



DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Justis- og beredskapsministeren

Til Nordisk råd

Deres ref.

Vår ref.
21/1478 - EJK

Dato
16.08.2022

Svar på skriftlig spørsmål E9/2022 om nordisk cybersikkerhetssamarbeid

Finlands delegasjon til Nordisk råd har den 17. juni 2022 stilt følgende spørsmål til de nordiske regjeringer:

Inom vilka sektorer och i vilken form samarbetar de nordiska länderna inom cybersäkerhet? Vilket slags konkret gränsöverskridande samarbete mellan myndigheter kommer att göras mellan de nordiska länderna i framtiden?

Svar:

Jeg vil takke Finlands delegasjon for et aktuelt og viktig spørsmål. De nordiske lands regjeringer har merket seg Nordisk råds engasjement for, og den brede støtten til, cybersikkerhetssamarbeid i Norden for å møte nye sikkerhetsutfordringer. Det vitner også om den brede folkelige støtten til økt sikkerhetspolitisk samarbeid i Norden.

Nordiske land samarbeider allerede godt om cybersikkerhetsspørsmål. På overordnet nivå er det et pragmatisk samarbeid mellom landene på cyberområdet, der det legges vekt på at eksisterende samarbeidsstrukturer ikke dupliseres. Det er en god dialog om cybertrusselen og arbeidet med cybersikkerhet mellom nordiske justis-, samferdsels-, utenriks- og forsvarsdepartementer. I tillegg gjennomføres bilaterale møter med de nordiske landene ved behov, f.eks. ved utvikling av nasjonale strategier, for å få bedre innsikt i tiltaksutvikling mv.

De nordiske landene har også et fordelaktig og velfungerende samarbeid om cybersikkerhet med de baltiske landene. Landene deltar årlig i NB8-møter (de åtte nordisk-baltiske landene) om cybersikkerhet, hvor aktuelle saker tas opp og det gis orienteringer fra landene på status og prioriterte saker. Fokus er på kunnskapsdeling

og koordinering, både i forhold til trender i trusselbildet, policyutvikling og aktuelle prosesser i EU, FN og NATO.

Det er også et velfungerende samarbeid mellom de nasjonale cybersikkerhetsmyndighetene og responsmiljøene i de nordiske landene. De operative enhetene, CERTene (Computer Emergency Response Team), skal forebygge, oppdage og håndtere cyberangrep løpende. I regi av Nordic CERT Cooperation (NCC) arrangeres det flere møter årlig. Her deler de nordiske landene kunnskap og erfaringer gjennom regelmessige styregruppemøter og seminarer. I NCC deles også trusselvurderinger og felles situasjonsforståelse.

Lignende samarbeid finnes også på sektornivå i næringslivet, bl.a. i finanssektoren gjennom Nordic Financial CERT. Finanssektoren spesielle situasjon som viktig digital infrastruktur, gjør at sektoren må kunne slå tilbake cyberangrep. Derfor har sektoren i hele Norden gått sammen om et felles operasjonssenter. Nordic Financial CERT har hovedkontor i Oslo, og er til stede i alle de nordiske landene.

Offentlig-privat samarbeid er også sentralt for cybersikkerhet. Statlige myndigheter, private selskap og forsknings- og utviklingsmiljøer har legitime interesser og ansvar i forvaltningen av det digitale rom. De nordiske landene er derfor opptatt av å fremme denne typen samarbeid internasjonalt.

I det nordiske forsvarssamarbeidet har cybersikkerhet blitt satt høyere på dagsordenen de siste årene. I NORDEFECO sin Visjon 2025 vil de nordiske landene arbeide for økt motstandsdyktighet mot cybertrusler. Dette foregår blant annet i arbeidsgruppen for cyberforsvar (Cyber Defence) og ad hoc-arbeidsgruppen for cyberutdanning (Cyber Education). NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) i Estland er også en sentral arena hvor alle de nordiske landene deltar med både finansiering og personell.

Med hilsen



Emilie Mehl