tid har vi bla nå senest fått Nasjonal sikkerhetsstrategi og regjeringens Nasjonale sikkerhetsplan for digital infrastruktur. Men vi mener det er nødvendig å ha en oppdatert helhetlig cyberstrategi som dekker alle samfunn-sektorer og nivåer. Cyberangrep, er og vil være, det mest sentrale virkemiddelet mot Norge og norsk virksomhet i fredstid, for både statlige aktører, deres proxys og kriminelle.
- Som del av denne strategien bør det foretas en kartlegging av “nå-situasjonen” for at ønsket målbilde skal realistisk kunne etableres, og gap identifiseres. Det gjøres et slik arbeid i Sverige og Finland. Dette bør også gjøres i Norge, slik at strategier som foreslås er tilpasset den faktiske situasjonen.
- Strategien bør revideres så fort som mulig i 2026, med mål om at en ressurssatt handlingsplan er utarbeidet i tide til budsjettprosessen i 2027.

2.2 Nasjonalt cybersikkerhetssamarbeid

- TEK Norge mener våre cyber-myndigheter som NSM og PST må styrke plattformen for samarbeid med privat cybersikkerhets-bransje og sikre løpende gjensidig informasjons- og rådgivningsutveksling. Her bør vi lære av de beste, for eksempel Finland.

  Det pågår et visst samarbeid i Nasjonalt cybersikkerhetsforum i regi av NSM, hvor

sentrale offentlige etater og enkelte representanter fra næringslivet møtes. Det foregår også løpende informasjons-utveksling gjennom Nasjonalt cybersikker-hetssenter (NCSC) - NSM sitt partner-program. Disse arenaene må styrkes, cybersikkerhetsbransjen incentiveres og involveres bredere og dypere, arbeidet må gjøres mer helhetlig, og informasjon må gå begge veier i større grad, slik at cyber-hendelser kan avverges og begrenses i størst mulig grad, og raskest mulig bekjempes. Det er et særlig behov for initiativ som sikrer god situasjonsforståelse i det store omfanget av bedrifter som ikke omfattes av Sikkerhetsloven, men likevel er sentrale i å sikre at Norge fungerer i krise, og som ofte er underleverandør til selskaper, etater og organisasjoner. Dette er også noe annet enn Sentralt Totalforsvarsforum (STF) som har en god representasjon av viktige offentlige etater, men helt mangler privat sektor.

2.3 Nasjonalt og nordisk benchmark-program

- TEK Norge foreslår at vi har en årlig gjennomgang av hva som er dokumentert status når det gjelder cybersikkerhet i sivil og offentlig sektor. Offentlig sektor bør også omfatte kommunene, som vi vet har problemer med et enormt mangfold av systemer, teknisk gjeld og varierende grad av økonomi og kompetanse innen cyber.
- TEK Norge mener vi bør måle vår progresjon og utvikling på området årlig mot de landene det er mest naturlig å sammenligne oss med, som er øvrige nordiske land.

2.4 Cybersikkerhet i budsjett- og styrings-dialog

- Cybersikkerhet må høyere på agendaen i det offentlige. Det offentlige er bærere av tjenester til oss alle, og TEK Norge mener tildelingsbrev fra alle departementene til alle underliggende etater må ha eksplisitte (cyber)sikkerhetsmål og måleparametere som fokuserer på effekt.
Det er bra at digitaliseringsrundskrivet i 2025 fikk et viktig tillegg om å prioritere informasjonssikkerhet, men målstyring av dette må følges opp konkret gjennom tildelingsbrev og styringsdialog.

3. Totalberedskap og sivil motstandskraft

Totalberedskapsmeldingen har etablert et nytt fundament for sivil motstandskraft med over 100 konkrete tiltak og en styrking av Sivilforsvaret. Men vi savner fokus på cybersikkerhet i større grad, samt kraftfull samordning av sivil og privat sektor på området. Vår analyse viser at vi er sterke på policy, men svake på operativ implementering av beredskap i forhold til andre.

TEK Norge mener cybersikkerhet må integreres mer som essensiell del av totalberedskapen. Vi må tenke nytt og siden digitale trusler er de mest aktuelle vi står overfor, både som storsamfunn og enkeltpersoner, må vi styrke vår motstandsevne. Aktiv erfaringsoverføring fra relevante offentlige og private virksomheter i Ukraina bør tilstrebes for økt innsikt, som grunnlag for implementering i det norske Totalforsvaret.

Videre bør det utvikles cyberberedskapsteam i alle kommunale og regionale beredskapsråd som nå lovpålegges. Og det må sikres cyberrobusthet i alle kritiske samfunnsfunksjoner som er identifisert i meldingen.

For å styrke samfunnets motstandskraft, eller resiliens som det kalles, bør man videre implementere digital infrastruktur og cyberelementer i den lovfestede plikten til å bygge tilfluktsrom i nye bygg, bevilge ytterligere midler til å sikre digital kommunikasjon under kriser, gjennom robuste backup-løsninger.

Ikke minst må man gjennom mye mer aktiv opplysningsaktivitet gjøre befolkningen mer robust og kompetent om digital sikkerhet som del av den brede beredskapskultur-satsingen.

Norge må også bruke Nansen-programmet til Ukraina til å utvikle norsk industri utover tradisjonell våpenindustri. Nå gjelder droneutvikling og moderne digital krigføring, noe Norge må styrke seg vesentlig på.

TEK Norges forslag til konkrete tiltak:

3.1 Regionale/kommunale cyberberedskapsteam

- Vi har i dag en ordning med fylkesvise beredskapsråd. Regjeringen har varslet i Totalberedskapsmeldingen (Meld St. 9 (2024-2025) at disse skal styrkes, hvilket er bra. Men vi ser ikke at cyberberedskap er hensyntatt i tilstrekkelig grad her og mener det må inkluderes, siden dette er en av de mest aktuelle truslene vi står overfor.

3.2 Tilfluktsrom 2.0 (digitale krav)

- Regjeringen har også i Totalforsvarsmeldingen varslet nytt fokus på tilfluktsrom. TEK Norge er opptatt av at det også legges godt til rette for en digital tilstedeværelse med god konnektivitet og reservestrøm.

3.3 Virksomhetsopplæring

- Det er identifisert et betydelig behov for økt robusthet og digital sikkerhet i norske private virksomheter og kommuner. Små- og mellomstore bedrifter som inngår i verdi- og forsyningskjeder som er av betydning for Totalforsvaret er spesielt utsatt. Disse bedriftene behøver praktisk hjelp og bistand til å planlegge for å implementere reelle risikoreduserende tiltak på cyber området, utover ulike veiledere fra offentlige myndigher. TEK Norge mener det bør incentiveres og legges til rette for målrettet bruk av

kapasiteten og kompetansen til norske cybersikkerhetsselskaper til prioritert virksomhetsopplæring, i et offentlig/privat samarbeid.

3.4 Befolkningsopplæring “Sikker Digital Hverdag”

- Det er nødvendig å styrke befolkningens motstandsevne på cyberområdet. Med kunstig intelligens og datakraft viser tall fra Økokrim at økonomisk cyberkriminalitet øker i omfang og kompleksitet. Myndighetene må bistå med å legge til rette for at denne utviklingen stoppes ved å stå bak opplæringstilbud til befolkningen slik at terskelen for å beskytte seg blir så lav som overhodet mulig. I tillegg må all informasjon samles i en portal så alle vet hvor man finner informasjon eller skal henvender seg rundt sikkerhetssprsmål eller hendelser – både for enkeltpersoner og bedrifter.

4. Situasjons-forståelse og trusselrespons

Digitalsikkerhetsloven som trådte i kraft 1 oktober i år har etablert obligatorisk hendelsesrapportering, men analyser viser at Norge har færrest rapporterte sikkerhets-hendelser. Dette tyder på systematisk under-rapportering i Norge, snarere enn at vi har bedre sikkerhet. Vår benchmark-analyse viser at vi i Norge er dårligere på systematisk sikkerhetsstyring enn våre naboland.

TEK Norge mener det er et kritisk behov for forbedret rapportering, felles situasjons-forståelse og respons. Vi må åpent adressere underrapportering av hendelser, undersøke årsaker til lav rapportering - er det manglende bevissthet, kapasitet eller incentiver? Igjen er det viktig med god situasjonsforståelse for å sette inn riktige tiltak.

TEK Norges forslag til konkrete tiltak:

4.1 Stimulere rapportering av cyberangrep og styrke situasjonsforståelse

- TEK Norge mener vi må styrke støtte-systemene for virksomheter som rapporterer hendelser, og utvikle automatiserte rapporteringssystemer for å redusere terskelen for rapportering.
- Etablere felles standarder for beskrivelse og rapportering av cyberangrep, både som del av felles rapportering og innad i sikkerhetsmiljøet, for å sikre høy kvalitet på datagrunnlaget som etableres
- Videre mener vi det er helt nødvendig å styrke situasjonsforståelsen på tvers av sektorer, korrigere for underrapportering i nasjonale situasjonsbilder, koble sammen flere datakilder for å kompensere for manglende rapportering og å utvikle prediktive overvåkningssystemer som ikke er avhengig av frivillig rapportering. Herunder, må det legges til rette for løpende deling av merkede og strukturerte data, på standardiserte formater inn i felles datamodeller, som muliggjør økt grad av automatisering og flerkilde analyse, i den hensikt å kunne gi aksjonerbar beslutnings-støtte
- Norge kan lære av Finlands "ISAC"-struktur, som kombinerer horisontal og vertikal deling mellom privat sektor(er) og det offentlige på en strukturert måte. Sveriges "Cyber Defence Group", som består av over 80 bedrifter som samles om å dele informasjon og fremme dialog på tvers og med myndigheter på cyberdomenet, er også interessant å lære av.

4.2 Styrket hendelses- og krisehåndtering

- TEK Norge mener det haster med å forbedre vår hendels- og krisehåndtering. Dette er Norges svakeste område ifølge indekser. Vi må straks foreta oppgradering av krisehåndteringskapasitet basert på National CyberSikkerhet Index-funn, og implementere nordiske beste praksis for krisehåndtering.
- Regjeringen har basert på Totalberedskapsmeldingen startet et arbeid med å etablere en nasjonal cyberberedskapsordning. Det er ennå uklart hva dette arbeidet leder ut i. TEK Norge mener det er nødvendig at man ikke kun tenker på hvordan privat sektor kan understøtte myndighetene i deres bekjempelse av større cyberangrep, men at vi også utvikler et mer koordinert program for løpende bekjempelse av cyberangrep mot både offentlig og privat virksomhet.
- Norsk næringsliv bør også i større grad vurdere forsikring mot cyberhendelser, her ligger vi lavt og bør sikre oss mot tap i større grad når trusselen øker.
- Koordinering av hendelseshåndtering fra myndighetshold må ligge ett sted. Gitt at NSM over tid har hatt den denne rollen, er

det hensiktsmessig at ansvaret fortsatt ligger her. Det må vurderes om NSM bør få en mer eksplisitt koordinerende rolle, og i mindre grad være aktivt involvert i selve hendelshåndteringen.

- For virksomheter som ikke har, eller ikke kjenner til et sektorvist responsmiljø (SRM) eller sektormyndighet som kan bistå, skal saker fortsatt kunne meldes til NSM.
- NSM skal så langt det lar seg gjøre videreformidle saker til andre aktører for videre oppfølging, enten dette er til et SRM eller gjennom virksomheter som inngår i Kvalitetsordningen for håndtering av IKT-sikkerhetshendelser (KVO).
- Ved saker/hendelser som har nasjonal sikkerhetsbetydning, og hendelsen får konsekvenser i flere sektorer, bør NSM ha en koordineringsrolle og bistå med spesialkompetanse dersom rammet virksomhet eller ansvarlig sektormyndighet trenger bistand.
- Kripos, ved NC3, bør i større grad rette sine ressurser inn mot etterforskning og oppfølging av alvorlig cyberkriminalitet og omfattende etterforskninger.
- Det må avklares om digital svindel eller annen, «mindre alvorlig» cyberkriminalitet skal henvises til Økokrim, Norsis, Næringslivets sikkerhetsråd eller bare hjelp-til-selvhjelp på den kommende myndighetsportalen for digital sikkerhet.
- I lys av nye krav som følger av digitalsikkerhetsloven, må regjeringen klargjøre hvilke sektormyndighet som fungerer som nasjonalt kontaktpunkt for den enkelte virksomhet.

5. Robust infrastruktur og digital grunnmur

Regjeringen har lansert en nasjonal sikkerhets-plan for digital infrastruktur med 400 millioner kroner årlig fram til 2030, totalt 2,4 milliarder kroner.

TEK Norge er glad for denne satsingen, men mener det nye 1,5% målet til NATO om å investere i sivil infrastruktur som kan underbygge forsvarsevnen tilsier ytterligere satsing på den digitale grunnmuren. Med disse midlene kan man realisere målet om reservestrøm i opptil tre døgn på alle base-stasjoner, forsterke e-kom i flere kommuner som planlagt i sikkerhetsplanen, utvikle satellitt-kommunikasjon som backup for jordbasert infrastruktur og ikke minst styrke nasjonal/nordisk beredskap for kritiske digitale komponenter.

TEK Norge har ikke prissatt denne satsingen, den vil bero på avviksanalyser og risiko-analyser som skal utføres.

TEK Norges forslag til konkrete tiltak:

5.1 (Cyber)sikkerhet som obligatorisk anskaffelseskriterium

- Et viktig krav for TEK Norge er at offentlige anskaffelser skal ha obligatorisk krav til (cyber)sikkerhet som en del av anskaffelseskriteriene. Det er ingen slike krav i dag, og det foreligger forslag om at det skal innføres som «kan»-krav i anskaffelsesloven. Men det anses ikke nødvendig (eller rettere sagt ønskelig) med et «skal»-krav. Det er TEK Norge sterkt uenig i. Bærekraft har blitt et obligatorisk krav og skal i tillegg vektes 30%. Sikkerhet er i høyeste grad også bærekraft, og vi har ingen bærekraft uten sikkerhet.

  TEK Norge mener derfor at sikkerhet bør innføres som obligatorisk krav i alle offentlige anskaffelser og telle på lik linje med bærekraft. Offentlige innkjøp gjelder våre felles tjenester og de må være sikre. Det gjelder innkjøp for omlag 800 milliarder kroner årlig og er kritisk for å høyne sikkerheten i samfunnet. Der det offentlige går foran, vil også privat sektor komme etter, leverandører må høyne sin kompetanse og leveranse og man oppnår en totalt vesentlig styrket situasjon.

5.2 Fortsatt styrket utbygging av digital infrastruktur

- Det er nødvendig å fortsatt investere i nettene, særlig for å bygge robusthet og redundans, men utbyggingen har kommet til et nivå hvor det ikke lenger er kommersielt forsvarbart for aktørene. TEK Norge anbefaler derfor at det innføres incentivordninger for fortsatt privat sektor investeringer der det ikke er kommersielt forsvarbart som et alternativ til direkte offentlig finansiering.

- TEK Norge mener videre det er nødvendig å fortsatt utvikle redundans i nettene ved å sikre ytterligere cyber-robuste forbindelser til alle deler av Norge, inkludert Nord-Norge og øyområder og å få på plass backup-løsninger med nordiske partnere for nettverk og kritiske systemer. En betydelig del av 1,5% målet for såkalt artikkel 3 formål i NATO-traktaten bør benyttes til dette.

5.3 Kvalitetsmerking av leverandører

- Det bør vurderes å innføre en kvalitets-merking av markedsaktører som har et grunnleggende kvalitets- og sikkerhetsnivå i sine tjenester til markedet, etter mal av Kvalitetsordningen for håndtering av IKT-

sikkerhetshendelser. TEK Norge anbefaler at kvalitetsmerkingen også omfatter cybersikkerhetskapabiliteter som:
    - Sikkerhetsledelse og -rådgivning
    - Sikkerhetsovervåkning
    - Sikkerhetstesting
- I denne sammenhengen er det viktig at relevante private aktører tilfredsstiller minimum kvalitets- og kapasitetskrav, slik at virksomheter som kontraherer disse tjenestene er garantert resultater og ønsket effekt. Det er TEK Norges oppfatning at et slikt tiltak vil kunne få rask og positiv effekt på den nasjonale digitale grunnsikringen, ved at godkjente private aktører, med de riktige kapabilitetene, kan være «lettere» tilgjengelige for virksomheter som har behov for støtte. Det er vår erfaring at både EU/EØS direktiver og nasjonale lover og regler (NIS 1 og 2, S-lov, VFS, DSL, DORA mfl.) medfører økt etterspørsel etter digital sikkerhetskompetanse, fra et økende antall virksomheter, og at en slik liste over godkjente sikkerhetsleverandører vil kunne bidra til økt tilgjengelighet av en begrenset fagkompetanse og økt nasjonal digital grunnsikring.
- En slik ordning kan i sin enkleste form være basert på NSMs Cybersjekk, og vil gi både tilbydere og forbrukere økt bevissthet rundt valg av leverandører. Dette vil også være et tiltak for å møte kravene i Cyber Resilience Act.

6. Lover, regler og regulatorisk rammeverk

Digitalsikkerhetsloven er i kraft, og Norge forbereder seg på NIS2-direktivet.

TEK Norge er opptatt av at det gis god veiledning i forbindelse med loven. Det er ingen overgangsordninger for digitalsikkerhetsloven, slik at det må arbeides godt med informasjon og veiledning. Likeledes må loven håndheves på en måte som ikke stiller norsk næringsliv i en strengere posisjon enn våre konkurrenter, og reaksjonsnivå være moderat.

Det er kritisk for næringslivet at denne lovgivning, sammen med kommende NIS2-lov, KI-lov, DORA og Cyber Resilience Act mfl håndheves på en koordinert måte av myndighetene. Vi har svak tradisjon for dette i Norge, men EU går foran med lovgivning som forutsetter sektorovergripende håndheving, og det må vi klare i Norge også.

Noe av årsaken til at Norge ligger etter våre naboland på helhetlig sikkerhetstenking tror vi kan henge sammen med at vi ligger etter i å implementere sentrale regelverk som har introdusert dette i EU for lengst, som NIS-regelverket. NIS 1 ble nylig implementert i Norge gjennom Digitalsikkerhetsloven. Dette rammeverket ble vedtatt i EU for 9 år siden og har vært i kraft i 7 år og blitt erstattet av NIS 2 i mellomtiden, i tillegg til at det har kommet ytterligere sentral sikkerhetslovgivning som utfyller NIS 2. Denne nye lovgivningen stiller krav til gjennomgående sikkerhetskultur og verdikjedekontroll. Så lenge vi ligger etter med å implementere slike regelverk vil vi også ha en svakere gjennomgående sikkerhetskultur.

TEK Norges forslag til konkrete tiltak:

6.1 Koordinert håndheving av regelverk og «harmoniseringsveileder»

- Regjeringen ved Justisdepartementet oppfordres til å forsere lovarbeidet på digitalsikkerhetsområdet. Det foreslås å etablere en hurtigarbeidende «innsatsgruppe» som får i oppdrag å forberede implementering av alle gjenværende EU-direktiv og forordninger som fortsatt ikke er innført i norsk rett. Dette omfatter eksempelvis følgende: NIS2, CER, CRA og KI-forordningen. Målet må være full etterlevelse av europeisk rett på området innen 2027.
- TEK Norge foreslår at aktuelle myndigheter med ansvar for digitalsikkerhetslover pålegges et koordineringsansvar overfor næringslivet i form av et «tilsynsforum» for å sikre koordinering, felles forståelse av tilsvarende krav i ulike lover og håndheving.

6.2 Forsert implementering av sentral sikkerhetslovgivning

- TEK Norge mener det er nødvendig å forsere innføring av sentral lovgivning som styrker vår sikkerhet, som NIS 2, Cyber Resilience Act og Critical Entities Resilience directive. Det vil styrke Norges motstandskraft og innføre sentrale krav raskt som allerede gjelder ellers i Europa. Å redusere det regulatoriske gapet til våre naboland har også stor verdi for næringslivet.

7. Utdanning og bevisstgjøring

Benchmark-data viser at norske bedrifter har betydelig lavere andel med grunnleggende sikkerhetsrutiner enn nordiske naboer. Kun 63% gjør ansatte oppmerksomme på IKT-sikkerhetsforpliktelser, og bare 32% har dokumenterte sikkerhetsprosedyrer. Her må bransjeorganisasjoner og myndigheter sammen gjøre et arbeid for å styrke sikkerheten.

TEK Norge mener videre at vi må ha forsterket utdanning på alle nivåer. Vi trenger å øke antall cybersikkerhetsstudieprogram - Norge har færre enn andre nordiske land. Vi må etablere praksisprogram mellom utdannings-institusjoner og næringsliv, og sikre muligheter for nordisk utveksling av studenter og fag-personell for å lære av beste praksis.

TEK Norges forslag til konkrete tiltak:

7.1 2000 nye studieplasser i cybersikkerhet/IKT-sikkerhet

- I rapporten «Kompetanseløft for nasjonal sikkerhet" (NSM) framkommer et behov for totalt 40.000 flere med IKT-kompetanse i 2030 i forhold til i 2019. Vi er over halvveis i perioden og antall studieplasser har kun økt marginalt. Det er sterk økning i søkningen til cybersikkerhetstudier uten at antallet studieplasser har økt tilsvarende og behovet er stort. TEK Norge mener at her må det gjøres et betydelig løft nå.

7.2 Obligatorisk opplæring i IKT-sikkerhet i offentlig og privat sektor

- TEK Norge mener det bør innføres obligatorisk opplæring i IKT-sikkerhet i alle offentlige virksomheter, i første omgang for ledelsen. NSM har utmerkede kurs, for eksempel «Grunnprinsipper for IKT-sikkerhet» som kan gjøres påkrevd å gjennomgå.

7.3 Lærerkompetanse – sikkerhet i skolen

- Barn og unge lever digitale liv og digital sikkerhet må være en del av utdanningen. TEK Norge vil derfor at lærere skal styrke sin kompetanse innen IKT-sikkerhet på lik linje med offentlige virksomheter som nevnt over. Videre bør IKT-sikkerhet inn i læreplanen, slik at barn og unge får god kultur på sikkerhet som en del av sin digitale hverdag.

8. Forskning, utvikling og innovasjon

Norge har etablert en base for cybersikkerhetsinnovasjon gjennom økte offentlige investeringer. Men TEK Norge ser at mer må gjøres. Vi mener det er nødvendig å styrke eksisterende miljøer som NTNU, UiO, og Simula med økte bevilgninger og å utvikle spesialiserte programmer innen kryptografi og KI-sikkerhet. Det er svært gledelig at regjeringen har styrket satsting på kvante-teknologi i årets statsbudsjett.

TEK Norge ønsker også at offentlig-private partnerskap styrkes for å øke innovasjons-graden og -evnen. Det kan gjøres ved å koble sammen forskningsinvesteringer med en andel av de vedtatte 400 millioner kroner årlig til styrking av den digitale grunnmur. Et grep er å utvikle testmiljøer og laboratorier for realistisk testing av cybersikkerhetsløsninger utover det eksisterende miljøet på NTNU Gjøvik.

Norge bør også i enda større grad delta aktivt i EU-forskningsprogrammer innen cybersikkerhet og utvikle nordisk forsknings-samarbeid om felles cybersikkerhet-utfordringer.
TEK Norge mener at norsk sikkerhetsindustri bør fremmes av nasjonale hensyn. Vi må bruke offentlige anskaffelser strategisk til å dyrke og utvikle norsk cybersikkerhetsindustri.

TEK Norges forslag til konkrete tiltak:

8.1 Økt grunnfinansiering (kryptologi og KI-sikkerhet)

- TEK Norge mener vi bør øke innsatsen med å bevilge ytterligere 300 mill kroner til å styrke forskning og innovasjon innen kryptologi og KI-sikkerhet utover hva som er satt av til kvanteteknologi. Dette bør også brukes til å utvikle norsk sikkerhetsindustri ved å knytte innovasjonsmidler til klynger rundt akademia-miljøene.

8.2 Tilrettelegge for og stimulere til tett samarbeid akademia og næringsliv

- Cybersikkerhet beveger seg lynraskt. Mye raskere enn de fleste andre fagfelt. Medisinske forskningsmiljøer ligger gjerne på sykehusene, dette kan vi ikke få til innen cybersikkerhet. Cybersikkerhet er også et fagfelt som i stor grad drives frem reaktivt: når nye teknologier kommer blir det en del av det som skal forsvares. Det betyr at ny-vinningene i stor grad drives i industrien/virkelig verden og ikke i universitetene. Vi har derfor et ekstra stort behov for at akademiske miljøer knyttes svært nære de virkelige miljøene. Mye i dette handler om tilganger og sikkerhets-klareringer osv. Forskningsmiljøene mangler tilgang på reelle data og observasjoner. Lab-er osv. er fint for øving, men ikke for innovasjon og realkompetanse. Vi må derfor i større grad være villige til å bevilge mer til miljøene som kan gi denne tilgangen, og industri/akademia må knyttes mye tettere sammen.

9. Internasjonalt samarbeide og alliansepartnere

TEK Norge mener vi må bygge opp under nordisk cybersikkerhets samarbeid langt raskere og besluttsomt enn i dag, og ha en visjon om Norden som en felles sikkerhets-sone.

Norge har styrket sitt internasjonale samarbeid gjennom både NATO-forpliktelser og nordisk samarbeid. Dette kan vi forsterke ved å integrere dual-use cyberelementer i det historiske forsvarsløftet på 1624 milliarder kroner. Vi bør også styrke cybersikkerhet som element i EØS-samarbeidet.

TEK Norges konkrete forslag til tiltak:

9.1 Gjensidig nordisk sikkerhetsklarering

- I tillegg til de pan-nordiske virksomhetene som har samfunnskritisk infrastruktur opplever problemer med å drifte sine operasjoner på tvers på grunn av stivbent og ukoordinert sikkerhetsklareringer på tvers av landene, hindrer dette også effektiv tilgang til relevant kompetanse og kapasitet ved hendelser. Med felles deltakelse i NATO bør også det sivile klareringssystemet ko-ordineres snarest.

9.2 Dual-use cyber i forsvarsløftet

- Droner har blitt helt essensiell del av et moderne forsvar. Krigen i Ukraina har vist og viser dette daglig. Men dronene kan også brukes for sivile formål og er således et godt eksempel på såkalt «dual-use»-virkemiddel. Det er bra at det nylig er inngått samarbeid om droneutvikling og anskaffelser. Knyttet til cybersikkerhet, så mener TEK Norge av det som en del av forsvarsløftet bør stimuleres til mer innovasjon og utvikling av cybersikkerhetsprodukter som både har sivil og millitær nytte og bruk.

9.3 Styrket nordisk samarbeid forøvrig

- Norge, Sverige og Finland er en halvøy med sårbarheter som følger av det. Vi bør derfor styrke vår felles digitale infrastruktur med muligheter for fiber og mobil re-ruting på tvers av landegrenser og back-up løsninger som styrker vår felles digitale motstands-kraft. Det samme gjelder for en felles oversikt/lager eller beredskap av kritisk reservemateriell og –komponenter på sentral infrastruktur i de enkelte land. Det bør også utredes mulighetene for en nordisk cybersikkerhets operasjonssenter for informasjonsutveksling og respons-støtte.
- TEK Norge oppfordrer til tettere samarbeid i Norden, og at Regjeringen støtter opp om initiativ som styrker samarbeid på cybersikkerhetsfeltet i regionen. TEK Norge ber om en plan for hvordan Regjeringen ser for seg at Norge skal «slutta[r] seg til det nordisk-baltiske samarbeidet for cyber-tryggleik»[1].

[1] Prop 1 S (2024-2025)

10. Øvelser

Med et nytt trusselbilde må Norge gjennomføre bi-årlige nasjonale cyber-øvelser som del av den bredere beredskaps-øvingen og etablere sektorvise øvelser for virksomheter omfattet av sikkerhetsloven og digitalsikkerhetsloven.

TEK Norges forslag til konkrete tiltak:

10.1 Nasjonal bi-årlig cyberøvelse

- Norge bør utvikle eksisterende cyber-øvelsesprogram med å se hen til de nasjonale cyberøvelsene som bla Storbritannia og USA holder (NCEX) for å sikre gjennomgående øving av cyber-beredskap. Det bør også gjøres såkalte "black sky"-simuleringer, der man ser på effektene av tverr-sektoriell, langvarige utfall av digitale tjenester for å styrke beredskap for verste-fall scenarier.

10.2 Sektorvise øvelser for Digitalsikkerhetslov-virksomheter

- Digitalsikkerhetsloven omfatter virksomheter som har kritiske samfunns-funksjoner. TEK Norge mener det bør bevilges midler fra det offentlige til å bidra til gjennomføring (cyber)øvelser for disse virksomhetene for å sikre god beredskap.

10.3 Øvelser under NATO ledelse

- Norge bør i økende grad delta med felles cyberressurser fra offentlige (mil/siv) virksomheter og private norske selskaper i NATO ledede øvelser, som for eksempel Locked shields (fokus defensive cyber-operasjoner) og Crossed Swords (offensive cyberaktiviteter), i regi av NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Dette, med mål om å styrke vår felles situasjonsforståelse og vår samlede evne til å oppdage, håndtere og avskrekke avanserte cybertrusler, og slå tilbake. TEK Norge anbefaler at det identifiseres en «pool» av sertifiserte norske private selskaper som kan planlegge med og inngå et fast øvings-program i NATO regi.

11. Budsjettramme – nye/økte årlige midler (MNOK)

TEK Norge foreslår i det følgende beløp som knytter seg til de tiltakene som er identifisert over. Beløpene er å anse som ambisjoner for å kunne realisere målsettingen som er angitt.

Kapittel 2: Strategi og nasjonal lederskap	50
Kapittel 3: Totalberedskap og sivil motstandskraft	100
Kapittel 4: Situasjonsforståelse og trusselrespons	80
Kapittel 5: Robust infrastruktur og digital grunnmur	400
Kapittel 6: Lover, regler og regulatorisk rammeverk	20
Kapittel 7: Utdanning og bevisstgjøring	800
Kapittel 8: Forskning, innovasjon og næringsutvikling	400
Kapittel 9: Internasjonalt samarbeid	50
Kapittel 10: Øvelser	100
SUM kroner	2.000 millioner

Dette oppdaterte veikartet tar høyde for de betydelige politiske beslutningene som er tatt siden 2023 og skisserer en vei framover som bygger på eksisterende investeringer og regelverk. Norge har et godt utgangspunkt for å realisere visjonen om å bli et ledende cybersikkerhetsnasjon, men det krever vilje og kraft.

TEK Norge
November 2025

Rapporten er utgitt av: TEK Norge

Forfatter: Pål Wien Espen, direktør for infrastruktur, sikkerhet og forsvar i TEK Norge

Innspill: Øyvind Husby, administrerende direktør i TEK Norge

Mnemonic, Accenture og Radar

Grafisk: Vilde Sollien, kommunikasjonsrådgiver i TEK Norge

Kontakt oss

Kontakt Pål Wien Espen:

pwe@teknorge.no
(+47) 900 43 140

Kontakt TEK Norge:

post@teknorge.
(+47) 960 08 142
Prinsens gate 22
0157 Oslo

Følg TEK Norge på LinkedIn

Abonner på nyhetsbrev