Avsender:
Lillehammer kommune
Postboks 986
2626 Lillehammer

Det Kongelige Forsvarsdepartement
Pb. 8126 Dep.
0032 OSLO

349.1.42

HØRINGSUTTALELSE FRA LILLEHAMMER-REGIONEN PÅ NOU 2023:14, FORSVARSKOMMISJONEN AV 2021, FORSVAR FOR FRED OG FRIHET 2023-08-31

Vedlagt følger brev fra Lillehammer kommune.

Med hilsen
Lillehammer kommune

1#3:f031dac0-357a-4a02-98cc-0a9c9543595f:1

Lillehammer kommune

Dato: 29.08.2023
Vår ref.: ESPJOH 23/7108-1
Arkivkode:
Løpenum: 23/24042
Deres ref:

Det Kongelige Forsvarsdepartement
Pb. 8126 Dep.

0032 OSLO

1.2.

1#5:f031dac0-357a-4a02-98cc-0a9c9543595f:3

HØRINGSUTTALELSE FRA LILLEHAMMER-REGIONEN PÅ NOU 2023:14, FORSVARSKOMMISJONEN AV 2021, FORSVAR FOR FRED OG FRIHET 2023-08-31

I den verdenssituasjonen vi står i, blir det aldri feil å satse på cyberkompetanse og cyberkapasiteter. Dette representerer fremtiden i et stadig mer digitalisert samfunn, og vil være etterspurt både innenfor Forsvaret, næringslivet og akademia.

Innledning

Forsvarskommisjonen beskriver et utfordringsbilde som krever prioritering og handling. Kommisjonen bekrefter at det er behov for en omfattende satsning på sikkerhet, forsvar og beredskap, og den tar til orde for å forsere investeringer og utvikling av forsvars- og beredskapskapasiteter. Forsvaret må styrkes, og det må gjøres nå. Tilsvarende budskap fremmes av Totalberedskapkommisjonen (NOU 2023:17), av Forsvarsjefen (Fagmilitært råd) og av direktøren for Nasjonal sikkerhetsmyndighet (Sikkerhetsfaglig råd).

Lillehammer-regionen deler denne forståelsen av situasjonen, og mener det er riktig å prioritere en vesentlig satsning på sikkerhet, forsvar og beredskap.

I denne høringsuttalelsen vil vi konsentrere oss om de forhold som berører cyberområdet[1], da dette er et område som regionen allerede prioriterer høyt for å utvikle. Vi mener det krever ytterligere satsning og raskere handling fra Stortingets side, og vil i det etterfølgende fremheve og supplere Forsvarskommisjonens beskrivelser og anbefalinger.

Forsvaret, Totalforsvaret og nasjonen har et stort behov for økt kapasitet og kompetanse innenfor cyberområdet. Ved å bygge videre på utviklingen i Lillehammer-regionen og Innlandet vil man få mye ut av satsningen. Regionen vil kunne tilby alt det Forsvaret og Totalforsvaret trenger for å lykkes.

[1] Cyberområdet inkluderer det kommisjonen omtaler som hybrid krigføring, teknologi, påvirkningsoperasjoner og psykologisk krigføring, digitalisering, cybersikkerhet, digital sikkerhet, cyberkriminalitet, cyberspionasje og cyberangrep.

KOMMUNEDIREKTØREN
ADRESSE
Storgata 51, Postboks 986
2626 Lillehammer
EPOST
postmottak@lillehammer.kommune.no
TELEFON
61107700

Sammendrag

Det Forsvaret og Totalforsvaret trenger for å lykkes

Norge, spesielt Forsvaret og Totalforsvaret, har et presserende behov for å styrke sin kapasitet og kompetanse innen cyberområdet. Lillehammer-regionen og Innlandet fremstår som en bastion for cyber- og informasjonssikkerhet i landet. Dette økosystemet, hvor akademia, næringsliv og offentlig sektor samarbeider, gir en unik mulighet. Ved å investere og bygge videre på denne regionens ressurser, kan Forsvaret og Totalforsvaret oppnå de målene Forsvarskommisjonen anbefaler.

Rask handling for å styrke samfunns- og statssikkerheten

Forsvarskommisjonen har understreket behovet for umiddelbare tiltak for å forsterke både samfunns- og statssikkerheten. For å oppnå dette, er det essensielt å konsentrere innsatsen rundt allerede etablerte miljøer. Innlandet, med sitt mangfold av offentlige og private cybervirksomheter og samarbeidsplattformer, gir det ideelle utgangspunktet for å implementere Forsvarskommisjonens anbefalinger.

Samarbeid mellom Forsvaret og sivilsamfunnet

I lys av den raske teknologiske utviklingen og digitaliseringen, har informasjon og data blitt uvurderlige ressurser. Ethvert bortfall av disse kan ha alvorlige konsekvenser, spesielt for kritiske samfunnsfunksjoner. Med trusler som stadig blir mer avanserte, blir samarbeidet mellom Forsvaret og sivilsamfunnet innen cyberdomenet enda viktigere. Dette samarbeidet kan sikre nasjonal sikkerhet mot sofistikerte trusler.

Styrket forsvarsvilje gjennom geografisk spredning

Å diversifisere og utvikle forsvarskapasiteter utenfor de store bysentrene kan øke nasjonal oppmerksomhet og engasjement rundt forsvarsspørsmål. Dette kan i sin tur styrke forsvarsviljen ved å involvere bredere deler av befolkningen og fremme en følelse av nasjonal enhet.

Forsvar mot påvirkningsoperasjoner

I en tid hvor statlige aktører forsøker å underminere demokratier, er det avgjørende å beskytte nasjonen mot påvirkningsoperasjoner. Disse operasjonene kan ha som mål å svekke tilliten mellom myndigheter og befolkning. I Forsvaret har ikke dette blitt sett i sammenheng, verken kompetanse- eller kapasitetsmessig. Gjennom sin virksomhet og kompetanse, vil Cyberforsvaret ha et godt utgangspunkt for å få et ansvar for å beskytte forsvarssektoren mot denne typen aktiviteter. I dette vil det også være et naturlig grensesnitt mot totalforsvaret og samfunnet for øvrig

Teknologisk integrasjon

Forsvaret må anerkjenne og tilpasse seg den stadig økende integrasjonen mellom operasjonell teknologi (OT) og informasjonsteknologi (IT). Dette er spesielt viktig når man vurderer fremtidig organisering og utvikling av IKT-funksjoner i forsvarssektoren. Utviklingen er et argument for å holde disse miljøene og kapasitetene samlet i én organisasjon. Med andre ord bør Cyberforsvaret beholde og utvikle sine miljøer og kapasiteter innen IKT-virksomhet (IT) og CIS-operasjoner (OT).

Kultur for innovasjon

Det må bygges en sterkere kultur og motivasjon for innovasjon og nytenking i Forsvaret. Næringsklynger er en viktig arena for samarbeid mellom forskning- og utdanningsmiljøer, og næringslivet kan bidra til å styrke koblingen mellom utdanning, forskning og innovasjon som Forsvaret

trenger. Dette kan Lillehammer-regionen tilby der cyberklyngen er etablert samt koblingen mot akademia som NTNU-miljøet på Gjøvik.

Umiddelbart behov for kompetanse

Forsvarskommisjonen har påpekt at Forsvaret står i fare for å møte en kritisk mangel på kvalifisert personell, spesielt innen teknologi. Det er avgjørende å ta tak i dette problemet raskt for å sikre nasjonens forsvarsevne.

Trusselbildet på cyberområdet

I tillegg til kommisjonens beskrivelse av trusselbildet knyttet til cyberområdet, ønsker vi å trekke frem noen ytterligere argumenter som forsterker kommisjonens budskap.

Cyberdomenet – et eget krigs- og operasjonsdomene

Cyberdomenet ble i 2016 bekreftet av NATO og Norge som et eget krigs- og operasjonsdomene, på samme måte som land-, sjø- og luftdomenene. Cyberangrep som militært verktøy fungerer noe annerledes enn de konvensjonelle maktmidlene. Dermed endrer også innføringen av cybermakt noe av karakteren rundt militære konflikter.

Under krigen i Ukraina har vi sett militær cybermakt blitt brukt langt ut over det som en vil definere som folkerettslig akseptabelt. Mot medier, mot sivile selskaper, mot kritisk nasjonal infrastruktur og mot offentlige institusjoner som ikke er en del av militærmakten. Dette beskriver kommisjonen godt.

Sammensatt aktørregister med varierende intensjon og motivasjon

I tillegg til de statlige aktørene som utkjemper en digital konflikt i Ukraina, så ser vi et betydelig antall aktive grupperinger som ikke svarer til nasjonalstater. Dette er selvorganiserende og delvis statsfinansierte hacker-nettverk, aktivistgrupper og leiesoldat-liknende aktører. I tillegg kompliseres bildet ytterligere med aktiviteter som svindel, vinningskriminalitet, propaganda og desinformasjon. Mye tyder på at utviklingen fortsetter, og at fremtidens konflikter blir langt mer komplekse enn de vi har sett tidligere som følge av dette bildet. Trusselaktørene forholder seg ikke til folkeretten eller konvensjonene som nasjonalstater har skrevet under på, men rammer bredt og rammer de målene - sivile som militære - som de klarer å finne.

Under pandemien så vi en markant økning i antall cyberhendelser rundt omkring i verden. Kriminelle, hacktivister og andre som bruker internett til økonomiske forbrytelser og påvirkningskampanjer, viste evne til å hurtig skifte sin oppmerksomhet mot de områdene der pandemien til enhver tid skapte mest kaos. Dette er også en logisk måte å operere på, fordi sannsynligheten for at deres operasjoner skal lykkes bygger på lokal frykt, usikkerhet, bekymring og et informasjonsvakuum. Siste året rapporterte Falcon OverWatch en økning i antall hackerangrep på 40% globalt. Tidligere år har økningen vært enda høyere.

Dette er globale trusler og globale trusselaktører. Den globale markedsplassen og internetts utbredelse gjør det mulig for dem å operere i sanntid fra hvor som helst i verden. Det betyr også at de ikke trenger en global krise for å lykkes, de kan med letthet utnytte en regional eller lokal krise ganske raskt etter at den oppstår. Disse trusselaktørene opererer utenfor det juridiske området som deres ofre befinner seg i, noe som gjør det svært vanskelig å forfølge dem rettslig. Sannsynligheten for å bli tatt er minimal, og gevinstpotensialet er stort.

Kriser oppstår nå med en frekvens og intensitet vi tidligere ikke har sett. Disse krisene tiltrekker seg cyberaktører som ser muligheter i kaoset. Med klimaendringer, geopolitiske spenninger, kriger og pandemier, lever vi i en tid med økt usikkerhet. Cyberaktører utnytter disse krisene.

Sivile virksomheter rammes av militære cyberaktører

Militære og sivile cyberoperasjoner vil kunne medføre at vi i fremtidens kriser og konflikter, i større grad vil se at bredere lag av samfunnet vil kunne rammes, og det vil fordre en annen form for beredskap og reaksjonsevne hos oss alle. Sivile virksomheter vil bli truffet av svært kompetente militære og statlige motstandere. Det er motstandere som besitter vesentlig mer kapasitet og kompetanse enn de kriminelle trusselaktørene som mange virksomheter møter og bekymrer seg for til daglig. Og vesentlig mer enn det organisasjoner, statlige eller private, velger å investere i å beskytte seg mot i dag. Samtidig er det en stor bekymring at det i enkelte land ser ut til å utvikle seg forbindelser mellom statlige cyberorganisasjoner og kriminelle grupper. Dette vil medføre at mange av de kriminelle gruppene øker sin kompetanse og blir stadig mer avanserte. Angrep fra kriminelle grupper generelt, og kanskje spesielt angrep som omfatter utpressing, har etter hvert blitt et stort samfunnsikkerhetsproblem. På global basis er det økonomiske omfanget av denne typen kriminalitet svært stort. Det anerkjente Center for International and Strategic Studies skrev i en rapport fra september 2022, at finansnæringen i USA hadde anslått at det ble utbetalt mer enn 590 millioner dollar i løsepenger bare i løpet av første halvår 2021. Det er ingen indikasjoner på at den cyberrelaterte kriminaliteten vil reduseres i omfang. Snarere tvert imot, mye tyder på at bruken av kunstig intelligens og Deep Fakes vil tilta, og gjøre det enda vanskeligere å beskytte seg mot kriminell virksomhet i cyberdomenet.

Sårbare verdi- og leveransekjeder

Dagens moderne samfunn er langt mer sammensatt enn tidligere. Nasjonalstatenes maktapparat har avhengigheter som strekker seg langt inn i samfunnet, og verdikjeder som treffer både sivile virksomheter, næringsliv og andre aktører. For de kritiske samfunnsfunksjonene i Norge så inkluderer verdikjedene et utall av aktører. De består av andre offentlige sektorer og etater, private næringslivsaktører, materiellprodusenter, materielleverandører, matvareprodusenter, matvareleverandører, medieaktører, energiselskaper, telekom-aktører og sågar utenlandske aktører, spesielt på teknologisiden. Alle disse kontraktspartene har sine underleverandører og respektive verdikjeder – og alle utgjør i større eller mindre grad en sårbarhet for virksomhetens operasjoner. Det betyr at det er risiko for at en vil kunne søke å ramme virksomhetens operasjoner og leveranser gjennom å ramme underleverandører. Det finnes eksempler på vellykkede cyberangrep mot store norske virksomheter, hvor svakheter hos en underleverandør ble utnyttet.

Ledere i både statlige og private virksomheter har liten oversikt og kontroll over sine verdikjeder. Trusselaktører har verdikjedeutfordringene på radaren – og ledere i virksomheter må definitivt også få søkelyset på disse områdene dersom vi skal kunne evne å forsvare virksomheten vår, verdiene våre og samfunnet vårt.

Lederansvaret

I det samfunnet som vi nå lever i, vil cybertrusler, teknologiske utfordringer og ledelsesutfordringer være del av alle kriser. Grensene mellom stats- og samfunnssikkerhet viskes ut når både mulighetene og sårbarhetene i det digitale rom vokser frem i et voldsomt tempo. Det er vesentlig at alle ledere i offentlig og privat sektor motiveres til å tenke på samfunnets og statens sikkerhet, ikke bare sin virksomhet i isolasjon, fordi de aller fleste er del av verdi- og leveransekjeder med betydning for samfunns- og statssikkerheten. Derfor engasjerer Lillehammer-regionen seg sterkt i utviklingen av cybermiljøer og cyberkompetanse i Innlandet, for samfunnets og Totalforsvarets beste.

Konsekvenser av økt digitalisering og nye cybertrusler

Digitale angrep mot både norske offentlige og private virksomheter og bedrifter, viser tydelig hvilke konsekvenser bortfall av både informasjon, systemer og tjenester vil ha i det moderne samfunn. Data og informasjon representerer store verdier, således blir det svært viktig å sikre nødvendig konfidensialitet, integritet og tilgjengelighet på informasjonen. Erfaringer fra blant annet krigen i Ukraina viser betydningen av å ha både robuste (mer av samme teknologi) og redundante (forskjellige teknologier) løsninger for prosessering og lagring av data. I krisesituasjoner er det åpenbart viktig å legge til rette for å opprettholde samfunnets kritiske funksjoner. Et vesentlig forhold for å kunne lykkes er å ha tilgang på data og informasjon (øyeblikkelig kommunikasjon) til enhver tid. Redundans og robusthet krever nye investeringer i flere kapasiteter – både i antall og typer – og en geografisk spredning av kapasitetene. En slik spredning må også vurderes å inkludere Norden og Europa. Som eksempel kan nevnes at Ukraina flyttet sine data ut av landet for å sikre dem mot angrep.

Enkeltindivider, både som ansatte i virksomheter og som privatpersoner blir stadig mer utsatt for uønskede digitale hendelser. Ofte er det enkeltpersonene som også blir benyttet «angrepspunkt» ved store og alvorlige angrep. Ofte benyttes det forskjellige former for er sosial manipulering. Dette kan skje gjennom utsending av falske e-mail og telefonoppringninger. Imidlertid benyttes også sosiale medier, herunder kontokapring, SMS, falske nettsider, Messenger o.l., datingsider, i forbindelse med manipulering.

Dette er en av de vanligste måtene å skaffe seg uautorisert tilgang til systemer, applikasjoner og informasjon. Utfordringen med denne type angrepsmetoder er at det i svært liten grad kan forhindres ved hjelp av teknologiske løsninger, men at det er kunnskapen, oppmerksomheten og bevisstheten til den enkelte av oss som avgjør om angriperen vil lykkes eller ikke. Det er derfor svært viktig å legge vekt på å øke kunnskap og forståelse også på individnivå.

Konsekvenser av den teknologiske utviklingen

Data i sentrum for enhver organisasjon

Mange virksomheter, Forsvaret og forsvarssektoren er intet unntak, beskriver og forholder seg til IKT og cyberkapasiteter som rene støttefunksjoner. En slik forståelse gir et misvisende bilde av hvor eksistensielt viktig dette nå har blitt, og det bidrar til dysfunksjonelle organiserings- og styringsformer. Det bidrar også til den manglende satsningen Forsvarskommisjonen etterspør.

Vi må ta inn over oss at IKT nå går fra å være verktøy som understøtter virksomheter og samfunnsfunksjoner, til en premissgiver for organisering og prosesser. IKT står nå i sentrum i moderniseringen, i sentrum for digitaliseringen og i sentrum for operasjonene.

Det er fundamentalt viktig for enhver virksomhet at man klarer å forene operatørene – eller brukerne av teknologien – med teknologene. Altså brukerkompetanse sammen med teknologi- og sikkerhetskompetanse. Dette er viktig for at man skal evne å utvikle, drifte og videreutvikle sikre tjenester, prosesser og organisasjoner på en fordelaktig måte. Dette handler mye mer om organisasjonskultur og kompetanse enn om teknologi.

Denne forståelsen av IKT-ens plass i samfunnsutviklingen får noen konsekvenser:

- Data er en strategisk ressurs - og er virksomhetens verdier
- Beskyttelse av IKT og data - altså cybersikkerhet - blir eksistensielt viktig
- Totalkostnader knyttet til IKT i enhver virksomhet vil øke

- Teknologi både former og formes av organisering og ledelse
- Brukere og ledere må lære mer om IKT og ta et større ansvar for IKT-virksomheten, og IKT-personell må ta et større ansvar for den operative virksomheten

Denne samfunnsutviklingen stiller nye krav til kunnskap og kompetanse. Det krever også en ny type lederskap, som kombinerer tradisjonell forretningsforståelse med en forståelse av hvordan teknologien samvirker med, påvirker og motvirker organisasjonen. Det er ikke lenger nok å bare forstå virksomheten; man må også forstå det dynamiske og komplekse digitale landskapet og trusselbildet virksomheten opererer i.

Operasjonell teknologi (OT) og informasjonsteknologi (IT) smelter sammen

Cyberteknologi er nå essensielt for daglig drift i alle typer virksomheter, fra små bedrifter til store multinasjonale selskaper. Denne teknologiske integrasjonen gir økt sammenkopling og økt verdiskaping, men også økt sårbarhet - hvor et cyberangrep kan ha store ringvirkninger. Operasjonell teknologi (OT), som brukes for tjenesteproduksjon i for eksempel kritisk infrastruktur, er i ferd med å smelte sammen med informasjonsteknologi (IT) og kobles til internett. OT er tradisjonelt sett mindre avansert når det gjelder cybersikkerhet, og organisasjonskulturen i virksomheter som benytter OT er i mindre grad konsentrert rundt cybersikkerhet. Derfor introduseres nå disse virksomhetene for nye trusler og sårbarheter. I en verden hvor teknologi representerer premisset for globalisering og øyeblikkelig kommunikasjon, kan selv små sammenbrudd ha store konsekvenser for økonomier og samfunn.

Dette faktum bør Forsvaret ta inn over seg når man nå skal forbedre etatsstyringen og utvikle og omorganisere IKT-funksjonene i forsvarssektoren. I Forsvaret er trolig OT i stor grad det samme som CIS-operasjoner. Utviklingen beskrevet over er et argument for å holde disse miljøene og kapasitetene samlet i én organisasjon. Med andre ord bør Cyberforsvaret beholde og utvikle sine miljøer og kapasiteter innen IKT-virksomhet (IT) og CIS-operasjoner (OT).

Dette vil representere en naturlig og riktig videreutvikling av de politiske beslutningene som har blitt fattet, basert på tidligere langtidsplaner for forsvarssektoren. I denne sammenheng vises det blant annet til Stortingsproposisjon 14 S (20-21), hvor det ble lagt til grunn at Cyberforsvaret skulle styrkes med blant annet flere ansatte til Cybersikkerhetssenteret.

Cyberforsvaret bør også beholde sitt navn – i lys av utviklingen innenfor cyberområdet blir det helt feil å endre dette nå. Begrepet "cyber" har kommet for å bli, noe som kommer godt frem i det sikkerhetsfaglige rådet til NSM. Der benyttes dette begrepet gjennomgående for første gang.

Forsvar mot påvirkningsoperasjoner

Det er ikke usannsynlig at flere statlige trusselaktører har et langsiktig perspektiv på sine mål og sin virksomhet. Ett av målene kan være å påvirke demokratiet, og tilliten mellom myndigheter og befolkning. En trusselaktører kan også ha som mål å påvirke beslutninger og handlemåter i en spesifikk sak. Denne type virksomhet er i stor grad innrettet mot det kognitive domenet. Informasjonsoperasjoner kan sies å være en del av påvirkningsoperasjoner, men har tradisjonelt vært benyttet i militær sammenheng, hvor elektronisk krigføring, cyberoperasjoner, psykologiske operasjoner, villedning og operasjonssikkerhet inngår. De fleste utviklingstrender indikerer at det blir stadig viktigere å beskytte seg mot denne typen aktiviteter og virksomhet i fremtiden. Dette gjelder i både sivil og militær sammenheng. I Forsvaret har ikke dette blitt sett i sammenheng, verken kompetanse- eller kapasitetsmessig. Gjennom sin virksomhet og kompetanse, vil Cyberforsvaret ha et

godt utgangspunkt for å få et ansvar for å beskytte forsvarssektoren mot denne typen aktiviteter. I dette vil det også være et naturlig grensesnitt mot totalforsvaret og samfunnet for øvrig.

Konsekvenser av klimaendringene - bærekraft og innovasjon

Mens verden beveger seg mot mer bærekraftige løsninger og det grønne skiftet, øker samtidig vår avhengighet av digitale verktøy – og dermed sårbarheten. Selv om overgangen til bærekraftige løsninger er avgjørende for planetens fremtid, må vi også anerkjenne de potensielle risikoene. Hver ny digital løsning gir også nye angrepsvektorer for potensielle trusler, og det er viktig for virksomheter å integrere innovasjon og utvikling med cybersikkerhet. Hvis ikke dette gjøres kan cybersikkerhet bli en *barriere* for økt bærekraft.

Regional utvikling tilrettelagt for en satsning på sikkerhet, forsvar og beredskap

Forsvarskommisjonen tar til orde for rask handling og økt satsning for å realisere en nødvendig styrking av samfunns- og statssikkerheten. Vi mener den riktige og sannsynligvis eneste måten å oppnå et slikt mål på er å konsentrere kraft og oppmerksomhet rundt allerede etablerte miljøer, organisasjoner og kapasiteter. I Innlandet finnes det et stort antall cybervirksomheter og samarbeidsarenaer for disse, noe som representerer det beste utgangspunktet for å realisere Forsvarskommisjonens anbefalinger.

Innlandet representerer Norges ledende økosystem innenfor cyber- og informasjonssikkerhet, hvor både akademia, næringsliv og offentlig sektor ved blant andre Cyberforsvaret møtes.

NTNU, CCIS og NORCCICS på Gjøvik

NTNU Gjøvik med institutt for informasjonssikkerhet og kommunikasjonsteknologi representerer et stort, kompetent og innovativt akademisk fagmiljø innenfor cyber- og informasjonssikkerhet. De har sterke fagmiljøer innenfor både biometri, krypto og digital etterforskning. I tillegg til å gjennomføre kompetanseheving og utdanningsvirksomhet fra enkeltkurs til doktorgradsprogrammer, er NTNU vertskap for Centre for Cyber og Informations Security (CCIS) som har en rekke norske offentlige og private virksomheter og bedrifter som medlemmer. CCIS er i tillegg medlem av The European Cyber Security Organization. NTNU er vertskap for Norsk senter for cybersikkerhet i kritiske virksomheter (Norwegian Centre for Cybersecurity in Critical Sectors – NORCCICS). Ut over dette har NTNU også bygget opp The Norwegian Cyber Range som gir mulighet for å trene og øve både enkeltindivider, grupper og staber på cyberrelaterte hendelser og kriser.

NTNU på Gjøvik representerer et unikt innovasjonsmiljø, som gir grobunn for start-ups og nye virksomheter som leverer unike løsninger og produkter som er i fremste rekke på verdensbasis. Eksempler på dette er MOBAI som utvikler unike biometriske gjenkjenningsløsninger. AIBA er et annet eksempel på en virksomhet som har sitt utspring fra NTNU. Dette firmaet utvikler løsninger basert på kunstig intelligens for å beskytte barn fra overgrep på nett.

NTNU og Cyberforsvaret

Det er sterke faglige synergieffekter mellom NTNU og Cyberforsvaret på Jørstadmoen. Dette gjelder både i forskningssammenheng, samt i utdannings- og annet utviklingsrelatert arbeid. I tillegg til Cyberforsvaret er også Forsvarets høgskole representert på Jørstadmoen med Cyberingeniørhøgskolen. Gjennom mange år har det vært et meget tett samarbeid mellom Cyberingeniørhøgskolen og NTNU. Dette har bidratt til store gjensidige synergieffekter når det gjelder utveksling av akademisk personell, og annet faglig og administrativt samarbeid.

NTNU og Cyberforsvaret samarbeider også på et annet område. Sammen med Advansia leder de et felles, nasjonalt initiativ med mål om å utforske og dele kunnskap om utfordringer innen organisasjon og ledelse i sammenheng med cybersikkerhet. Initiativet legger opp til en bred forståelse av cybersikkerhet som organisasjons -og samfunnstema, og inkluderer strategiske og operative spørsmål i og mellom organisasjoner med ulike kritiske roller i samfunnssikkerhet og krisehåndtering.

Høgskolen Innlandet

Høgskolen i Innlandet tilbyr, både som heltids- og deltidsstudier, svært relevante emner i et Totalforsvarsperspektiv generelt, og i et Cybersikkerhetsperspektiv spesielt. Dette bidrar til å gi en relevant og hensiktsmessig akademisk bredde, som styrker flerfagligheten, og som gir et svært godt utgangspunkt for å kunne ivareta nye oppgaver i regionen og bidra til næringsutvikling. Av relevante studietilbud kan nevnes beredskap og krisehåndtering, bærekraft, digital sikkerhetskultur, innovasjon, ledelse og digitalisering, samt spillteknologi og simulering.

Digitale aktører i Innlandet

Digital Innlandet er et nettverk bestående av nærmere 70 virksomheter som utgjør et sterkt kompetansemiljø innen digitalisering og digital transformasjon. Som en del av Digital Innlandet, er The Norwegian Cluster for Cyber Security, cyberklyngen, etablert. Hensikten med denne klyngen er å utvikle innovative cybersikkerhetsløsninger for å kunne håndtere stadig mer utfordrende trusselaktører. I tillegg er det en uttalt målsetning å styrke samarbeidet mellom partnerne på den ene siden, og mellom partnerne og akademia på den andre.

I tillegg til disse virksomhetene, er Norsk senter for informasjonssikring (NorSIS) på Gjøvik. NorSIS er en aktør som har cybersikkerheten til befolkningens som fokusområde og samfunnsoppdrag. NorSIS har etablert et godt samarbeid med både NTNU og cyberklyngen.

På Lillehammer har vi Nasjonalt senter for informasjonssikkerhet i kommunesektoren. Kommune-CSIRT støtter kommuner og fylkeskommuner med relevant informasjon om trusler, hendelser og sårbarheter i det digitale domenet. CSIRT-en er et ressurssenter for praktisk rådgivning og støtte ved cyberhendelser og andre digitale utfordringer i kommunesektoren.

Beslutningen om å etablere Økokrims bedragerienhet på Gjøvik, som sannsynligvis vil ha cyberrelaterte oppgaver, vil bidra til å befeste og styrke de cyberrelaterte fagmiljøene i Mjøsregionen.

Det kan også nevnes at flere av de store kommersielle digitaliserings- og cybersikkerhetsaktørene er i ferd med å etablere seg i Innlandet, som Sopra Steria, Deloitte og Defendable.

CyberLand er et annet initiativ som er etablert av Innlandet fylkeskommune, Gjøvikregionen Utvikling og Lillehammer-regionen Vekst, i samarbeid med blant andre Statsforvalteren i Innlandet, NTNU og Cyberforsvaret. Dette initiativet handler om cybersikkerhet for både enkeltindivider og samfunnet, basert på kunnskap og kompetanse. Det legges også vekt på å benytte partnere for å få tilgang på internasjonale miljøer som er ledende på teknologiutvikling.

På arrangementssiden har Innlandet en meget sterk posisjon. Eksempler på dette er både Sikkerhetsfestivalen og Totalforsvarets Cybersikkerhetskonferanse som gjennomføres på Lillehammer, og Security Divas som er en veletablert konferanse for kvinner som jobber med eller er interessert i cybersikkerhet. Dette er blitt en viktig arena for å stimulere til større mangfold innenfor dette viktige fagområdet.

I Mjøsområdet finnes det en rekke store samfunnskritiske industri-/produksjonsbedrifter. Noen eksempler på dette er Nortura, Nammo, Hexagon Ragasco, flere større kraftprodusenter. Dette er

bedrifter som er sterkt avhengige av operasjonell teknologi for å gjennomføre sin produksjon. I den senere tid har integrasjoner og koblinger mellom IT-baserte systemer og løsninger og operasjonell teknologi blitt mer vanlig og nødvendig, blant annet for å effektivisere produksjonsprosessene. Dette har imidlertid introdusert nye og kritiske cyberrelaterte sårbarheter som det er svært viktig å kunne håndtere. Kunnskapen og kompetansen som finnes i Innlandet både i bedriftene og i akademia, er svært viktig både i et regionalt samt i et nasjonalt og internasjonalt perspektiv.

Denne oversikten viser tydelig både bredden og dybden i det etablerte cybersikkerhetsmiljøet i Innlandet. Som beskrevet er det allerede etablert et velfungerende samarbeid mellom flere av aktørene. Ved å satse ytterligere på dette miljøet, vil man bidra til en rask styrking av Forsvaret, Totalforsvaret og samfunnet for øvrig. Effekten av dette vil blant annet bli en bedre evne til å håndtere cyberrelaterte hendelser og angrep i både et samfunns- og statssikkerhetsperspektiv.

Mjøsregionen er Innlandets raskest voksende næringslivsregion og innenfor 50 minutters reiseavstand ligger de fem mjøsbyene Hamar, Gjøvik, Lillehammer, Brumunddal og Moelv. Med ny firefelts motorvei, og gode togforbindelser fra Oslo, fremstår vi som meget attraktivt med tanke på ny næringsetablering. Regionen er et meget attraktivt boområde, og er i stand til å tiltrekke seg etterspurt og høy kompetanse. Området har svært god kapasitet, erfaring og kompetanse på planlegging og gjennomføring av store arrangementer, noe som også bidrar til å gjøre området attraktivt, både i et nasjonalt og internasjonalt perspektiv.

Forsvarsvilje og næringsutvikling - en synergisk tilnærming

I en tid hvor trusler og utfordringer stadig endrer seg, er det avgjørende at Forsvaret og sivilsamfunnet jobber tett sammen for å sikre nasjonens sikkerhet og velferd. En integrert tilnærming mellom Forsvaret og sivil sektor i Innlandet kan bidra til økt forsvarsvilje og næringsutvikling.

Samarbeid mellom Forsvaret og Sivilsamfunnet

Forsvarets kapasiteter er ikke bare avgjørende for nasjonal sikkerhet, men også for støtte til sivil sektor. Forsvarskommisjonen peker på viktigheten av dette samarbeidet, og vi mener dette spesielt gjelder innen cyberdomenet. Med trusler som stadig blir mer sofistikerte, kan cybertotalforsvaret blitt en nøkkelfaktor i nasjonal sikkerhet. Potensialet for et styrket samarbeid mellom Forsvaret og sivilsamfunnet er stort, hvor begge parter kan dra nytte av hverandres ressurser og ekspertise.

Forsvarsvilje gjennom geografisk spredning

Ved å satse på og utvikle forsvarskapasiteter utenfor storbyene, skapes det en økt oppmerksomhet rundt forsvar i hele landet. Dette har en positiv innvirkning på forsvarsviljen, da det engasjerer flere deler av befolkningen og skaper en følelse av nasjonal enhet.

Fordelene med forsvarskommuner

Forsvarskommuner gir Forsvaret ideelle rammer for sin virksomhet. I motsetning til i større byer, hvor Forsvaret kan føle seg oversett, gir nærheten til Forsvarets avdelinger i disse kommunene en unik mulighet for samarbeid og integrasjon.

Bygge på eksisterende ressurser

Selv om det er viktig å utvikle nye samarbeidsklynger og kapasiteter, er det også avgjørende å bygge på det som allerede eksisterer. Som beskrevet i forrige kapittel har Innlandet allerede etablerte ressurser som kan utvikles og utnyttes for å styrke Forsvarets kapasiteter.

Næringsutvikling gjennom Startups og Spinoffs

Startups som Mobai, Aiba og Diri, som har sitt utspring fra etablerte miljøer i Innlandet - ref. Forrige kapittel - viser potensialet for næringsutvikling på cyberområdet i regionen. Disse selskapene representerer fremtiden for industrien, og kan bidra til å skape nye næringer og arbeidsplasser.

Kompetanseutvikling – regional satsning for nasjonal effekt

Forsvarskommisjonen stadfester at Forsvaret potensielt står overfor en kritisk personellmangel med for svak kompetanse på viktige områder, deriblant nødvendig teknologikompetanse. Dette vil gå ut over forsvarsevnen. Vi støtter kommisjonens analyse og konklusjon. Vi mener at det bør satses offensivt på kompetanseutvikling, og det bør startes umiddelbart - her er det ingen tid å miste.

Kommisjonen bekrefter at forsvarssektoren henger etter innen digitalisering og IKT. Evnen til å utnytte data er avgjørende for å kunne dra nytte av en rekke brytningsteknologier. Forsvarskommisjonen understreker at cyberforsvar, til syvende og sist handler om Forsvarets evne til å operere.

Når det gjelder hvem som har behov for kompetanseutvikling omfatter det til en stor grad alle nivåer i Forsvaret inkludert Forsvarsdepartementet. Dette betyr at fag- og funksjonsutdanning, nivådannende utdanning samt lederutdanning må styrkes. Departementet må ha nødvendig kompetanse innenfor brytningsteknologi som kunstig intelligens, cyber og romvirksomhet. Slik kan man forstå det fremtidige trusselbildet og nyttiggjøre seg fortrinnene Norge har for å motvirke trusler og anslag.

Kommisjonen stadfester videre at det må sees helhetlig på tre områder for å utvikle nødvendig kompetanse: En styrking av Forsvarets utdanning, økt bruk av sivile utdanningsmuligheter, og et tettere nordisk samarbeid om utdanning. Kommisjonen anbefaler at Forsvaret i større grad benytter sivile utdanningsmuligheter og anerkjenner relevant sivil utdanning og kompetanse der det er mulig. Karriereutvikling i Forsvaret og forsvarssektoren bør sees som en del av Totalforsvaret, der det legges til rette for å veksle mellom operativ tjeneste og perioder i sivil sektor, industri og næringsliv. Forsvarets cyberkompetanse må utnyttes bedre i et tettere samarbeid mellom militær og sivil sektor.

Vi mener det må bygges en sterkere kultur og motivasjon for innovasjon og nytenking i Forsvaret. Næringsklynger er en viktig arena for samarbeid mellom forskning- og utdanningsmiljøer og næringslivet kan bidra til å styrke koblingen mellom utdanning, forskning og innovasjon som Forsvaret trenger. Det er nettopp dette Lillehammer-regionen kan tilby der cyberklyngen er etablert samt koblingen mot akademia som NTNU-miljøet på Gjøvik. Her vil det ligge til rette for innovasjon i det digitale domenet, der det hentes effekter gjennom samarbeid mellom sivile og militære avdelinger – og akademia. Dette vil samtidig være svært positivt for regional næringsutvikling.

Innlandet har et svært godt utgangspunkt, antagelig det beste regionale utgangspunktet i Norge, når det gjelder både å utvide eksisterende utdanning ved NTNU på Gjøvik med koblingen mot cyberforsvarsmiljøet på Jørstadmoen, samt å tilby ny utdanning. Forsvarets høgskole er også representert på Jørstadmoen med Cyberingeniørskolen, noe som gir ytterligere muligheter. Et samarbeid mellom Cyberforsvaret, Forsvarets Høgskole, Innlands-kommuner og næringslivet kan bidra til et økt antall utdanningsplasser ved både Cyberteknikerutdanningen, Cyberingeniørutdanningen og utdanningen ved NTNU Gjøvik. Det å bygge på disse anerkjente lærestedene vil komme hele landet til gode.

Grunnleggende innføring i digitale trusler, og praktisk opplæring i hvordan man som soldat og sivil kan bidra til å redusere digital sårbarhet bør tilbys som del av førstegangstjenesten. Her ligger en mulighet for å utvikle nye kurs for dette behovet.

Digitale utdanningstilbud med fleksibilitet i kursenes omfang og som virkemiddel til å løse utfordringer sektoren står overfor bør tilbys. Det er behov for utdanningsinstitusjoner som tilrettelegger og fasiliteter kurs, gjerne med andre lærekrefter enn NTNU Gjøvik har, for å øke teknologikompetansen i hele bredden i sektoren, fra topp til bunn i Forsvaret, samt også bidra til å møte spesialistenes behov for formell kompetanse. Samarbeid med Forsvarets høyskole for å tilby utdanning som møter Forsvarets behov er en stor mulighet som bør benyttes. Dette tilbudet kan også bygges videre ut for å tilby generell IT- og cyberkompetanse til andre målgrupper hos myndighetene, i offentlig sektor og i næringslivet.

Regionen har også en unik mulighet til å tilby utvidet utdanningstilbud i form av kurs med kombinasjon mellom bærekraft og cybersikkerhet der NTNU på Gjøvik allerede tilbyr bachelor- og mastergrad innenfor dette emnet. Fra optimal styring av energi til løsninger som gjør at vi forbruker færre råvarer, reiser mindre eller utnytter data på nye områder, er det behov for systemer og komponenter som er koblet til internett. Dermed blir de mål for kriminelle, og cybersikkerhet er som nevnt tidligere en av de store barrierene for økt bærekraft. Et slikt kurs bør kunne tilbys til en stor del av Forsvarets personell samt alle som har en rolle hos aktører som er en del av Totalforsvaret.

Lillehammer-regionen er bekymret for kompetanse- og kunnskapsnivået i Norge. Det fremstår som at Norge ikke evner å produsere nok formalkompetanse til å dekke Norges behov. Det kan være tidsriktig å vurdere å etablere verneplikt knyttet til beskyttelse mot digitale trusler gjennom Forsvaret på Jørstadmoen for å produsere et antall personer hvert år med uformell kompetanse som kan bidra til å kompensere for det som fremstår som et betydelig gap mellom tilgjengelig kompetanse og samfunnets kompetansebehov. Unge mennesker med uformell kompetanse, men operativ erfaring fra Forsvaret, vil formodentlig kunne løse oppgaver som ikke krever tung formell kompetanse. Samtidig vil disse bidra til å frigjøre personellressurser til viktige oppgaver som krever tung formell kompetanse, og Forsvaret er nok den eneste institusjonen i samfunnet som kan produsere slik kompetanse.

Avslutning

Lillehammer-regionen anerkjenner og støtter Forsvarskommisjonens argumentasjon og anbefaling om et presserende behov for å satse på utvikling av kapasiteter og kompetanse innenfor cyberområdet. Dette må gjøres for at vi skal evne å håndtere det komplekse trusselbildet nasjonen står overfor, og for at vi skal oppnå tilstrekkelig sikkerhet, forsvar og beredskap.

Det er allerede etablert et omfattende og voksende cybermiljø bestående av militære og sivile, offentlige og private virksomheter i Lillehammer-regionen og Innlandet. Dette er i tråd med tidligere regjeringers og Stortings beslutninger tilbake til Prop. 73 S (2011-2012) og Innst. 388 S (2011-2012). Dette miljøet vil være det beste utgangspunktet for en satsning slik Forsvarskommisjonen tar til orde for, slik at Forsvaret, Totalforsvaret og nasjonen oppnår tilfredsstillende stats- og samfunnssikkerhet på kortest mulig tid.

Lillehammer-regionen mener Stortingets tidligere vedtak og momentene som framkommer i dette høringssvaret må legges til grunn i utviklingen av det Forsvarskommisjonen beskriver som en egen digital strategi for forsvarssektoren.

Med hilsen – på vegne av kommunene i Lillehammer-regionen

Espen Granberg Johnsen

Strategisk rådgiver i Lillehammerregionen

Kopi:

Gausdal kommune

Øyer kommune