**Skriftlig innspill fra Juristforbundet og Tech Forum JF til Stortingets justiskomité om Meld. St 9 (2022-2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet**

## En spent sikkerhetspolitisk situasjon

Det er krig i Ukraina og en svært spent sikkerhetspolitisk situasjon. Et autoritært Kina blir stadig mer selvhevdende og demokratiet er på retur i større deler av verden. Verden er preget av sterk polarisering. Begrepet «hybrid krigføring» var for få år siden et begrep som kun en engere krets hadde et forhold til. Men som en stadig raskere digital utvikling og endret trusselbilde på grunn av denne har gjort at både befolkning, næringsliv, offentlig sektor og myndigheter har fått et forhold til begrepet. Vi er i en tid med et digitalt demokrati hvor stater vil fortsette å bruke cyberangrep for å nå politiske mål. Teknologi påvirker stadig større deler av våre liv. Med koronapandemien som katalysator, har digitaliseringen skutt fart særlig de to siste årene. Ekspressdigitaliseringen gjør oss mer sårbare for cyberangrep.

## Regulering i tråd med teknologiutviklingen

Digital motstandsdyktighet forutsetter forståelse av at dette er grenseoverskridende utfordringer. Regelverk må harmoniseres med resten av Europa. Norge mangler i dag regulering av området. EUs NIS-direktiv er ikke innført. Dette må implementeres i norsk rett, herunder **NIS2 som er trådt i kraft og** erstatter NIS-direktivet. Regjeringen må i sitt arbeid sikre at vi raskt får på plass et harmonisert regelverk med EUs nylig lansert Cyber Resilience Act og kommende Cyber Security Act.

## Nye utfordringer og nye krav- Å lære av tidligere feil

Forsterket privat-offentlig samarbeid, økt kompetanse og lovmessige reguleringer som følger teknologiutviklingen må på plass. Basert på gode analyser av fremtidige scenarioer. Justis- og beredskapsdepartementet må ivareta sitt samordnings- og pådriveransvar. Digital sikkerhet er avgjørende for å ivareta Norges kritiske samfunnsfunksjoner og nasjonale sikkerhetsinteresser. Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor (Dok 3:7 (2022-2023) er nedslående lesning etter at departementet har hatt dette ansvaret siden 2013. Det samme gjelder Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer ( Dok 3:3(2022-2023). Funnene må danne et viktig grunnlag for å gjennomføre de forslag og tiltak som behandlingen av denne stortingsmeldingen adresserer.

## Forsterket kollektivt motstandskraft gjennom privat-offentlig samarbeid

Private teknologiaktører utvikler teknologien, opererer og eier infrastrukturen. Teknologiaktører er de første til å beskytte enkelt-individer og virksomheter. Norge må utnytte den nasjonale kapasiteten på privat og offentlig side for å avdekke og håndtere digitale angrep i fellesskap. Sårbarheter ett sted kan få store konsekvenser for mange virksomheter. Styrket cybersikkerhet vil være avhengig av et tettere, mer transparent og relevant partnerskap mellom myndigheter og teknologinæringen. Formaliserte partnerskap og samlokalisering er forutsetningen for bedre utnyttelse av de kapasitetene man har. **Nasjonalt cybersikkerhetssenteret (NCSC)** med fysisk samlokalisering og partnerskap mellom private og offentlige bør videreutvikles for å styrke Norges nasjonal operative evne.

IKT sikkerhetsforum i regi av Justis- og beredskapsdepartementet under ledelse av NSM bør evalueres. Forumet bør erstattes med et **privat-offentlig advisory board** med representanter fra

næringen for å sikre et godt strategisk samarbeid gjennom kompetansedeling og et felles situasjonsbilde. Dette organet bør ha god juridisk digital kompetanse. Vi støtter også Justis- og beredskapsdepartementets arbeid med å etablerer Norges **nasjonale koordineringssenter for digital sikkerhet**, som kan bidra til tett samarbeid med øvrige privat-offentlige IKT-sikkerhetsmiljøer.

### Akutt kompetansebehov

Behovet for tilgang til data og datakraft øker. Det samme gjør behovet for digital kompetanse og kunnskap. NHOs Kompetansebarometer 2022 viser at 2 av 3 bedrifter har et udekket kompetansebehov der nesten halvparten har behov ingeniør og teknisk fagkompetanse. Cybersikkerhetsutfordringene forsterkes av mangel på arbeidskraft. I Norge forsterkes dette ytterligere av behovet for kompetanse og fagfolk innenfor digital sikkerhet. Behovet for cybersikkerhetsfagfolk er akutt. Anslag viser at vi vil mangle 4.100 personer med digitale sikkerhetskompetanse i 2030 . Mangel på digital og IKT-sikkerhets kompetanse er en stor flaskehals for trygg digital omstilling av Norge. Fremtidens og nåværende **jurister** må også selv ha en grunnleggende forståelse for teknologien og hvilke muligheter og begrensninger som ligger i lovverket for å regulere og legge til rette bruken av denne. Styrket forskningsinnsats på rettsvitenskapens rolle, utredning av juristprofesjonens utfordringer når den nye stortingsmeldingen om profesjonsutdanningene blir fremlagt i 2024 og utfordringene som jusutdanningen møter som følge av økt digitalisering, må adresseres. For å skape økt digital trygghet.

Justisdepartementet og justisministeren har et særskilt ansvar for å sørge for at de ulike departementene og fagstatsrådene koordinerer seg slik at utredninger av fremtidig kompetansebehov inkluderer det digitale sikkerhetsperspektivet. Regjeringens videre arbeid må ha særlig fokus på et felles kompetanse- og kunnskapsløft innen sikkerhet. Dette forutsetter at kompetansebehovsutvalget drøfter dette særskilt, herunder jussen og rettsvitenskapens ulike formål: Den er et verktøy som fungerer som en ***forutsetning*** for å nå alle de ulike politiske målene som settes og for å sikre innbyggernes rettssikkerhet. For å sikre at juridiske reguleringer og lovverk som utformes er basert på god digital sikkerhetsforståelse.

### Datasentre en digital grunnmur.

Datasentre er en del av vår digitale grunnmur på linje med ekom. «Skyen» er dataene og tjenestene som befinner seg i datasentre. Disse er ekte, fysiske steder/bygninger som rommer databehandlingsenheter som summer i takt med våre digitale liv tilgjengelig fra datasentre innenfor Norges grenser. Krigen i Ukraina, et økt hybrid og digitalt trusselbilde, har skapet trusler vi aldri før har sett. Krigen i Ukraina har tydeliggjort sårbarheten ved å ha all datasentre plassert i eget land. Debatten om nasjonal suverenitet preget av fredstid i Europa er nå over. Flere nasjoner har nå flyttet fokus fra teknologisk suverenitet og proteksjonisme, der lagring av data på datasentre i eget land har stått sentralt, til å tenke hvordan opprettholde digital suverenitet i tilfelle invasjon ved datalagring på datasentre i alliert land. Som eiere av datasentre verden over spiller teknologiaktørene en hovedrolle i å hjelpe til med å forebygge og forsvare virksomheter, regjeringer og land mot cyberangrep. Tidlig observerte teknologiaktører det russiske militærest målrettede angrep mot Ukrainas statlige datasenter ved bruk av konvensjonelle våpen, koordinert med cyber angrep. Ukraina lyktes likevel å opprettholde sivile og militære operasjoner muliggjort av hjelp fra teknologisektoren. Kritiske offentlige data ble "evakuert" inn i datasentre over hele Europa. Uten teknologien som datasentre muliggjør ville dette trolig vært umulig. Juristforbundet støtter derfor regjeringens behov for å sikre tilstrekkelig redundans, ved å kunne «evakuere» kritiske offentlige data inn i et alliert land gjennom internasjonalt samarbeid og avtaler.