Regeringskansliet

Faktapromemoria
Riksdagsår: 2025/26
FPM-nummer: 110
2026-08-31

Meddelande om handlingsplan för cybersäkerhet och artificiell intelligens

Försvarsdepartementet

Dokumentbeteckning

COM(2026) 577 Celexnummer 52026DC0577

Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska och sociala kommittén samt Regionkommittén. Handlingsplan för cybersäkerhet och artificiell intelligens

Sammanfattning

Handlingsplan för cybersäkerhet och artificiell intelligens (AI) syftar till att göra Europa bättre rustat för att såväl tillvarata möjligheterna som bemöta riskerna med avancerad AI. I planen betonas att AI kan användas för att stärka cybersäkerheten genom att snabbt upptäcka sårbarheter, förebygga cyberattacker och skydda kritisk infrastruktur. Samtidigt kan tekniken utnyttjas av angripare för att automatisera attacker och hitta säkerhetsbrister i mycket större skala och hastighet än tidigare.

Handlingsplanen har tre huvudmål: att främja en säker och ansvarsfull användning av avancerad AI, att stärka EU:s cybersäkerhet och motståndskraft samt öka Europas egen AI-

kapacitet inom cybersäkerhetsområdet. I planen föreslås bland annat att möjligheterna att testa och utvärdera avancerade AI-modeller innan driftsättning ska förbättras, att en säker testplattform för kritiska sektorer ska skapas samt att samarbetet kring cybersäkerhet inom ramen för EU:s cybersäkerhetsbyrå Enisa ska stärkas. Handlingsplanen betonar också att befintliga regelverk, som AI-förordningen, NIS2-direktivet, cyberresiliensförordningen och cybersolidaritetsförordningen ska genomföras och användas mer effektivt.

Regeringen välkomnar initiativet till en handlingsplan gällande cybersäkerhet och AI.

Regeringen delar kommissionens bedömning att AI snabbt förändrar cyberhotbilden genom att göra det enklare och snabbare att identifiera, utveckla och utnyttja sårbarheter. Att stärka samhällets motståndskraft mot dessa hot är därför en prioriterad fråga för regeringen.

Regeringen anser att EU-samarbetet bör utformas så att medlemsstaternas nationella kapacitet fortsatt kan utvecklas och användas. Regeringen anser därför att en ordning där tillgången till avancerade AI-modeller i huvudsak centraliseras till Enisa bör undvikas.

1. Förslaget

1.1 Ärendets bakgrund

Handlingsplan för cybersäkerhet och artificiell intelligens presenteras mot bakgrund av den snabba utvecklingen av avancerade AI-modeller och deras ökande betydelse för cybersäkerhetsområdet. I handlingsplanen anges att befintliga åtgärder och initiativ inom området behöver kompletteras med insatser som stärker EU:s beredskap och förmåga att hantera AI-relaterade cyberhot.

Handlingsplanen presenterar mot denna bakgrund ett antal åtgärder för att stärka EU:s förmåga att bedöma och hantera risker med avancerad AI, främja en säker användning av AI inom cybersäkerhetsområdet samt stödja utvecklingen av europeisk kompetens och teknisk kapacitet.

Kommissionen presenterade handlingsplanen 7 juli 2026.

1.2 Förslagets innehåll

En central utgångspunkt i handlingsplanen är att avancerad AI både kan stärka cybersäkerheten och skapa nya säkerhetsrisker. AI kan bland annat bidra till att snabbare upptäcka och hantera säkerhetsbrister och cyberangrepp, men kan samtidigt användas av angripare för att genomföra mer omfattande och avancerade angrepp.

Handlingsplanen innehåller nio så kallade nyckelåtgärder, fördelade på tre huvudområden:

1. Testning och säker användning av avancerad AI:

- Europeisk kapacitet för utvärdering av AI-modeller ska utvecklas med särskild kompetens inom cybersäkerhet (2027).

- Kommissionen och EU:s cybersäkerhetsmyndighet Enisa ska ta fram en europeisk modell för hur myndigheter, företag och andra relevanta aktörer kan få säker och snabb tillgång till avancerade AI-modeller för cybersäkerhet (2026).

- Enisa och kommissionens gemensamma forskningscentrum (JRC) ska utveckla en säker europeisk testmiljö där AI-modeller kan prövas för cybersäkerhetsändamål. I första hand ska befintliga så kallade cyberövningsmiljöer byggas ut och användas (2026).

2. Stärkt beredskap och snabbare hantering av säkerhetsbrister

- Enisa ska ta fram vägledning, rekommendationer och goda exempel för skydd mot AI-drivna cyberhot och för säker användning av AI i cybersäkerhetsarbetet.

- Kommissionen, medlemsstaterna, Enisa och näringslivet ska se över befintliga arbetssätt för att upptäcka, prioritera och åtgärda säkerhetsbrister snabbare.

- Enisa ska tillsammans med medlemsstaterna, EU-institutionerna, näringsliv och utvecklare av öppen programvara genomföra ett pilotprojekt för att stärka säkerheten i viktig öppen programvara, bland annat genom att använda AI för att identifiera och åtgärda säkerhetsbrister.

3. Europeisk AI-kapacitet, investeringar och kompetens

- Kommissionen ska tillsammans med EU:s kompetenscentrum för cybersäkerhet (ECCC) och Enisa starta en europeisk satsning på AI-baserade cybersäkerhetslösningar, bland annat för att förbättra möjligheterna att snabbt åtgärda säkerhetsbrister.

- Medlemsstaterna ska få möjlighet att använda så kallade AI-fabriker och deras kompetens för att utveckla, testa och använda AI för cybersäkerhetsändamål.

- Kommissionen ska under 2026 tillsammans med medlemsstater och näringsliv ta fram utbildningar för cybersäkerhetspersonal om användning av AI.

Utöver dessa tre huvudområden betonas stärkt internationellt samarbete med likasinnade länder och organisationer, bland annat inom G7, FN och NATO, kring exempelvis gemensamma metoder för att bedöma avancerade AI-modeller, skydd av samhällsviktig infrastruktur och hantering av säkerhetsbrister.

1.3 Gällande svenska regler och förslagets effekt på dessa

Meddelandet utgör inte bindande lagstiftning och har därför ingen omedelbar effekt på svenska regelverk.

1.4 Budgetära konsekvenser och konsekvensanalys

Meddelandet har inga omedelbara budgetära effekter nationellt eller på EU-nivå eftersom det inte utgör bindande lagstiftning.

2. Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar att kommissionen tar initiativ till en handlingsplan för AI och cybersäkerhet. AI-utvecklingen förändrar förutsättningarna för cybersäkerhetsarbetet och ställer ökade krav på både offentlig och privat sektor. Regeringen anser att handlingsplanen kan bidra till att stärka EU:s förmåga att möta den förändrade hotbilden.

Regeringen betonar vikten av att nya EU-initiativ stärker, snarare än belastar, befintlig kapacitet. Mot bakgrund av det nuvarande säkerhetsläget är det viktigt att nya samordnings- och

stödstrukturer inte medför ytterligare resursbelastning eller sker på bekostnad av medlemsstaternas operativa förmåga. Regeringen instämmer därför i ansatsen att fokus i första hand bör ligga på genomförande och operativ effekt, och att föreslagna EU-gemensamma åtgärder så långt som möjligt bör bygga vidare på befintliga strukturer och bidra till att effektivisera det arbete som redan bedrivs nationellt.

Regeringen välkomnar kommissionens ambition att snabbt etablera gemensamma strukturer för testning och utvärdering av avancerade AI-modeller med fokus på cybersäkerhet. Det är angeläget att arbetet leder till praktiskt användbara resultat och att gemensamma standarder, processer och arbetssätt utvecklas.

Regeringen anser att kommissionen och Enisa bör ha en stödjande och samordnande roll i arbetet med testning av avancerade AI-modeller. Det är viktigt att tillvarata den expertis som finns i medlemsstaterna och skapa förutsättningar för kunskapsdelning och gemensamma arbetssätt. Samtidigt bör EU-samarbetet utformas så att medlemsstaternas nationella kapacitet fortsatt kan utvecklas och användas. Regeringen anser därför att en ordning där tillgången till avancerade AI-modeller i huvudsak centraliseras till Enisa bör undvikas.

Regeringen anser att åtgärder för att stärka motståndskraften bör ges hög prioritet. Det finns därför behov av att prioritera konkreta åtgärder för att minska befintliga säkerhetsbrister.

Regeringen instämmer i behovet av en stark europeisk kapacitet inom AI och cybersäkerhet. AI kan ge försvarare bättre förutsättningar att upptäcka, analysera och hantera cyberhot. Samtidigt innebär utvecklingen att angripare kan agera snabbare och i större skala. Det är därför angeläget att Europa utvecklar förmåga att använda AI i cybersäkerhetsarbetet i samma takt som hotbilden utvecklas. En stärkt europeisk kapacitet är även viktig för att minska strategiska beroenden och bidra till långsiktig säkerhet i EU.

Regeringen välkomnar åtgärder som syftar till att främja kunskapsutbyte, innovation och samverkan mellan offentliga och privata aktörer inom AI och cybersäkerhet. Sådana initiativ bör samtidigt utformas med tydligt ansvarstagande och med utgångspunkt i befintliga strukturer, för att undvika överlappande insatser, ökade kostnader och onödig administration.

Kostnader som förslagen kan leda till för den nationella budgeten ska finansieras i linje med de principer om neutralitet för statens budget som riksdagen beslutat om (prop. 1994/95:40, bet. 1994/95FiU5, rskr. 1994/95:67). Utgiftsdrivande åtgärder för EU-budgeten ska finansieras genom omprioriteringar inom den

befintliga fleråriga budgetramen (MFF). Det är viktigt för regeringen att förhandlingen av nästa fleråriga budgetram inte föregrips.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är ännu inte kända.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter är ännu inte kända.

2.4 Remissinstansernas och andra intressenters ståndpunkter

Meddelandet har inte remitterats.

3. Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Ej tillämpligt. Kommissionens meddelande informerar endast om kommande politiska strategier och åtgärder.

3.2 Subsidiaritets- och proportionalitetsprinciperna

Ej tillämpligt. Kommissionens handlingsplan avser ett meddelande som endast informerar om kommande politiska strategier och åtgärder.

4. Övrigt

4.1 Fortsatt behandling av ärendet

Diskussioner förväntas i rådet, t.ex. Telekområdet.

4.2 Fackuttryck och termer

AI-fabriker: EU:s AI-fabriker (AI Factories) är ett initiativ som syftar till att bygga upp ekosystem för artificiell intelligens. Se bl.a. Faktapromemoria **2024/25:FPM8** om kommissionens meddelande **COM(2024) 490** om det europeiska forskningsområdet (ERA).