CYBERSIKKERHET I NORGE

NORDISK BENCHMARK 2025

November 2025

Ny Analyse

Innhold

Ny Analyse

Innledning

Denne rapporten gir en samlet vurdering av Norges cybersikkerhetsposisjon i et nordisk perspektiv, sammenlignet med Finland, Sverige og Danmark. Analysen dekker seks sentrale delområder: teknologisk infrastruktur, forskning og utvikling, utdanning og kompetanse, sikkerhetsrutiner i næringslivet, faktiske sikkerhetshendelser samt nasjonal styring, regelverk og beredskap.

Datagrunnlaget er hentet fra åpne og anerkjente internasjonale og europeiske kilder:

- **World Bank og Netcraft**: for statistikk om sikre internettservere og digital infrastruktur
- **Eurostat**: for tall om skytjenester, IKT-sikkerhetstiltak og sikkerhetshendelser i næringslivet
- **Espacenet**: for godkjente patenter relatert til cybersikkerhet
- **OpenAlex**: for vitenskapelig publisering innen cybersikkerhet
- **JRC og Edurank**: for utdanningsprogrammer og rangeringer av universiteter
- **NCSI (National Cyber Security Index)**: for vurdering av nasjonalt cybersikkerhetsrammeverk og beredskap

Dette er den første fullskala benchmarken med denne metoden i en nordisk kontekst.

Metode og indikatorvalg

For å gi et helhetlig bilde av cybersikkerhet, er det valgt ut indikatorer som dekker både teknisk kapasitet, kunnskapsgrunnlag og organisatorisk robusthet. Hver indikator er skalert til 0–100 basert på beste nordiske resultat, slik at resultatene er sammenlignbare.

De seks delområdene er definert slik:

- **Infrastruktur**: måler den digitale grunnmuren – bl.a. sikre servere og avanserte skytjenester (World Bank, Eurostat)
- **Forskning og utvikling**: dekker akademisk publisering og teknologiske patenter innen cybersikkerhet (OpenAlex, Espacenet)
- **Utdanning og kompetanse**: vurderer utdanningstilbud og rangering av utdanningsinstitusjoner (JRC, Edurank)
- **Næringslivets sikkerhetsrutiner**: ser på implementerte tiltak og bruk av forsikring (Eurostat, forsikringsdata)
- **Sikkerhetshendelser**: registrerer reelle cyberangrep og datatap i næringslivet (Eurostat)
- **Regelverk og nasjonal beredskap**: bygger på vurderinger av strategier, krisehåndtering og lovgivning (NCSI, 2024)

Rapporten gir et sammenlignbart bilde av cybersikkerheten i Norden, og peker på hvor Norge står sterkt, og hvor gapene er størst.

Hovedfunn

Nordisk rangering 2025

Rangeringen bygger på en uvektet gjennomsnittsscore (0–100) basert på seks sentrale delområder innen cybersikkerhet.

Finland – 1. plass (Score 72)

Finland fremstår som den klare nordiske lederen i cybersikkerhet i 2025. Landet utmerker seg med høy modenhet innenfor både styring, utdanning, FoU og regulatorisk rammeverk. Det er særlig styrken i institusjonell struktur og digital beredskap som skiller Finland fra de øvrige nordiske landene.

Sverige – 2. plass (Score 69)

Sverige har en sterk profil innen forskning, utdanning og næringslivets sikkerhetsrutiner. Landet scorer høyt på utdanningskapasitet og FoU, men noe lavere på regulatorisk modenhet og nasjonal styring. Dette gir en robust teknologisk base, men etterlater enkelte strukturelle svakheter.

Danmark – 3. plass (Score 66)

Danmark har scoret høyt på infrastruktur og næringslivets cybersikkerhetsrutiner. Dette er sterke strukturelle fortrinn som gir høy praktisk modenhet, men relativt svakere resultater i FoU og utdanning trekker den samlede scoren noe ned sammenlignet med Finland og Sverige.

Norge – 4. plass (Score 64)

Norge scoret høyt på sikkerhetshendelser (lavt) og har et solid utdanningstilbud. Samtidig er det svakheter i infrastruktur, næringslivets sikkerhetsrutiner og nasjonal styring. Den nasjonale cybersikkerhetsmodenheten er fragmentert, og selv om det finnes styrker, fremstår helheten som mindre robust enn i de øvrige nordiske landene.

Hva betyr dette for Norge?

Norge har et solid fundament for cybersikkerhet, men står overfor et fragmentert modenhetsbilde. Landet utmerker seg ved svært lav forekomst av sikkerhetshendelser i næringslivet og har et godt utdanningstilbud innen cybersikkerhet. Samtidig viser analysen at Norge fortsatt har lavere modenhet enn andre nordiske land på infrastruktur, nasjonal styring og systematisk sikkerhetsarbeid i virksomheter.

Nasjonal beredskap og koordinering: hvorfor Finland leder

Finland oppnår høyest score i Norden innenfor nasjonalt regelverk og beredskap. Landet har etablert et bredt spekter av regulatoriske og strategiske mekanismer, inkludert helhetlig koordinering, klare ansvarslinjer og systematiske beredskapsøvelser. Norge har et godt lovverk og sterke fagmiljøer, men scorer betydelig lavere på nasjonal koordinering og operativ respons. Sammenlignet med Finland mangler Norge flere sentrale komponenter i gjennomføringsapparatet, inkludert etablert samordning, tydelige tiltaksplaner og nasjonale kriseøvelser.

Infrastruktur: Danmark drar fra

Danmark skårer høyest på infrastruktur og digital grunnmur – med høy tetthet av sikre internettservere, avansert bruk av skytjenester og høy andel validerte IPv4-prefikser. Norge ligger sist blant de nordiske landene i dette delområdet. Det er særlig tettheten av sikre servere og utbredelsen av RPKI-sikret routing (IPv4) som trekker Norge ned. Dette svekker det teknologiske utgangspunktet for sikker digital tjenesteproduksjon og gjør Norge mer sårbar for tekniske sårbarheter i nettinfrastruktur.

Systematisk sikkerhetsarbeid i næringslivet

Danske virksomheter utmerker seg med omfattende tiltak, dokumenterte rutiner og høy bruk av cybersikkerhetsforsikring. I Norge er risikoen for hendelser lav, men de systematiske tiltakene er svakere forankret. Norske virksomheter scorer lavere på styringstiltak, kjennskap blant ansatte og dokumentasjon. Dette antyder at mye av sikkerhetsarbeidet fortsatt er basert på initiativ fra enkeltvirksomheter – fremfor standardiserte krav og strukturer. Dette kan gi økt sårbarhet i møte med mer avanserte trusler.

Norges styrker: et fundament å bygge på

Norge har et bredt og spesialisert utdanningstilbud på bachelor- og masternivå, og plasserer seg nest høyest i Norden på dette området. Det er god bredde og geografisk spredning i studieprogrammene, og Norge har også høy score i Edurank, som vurderer institusjonenes faglige kvalitet. Til sammen gir dette grunnlag for en sterk fremtidig kompetansebase, forutsatt at studentopptak og kapasitet holdes oppe.

Få sikkerhetshendelser, høy motstandsdyktighet

Norge rapporterer lavest andel virksomheter som har opplevd alvorlige sikkerhetshendelser som tjenesteutfall, datatap eller lekkasjer. Dette gir Norge høyest score i Norden på dette delområdet, og tyder på høy faktisk robusthet i næringslivet. Denne motstandsdyktigheten er en styrke – men bør støttes av mer strukturert og koordinert styring fremover.

Implikasjon: nasjonal robusthet krever samordning

Utfordringen for Norge er ikke fravær av kompetanse – men mangelen på samordning og systematisk gjennomføring. For å tette gapet til Finland og Danmark, må Norge styrke sin nasjonale styring, operasjonalisere beredskapen og etablere tydeligere forventninger til grunnsikring i både offentlig og privat sektor. Det krever:

- Bedre nasjonal koordinering og kriseøvelser
- Minimumskrav til sikkerhetsrutiner i næringslivet
- Økte investeringer i digital infrastruktur

Data og metode

Denne analysen bygger på et bredt sett av åpne og etterprøvbare kilder som til sammen gir en strukturert vurdering av cybersikkerhet i Norden. Kildene inkluderer blant annet Eurostat, World Bank/Netcraft, Espacenet, OpenAlex, Edurank og National Cyber Security Index (NCSI). Alle data er hentet fra perioden 2023–2025 og gir et solid grunnlag for å sammenligne status og modenhet mellom landene på tvers av seks delområder.

Metodisk tilnærming

- **Indikatorscore**: Hver indikator er skalert fra 0 til 100, der beste nordiske verdi settes til 100.
- **Delområdescore**: Utregnet som et aritmetisk gjennomsnitt av indikatorene i hvert delområde (lik vekt).
- **Totalscore**: Summen av delområdenes snittscore gir en samlet vurdering av cybersikkerhet i hvert land.
- **Rangering**: Landene rangeres fra 1-4 kun etter uvektet totalscore (0–100) (1=best).

Et fullstendig oversikt over alle indikatorverdier, scores og rangeringer finnes i vedleggstabellene.

Delområde 1 – Infrastruktur

Hva måles: Modenhet i digital grunnmur.
Indikatorer:

- *Tetthet av sikre internettservere (per million innbyggere)*
- *Andel virksomheter som benytter avanserte skytjenester (%)*
- *Andel ROA-signerte prefikser (IPv4) – beskyttelse mot BGP-kapring*

Dette delområdet måler kapasitet og sikkerhetsnivå i det digitale fundamentet. Sikre servere og moderne skytjenester reflekterer kvaliteten på nasjonens nettinfrastruktur. ROA-signering indikerer beskyttelse mot routingangrep, og er en kritisk komponent i DNS- og internettets integritet.

Delområde 2 – Forskning og utvikling (FoU)

Hva måles: Kunnskaps- og innovasjonskapasitet.
Indikatorer:

- *Vitenskapelige publikasjoner innen cybersikkerhet (OpenAlex, 2020–2024)*
- *Godkjente cybersikkerhetspatenter (Espacenet, 2020–2024)*

Publikasjoner gir innsikt i akademisk aktivitet og forskningskapasitet. Patenter indikerer overgangen fra forskning til kommersialisering og innovasjon. Samlet reflekterer dette et lands evne til å drive kunnskapsbasert sikkerhetsutvikling.

Delområde 3 – Utdanning og kompetanse

Hva måles: Tilgang på utdanning og kvalitet i toppmiljøer.
Indikatorer:

- *Antall bachelorprogrammer (bredde og spesialisering)*
- *Antall masterprogrammer (bredde og spesialisering)*
- *Edurank (gjennomsnittlig rangering av de tre høyest rangerte utdanningsinstitusjonene innen cybersikkerhet)*

Dette delområdet kartlegger utdanningskapasitet og institusjonell kvalitet. Breddeprogrammer gir generell kompetanse, mens spesialisering gir fordypning. Edurank fanger opp internasjonal anerkjennelse og forskningsstyrke.

Delområde 4 – Næringslivets sikkerhetsrutiner

Hva måles: Teknisk og organisatorisk modenhet i privat sektor.
Indikatorer:

- *Andel virksomheter med minst fem cybersikkerhetstiltak*
- *Dokumenterte rutiner og prosedyrer*
- *Ansatte gjort kjent med retningslinjer*
- *Bruk av avanserte overvåkingssystemer*
- *Andel virksomheter med cyberforsikring*

Indikatorene viser graden av systematisk sikkerhetsstyring i virksomheter. Cyberforsikring signaliserer risikobevissthet og modenhet i håndtering av digitale trusler.

Delområde 5 – Sikkerhetshendelser i næringslivet

Hva måles: Faktisk forekomst av cyberangrep og skade.
Indikatorer:

- ***Hendelser (lavere=bedre, invertert):*** *Andel virksomheter som har opplevd: tjenesteutfall, datatap eller informasjonslekkasje.*

Lav forekomst av hendelser tolkes som høy robusthet og effektiv forebygging i næringslivet.

Delområde 6 – Regelverk og nasjonal beredskap

Hva måles: Nasjonal kapasitet til å lede, koordinere og håndtere hendelser.
Indikator:

- *National Cyber Security Index (NCSI 2024)*

Indeksen vurderer strategisk styring, beredskap, responskapasitet og internasjonalt samarbeid. Den gir et konsolidert bilde av statens cybersikkerhetsinfrastruktur.

Delområde 1: Infrastruktur

Indikatorer:

- *Sikre internettservere per million innbyggere (World Bank/Netcraft, 2024)*
- *Andel foretak som benytter avanserte skytjenester (Eurostat, 2024)*
- *Andel ROA-signerte prefikser (IPv4) (Internet Society, 2025)*

Land	Snittscore (0–100)	Rangering
Danmark	100	1
Finland	88	2
Norge	68	3
Sverige	64	3

Danmark er klart sterkest på digital infrastruktur og skårer høyest på alle tre indikatorer. Landet har høyest tetthet av sikre internettservere, stor utbredelse av avanserte skytjenester i næringslivet og det høyeste nivået av ROA-signerte nettverksruter – en viktig indikator på beskyttelse mot routingangrep (BGP hijacking).

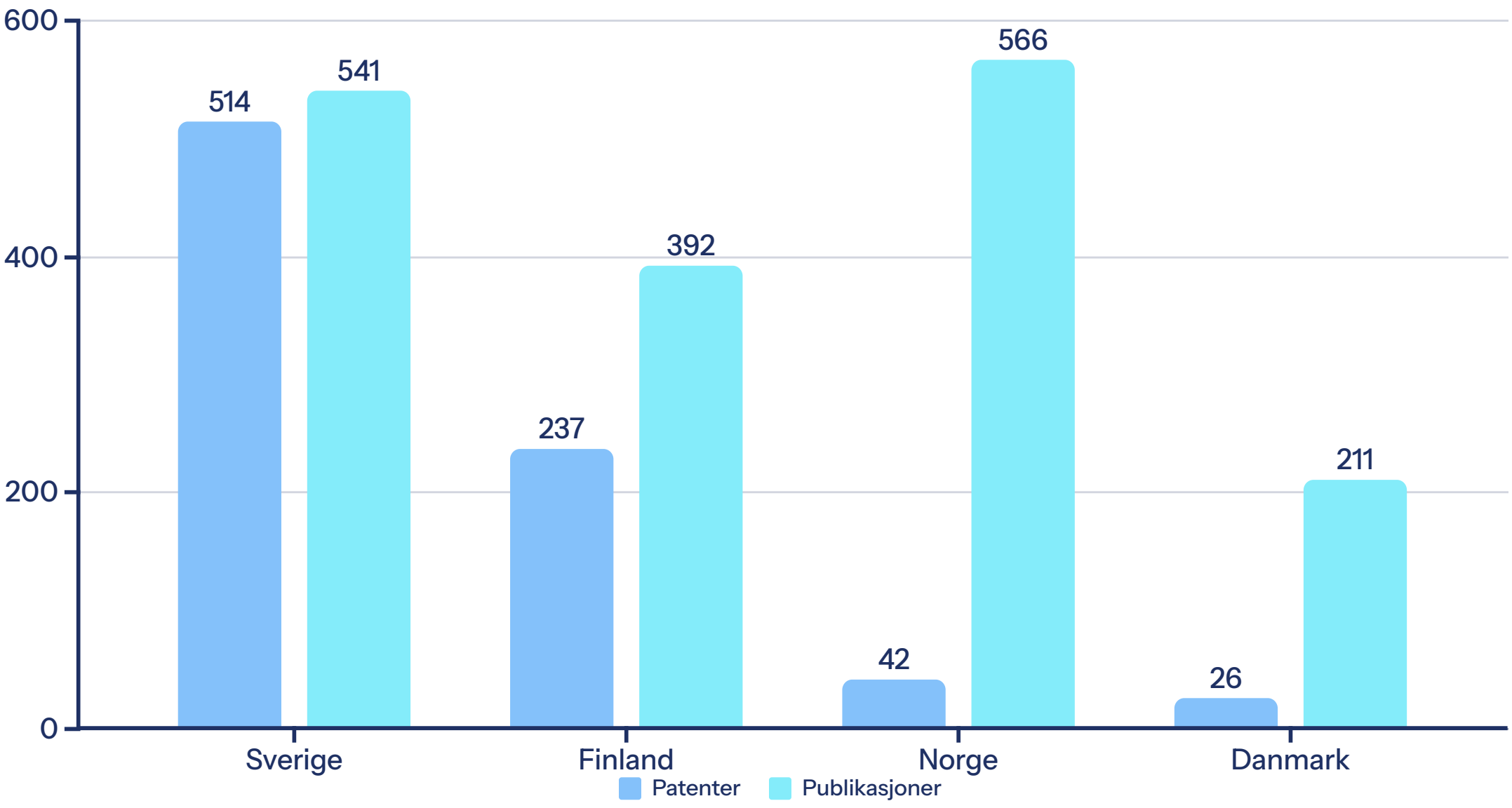
Finland følger som nummer to, med særlig høy bruk av avanserte skytjenester og en solid grad av sikker ruting. Sveriges infrastruktur er teknisk moden, men preges av lavere servertetthet. Norge kommer sist på delområdet, hovedsakelig på grunn av svært lav tetthet av sikre servere per million innbyggere, som trekker totalen ned, til tross for høy skybruk og relativt god IPv4-sikring.

Delområde 2: Forskning og utvikling i Cybersikkerhet

Indikatorer:

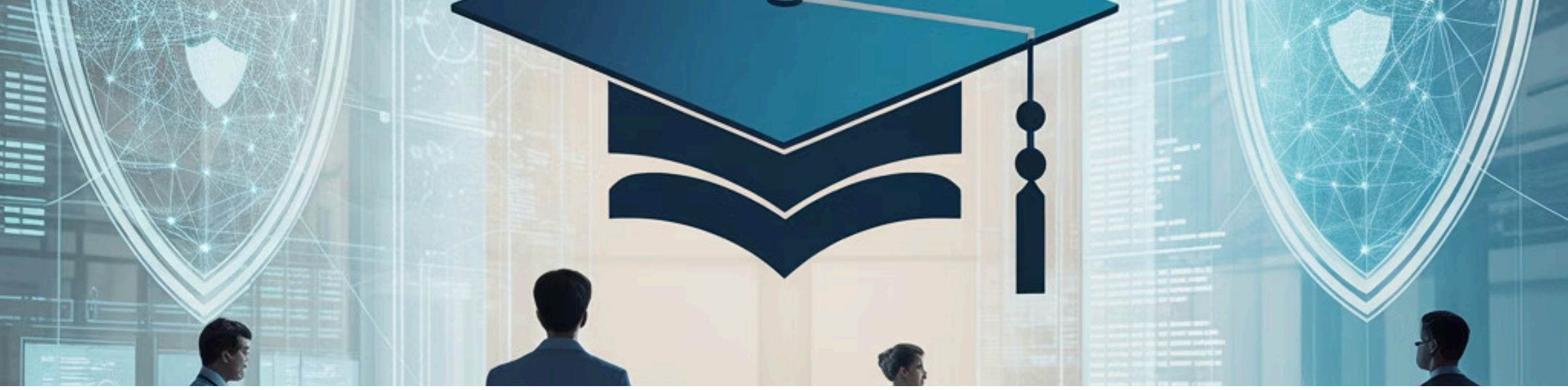
- Antall cybersikkerhetsrelaterte vitenskapelige publikasjoner (OpenAlex, 2020–2024)
- Antall godkjente cybersikkerhetspatenter (Espacenet, 2020–2024)

Dette delområdet måler kunnskaps- og innovasjonskapasitet i cybersikkerhet, gjennom faglig produksjon og kommersialisering. Publikasjoner reflekterer akademisk styrke og forskningsvolum, mens patenter viser evne til å omsette ny kunnskap i anvendbare og markedsnære løsninger.



Sverige rangeres øverst fordi landet kombinerer høy faglig produksjon med høy patenteringsaktivitet. Norge publiserer mye, men patenterer lite – det trekker ned totalscoren.

- **Sverige (Snittscore 98)**
  Sverige er tydelig ledende i Norden når det gjelder cybersikkerhetsforskning og -innovasjon. Landet har svært høy publikasjonsaktivitet og den høyeste andelen cybersikkerhetsrelaterte patenter. Det er en nær balanse mellom vitenskapelig produksjon og kommersialisering, noe som signaliserer en sterk innovasjonskultur og velfungerende samspill mellom akademia, næringsliv og myndigheter. Patenteringsaktiviteten dekker blant annet områder som nettverkssikkerhet, 5G-infrastruktur og kryptografi.
- **Finland (Snittscore 58)**
  Finland har god balanse mellom forskning og patentering, med særlig styrke på IoT-sikkerhet, programvaresikkerhet og anvendt kryptografi. Dette antyder at Finland har utviklet strukturer som gjør det mulig å overføre forskningsresultater til konkrete løsninger, uten nødvendigvis samme volum som Sverige.
- **Norge (Snittscore 54)**
  Norge har det høyeste antallet publikasjoner, men et lavt antall patenter. Det viser et tydelig "innovasjonsgap": forskningen er omfattende, men kommersialiseringen er begrenset. Årsakene kan ligge i svak kobling mellom akademia og næringsliv, manglende insentiver for patentering og teknologioverføring, og en forskningsmodell som i stor grad prioriterer grunnforskning fremfor anvendelse. Dette innebærer at Norge i liten grad kapitaliserer på sin sterke faglige basis i form av nye løsninger, tjenester eller teknologiselskaper. For å styrke dette må Norge bygge bro mellom fagmiljøer og marked – gjennom insentivordninger, støtte til spinouts, og styrkede overføringsmekanismer.
- **Danmark (Snittscore 22)**
  Danmark har lavest forskningsvolum og lavest antall cybersikkerhetspatenter i Norden. Det indikerer en mer begrenset FoU-base innen feltet. Selv om landet er sterkt på infrastruktur og tiltak i næringslivet, har det en svakere akademisk og innovativ kapasitet på cybersikkerhetsområdet. For å styrke den langsiktige evnen til å møte nye trusler og drive teknologisk utvikling, bør Danmark etablere en nasjonal forskningssatsing på cybersikkerhet med målrettet finansiering, samarbeidsarenaer og kompetansebygging.



Delområde 3: Utdanning og kompetanse

Indikatorer:

- Antall bachelor- og masterprogrammer i cybersikkerhet (JRC 2024)
- Edurank-rangering av topp-3 universiteter innen IT og cybersikkerhet

Dette delområdet måler utdanningstilbudets bredde (generelle programmer), spesialisering (dedikerte cybersikkerhetsprogrammer vektes 1,5 mer ved score) og institusjonell kvalitet. En sterk utdanningsbase er avgjørende for å sikre fremtidig tilgang på kompetanse og for å bygge et robust fagmiljø nasjonalt.

Land	Snittscore (0–100)	Rangering
Sverige	100	1
Norge	83,6	2
Finland	76,8	3
Danmark	67,5	4

Sverige

Sverige har det bredeste tilbudet av masterprogrammer (25 brede, 16 spesialiserte), noe som gir landet en stor utdanningskapasitet og dyp spesialisering. I tillegg rangeres svenske universiteter høyt internasjonalt. Dette gjør Sverige til det klart sterkeste landet i Norden på utdanningsdimensjonen innen cybersikkerhet.

Norge

Norge har et balansert og omfattende utdanningstilbud, med fire brede og fire spesialiserte bachelorprogrammer, samt et variert mastertilbud. Samtidig er norske toppinstitusjoner relativt godt rangert på Edurank. Dette gir Norge en solid andreplass, og viser at utdanningssystemet støtter opp om nasjonale kompetansemål.

Danmark

Danmark har en god kombinasjon av spesialiserte bachelorprogrammer og hele 14 brede masterprogrammer. Toppuniversitetene (bl.a. DTU) rangeres også høyt. Samlet sett gir dette Danmark en sterk posisjon. Selv om mastertilbudet er noe smalere i spesialisering enn i Finland og Sverige, er grunnlaget godt.

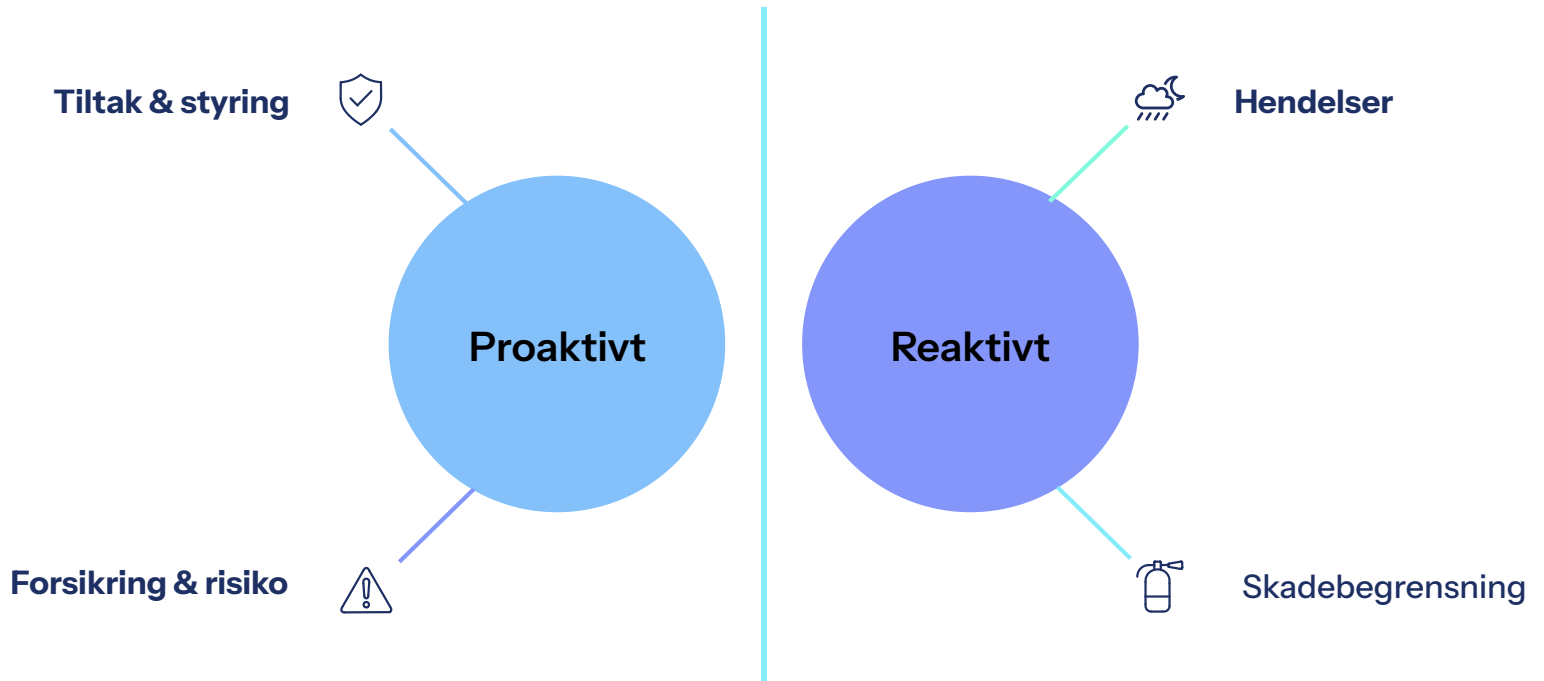
Finland

Finland har fire brede bachelorprogrammer, men færre spesialiserte tilbud på bachelornivå. Mastertilbudet er solid og sterkt på spisskompetanse (7 programmer). Edurank-score trekker noe ned, men samlet sett har Finland en kompetansebase i utvikling med økende institusjonell kapasitet.

Næringslivet: sikkerhetstiltak, rutiner og hendelser

Hvor godt jobber næringslivet med cybersikkerhet i praksis – ikke på papiret, men i drift?

For å fange det, bruker vi tre typer input fra Eurostat (IKT-sikkerhet i bedrifter, 2024):



Tiltak / rutiner / styring internt

- Andel foretak med etablerte IKT-sikkerhetstiltak (minimumspakke av tekniske kontrolltiltak).
- Andel foretak med formaliserte sikkerhetsrutiner / prosedyrer / ansvar.
- Andel foretak som gir opplæring / bevisstgjøring til ansatte om IKT-sikkerhetsplikter.
- Andel foretak med avanserte overvåkningssystemer (utover antivirus og brannmur).
- Andel foretak som har tegnet cyberrelatert forsikring / IKT-sikkerhetsforsikring.

Intuisjon: Høyere er bedre. Dette sier noe om moden internkontroll, samt budsjettert risiko.

Hendelser siste 12 måneder (invertert):

- Andel foretak som har hatt utilgjengelighet av IKT-tjenester som følge av angrep.
- Andel foretak som har hatt korrupsjon/tap av data.
- Andel foretak som har hatt lekkasje av konfidensiell informasjon.

Intuisjon: Lavere er bedre, men score er invertert. Få hendelser gir høy score. Dette sier noe om faktisk eksponering / sårbarhet i praksis.

Delområde 4: Næringslivets sikkerhetsrutiner og robusthet

Indikatorer:

- **Tiltak og styring** (Eurostat, 2024): Andel virksomheter med minimum fem sikkerhetstiltak, dokumenterte rutiner, ansatte gjort kjent med sikkerhetsansvar og avanserte overvåkingssystemer.
- **Cyberforsikring** (forsikringsdata, 2022): Andel virksomheter med tegnet cyberforsikring.

Dette delområdet vurderer den operasjonelle modenheten i nordiske virksomheter gjennom en kombinasjon av tekniske og organisatoriske sikkerhetstiltak. Indikatorene reflekterer i hvilken grad cybersikkerhet er integrert i virksomhetenes praksis, ikke bare på papiret, men i faktisk drift.

Land	Snittscore (0–100)	Rangering
Danmark	97,9	1
Finland	88,9	2
Sverige	79	3
Norge	71,3	4

Danmark fremstår som ledende på tvers av alle indikatorer. Særlig høy andel virksomheter har implementert minimum fem tekniske tiltak, etablert dokumenterte rutiner og bruker avansert overvåking. Samtidig har Danmark også høyest andel virksomheter med cyberforsikring (70,6 %), noe som indikerer høy bevissthet om risiko og moden håndtering.

Finland har høyest andel virksomheter med fem eller flere sikkerhetstiltak (80 %) og den sterkeste innsatsen for å gjøre ansatte kjent med sikkerhetsansvar (75 %). Samlet sett viser dette en bred implementering, men lavere forsikringsdekning (33,5 %) trekker ned det helhetlige risikobildet.

Sverige har en noe svakere sikkerhetsstyring, spesielt med tanke på dokumenterte rutiner (47 %) og overvåkingssystemer (54 %). Samtidig er andelen med cyberforsikring relativt høy (46,3 %), noe som kompenserer noe for svakere intern struktur.

Norge ligger lavest blant de nordiske landene på alle indikatorer unntatt overvåkingssystemer (54 %, likt med Sverige). Kun 32 % av norske virksomheter har dokumenterte rutiner, og bare 38 % har cyberforsikring. Dette tyder på at det fortsatt er betydelig rom for forbedring i norsk næringslivs sikkerhetsstyring og formalisering av praksis.

Delområde 5: Sikkerhetshendelser i næringslivet

Dette delområdet fanger faktisk sårbarhet i næringslivet, målt som andel virksomheter som har rapportert minst én cybersikkerhetshendelse de siste 12 månedene. Vi bruker **samlet forekomst** av tre typer hendelser:

- Utilgjengelighet av IKT-tjenester
- Datatap
- Lekkasjer av konfidensiell informasjon

Scoringen er invertert: **Lavere forekomst = høyere score (bedre robusthet)**.

Land	Total forekomst (%)	Score (0–100)	Rangering
Norge	12,5 %	100,0	1
Danmark	19,0 %	65,7	2
Sverige	20,4 %	61,3	3
Finland	42,2 %	29,6	4

Norge har lavest samlet forekomst av cybersikkerhetshendelser i Norden: Kun 12,5 % av virksomhetene har rapportert datatap, tjenesteutfall eller lekkasjer det siste året. Dette gir Norge full score og peker på høy operasjonell robusthet – til tross for svakere formell styring (jf. Delområde 4).

Danmark og **Sverige** har omtrent lik total hendelsesfrekvens (19–20 %), og scorer solid i dette delområdet. I Danmarks tilfelle samsvarer dette med høy styring og forsikringsdekning. I Sverige antyder det en fungerende praksis på tross av lavere andel med formalisert styring.

Finland skiller seg klart ut med høyest andel virksomheter som rapporterer sikkerhetshendelser (42,2 %). Dette trekker snittet markant ned, og tyder på større eksponering for trusler eller svakere forebygging på bedriftsnivå.

Dette delområdet gir et viktig korrektiv til policy og beredskap: **Norge scorer best når vi ser på faktisk skadeomfang i næringslivet.** Robustheten er høy, og hendelsesfrekvensen lav. Danmark og Sverige ligger tett bak, mens Finland har størst forbedringspotensial.

Delområde 6: Regelverk og nasjonal beredskap

Dette delområdet vurderer **statens evne til å regulere, koordinere og håndtere cybersikkerhet på nasjonalt nivå**, målt gjennom den internasjonale NCSI-indeksen (National Cyber Security Index, 2024). Indeksen inkluderer blant annet nasjonal strategi, ansvarsfordeling, evne til hendelseshåndtering, internasjonalt samarbeid og beskyttelse av digitale tjenester.

Land	NCSI-score (0–100)	Rangering
Finland	100,0	1
Danmark	33,3	2
Norge	11,4	3
Sverige	9,8	4

Finland: full pott og operativt lederskap

Finland utmerker seg med **maksimal score (100)**. De har:

- Komplett og gjennomført strategi med tiltaksplan.
- Full nasjonal koordinering.
- Operasjonell beredskap og internasjonal responskapasitet (CERT, rapportering, kontaktpunkt).
- Helhetlig dekning av utdanning, forskning, lovgivning og militær cyberberedskap.

Danmark og Sverige: mellomposisjon og fragmentering

- **Danmark** har moderat struktur med styrker innen beredskap og utdanning, men mangler tiltaksplan og har ikke samme operative dybde som Finland.
- **Sverige** scorer lavest sammen med Norge, tross tilstedeværelse av strategi. De mangler koordinering, tiltak og krisehåndteringsplan, og utmerker seg negativt på offentlig sektor- og cloud-regulering.

Norges posisjon: svak koordinering og manglende verktøy

Selv om Norge har en nasjonal cybersikkerhetsstrategi (score 3/3) og solide resultater innen utdanning, forskning og lovverk, skårer vi svært lavt på koordinering og beredskap:

- **Ingen handlingsplan for cybersikkerhetsstrategien** – til forskjell fra Finland (3/3), som har full implementeringsstruktur.
- **Manglende nasjonal koordinering** – Norge mangler en fast struktur (komité, råd eller arbeidsgruppe) for tverrsektoriell samordning av cybersikkerhet. Dette trekker poengene markant ned.
- **Ingen offentlig verktøy for hendelsesrapportering** – det finnes ikke et tilgjengelig digitalt verktøy for å rapportere cyberhendelser (0/2), i motsetning til Danmark og Finland.
- **Lav grad av internasjonal responskoordinering** – Norge har ikke utpekt et nasjonalt kontaktpunkt for internasjonalt cybersamarbeid (0/3), og faller derfor bakpå i operativ interoperabilitet.

Cybersikkerhet - total score

Land	Total (0–100)	Rangering
Finland	71,9	1
Sverige	69,3	2
Danmark	65,9	3
Norge	64,1	4

Resultat

Finland (71,9) er det mest balanserte landet i Norden når det gjelder cybersikkerhet. Landet skårer høyt på tvers av styring, utdanning, teknologi, operativ beredskap og institusjonell modenhet. Finland er også det eneste landet med full pott på nasjonal beredskap og koordinering i NCSI-indeksen.

Sverige (69,3) har solid teknologisk og akademisk kapasitet, særlig på utdanning og FoU, men faller noe bak på regulatoriske strukturer og nasjonal koordinering. Det er også lavere formell dekning av sikkerhetstiltak og forsikring i næringslivet.

Danmark (65,9) har styrker innen sikkerhetstiltak i næringslivet og høy bruk av cyberforsikring. Derimot trekker svakere resultater innen utdanning, forskning og nasjonal koordinering ned helhetsvurderingen.

Norge (64,1) ligger sist i nordisk sammenheng, men har høy score på befolkningens digitale bevissthet og lav forekomst av hendelser. Svakere styring, manglende koordinering og lavere dekning av tiltak og forsikring i næringslivet utgjør de viktigste forbedringspunktene. Norges utfordring er ikke mangel på strategi, men svak operasjonalisering.

Læringspunkter fra nordisk sammenligning

- ### Finland
  viser hvordan nasjonal koordinering og institusjonell beredskap skaper operasjonell styrke.
- ### Danmark
  demonstrerer hvordan bred næringslivsforankring og teknisk robusthet kan gi praktiske resultater.
- ### Sverige
  fremhever verdien av kunnskapsdrevet politikk og innovasjon i utdanning og forskning.

Implikasjoner og anbefalinger for Norge

Norge har et godt strategisk rammeverk og lav antall alvorlige hendelser i næringslivet, men skårer lavt på operasjonalisering, teknisk infrastruktur og nasjonal koordinering. For å styrke cybersikkerheten og få bedre effekt av eksisterende innsats, anbefales følgende tiltak:

1

Bygg ut den digitale grunnmuren

Norge skårer lavest blant de nordiske landene på teknisk infrastruktur. Det er behov for investeringer i grunnsikring, blant annet gjennom bruk av DNSSEC, RPKI og krav til sikkerhet i offentlige anskaffelser. Dette gir bedre motstandsdyktighet og reduserer sårbarheter på tvers av sektorer.

2

Styrk koordinering og beredskap

Fragmenterte ansvarslinjer og svak samordning reduserer effekten av dagens tiltak. Det bør etableres en tverrsektoriell koordineringsenhet med klare mandat og ansvar. I tillegg bør det innføres et felles nasjonalt verktøy for hendelsesrapportering og utarbeides en nasjonal beredskapsplan for cyberhendelser.

3

Etabler forpliktende offentlig-privat samarbeid

Samarbeid mellom myndigheter og næringsliv bør styrkes gjennom faste arenaer for informasjonsdeling og koordinering. Dette gjelder særlig på områder som grunnsikring, felles standarder og beredskap i verdikjeder.

4

Øk trygg bruk av skytjenester og leverandører

Det bør innføres tydelige krav til risikovurdering og sikkerhetsrutiner ved bruk av skytjenester og leverandørkjeder i offentlig sektor. Dette bør suppleres med minimumsstandarder og støtteordninger som gjør det enklere for SMB å etablere god praksis.

5

Forsterk regelverk og etterlevelse

NIS2 må implementeres raskt og følges opp med sektorvise kontrollprogrammer. Tilsyn bør være risikobasert og koblet til veiledning og kapasitetsbygging, særlig i små og mellomstore virksomheter.

6

Skap koblinger mellom innovasjon, eksport og kompetanse

Norge har høy forskningsproduksjon men lav kommersialisering. Det bør legges bedre til rette for samarbeid mellom akademia og næringsliv, styrket satsing på sikkerhet i oppstartsbedrifter og bedre eksportbetingelser. Samtidig bør utdanningskapasiteten utvides og etterutdanning innen sikkerhet prioriteres.

Kildehenvisning

Infrastruktur: World Bank/Netcraft (sikre internettservere per million, 2024), Eurostat (avanserte skytjenester, 2024), Internet Society (Route orgin authorization (ROA, IPv4), 2025).

Forskning og utvikling: OpenAlex (vitenskapelige publikasjoner, 2020–2024), Espacenet (godkjente CS-relaterte patenter, 2020–2024)

Utdanning og kompetanse: JRC (læreplaninnhold), Edurank (universitetsrangering av topp-3 universiteter)

Personvern og individatferd: Eurostat (2023): anti-tracking, tilgangskontroll, informasjonskapsler, personvernerklæringer

Næringslivets sikkerhetsrutiner: Eurostat (implementerte tiltak, sikkerhetshendelser, cyberforsikring, 2024)

Regelverk og nasjonal beredskap: National Cyber Security Index (NCSI, 2024)

VEDLEGG

Delområde 1 – Infrastruktur

Indikator	DK (verdi / score)	FI	SE	NO
Sikre servere per mill.	246 546 / **100,0**	177 387 / **71,9**	55 097 / **22,3**	35 470 / **14,4**
Avanserte skytjenester (%)	62,84 / **98,8**	63,62 / **100,0**	56,12 / **88,2**	61,26 / **96,3**
ROA-signerte prefikser (%)	90 / **100**	82 / **91,1**	83 / **92,2**	73 / **81,1**
Snitt (0–100)	**100**	**88**	**68**	**64**

Kilde: World Bank/Netcraft (sikre internettservere per million, 2024), Eurostat (avanserte skytjenester, 2024), Internet Society (Route orgin authorization (ROA, IPv4), 2025).

Delområde 2 – Forskning og utvikling (FoU)

Indikator	DK (verdi / score)	FI	SE	NO
CS-publikasjoner	211 / **37,3**	392 / **69,3**	541 / **95,6**	566 / **100,0**
CS-patenter	36 / **7,0**	237 / **46,1**	514 / **100,0**	42 / **8,2**
Snitt (0–100)	**22**	**58**	**98**	**54**

Kilde: OpenAlex (vitenskapelige publikasjoner, 2020–2024), Espacenet (godkjente CS-relaterte patenter, 2020–2024)

Delområde 3 – Utdanning og kompetanse

Indikator	DK (verdi / score)	FI	SE	NO
Bachelor bredde	2 / **50**	4 / **100**	2 / **50**	4 / **100**
Bachelor spes.	4 / **100**	2 / **50**	3 / **75**	4 / **100**
Master bredde	14 / **56**	12 / **48**	25 / **100**	12 / **48**
Master spes.	3 / **18,8**	7 / **43,8**	16 / **100**	6 / **37,5**
Edurank (topp-3)	37 / **100**	76 / **48,7**	42 / **88,1**	58 / **63,8**
Snitt (0–100)	**76,8**	**67,5**	**104**	**83,6**

Kilde: NyAnalyse, JRC (læreplaninnhold), Edurank (universitetsrangering av topp-3 universiteter).

Delområde 4 – Næringslivets sikkerhetsrutiner og robusthet

Tiltak & styring (høyere=bedre)

Indikator	DK (verdi / score)	FI	SE	NO
⩾5 tiltak	77 / **96,3**	80 / **100,0**	64 / **80,0**	67 / **83,8**
Dokumenterte rutiner	59 / **100,0**	59 / **100,0**	47 / **79,7**	32 / **54,2**
Ansatte gjort kjent	70 / **93,3**	75 / **100,0**	67 / **89,3**	63 / **84,0**
Avansert overvåking	67 / **100,0**	65 / **97,0**	54 / **80,6**	54 / **80,6**
Cyberforsikring	70,6 / **100,0**	33,5 / **47,5**	46,33 / **65,6**	37,98 / **53,8**
Snitt (0–100)	**97,4**	**99,3**	**82,4**	**75,6**

Kilde: Eurostat (implementerte tiltak og rutiner, cyberforsikring, 2024)

Delområde 5 – Sikkerhetshendelser i næringslivet

Hendelser (lavere=bedre; score invertert)

Indikator	DK (verdi / score)	FI	SE	NO
Utilgj. pga angrep, datatap pga. angrep eller lekkasje	19 / **65,7**	42,2 / **29,6**	20,4 / **61,3**	1 / **100**

Kilde: Eurostat (sikkerhetshendelser, 2024)

Delområde 6 – Regelverk og beredskap

Indikator	DK (verdi / score)	FI	SE	NO
NCSI-score	Rank 12 / **33,3**	Rank 4 / **100,0**	Rank 41 / **9,8**	Rank 35 / **11,4**

Kilde: National Cyber Security Index (NCSI, 2024)

Cybersikkerhet totalt (uvektet snitt av delområder, 0–100)

Land	Total (0–100)	Rangering
Finland	**71,9**	1
Sverige	**69,3**	2
Danmark	**65,9**	3
Norge	**64,1**	4

Ny Analyse

NyAnalyse er et uavhengig fagmiljø med samfunnsøkonomer og analytikere. Vi leverer etterprøvbare analyser, prognoser og utredninger til offentlig og privat sektor, med særlig styrke innen næringsutvikling, arbeidsmarked, ringvirkninger og regional verdiskaping. I arbeidet med denne nordiske cybersikkerhetsbenchmarken har vi kombinert samfunnsøkonomisk metode med operasjonelle indikatorer for digital sikkerhet, beredskap og robusthet i næringslivet.

Rapporten er utarbeidet av:

Terje Strøm

Sjeføkonom og partner

terje@nyanalyse.no

Rajee Sivam

Seniorøkonom/konsulent

rs@nyanalyse.no