NSM

Ny nasjonal sikkerhet

Digital etikk og kunstig intelligens

torsdag 24. mars 2022

Forord av direktør NSM

Norge er et av verdens mest digitaliserte land. Med vår offentlige sektor, industri og våre utdanningsinstitusjoner ligger vi i verdensklasse innen digitalisering. Den digitale infrastrukturen og satsningen på kunstig intelligens (KI) må sikres godt. Og det er her NSM har en viktig rolle. NSM skal både sikre samfunnet og staten. Med den mest moderne teknologien tilgjengelig. Det har vi gjort siden NSM ble opprettet i London under krigen og det skal vi fortsette med.

Økende bruk av KI vil bli grunnleggende for NSMs oppdrag om å holde nasjonen trygg. NSM er ansvarlig for varslingssystemet for digital infrastruktur (VDI), personkontroll i Norge og Krypto-systemer. KI vil være avgjørende for vår evne til å håndtere det stadig økende volumet og kompleksiteten til data, og for å utvikle evnene som trengs for å forsvare oss mot KI-aktiverte trusler fra ondsinnede aktører.

I NSM vil KI handle om å gjøre mennesker i stand til å ta gode beslutninger. Vår innsats vil bruke KI til å utvikle deteksjon av fiendtlige cyberoperasjoner, samle informasjon fra relevante kilder og fremheve viktige data for vurdering av våre analytikere; støtte beslutningsprosessen i stedet for å bestemme den.

KI-systemer blir ansvarlige når de er lovlige, sikre og etiske. Uavhengig tilsyn fra EOS-utvalget sikrer at måten vi utøver våre fullmakter, inkludert gjennom bruk av KI, gjøres i samsvar med loven. Et sterkt fokus på digital etikk er i tillegg nødvendig. Utviklingen og distribusjonen av KI for nasjonal sikkerhet byr på noen spesielle digitaletiske utfordringer. NSM ønsker å unngå KI-relatert partiskhet (bias) og diskriminering, og sikre et godt beslutningsgrunnlag. Godt utviklede prosesser for anskaffelse og evaluering vil derfor være nødvendig, sammen med økt kompetanse på ansvarlig KI gjennom opplæring av personell og gode retningslinjer.

Det er i tillegg viktig og etisk riktig for NSM å være åpne om bruken av ny teknologi. NSM vil derfor reflektere over hvordan vi benytter ny teknologi i disse oppgavene på en etisk forsvarlig måte for å skape tillit og trygghet.

Innhold

Sammendrag

Denne utgivelsen beskriver dagens digitale NSM, og vår verdistyrte tilnærming for områdene der mennesker, informasjon og teknologi møtes. Den beskriver NSMs bruk av kunstig intelligens, KI, og vårt rammeverk for digital etikk, og hvordan vi har tenkt å bruke KI i våre operasjoner. Utgivelsen er en del av vårt engasjement for inkludering, debatt og åpenhet. Denne utgivelsen er det første trinnet på en mye lengre reise: vi vil gjerne at du blir med oss på den.

Kunstig intelligens – en form for programvare som kan lære å løse problemer i en skala og hastighet som er umulig for mennesker – er stadig viktigere for måten vi lever og jobber på. Den er allerede i ferd med å forvandle sektorer så forskjellige som sikkerhet, helsevesen, telekommunikasjon og finans. KI-programvare informerer satellittnavigatorene våre, veileder våre internettsøk og beskytter oss hver gang vi foretar et elektronisk kjøp eller åpner en app på smarttelefonen vår.

Hele tiden siden grunnleggelsen, har NSM vært i forkant av innovasjon innen nasjonal sikkerhet. Generasjoner av strålende ingeniører har brukt sin tekniske oppfinnsomhet, banebrytende teknologi og omfattende partnerskap for å identifisere svakheter og stanse trusler mot landet vårt. I dag, mens teknologiske endringer fortsetter å akselerere, finner vi nye tilnærminger for å forstå den komplekse og sammenkoblede verden rundt oss. Vi har lenge vært forkjemper for ansvarlig bruk av datavitenskap, og tror at KI vil være kjernen i organisasjonens fremtid.

I NSM vil KI primært handle om å forbedre beslutningsgrunnlaget.

For å sikre etisk forsvarlig utvikling og bruk av KI behøves et stort fokus på digital etikk. Digital etikk handler om å forstå hva ny teknologi er og hva den kan gjøre, å analysere mulige konsekvenser av utvikling og bruk, og å diskutere hvordan teknologien bør brukes for å bidra til beste for enkeltmennesker og samfunn.

I vårt videre arbeid med KI-systemer vil NSM arbeide for å integrere etikk på alle nivåer:

1. Økt etisk kompetanse for utviklere og andre som er involvert i utvikling, implementering, anskaffelser, bruk og evaluering av KI-systemer, inkludert kjennskap til de syv prinsippene for etisk forsvarlige KI-systemer og trening i å anvende dem
2. Økt fokus på etisk forsvarlige prosesser for utvikling av KI-systemer, inkludert de syv prinsippene for etisk forsvarlige KI-systemer og tilpassede etiske retningslinjer for anskaffelse og bruk av KI.
3. Ethics by Design - etikk bygges inn i utvikling, drift og forvaltning av KI-løsninger.

Kaptittel 1: Hva er kunstig intelligens?

Veldig mange dataprogrammer bruker i dag KI uten at vi legger merke til det. Du har sannsynligvis allerede brukt det før du kom på jobb. Smart-telenoner bruker det, apper som Google og Facebook tilpasser innhold basert på det. Moderne biler bruker deti.

Til tross for dette er de KI-systemene vi for øyeblikket har, kun i stand til å takle svært begrensede, presist definerte problemer. Og da bare med menneskelig støtte. I det minste i overskuelig fremtid vil KI-ingeniører absolutt ikke lage noen intelligente datamaskiner som virkelig kan erstatte menneskerii. Datamaskiner med såkalt "generell kunstig intelligens", forblir foreløpig bare på film.

Det er mange ulike definisjoner av kunstig intelligens (KI) og definisjonene endrer seg gjerne i takt med hva som er teknologisk mulig. Vi tar utgangspunkt i EUs ekspertgruppes definisjon for KI, som også er brukt i nasjonal strategi for kunstig intelligens:

> *Kunstig intelligente systemer utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål. Enkelte KI-systemer kan også tilpasse seg gjennom å analysere og ta hensyn til hvordan tidligere handlinger har påvirket omgivelsene.*

Dagens regelbaserte systemer for automatisering

Slik det er i dag er det regelbaserte systemer for automatisering som dominerer. Et regelbasert IT-system er oftest bygget opp av regler av typen «HVIS x, GJØR y». Slike regler kan settes sammen til kompliserte beslutningstrær. Regelbaserte systemer for automatisering kan brukes til å modellere et regelverk, forretningsregler eller erfaringsbasert praksis (skjønnsutøvelse). Flere av løsningene som benyttes innenfor automatisert saksbehandling i offentlig sektor er slike regelbaserte systemer. Enkelte slike komplekse løsninger kan fremstå som kunstig intelligens i dag. [iii]

Kunstig intelligens

Et system basert på kunstig intelligens kan enten tolke data fra for eksempel sensorer, kameraer, mikrofoner eller trykkmålere, eller det kan få inndata fra andre informasjonskilderiv. Systemet analyserer dataene, tar beslutninger, og utfører handlinger. Både behovet for data og det at systemet selv tar beslutninger og utfører handlinger reiser etiske spørsmål som drøftes senere i heftet. I noen typer systemer er det en tilbakemeldingssløyfe som gjør at den kunstige intelligensen lærer – enten av egne erfaringer, eller av direkte tilbakemeldinger fra bruker eller operatør. Trening av KI kan deles i tre kategorier[v]:

• Veiledet læring: Algoritmen trenes med et datasett der både inndata og resultat er gitt. Man kan si at algoritmen både får «oppgaven» og «fasiten» og bruker dette til å bygge modellen. Ut fra dette vil den senere være i stand til å ta en beslutning basert på inndata.

• Ikke-veiledet læring: Algoritmen får bare et datasett uten «fasit» og må selv finne mønstre i datasettet som den senere kan bruke for å ta beslutninger om nye inndata.

• Forsterkende læring: Algoritmen bygger modellen sin basert på ikke-veiledet læring, men får tilbakemelding fra bruker eller operatør om beslutningen den foreslår er god eller dårlig. Tilbakemeldingen mates inn i systemet og bidrar til å forbedre modellen.

Hva KI kan og ikke kan gjøre

KI-systemer har vist seg å være gode til å løse veldefinerte, snevre problemer, hvor nødvendig data og tilbakemelding er fullt tilgjengelig for systemetvi. Når de står overfor denne typen oppgaver, er KI-systemer vanligvis mye raskere og ofte mer nøyaktige enn mennesker. KI-systemer er nå i stand til å utføre oppgaver som ville vært så tidkrevende for et menneske at de ellers ville vært umulige å oppnå. Men KI-systemer er ikke gode til alt. Noen ganger kan det koste mer å distribuere en KI-løsning enn et konvensjonelt programvarekodingsalternativ, eller rett og slett å få et menneske til å gjøre en oppgave i utgangspunktet. KI fungerer ikke bra når man takler tvetydige, brede utfordringer, spesielt hvis det er utilstrekkelig data som den kan trene og lære på. Den møter problemer i situasjoner der fortiden ikke forutsier fremtiden godt. Og som vi vil diskutere senere, kan KI-systemer bli påvirket av svakheter i dataene deres, innlemme skjevheter eller vise seg mulig å lure eller villede. I tillegg tar KI ikke hensyn til den bredere konteksten, eller mange enkle ting som mennesker tar for gitt, for eksempel psykologi eller følelser. Av disse grunner hevder de fleste spesialister at stor forsiktighet bør utvises ved bruk av KI for å analysere individuell atferd. Utplassert på riktig måte er imidlertid KI-systemer et enormt kraftig verktøy for enhver organisasjon eller utvikler i Norge i dag.

Kapittel 2: Hva gjør NSM?

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for forebyggende sikkerhet. Direktoratet er det nasjonale fagmiljøet for digital sikkerhet og varslings- og koordineringsinstans for alvorlige digitale angrep og sikkerhetshendelser.

Nasjonalt cybersikkerhetssenter (NCSC) er en del av NSM og samtidig et partnerskap mellom NSM og ulike offentlige og private virksomheter. Senteret skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberoperasjoner. NCSC har et spesielt fokus på rådgiving og krav innen forebyggende tiltak, tekniske sikkerhetsløsninger og yter bistand ved håndtering av digitale hendelser.

Norsk lovgivning regulerer bruk av kunstig intelligens og beskyttelse av innbyggernes data. Med dagens lovgiving tror vi at vi trygt kan bruke KI til sikring av samfunnet på en trygg måte. Vi håper at eksemplene i denne artikkelen har forklart hvorfor dette er så viktig for nasjonen. Tidligere har NSM jobbet i det skjulte som en hemmelig tjeneste. I dag er vi forpliktet til å være mye mer åpne i å engasjere oss med det bredere norske samfunnet om teknologiene og valgene vi tar på vegne av nasjonen. Vi håper denne utgivelsen har gitt deg litt innsikt i vår tilnærming, og vi ser frem til å fortsette samtalen.

Digitalisering av nasjonal sikkerhet: Cybertrusselen

NCSC skal være i stand til å oppdage hendelser i det digitale rom som vil kunne ha alvorlige konsekvenser. For å møte denne utfordringen er det viktig at NCSC er ledende fagmiljø innen KI som støtte til defensive cyberoperasjoner. Et viktig prinsipp i den videre utviklingen av KI innenfor dette området er at dagens etiske retningslinjer videreføres. Aktivitetene skal være objektive og rettet mot å forebygge, avdekke og avverge cybertrusler.

Innenfor cyberdomenet er det tre KI-områder som er spesielt viktige for NCSC: Anvendelse av KI-metodikk til å understøtte og forbedre prosesser, cybertrusler mot KI-systemer, KI som en cybertrussel.

Anvendelse av KI-metodikk – Et av områdene NCSC søker å utnytte KI er for å understøtte beslutningsprosesser knyttet til oppdagelse og håndtering av cyberhendelser. Her kan KI-metoder benyttes til å løfte frem relevant informasjon fra datamengder som er for store til at mennesker manuelt kan håndtere disse. KI-metoder vil også kunne bidra til å fremheve sammenhenger, avgjøre om aktiviteter i nettverk er som forventet eller unormalt, avgjøre om det er ekte eller falske alarmer, eller kunne avgjøre om en ondsinnet aktivitet eller skadevare kan assosieres med en gitt trusselaktør.

Cybertrusler mot KI-systemer – Som med andre tekniske systemer, vil også KI-systemer kunne inneholde sårbarheter. KI-systemene introduserer imidlertid en ny dimensjon med sårbarheter, da KI-modellene også kan bli utsatt for ondsinnede cyberoperasjoner. Det er således viktig å utarbeide råd og anbefalinger for beskyttelse av KI-systemer, som da omfatter KI-modellene i alle stadier, treningsdata og treningsprosessene.

KI som en cybertrussel – På samme måte som at KI kan benyttes til defensive cyberoperasjoner, kan trusselaktører benytte seg av KI til å understøtte eller utføre offensive cyberoperasjoner mot sine mål. Det må da forventes at cybertrusselbildet endres. Trusselaktører kan få tilgang til et mer komplett bilde av sine mål og sammenhenger som kan utnyttes, kan fatte beslutninger i aktive cyberoperasjoner på kortere tid, eller KI-metodene vil gjør dem i stand til å omgå etablerte sikringstiltak i sine måls IT-systemer. Denne utviklingen vil også medføre at råd og veiledninger for sikring av IT-systemer må holdes relevant også mot nye cybertrusler.

Felles for disse områdene er behovet for videre forskning og utviklingsaktiviteter. Innen mange kunnskapsdomener har den operative anvendelsen av KI kommet langt, men når det gjelder bruk av KI knyttet til cyberoperasjoner er man fortsatt i en tidligfase og på et teoretisk bruksplan. NCSC må derfor gjennom trygge rammer implementere og videreutvikle beste praksiser og nye metoder. Etter hvert som KI-systemer og -metoder videreutvikles, krever det et tilsvarende arbeid innen det forebyggende sporet for å hele tiden minske eventuelle sårbarhetsflater. Videre er kunnskaps og kompetansebygging på hvordan KI kan utgjøre en cybertrussel helt essensielt for å være i stand til å avverge og oppdage ondsinnede cyberoperasjoner.

Som et ledd i å lede Norges innsats for å forbedre cybersikkerheten skal NCSC også lede arbeidet innen KI for defensive cyberoperasjoner. Vi tror at åpen debatt mellom grupper med ulike perspektiver og erfaringer vil være avgjørende for å løse utfordringene rundt både teknisk og etisk bruk av KI. De siste årene har vi møtt akademiske forskere som spesialiserer seg på KI, sivilsamfunnsorganer som forkjemper for personvernrettigheter og datavern, og ledere fra privat sektor. Slike former for aktiviteter og erfaringsutveksling vil være viktig for den videre utviklingen av KI.

Digitalisering av nasjonal sikkerhet: Sikkerhetsklarering

Hvert år blir 30.000 personer sikkerhetsklarert i Norge. Sikkerhetsklarering blir gitt etter en vurdering om en person er antatt skikket for behandling av sikkerhetsgradert informasjon. Vurderingsgrunnlaget er bygget på opplysninger personen selv har gitt, og informasjon fra relevante registeropplysninger.

Ved avgjørelse skal det bare legges vekt på forhold som er relevante for å vurdere personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av sikkerhetsgradert informasjon. Avgjørelsen skal baseres på en konkret og individuell helhetsvurdering av de foreliggende opplysninger.

NSM er nå i ferd med å digitalisere denne prosessen. Det gjør den både hurtigere og bedre. Prosessen bruker ikke kunstig intelligens ved innsamling eller prosessering av data. Prosessen er digitalisert, hvilket vil si at de som søker om sikkerhetsklarering får tilsendt de opplysningene som allerede er tilgjengelig om dem, bedt om å godkjenne disse og fylle inn svar på enkelte andre spørsmål. Tilsvarende som skattemeldingen. Deretter vil det bli bedt om informasjon fra andre registre for å opplyse søknaden på en best mulig måte. Til slutt vil søknaden gå til en saksbehandler som manuelt går igjennom søknaden og godkjenner den. Målet er at denne prosessen skal kunne gå så raskt som mulig uten at det går utover kvaliteten.

Hele prosessen er sporbar og mulig å forklare. Ved at det ikke er benyttet kunstig intelligens er alle ledd i prosessen åpne og det er mulig å vise hvordan det er kommet frem til en avgjørelse.

Digitalisering av nasjonal sikkerhet: Kryptoanalyse

Kryptoanalyse har alltid inkludert analyse av store mengder data for å finne utilsiktede mønstre. Filtrering og kategorisering i analysen ble tidlig avgjørende, da mengdene ble for store for uttømmende søk.

Strukturer og sammenhenger kan være svært vanskelig å finne for et menneske. De tidligste sporene av maskinlæringsteknikker finner vi helt tilbake til andre verdenskrig. Den norske statistikeren Erling Sverdrup utførte under krigen arbeid som fortsatt står sentralt; statistisk modellering. Statistisk modellering er blitt videreført og utviklet til det vi kjenner som KI i dag.

Innen TEMPEST (utilsiktet elektronisk stråling) både brukes det og forskes på ulike KI-løsninger for å analysere og potensielt automatisere testarbeid.

NSM har videre startet forskning på bruk av KI på krypterte data. Eksempelvis forskes det på beregninger på sammenkoblede data fra ulike eiere som ikke kan dele sine databaser med hverandre. Beregningene respekterer både gradering og autorisasjon.

Kryptografi kan også sørge for integritetsbeskyttelse av KI-modeller. Dette innebærer at man får en bekreftelse på at resultatet kommer fra rett KI-modell, og ikke en som har blitt manipulert.

Kapittel 3: Digital etikk

NSM er forpliktet til å skape og bruke KI på en måte som støtter rettferdighet, myndighet, åpenhet og ansvarlighet – og til å beskytte nasjonen mot KI-aktiverte sikkerhetstrusler benyttet av våre motstandere. Vi tror at ved å jobbe sammen med våre partnere over hele Norge og internasjonalt, kan vi levere denne visjonen.

Norge er kjennetegnet av høy tillit mellom befolkning og myndigheter, og NSM vil bidra til å opprettholde og forsterke denne tilliten samtidig som KI tas i bruk. Det krever at KI-løsningene er ansvarlige og pålitelige.

Å tenke på KI oppmuntrer oss til å tenke på oss selv, og hva det vil si å være menneske: vår foretrukne livsstil, våre verdier og vår felles etikk. Vi vil ikke late som om det ikke er utfordringer foran oss. Ved å bruke KI vil vi strebe etter å minimere og der det er mulig eliminere skjevheter, enten det er knyttet til kjønn, tilhørighet eller religion.

KI-systemer kan bidra til et sikrere og tryggere samfunn, men systemene har også et stort skadepotensial. Det er vanskelig om ikke umulig å ha oversikt over alle virkninger og konsekvenser av KI-systemer. Både ondsinnede illegale aktører og velmenende legale aktører kan forårsake skade.

For å sikre etisk forsvarlig utvikling og bruk av KI behøves et stort fokus på digital etikk. Digital etikk handler om å forstå hva ny teknologi er og hva den kan gjøre, å analysere mulige konsekvenser av utvikling og bruk, og å diskutere hvordan teknologien bør brukes for å bidra til beste for enkeltmennesker og samfunn.

Digital etikk er et verktøy for å hjelpe organisasjoner med å gjøre etiske prinsipper til praktisk veiledning for programvareutviklere – og bidra til å bygge inn kjerneverdiene våre i datamaskinene og programvaren, prosesser og kompetanse. Norsk råd for digital etikk (NORDE) og andre initiativer for en bærekraftig utvikling hjelper til med å vise oss hvordan vi kan bygge og bruke KI på en mer etisk og ansvarlig måte.

Pålitelige KI-systemer er lovlige, sikre og etiske, slik det også står i Norges nasjonale strategi for KI. Strategien bygger på arbeidet til EUs ekspertgruppe, som prioriterer syv etiske prinsipper som bør ligge til grunn for utvikling av pålitelige KI-systemer som vil støtte opp om og bidra til et demokratisk og rettferdig samfunn. Alle prinsippene legger på ulike måter til rette for evaluering og revisjon i tråd med demokratiske prinsipper:

Syv etiske prinsipper

1) KI-baserte løsninger skal respektere menneskets selvbestemmelse og kontroll, og slik styrke og fremme enkeltmenneskets grunnleggende friheter og rettigheter. Mennesker skal være inne i beslutningsprosessene for å kvalitetssikre og gi tilbakemelding i alle ledd i prosessen («human-in-the -loop»). Å fylle dette prinsippet innebærer også at menneskene har relevant kompetanse slik at de kan oppdage og diskutere digitaletiske dilemmaer når de oppstår.

2) KI-baserte systemer skal være sikre og teknisk robuste. Det innebærer at systemene er nøyaktige, pålitelige og etterprøvbare, men også at systemene fungerer slik de er tenkt. Risikoen for uintenderte og uventede skader skal være minimal. Slik sett handler dette prinsippet både om en teknisk sikkerhet og en sosial sikkerhet, altså at også de etiske verdiene til samfunnet er forstått og sikret forsvarlig.

3) KI skal ta hensyn til personvernet, altså være lovlig også i henhold til personvernforordningen.

4) KI-baserte systemer må være sporbare, forklarbare og forståelige (transparente). Dette innebærer at systemene skal kunne underlegges tilsyn, revisjon og forklaring. At et system er forklarbart sikrer ikke i seg selv at det blir etisk, men er med å legge til rette for evaluering og forbedring når systemene ikke er det.

5) KI-systemer skal legge til rette for inkludering, mangfold og likebehandling, som igjen støtter opp om et demokratisk og rettferdig samfunn og de verdiene vi ønsker å fremme gjennom menneskerettighetene. Data kan inneholde skjevheter, skjevheter kan også oppstå under databehandling og i modeller. Derfor er det viktig å innføre kontrollprosesser som analyserer og korrigerer systemets beslutninger i lys av formålet.

6) KI skal være nyttig for samfunn og miljø, og skal ikke ha negativ innvirkning på institusjoner, demokratiet og samfunnet som helhet.

7) Ansvarlighet er det siste prinsippet. Dette prinsippet skal utfylle de andre prinsippene.

NSM er engasjert i arbeidet for digital etikk og etisk forsvarlig utvikling og bruk av KI både nasjonalt og internasjonalt. NSM har blant annet deltatt i Europarådets gruppe for å regulere kunstig intelligens som særlig har vurdert muligheter og trusler som KI medfører for menneskerettigheter. Nasjonalt samarbeider NSM tett med Norsk råd for digital etikk (NORDE) og har støttet bokutgivelser om digital etikk.

I vårt videre arbeid med KI-systemer vil NSM arbeide for å integrere etikk på alle nivåer:

1. Økt etisk kompetanse for utviklere og andre som er involvert i utvikling, implementering, anskaffelser, bruk og evaluering av KI-systemer, inkludert kjennskap til de syv prinsippene for etisk forsvarlige KI-systemer og trening i å anvende dem

2. Økt fokus på etisk forsvarlige prosesser for utvikling av KI-systemer, inkludert de syv prinsippene for etisk forsvarlige KI-systemer og tilpassede etiske retningslinjer for anskaffelse og bruk av KI.

3. Ethics by Design - etikk bygges inn i utvikling, drift og forvaltning av KI-løsninger.

Kapittel 4: Konklusjon og vår fremtidige reise

NSM ønsker offentlig debatt om etisk bruk av kunstig intelligens og hvordan vi kan bruke kunstig intelligens og ny teknologi til å sikre Norge.

Dagens varslingssystem for digital infrastruktur (VDI) har blitt brukt til å oppdage målrettede digitale angrep i snart 20 år. NSM utvikler nå ny sensorteknologi basert på kunstig intelligens. Plattformen skal gi mulighet for automatisk analyse av skadevare som oppdages, og automatisk deling av resultater. Her ønsker vi å være åpne for å skape trygghet og tillit, men også for å dele vår kompetanse med resten av miljøene i Norge.

NSM har også kommet langt siden de tidlige dager med kryptoutvikling. Vi står på skuldrene til våre tidligere ingeniører og forskere, mens vi bygger kapasiteter som våre forgjengere bare kunne ha drømt om. Denne reisen skal vi fortsette sammen med norsk industri slik at den kan være verdensledende også i årene som kommer.

Innen personkontroll har vi nå digitalisert prosessen, noe som gir en betydelig raskere klareringstid. Dette er til fordel for den som skal klareres og for arbeidsgivere som trenger sikkerhetsklarert personell. I denne prosessen har vi brukt tradisjonell digitalisering. Alle prosessene er mulig å forklare og åpne. Det er viktig i en prosess som kan fremstå som inngripende.

Det er viktig for NSM å ligge i forkant av den teknologiske utviklingen og samtidig ta gode etiske valg. NSM forplikter seg til å følge Nasjonal strategi for kunstig intelligens og derigjennom

- utvikle og bruke kunstig intelligens som bygger på etiske prinsipper, og respekterer menneskerettighetene og demokratiet
- sikre at forsking, utvikling og bruk av kunstig intelligens i NSM bidrar til ansvarlig og pålitelig kunstig intelligens
- sikre at utvikling og bruk av kunstig intelligens i NSM ivareta den enkeltes integritet og personvern
- bidrar til at digital sikkerhet bygges inn i utvikling, drift og forvaltning av KI-løsninger i grunnleggende nasjonale funksjoner i Norge
  Støtter tilsynsmyndigheter som fører kontroll med sikkerhetsloven i egen sektor med kompetanse på å sikre systemer som bruker kunstig intelligens.

[i] GCHQ (2021) The Ethics of Artificial Intelligence (https://www.gchq.gov.uk/files/GCHQAIPaper.pdf)
[ii] GCHQ (2021) The Ethics of Artificial Intelligence (https://www.gchq.gov.uk/files/GCHQAIPaper.pdf)
[iii] Regjeringen (2020) KI strategi punkt 1.1 (ki-strategi.pdf (regjeringen.no))
[iv] Regjeringen (2020) KI strategi punkt 1.2 (ki-strategi.pdf (regjeringen.no))
[v] Regjeringen (2020) KI strategi punkt 1.2 (ki-strategi.pdf (regjeringen.no))
[vi] GCHQ (2021) The Ethics of Artificial Intelligence (https://www.gchq.gov.uk/files/GCHQAIPaper.pdf)