SÄRTRYCK UR *STRATEGISK UTBLICK 8*

Artificiell intelligens – möjligheter och utmaningar för Sveriges nationella säkerhet

Christer Andersson, Tove Gustavi och Maja Karasalo

Artificiell intelligens (AI) antas av många få en betydande påverkan på samhällsutvecklingen under de kommande åren. AI kommer att tillämpas i många olika tekniska system vilket innebär att AI också kommer att påverka vitala delar av den svenska försvarsförmågan och den nationella säkerheten i bred bemärkelse. Frågan är om svenska myndigheter, och samhället i stort, är förberett för att nyttja de möjligheter som tekniken erbjuder och – inte minst – möta de utmaningar och hot som ett nytt säkerhetspolitiskt landskap med AI medför?

Artificiell intelligens - ett omtvistat begrepp

En del menar att Artificiell Intelligens (AI) handlar om att få datorer att imitera mänskligt beteende. Andra anser att det istället handlar om att skapa datorsystem som, till skillnad från människan, resonerar och beter sig ”rationellt” i alla situationer. Det finns ingen allmänt vedertagen definition av AI, men generellt refererar begreppet till förmågan hos ett datorsystem att i något rimligt avseende resonera eller agera korrekt utifrån tillgänglig information och tidigare erfarenheter.

Rent tekniskt skapas AI genom att information hanteras med matematiska metoder och logik. AI baseras alltså inte på en specifik teknik utan det kan handla om olika typer av maskininlärning, men även exempelvis statistiska metoder. Maskininlärning kan beskrivas som metoder som använder tillgänglig information för att träna och förbättra matematiska modeller av omvärlden. Modellerna används för att tolka och analysera omvärlden. Ju mer information som finns tillgänglig för träning, desto mer exakta modeller och bättre analysresultat kan förväntas.

Den uppmärksamhet som AI har fått de senaste åren följer av att vissa centrala tekniker har nått en sådan mognadsgrad och tillförlitlighet att de kan byggas in i produkter och användas i samhället. För maskininlärning i synnerhet hänger teknikmognaden till stor del ihop med utvecklingen av kraftfulla datorer, samt med digitaliseringen av samhället vilket har gjort att stora mängder data har blivit allmänt tillgängliga. Dessa förutsättningar har bidragit till en utveckling av algoritmer och metoder som inte tidigare har varit möjlig.

AI är ett område som inte har några tydliga gränser mellan civila och militära tillämpningar. Ett tekniskt system som har tagits fram för att identifiera cancerceller i mikroskop kan i princip också läras att hitta bombmål i satellitbilder. Mycket av den framtagna tekniken finns fritt tillgänglig, vilket innebär att det är svårt att överblicka vilka aktörer som använder sig av den och för vilka syften. Tillgängligheten och de dubbla användningsområdena medför både för- och nackdelar ur ett nationellt säkerhetsperspektiv.

Möjligheter och utmaningar med AI i totalförsvaret

Rapporteringen om den praktiska militära användningen av AI kännetecknas av teknikoptimism, där olika tillämpningar av AI-metoder beskrivs med lyckade resultat, men också av oro för vad utvecklingen mot mer självständiga tekniska system kan innebära.

För Sveriges totalförsvar kan AI-metoder medföra förbättringar ur flera aspekter. För Försvarsmakten kan AI-system bidra till militära operativa och taktiska fördelar. För den administrativa verksamheten i både civila och militära delar av totalförsvaret kan till exempel effektiviseringar åstadkommas genom automatisering av olika arbetsuppgifter.

FOI Memo 6749
Projekt Nr I181103
Godkänd av Mike Winnerstig

Augusti 2019

Tillämpningar av AI

I dagens väpnade konflikter har konventionell militär krigföring ofta inslag av hybridkrigföring, såsom IT-attacker eller propagandakampanjer på sociala media. Analys av stora mängder data från olika domäner blir därmed nödvändig för att upprätthålla en korrekt lägesbild. Användning av AI kan mot bakgrund av detta ge avsevärda fördelar. Bearbetning av sensordata och analys av underrättelser är två områden där AI-tekniken tack vare sin förmåga att snabbt klassificera och hitta mönster i stora mängder data lämpar sig väl.

I militära sensorsystem gör AI det möjligt att samtidigt och på ett integrerat sätt analysera olika typer av sensordata, till exempel radarsignaler och sonardata, och att med hög hastighet dra slutsatser. Resultaten av databehandlingen kan sedan antingen bidra till ett självständigt agerande hos AI-systemet, eller användas för att skapa beslutsunderlag och rekommendationer för mänskliga beslutsfattare. Vid strid med system i samverkan, där ett stort antal sensorer samverkar med flera olika vapensystem, kan AI-system exempelvis bidra till att leverera en uppdaterad helhetsbild av snabba skeenden. I dagens stridssituationer, där kraven på snabba beslut hela tiden ökar, kan förmågan till snabba analyser av stora datamängder vara en avgörande överlevnadsfaktor.

För underrättelsetillämpningen erbjuder AI en möjlighet att hitta det oväntade – den så kallade ”svarta svanen” – genom analys av stora mängder traditionella underrättelsedata i kombination med öppen webbdata. Den totala mängden data som produceras i dag är inte möjlig att analysera med traditionella metoder. Bearbetningen begränsas därför ofta både till mängden data och till ett känt sammanhang. Detta minskar möjligheterna till upptäckt av oförutsedda händelser. Historien har gett oss flera exempel där underrättelsearbetet inte i tid har förutsett kommande händelser, däribland Pearl Harbor och 11 september-attackerna. AI har potential att förbättra säkerhetspolitiska analyser genom att underlätta upptäckten av såväl snabba som utdragna händelseförlopp. Med AI kan mindre uppenbar eller till och med vid första påseendet irrelevant information tas med i en analys.

AI kan bli ett kraftfullt verktyg för att förbättra och utveckla förmågan hos en rad olika funktioner inom totalförsvaret. För Försvarsmakten kan AI erbjuda kvalitets- och effektivitetsförbättringar gällande både analys av sensordata och hanteringen av komplexa lednings- och underrättelseoperationer. I andra delar av totalförsvaret kan AI användas till exempel för att upptäcka avvikelser i nätverkstrafik vilka kan tyda på attacker mot kritisk infrastruktur såsom el- och vattenförsörjning. Bredden i tänkbara tillämpningar tillsammans med förbättringspotentialen gör AI-tekniken attraktiv även av ekonomiska skäl. Det krävs dock kunskap och personella resurser för att realisera möjligheterna.

“AI kan bli ett kraftfullt verktyg för att förbättra och utveckla förmågan hos en rad olika funktioner inom totalförsvaret. För Försvarsmakten kan AI erbjuda kvalitets- och effektivitetsförbättringar gällande både analys av sensordata och hanteringen av komplexa lednings- och underrättelseoperationer.”

Nya sårbarheter att hantera

I takt med att utvecklingen inom AI-området går framåt växer en oro i samhället för vad teknikutvecklingen medför i termer av minskad insyn i och kontroll över självstyrande och intelligenta system.

Det finns gott om exempel på hur så kallade ”intelligenta system” som vanligen ger goda resultat i vissa fall kan göra anmärkningsvärda misstag. Ett exempel är ett automatiskt system från Amazon som har utvecklats för att värdera sökande till utlysta tjänster. Systemet hade tränats i att analysera ansökningar, men efter en tids användning upptäcktes att det diskriminerade kvinnliga sökande. Anledningen till detta var helt enkelt att det fanns så få resuméer från kvinnor i de data som systemet hade tränats på, att systemet under träningen uppnådde större precision om dessa ansökningar förkastades. Det oönskade utfallet belyser en aspekt av maskininlärning som är viktig att beakta: systemets beteende kommer att styras av de data det har tränats på. Om träningsdata inte speglar den verkliga problemställningen, så kommer

AI-baserade system emellanåt att göra oväntade och ibland synnerligen olämpliga ”fel”, som i säkerhetskänsliga sammanhang kan få allvarliga konsekvenser.

Utöver denna typ av oavsiktliga misstag finns även exempel på hur AI-system kan manipuleras av fientligt sinnade aktörer. Studier har visat att med kunskap om hur en viss AI-metod fungerar kan man manipulera den så att modellen ger felaktiga svar. Exempelvis kan en, för en mänsklig betraktare, omärkbar förändring av en bild på pixelnivå få AI-systemet att tolka bildinnehåll helt fel. Det har även demonstrerats att bildigenkänningssystem avsedda att identifiera olika typer av trafikskyltar kan manipuleras att ge fel svar om en skylt har försetts med ett klistermärke på ett visst ställe. En viktig aspekt vad gäller sårbarheter är att mycket av AI-tekniken är öppet tillgänglig, vilket innebär att även terrororganisationer och kriminella grupperingar kan ha tillgång till de senaste metoderna för att utnyttja svagheter i AI-system.

Mot bakgrund av exempel som ovan pågår en debatt om de etiska aspekterna av AI-användning, som bland annat handlar om möjligheten att utkräva ansvar för beslut och handlingar utförda av AI-baserade system. En i sammanhanget central fråga är hur man ska kunna säkerställa att AI-system fungerar tillförlitligt och begripligt. Säkerhet kopplat till AI är ett växande forskningsområde som studerar frågor som exempelvis:

- Transparens – hur kan man designa intelligenta system som samtidigt är transparenta och går att förstå för en människa?
- Väldefinierade mål – hur kan man säkerställa att det mål som sätts för ett intelligent system verkligen leder till önskat resultat utan allvarliga bieffekter?
- Robusthet och stabilitet vid ändrade förutsättningar – hur kan man säkerställa att oväntade förändringar i systemets förutsättningar (strömavbrott, kommunikationsproblem med mera) inte leder till allvarliga negativa effekter?
- Hantering av sårbarheter – hur kan man skapa och träna system för att minimera risken för felbedömningar på grund av avsiktlig manipulation?

För verksamheter kopplade till försvar och säkerhet är det rimligen mer kritiskt än för andra verksamheter att de AI-system som används fungerar robust och utan negativa bieffekter. I många militära tillämpningar är det också avgörande att systemen är transparenta för att det ska vara möjligt att spåra och motivera de beslut som fattas. Då fördelarna med AI är så stora får man utgå ifrån att tekniken ändå kommer att användas både i militära system och i samhällskritiska verksamheter såsom elkraftsdistribution, hälso- och sjukvård, och finanshandel. Det är därmed nödvändigt att det inom Sveriges totalförsvar finns kunskap om teknikens sårbarheter och en beredskap för möjliga incidenter.

Sveriges förutsättningar i en föränderlig värld

2017 genomförde Vinnova en utredning om AI:s utveckling och potential i svenskt näringsliv och samhälle. I utredningen konstateras att svensk AI-forskning i nuläget har ”begränsad internationell konkurrenskraft”. Man pekar på otillräckliga AI-investeringar i både större och mindre företag, brist på statlig styrning och på att AI-kompetens lämnar landet. Utredningen lyfter emellertid fram att Sverige har en teknikvänlig befolkning, hög teknikkompetens, ett utvecklat innovationssystem och att landet ligger långt framme med IT och digitalisering. Det finns alltså goda grundförutsättningar för Sverige att bli en större aktör inom AI.

En oroväckande slutsats i rapporten är att ”Omvärlden satsar mer och snabbare än Sverige”. På sikt kan en sådan utveckling få stora konsekvenser för den svenska industrins konkurrenskraft, men även för den nationella säkerheten. Länder som ligger i framkant på AI-området kommer bland annat att kunna skaffa sig ett informationsöverläge vilket kan förändra det säkerhetspolitiska landskapet. På den internationella arenan utmärker sig Kina med stora satsningar inom AI. Även länder som kan sägas vara mer jämförbara med Sverige satsar aktivt på AI-utveckling. Exempel på detta är Frankrike som 2018 lanserade en AI-satsning på över 15 miljarder kronor fram till 2022, och Finland som 2017 blev första land i EU att ta fram en nationell AI-strategi. I Sverige utgörs den enskilt största AI-satsningen av forskningsprogrammet *Wallenberg AI, Autonomous Systems and Software Program* (WASP), där en miljard är särskilt reserverad för AI-forskning. WASP är dock ett privat initiativ, finansierat av Knut och

Alice Wallenbergs Stiftelse. Programmets inriktning kan inte förväntas täcka svenska statens intressen, utan WASP bör ses som ett komplement till statliga satsningar.

Vinnovas slutsatser bör innebära att även den svenska försvarssektorn – myndigheter såväl som försvarsindustrin – har goda grundförutsättningar att kunna introducera mer AI-baserade system. Värt att notera i sammanhanget är att AI i kombination med annan teknik skulle kunna ha en stor påverkan på det som länge har varit en av Försvarsmaktens stora utmaningar att hantera, nämligen bevakningen av ett utsträckt och bitvis mycket glesbefolkat territorium. Inte minst den långa kustlinjen har ur försvarssynpunkt varit en utmaning. Autonoma över- och undervattensfarkoster i kombination med intelligenta sensorsystem skulle kunna ge bättre förutsättningar för gränsbevakning.

För att totalförsvarets verksamheter ska kunna ta till sig och utnyttja AI-tekniken behövs personal med specialistkompetens, samtidigt som kunskaperna om AI generellt behöver lyftas inom organisationerna. Personer med utbildning inom området är eftertraktade på den civila marknaden och därmed svåra att rekrytera till statlig och annan offentlig verksamhet. Lyckas man inte lösa kompetensförsörjningen riskerar överföringen av AI-teknik till försvarsmyndigheter att försvåras, och kunskapsgapet mellan offentlig och civil verksamhet att öka ännu mer.

Konkurrensen om AI-kompetens pågår inte bara mellan privat och offentlig sektor utan även mellan länder. Såväl svenska företag som myndigheter konkurrerar på en global marknad, där stora löneskillnader mellan olika nationer kan leda till kunskapsflykt från de nationer som inte kan erbjuda konkurrensmässiga löner eller arbetsvillkor. För att inte Sveriges nationella säkerhet ska bli helt beroende av utländsk expertis är det viktigt att agera för att bygga upp och behålla en inhemsk kompetens inom avancerad databehandling.

AI-kompetens central för Sveriges nationella säkerhet

För att totalförsvaret ska kunna nyttja de möjligheter som AI-tekniken erbjuder och möta de utmaningar som följer med utvecklingen, är det angeläget att kunskapen om AI ökar inom berörda organisationer. Att säkerställa kompetensförsörjningen inom ett område som utvecklas snabbt, och som i hög grad är utsatt för internationell konkurrens, är en stor men viktig utmaning för Sverige. En annan stor utmaning för totalförsvaret och samhället i stort är att lära sig hantera de nya sårbarheter som AI medför. Sverige har goda grundförutsättningar att ta sig an dessa utmaningar, men att i för stor utsträckning förlita sig på att industrin och privata forskningsinitiativ ska ta ansvar för frågor av nationellt intresse är riskabelt.

För vidare läsning

Tove Gustavi, Jörgen Karlholm, Daniel Oskarsson, Tam Beran, Oscar Björnham, Erik Gudmundson, Hugo Heden, Henrik Karlzén, Johannes Lindblom, Jonas Nordlöf, Ioana Rodhe, Theodor Sommestad, Peter Svenmarck och Markus Svensson, Försvarsnära tillämpningar av Artificiell Intelligens, 2019, FOI-R--4707--SE.

Joel Brynielsson, Martin Nilsson, Johan Schubert, Peter Svenmarck, Artificiell intelligens för beslutsstöd i ledningssystem, 2018, FOI-R--4678--SE.

Johan Schubert, Artificiell Intelligens för Militärt Beslutsstöd, 2017, FOI-R--4552--SE.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Telefon: +46 8 5550 3000
www.foi.se