NSM

Vår saksbehandler	Vår dato	Vår referanse
	30.11.2023	U-23/01481-1
	Deres dato	Deres referanse
	Antall vedlegg	Side
		1 av 6

Til
KOMMUNAL- OG DISTRIKTSDEPARTEMENTET
Postboks 8112 DEP
0032 OSLO

Innspill til ny nasjonal digitaliseringsstrategi

Nasjonal sikkerhetsmyndighet (NSM) viser til Regjeringen.no, og ønsker med dette å gi innspill til arbeidet med ny digitaliseringsstrategi. Innspillene beskriver NSMs forventninger til strategien, hvilke drivkrefter og utfordringer en digitaliseringsstrategi bør ta høyde for, samt konkrete innspill til tiltak.

1. Innledning

Nasjonal sikkerhetsmyndighet er Norges direktorat for nasjonal forebyggende sikkerhet. Tjenestens hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, forskning, tilsyn, testing, utredninger og kontrollaktiviteter bidrar NSM til at virksomheter sikrer sivil og militær informasjon, systemer, objekter og infrastruktur med betydning for nasjonal sikkerhet. NSM er det nasjonale fagmiljøet for digital sikkerhet, og skal understøtte og bidra til utøvelsen av Justis- og beredskaps-departementets og Forsvarsdepartementets ansvar på det digitale sikkerhetsområdet. NSM er ansvarlig for et nasjonalt varslingssystem for å avdekke og varsle om cyberangrep mot digital infrastruktur. NSM har også et nasjonalt ansvar for å koordinere håndteringen av alvorlige cyberangrep.

Innspillet er gitt med utgangspunkt i NSMs sektorovergripende ansvars- og myndighetsområde, rapporten *Nasjonalt digitalt risikobilde* og anbefalingene som er gitt i *Sikkerhetsfaglig råd - et motstandsdyktig Norge,* KVU for *nasjonale skytjenester* samt andre relevante arbeider.

2. NSMs forventninger til strategien

Digitalisering av Norge er høyt prioritert og den videre utviklingen vil få stor betydning for samfunnet frem mot 2030. Gjennom en nasjonal digitaliseringsstrategi må myndighetene sørge for at digitalisering og teknologiutvikling ikke går på bekostning av samfunnets grunnleggende verdier. Et overordnet innspill fra NSM er derfor at sikkerhet må inngå som et grunnpremiss gjennom hele digitaliseringsstrategien.

NSM forventer at den nye strategien bidrar til å oppnå de strategiske sikkerhetsmålene som er pekt ut i sikkerhetsfaglig råd (2023), og særlig følgende:

Postadresse
Postboks 814
1306 SANDVIKA

Telefon
+47 67 86 40 00
E-postadresse
postmottak@nsm.no

Internettadresse (URL)
www.nsm.no

- Legge til rette for god cybersikkerhet for norske virksomheter i hele krisespennet. Dette inkluderer fellesløsninger, etablering av motstandsdyktighet, hendelseshåndtering, rapportering av hendelsene, og en overordnet nasjonal sikkerhetsstyring.
- Norske myndigheter har en omforent situasjonsforståelse av det digitale trussel- og risikobildet.
- Norge har tilstrekkelig nasjonal kontroll over funksjoner og infrastruktur med betydning for nasjonal sikkerhet.
- Norge evner å motstå cyberoperasjoner som truer nasjonal sikkerhet i fred, krise og krig.
- Alle deler av det norske samfunnet har digital motstandskraft på et langt høyere nivå.

3. Drivkrefter og utviklingstrekk

Samfunnsutviklingen og de sikkerhetspolitiske utfordringene mot 2030 vil være preget av høy kompleksitet og stor usikkerhet. Sammenfall av flere utviklingstrekk, som pandemi, krig, geopolitisk rivalisering og klimaendringene, forsterker de negative konsekvensene og skaper uønskede langtidseffekter. NSM ønsker å fremheve særlig tre drivkrefter som digitaliserings-strategien bør ta høyde for.

Teknologiutvikling og verdiskaping

Hastigheten og kompleksiteten innen teknologisk innovasjon beskrives som en av århundrets megatrender. Flere av de fremvoksende teknologiene kalles gjerne «brytningsteknologier». Dette er teknologi som vesentlig kan endre hvordan stat og samfunn fungere. Denne transformasjonen er ikke knytte til én enkelt teknologisk nyvinning, men til samvirket mellom nyvinningene.

Den teknologiske utviklingen har stor betydning for hvordan verdier skapes frem mot 2030. Et datadrevet forsvar, næringsliv og sivilsamfunn endrer arbeids- og samhandlingsmønstre. Informasjonens konfidensialitet, tilgjengelighet og integritet blir stadig viktigere i hurtigere og mer komplekse behandlings- og beslutningsprosesser. Kommersielle behov og utsikter driver mye av teknologiutviklingen og forventes å styre hvilke teknologier som blir tatt i bruk. Myndighetene må likevel legge til rette for at teknologiutvikling i den grad det er mulig skjer på norske premisser.

Fremtidig konfliktutvikling og internasjonalt samarbeid

Et fremtredende trekk i den globale sikkerhetspolitiske utviklingen er rivalisering mellom stormaktene USA, Kina og til dels Russland. Rivaliseringen innebærer skjerpet konkurranse og konfrontasjoner med alle statens maktmidler i ulike regioner.

Demokratier er under press av flere årsaker. Intern misnøye med demokratiske prosesser, økonomisk tilbakegang, økt polarisering mellom grupper i samfunnet og generasjonskløfter er bare noen av dem. Denne misnøyen kan forsterkes av andre stater ved bruk av sammensatte trusler, en kombinasjon av virkemidler for å utøve påvirkning og press. Sammensatte trusler som svekker tilliten mellom befolkningen og myndighetene, er en av de mest alvorlige truslene mot nasjonal sikkerhet. For å kunne møte disse truslene, vil økt nordisk og alliert samarbeid bli viktigere.

Klimaendringer og omstillingsevne

Klimaendringene er vår tids største utfordring, og den nødvendige omstillingen som kreves for å nå klimamålene vil være preget av både samarbeid, konkurranse og rivalisering. Energiomstillingen endrer også internasjonale maktforhold. Det er en intens konkurranse om å vinne kontroll over og ha et forsprang innen fremtidens energi og teknologi blant annet gjennom industri, handels- og innovasjonspolitikk.

Ny teknologi, som kunstig intelligens, kan være en del av løsningen, gjennom forskning, mer effektiv energistyring eller utvikling av bedre klimamodeller. Samtidig påvirker også IT-industrien klimaet negativ, blant annet gjennom den enorme energibruken, og stort forbruk av kritiske mineraler. Ikke minst gjelder dette for datasentre og kunstig intelligens. Sentralisering, fellesløsninger og profesjonell drift kan bidra til å redusere energiforbruket i forhold til dagens tilstand hos hver enkelt virksomhet.

4. De viktigste digitaliseringsutfordringene

Digitalisering og teknologiutvikling kan gi banebrytende og verdiskapende muligheter, samtidig som det skapes nye utfordringer og sårbarheter. Utfordringene kan knyttes til selve anvendelsen av teknologien, dataene teknologien baserer seg på og infrastrukturen teknologien er avhengig av.

NSM vil nevne følgende som de viktigste utfordringene for digitalisering av Norge.

Mangelfull situasjonsforståelse og utilstrekkelig informasjonstilgang

Det er avgjørende at nasjonale, regionale og lokale myndigheter har en god og omforent situasjonsforståelse for å kunne avdekke, forhindre og håndtere sikkerhetstruende aktivitet. I tillegg er virksomheter avhengig av god tilgang til trussel- og sikkerhetsinformasjon for å kunne sikre egne verdier. Spesielt gjelder dette i cyberdomenet, der risikobildet er svært dynamisk. Endringer må fanges opp tidlig og formidles raskt dersom virksomhetene skal være i forkant av trusler. Det er et uutnyttet potensial i deling av datagrunnlag og sikkerhetsinformasjon mellom virksomheter og myndigheter.

Statlig IT-styring ivaretar hverken koordinering eller behov for samvirke i tilstrekkelig grad

Digitaliseringen i de ulike etatene og sektorene er ikke i tilstrekkelig grad styrt etter felles prinsipper. Dette gjelder både innen hver sektor og mellom sektorene. Dette fører til at virksomheter som har behov for digitalt samvirke og kommunikasjon, bygger egne løsninger som i for liten grad snakker sammen og ivaretar samvirkebehov. Totalforsvaret har behov for moderne IT-plattformer med digitale tjenester som fungerer godt i hele krisespekteret. Sammen skal plattformene bidra til at Norge har nødvendig datakraft for grunnleggende nasjonale funksjoner og andre viktige samfunnsfunksjoner når krisen inntreffer.

Kunstig intelligens har stor sikkerhetsmessig innvirkning

Systemer basert på kunstig intelligens favner bredt – fra å oppdage digitale angrep og medisinsk diagnostisering til finansiell stabilitet og en rekke andre bruksområder. Både de menneskelige og de ikke-menneskelige bidragene inn i slike systemer har stor sikkerhetsmessig innvirkning – og dermed et stort skadepotensial. Den økende kompleksiteten i algoritmene og systemene de brukes i gir redusert transparens. Dette fører til at menneskets forståelse av, og kontroll med algoritmene er vanskelig – og i mange tilfeller umulig.

Mangel på IT-kompetanse utfordrer digitaliseringen

Norge mangler i dag kompetanse for å effektivt kunne digitalisere på en forsvarlig måte. Det er mange oppgaver som skal løses både i offentlig og privat sektor, og det vil være krevende å få gjennomført ønsket digitalisering uten å løse denne ressursutfordringen. For å realisere en nasjonal digitaliseringsstrategi vil man fremover trenge en større satsning på både å få flere ressurser og å bedre utnytte de ressursene Norge allerede har. Dette gjelder for samtlige IT-fagområder inkludert IT-sikkerhet.

5. Anbefalinger og tiltak

NSM har observert en rekke forhold som kan være relevante for arbeidet med ny digitaliseringsstrategi:

Et målbilde for sikker digital transformasjon

En virksom og effektiv digitaliseringsstrategi bør inneholde et målbilde for en sikker digital transformasjon i hele samfunnet. Målbildet bør realiseres gjennom en langtidsplan for digital infrastruktur med langsiktig og forutsigbar finansiering. IT bør være en offentlig styrt samfunnsinfrastruktur og -funksjon på lik linje med samferdsel, ekom, strømforsyning, vannforsyning, helse etc.

Et målbilde bør legge premisser for hvordan digitale systemer og tjenester skal ivaretas gjennom krisespekteret og ved alvorlige hendelser. Målbildet bør også legge til grunn arkitekturprinsippene for en felles digital grunnmur, i tråd med tidligere anbefalinger fra NSM.

En nasjonal strategi bør gi retningslinjer for IKT-plattformer med tilhørende data og applikasjoner. Dette bør omfatte overordnet systemarkitektur og teknologivalg samt sikkerhetsløsninger. I noen tilfeller bør retningslinjene inkludere krav om styrket nasjonal kontroll. Det bør også etableres insentivordninger som sørger for at virksomheter velger løsninger som er i tråd med strategien.

Strukturer for samhandling, informasjonsutveksling og rapportering bør styrkes i hver sektor

For å øke situasjonsforståelsen i alle sektorer og bygge grunnlag for sektorvise situasjonsbilder, må det etableres hensiktsmessige strukturer for samhandling, informasjonsutveksling og rapportering i det digitale domenet. Dette bør gjøres ved å videreutvikle konseptet med sektorvise responsmiljøer som jobber med digital sikkerhet. Både offentlige og private virksomheter må inkluderes. Det bør også etableres samarbeidsstrukturer for sikkerhet på regionalt og kommunalt nivå. Økt situasjonsforståelse på disse nivåene styrker evnen til å avdekke sikkerhetstruende aktivitet og bidrar dermed til et helhetlig nasjonalt situasjonsbilde.

Det vil også være avgjørende å styrke den nasjonale deteksjonsevnen i perioden strategien skal gjelde. Uten et tilstrekkelig velutviklet varslingssystem for digital infrastruktur (VDI), med riktig hjemmelsgrunnlag, vil det bli utfordrende å avdekke fremtidige sikkerhetstruende cyberoperasjoner mot Norge. Det vil derfor være viktig at samfunnskritiske virksomheter oppfordres til å bidra til å øke den nasjonale evnen.

Norge har høy IT-kompetanse, men omfanget må styrkes

Det er knapphet på personer med IT-kompetanse, herunder IT-sikkerhetskompetanse. Vi må derfor bli bedre på både å utnytte de ressursene vi allerede har, samt utdanne flere. Dette betyr at det bør legges til rette for at offentlig sektor bedre kan samordne eksisterende og til dels fragmenterte IT-miljøer, blant annet gjennom felles drift av infrastruktur og datasentertjenester, standardisering av utviklingsprosesser, utvikle og ta i bruk et større spenn av fellestjenester. Om punktene nevnt over inkluderes i ambisjonene om deling og samarbeid, vil man få skalafordeler og muligens få frigjort ressurser som kan benyttes på andre IT-relaterte områder.

NSM mener at Norge har gode forutsetninger for å utdanne flere med IT-faglig kompetanse. I tillegg til teknologer vil dette for eksempel inkludere jurister og statsvitere med fordypning i IT-fagområdet. Det er NSMs oppfatning at norske universitetsmiljøer er et godt utgangspunkt for videre satsing og kompetanseutvikling. Norge trenger også styrking av yrkesfaglige miljøer innen dette fagområdet.

Innovasjonssenter for fremvoksende teknologier

Norges kompetanse og nasjonale initiativer må økes i møte med fremvoksende teknologier. Det nasjonale senteret for anvendt kryptologi ble opprettet hos NSM i oktober 2023. Ambisjonen er å videreutvikle kryptosenteret til et innovasjonssenter for sensitive teknologier. Et slikt senter, initiert av staten, kan samle interessenter fra myndigheter, akademia og industri og stimulere til kompetanse og industriutvikling på viktige teknologiområder som kunstig intelligens, kvanteteknologi mm. Slik kan man sørge for at Norge utvikler og tar i bruk blant annet sikkerhetsløsninger som ligger i forkant av trusselaktørene.

Konsentrasjonsrisiko, leverandøravhengighet og nasjonal IKT-beredskap

Markedet for IT-tjenester er tilsynelatende preget av god konkurranse, men ser man nærmere på de faktiske tjenestene som blir tilbudt og hvor de kommer fra er realiteten en annen. Dette er fordi de fleste av aktørene i det norske markedet er videreselgere av produkter og tjenester fra noen få utenlandske IT-leverandører. Dette resulterer blant annet i tilbud hvor løsningene/tjenestene understøttes av samme infrastruktur og man får en ubevisst konsentrasjon av informasjon og tjenester. Den kommende strategien bør forsøke å bevisstgjøre virksomhetene om at det er mindre konkurranse i markedet enn først antatt og da spesielt for allmenne skytjenester, og at konsentrasjonsrisikoen derfor er større en man kanskje skulle tro. Vi viser til rapporten Kartlegging av drift og forvaltning av IKT-løsninger (regjeringen.no).

Strategien bør derfor oppmuntre til å ta i bruk løsninger og tjenester fra norske, nordiske og europeiske IT-leverandører som vil kunne være viktige i etableringen av nasjonale IKT-tjenester. Dette er viktig for å reelt kunne påvirke sikkerhetsfunksjonalitet, men er også relevant for å få realisert andre norske behov. Ved å ta i bruk lokale leverandører bidrar man også til å styrke nasjonal kontroll, forsyningssikkerhet og beredskap for IKT-produkter og IKT-tjenester.

Sikre demokratisk og nasjonal kontroll over kunstig intelligens

Det må etableres et frittstående, rådgivende organ som bidrar til demokratisk kontroll av utvikling og bruk av kunstig intelligens. Organet skal vurdere samfunnsmessige, etiske og andre prinsipielle problemstillinger ved utvikling og bruk av ny teknologi. Norske myndigheter bør være pådriver for å etablere grunnleggende demokratiske prinsipper for utvikling av kunstig intelligens nasjonalt og internasjonalt, og ta en aktiv rolle for å påvirke utviklingen av relevant europeisk regelverk.

Det bør og etableres en nasjonal infrastrukturtjeneste for trening av maskinlæringsmodeller som baserer seg på data og informasjon som er ansett som sensitive, strategisk viktig eller hvor Norge har et komparativt fortrinn. Enkelte universitetsmiljøer tilbyr allerede i dag relevante tjenester med et høyt sikkerhetsnivå, og man bør se hen til disse i det videre arbeidet. Det bør videre tilrettelegges for at slike tilbud kan benyttes av virksomheter og organisasjoner som har data og informasjon som faller inn i overnevnte kategorier. Det bør kartlegges hva slags data som bør være under nasjonal kontroll og hva som kan deles med utenlandske selskaper.

Det bør etableres et tydelig og enhetlig regelverk for digital sikkerhet

Den rettslige reguleringen innen det digitale domenet er i rask utvikling i EU og internasjonalt. Norske myndigheter bør derfor se til pågående prosesser i EU og Norden i arbeidet med digitaliseringsstrategien. Det er særlig viktig med en felles tilnærming til hvilke virksomheter, systemer og verdier som skal være omfattet av reguleringene.

Videre er det uheldig når ulike sektorer kommer frem til ulike konklusjoner i tolkningen av lovverk, for eksempel arkivloven og taushetsbelagt informasjon. Det bør derfor oppmuntres til at forvalterne av lov- og regelverk kommer med offisielle tolkningsuttalelser som vil kunne påvirke beslutningstageren ved en eventuell tjenesteutsetting.

Sensitive og kritiske data må beskyttes

Det er avgjørende for tilliten til offentlige tjenester at sikkerheten ivaretas. Datasentre og skytjenester for sensitiv og kritisk informasjon, funksjoner og infrastruktur av betydning for nasjonale funksjoner bør etableres i Norge. Datakraft må sikres gjennom distribuerte skytjenester i regionale og lokale datasentre i Norge og beredskapsavtaler med nære allierte i tilfelle krise.

En nasjonal strategi bør gi retningslinjer mht. hva som er viktig for Norge å styrke nasjonal kontroll over. Strategien bør indikere hva som har høy verdi for nasjonen, eller vise til andre relevante prosesser. Eksempler på slike prosesser er utpeking av grunnleggende nasjonale funksjoner ref. sikkerhetsloven og kategoriene i NIS2-direktivet. Som et minimum bør strategien sette klare føringer for at departementene måler virksomhetene i sin sektor på informasjonssikkerhet og digital beredskap.

6. Avslutning

Gjennom en nasjonal digitaliseringsstrategi må myndighetene sørge for at digitalisering og teknologiutvikling ikke går på bekostning av samfunnets grunnleggende verdier. Et overordnet innspill fra NSM er derfor at sikkerhet må inngå som et grunnpremiss gjennom hele digitaliseringsstrategien.

NSM bidrar gjerne i videre arbeid med strategien der KDD ser det som hensiktsmessig

Med hilsen

Sofie Nystrøm
direktør

Dette dokumentet er elektronisk godkjent hos Nasjonal sikkerhetsmyndighet og sendes uten signatur.