

Regeringskansliet
Finansdepartementet
103 33 Stockholm

Er referens

Fi2026/01676

Vår handläggare

Alexander Engvers

Remissvar gällande *Remittering av Europeiska kommissionens förslag till förordning om utveckling av moln och AI KOM (2026)502*

Totalförsvarets forskningsinstitut (FOI) välkomnar EU-kommissionens ambition att stärka Europas utveckling av digital motståndskraft samt att genom förordningen ge en strategisk inriktning för uppbyggnad av europeisk moln- och AI-infrastruktur. FOI ser dock betydande risker i förslaget nuvarande utformning då de strikta kraven på suveränitet och certifiering riskerar att hämma förmågan att bygga avancerad teknologisk spets och att anpassa totalförsvaret till en snabbt föränderlig hotbild. Detta kan riskera vår försvarsförmåga mot framtida hot.

Medan förordningen fokuserar på att säkra kontrollen över leverantörer, menar FOI att den viktigaste målsättningen är att säkra verksamhetsutövarens handlingsfrihet, behov av säkerhet och funktionalitet samt verksamhetens förutsättningar för kontinuitet genom teknisk diversifiering.

FOI lämnar härutöver – från de utgångspunkter myndigheten har att beakta – följande generella och särskilda reflektioner på förslagen i remissen.

Generella reflektioner

Behovet av valfrihet

Tillgång till världsledande teknologisk innovation och kapacitet är avgörande för att i det aktuella omvärldsläget kunna utveckla nödvändiga och avgörande förmågor. I försvarssammanhang kan detta uttryckas som att en högre förmåga att använda AI och hantera stora mängder data effektivt skapar förutsättningar för informationsövertag och förkortade beslutsprocesser.

Förslaget till förordning introducerar emellertid en risk för stagnation i utveckling och tillämpning av ny teknisk förmåga genom en allt för strikt geografisk och juridisk kontroll som begränsar kompetensförsörjning, utbud av tjänster och kapacitet samt förmåga att möta kvalificerade hot. Genom att begränsa tillgången till det globala ekosystemet avseende moln och AI kan nya koncentrationsrisker uppstå med beroende till ett fåtal lokala aktörer som saknar den bredd och det djup som krävs för innovation och effektiv utveckling av t.ex. försvarsförmåga.

Krav på geografisk och juridisk kontroll kan i praktiken exkludera de mest avancerade AI-modellerna och världsledande infrastrukturer med specialiserade plattformar. Om myndigheter tvingas välja bort spetsteknologier och istället fokusera på certifierad suveränitet bygger vi förmågor som är politiskt säkra men tekniskt otillräckliga. Utöver de ledande aktörerna i USA är Asien och Oceanien viktiga regioner där ny kapacitet och mjukvaruförmåga utvecklas.

För att nå en hög förmåga inom AI krävs tillgång till en mycket kvalificerad infrastruktur och mjukvaruförmåga, specialiserade lösningar i egen drift såväl som globala hyperskalbara tjänster behöver samverka för att en organisation ska kunna hantera ett allt mer omfattande och komplext informationslandskap. För totalförsvarets behov krävs även en mycket kvalificerad, effektiv och väl integrerad säkerhetsarkitektur där de stora globala aktörerna idag driver utvecklingen inom cybersäkerhet framåt. Europeiska alternativ kan idag och inom överskådlig tid svårtligen konkurrera med marknadsledande leverantörer vad avser kostnad, funktionalitet samt skalbarhet i både kapacitet och säkerhet. Det är därför rimligt att, vid val av leverantör, även andra grunder än ekonomi används vid utvärderingen. Detta gäller särskilt inom områdena försvar och säkerhet.

Förslagets betoning på portabilitet och *open source first* är i regel bra men kan även skapa en målkonflikt där kravet på att snabbt kunna byta leverantör står i direkt motsats till förmågan att optimera och maximera prestandan i en avancerad integrerad miljö med höga krav på säkerhet, interoperabilitet och skalbarhet samt till att utveckla och implementera nya förmågor.

En strikt begränsning av var support och expertis får finnas riskerar även att strypa tillgången till den globala specialistkompetens som krävs för att driva och underhålla komplexa tjänster.

Suveränitet och resiliens

Förslaget vilar på en syn på suveränitet som fokuserar på vem som levererar tjänsten och var data lagras. FOI anser att detta är en otillräcklig modell för att möta aktuella säkerhetshot. För att skapa resiliens i förmågor och att kunna möta en föränderlig hotbild krävs omfattande förberedelser och övningar. Det krävs en arkitektur som

möjliggör både redundans och diversifiering. Istället för en endimensionell suveränitetsskala bör fokus ligga på riskhantering och på att förbereda förmåga genom flera olika tekniska plattformar.

Samtliga förutsättningar, behov och risker kan inte förutses. Att redan i designfasen tvinga organisationer att begränsa handlingsalternativen medför risker som är svåra att överblicka. Särskilt om lösningarna är begränsade till en kontinent. En myndighet kan ha en fullt certifierad europeisk leverantör med den högsta nivån avseende suveränitet men ändå stå helt försvarslös om en kritisk komponent, mjukvarulicens eller teknisk infrastruktur faller bort. Den verkliga suveräniteten ligger inte i att varje komponent är europeisk, utan i myndighetens förmåga att upprätthålla sin kritiska funktion trots störningar.

För att möta de strängaste kraven på suveränitet enligt förslaget krävs inte bara en europeisk molntjänst utan en hel vertikalintegrerad stack från kisel till applikationslager och data, som dessutom är verifierad och certifierat fri från utomeuropeisk kontroll. Eftersom den globala försörjningskedjan för halvledare och avancerad mjukvara är djupt integrerad och domineras av aktörer utanför EU skapas en situation där det för myndigheter som bedriver säkerhetskänslig verksamhet inte finns någon leverantör idag som kan uppfylla kraven.

FOI förespråkar att fokus flyttas från geografisk blockering, administrativ dokumentation och statiska certifieringar till praktiskt verifierbar förmåga och resiliens utifrån verksamheternas förutsättningar och behov. För de mest säkerhetskritiska verksamheterna kommer förmåga till kontinuerlig riskidentifiering och –hantering samt regelbundna övningar sannolikt värderas högre än ett certifikat utfärdat till en leverantör.

Övrig reglering inom området

Verksamhetsutövare kan tvingas hantera flera parallella och potentiellt motstridiga krav rörande riskbedömning och -hantering, vilket stjäl resurser från det faktiska säkerhetsarbetet. I praktiken skiftar fokus från hur man skyddar verksamheten till vem som äger tekniken. NIS2/CER-direktiven betonar i hög grad resiliens vilket är ett funktionellt och operativt säkerhetstänk till skillnad från CADA. Här riskerar CADA framstå som onödigt eller till och med kontraproduktivt om det tvingar verksamhetsutövare att överge tekniskt robusta lösningar som följer t.ex. NIS2/CER-direktiven bara för att de inte uppfyller de strikta suveränitetskraven för leverantörer.

Generell slutsats

FOI efterlyser en mer nyanserad reglering där suveränitet betraktas som en riskdimension som ska hanteras snarare än ett absolut tekniskt och regulatoriskt mål

som trumfar operativ förmåga. För att säkerställa att europeiska myndigheter kan leda den tekniska utvecklingen och samtidigt ha en hög grad av resiliens måste förslaget tillåta större valfrihet i valet av tekniska lösningar och stödja verksamhetsutövarnas förmåga till självständigt handlingsutrymme med fokus på effekt och kontinuitet.

Särskilda reflektioner

Behov av forskningsinitiativ avseende säkerhet för AI

Det bör övervägas att tydliggöra utmaningarna avseende säkerhet i avsnittet om Grand Challenges i Annex 1. På senare tid har det exempelvis observerats att leverantörerna av de nuvarande frontier AI-modellerna har stora problem med att deras AI-modeller utför oönskade handlingar inom säkerhetsdomänen. Exempel på detta är den omtalade incidenten där OpenAI:s modeller under träning kringgick begränsningar för att göra cyberangrepp mot Hugging Face. Leverantörer av frontier AI-modeller har också sett att flera av deras begränsningar kringgåts (eng. jailbreaks) av hotaktörer.

Forskningen inom detta område kan avse de extra attackytorna som AI medför samt hur begränsningar (eng. guard rails) och efterträning av modeller kan användas för att hindra att modeller utför eller beter sig på ett farligt eller oönskat sätt (eng. misalignment).

Försvarbarhet av datacenter

Datacenter är attraktiva måltavlor i konflikter och krig. Vid utformning av data acceleration zones bör även energi- och säkerhetsmässiga aspekter tas i beaktning av dess lokalisering.

Små modulära reaktorer förs fram i artikel 4 (e) som ett forskningsområde. Små modulära reaktorer är mindre kärnkraftsreaktorer. I detta forskningsområde bör man även beakta vad detta har för bäring på försvarbarheten av de datacenter de förs in i. Radioaktiva ämnen kan medföra att det är svårare att hålla datacenter i drift vid händelse av katastrofer eller fysiska angrepp mot datacentret.

Otydlig målsättning kring ökandet av EU:s datacenterkapacitet

I dokumentet framförs under rubriken *Framework of the proposal/initiative* två olika tidplaner för att datacenterkapaciteten inom EU ska tredubblas: till 2030 respektive inom fem till sju år. Detta kan behöva ensas.

Försörjningstrygghet

Med ökad mängd datorkapacitet följer ökat behov av kritiska resurser, såsom energi och vatten. Detta kan kräva ut- eller tillbyggnad av existerande infrastruktur, till exempel elnät. Det är då viktigt att säkerställa att denna infrastruktur är resiliënt, och

att den kan fungera även vid händelse av kris eller krig. Förslaget bör därför tydliggöra kraven på säkerheten i försörjningen av kritiska resurser för datacenter.

Tillgång till hårdvara

Det råder idag brist på hårdvara till följd av det ökade behovet av beräkningskraft. En viktig fråga är därför om EU kommer att kunna köpa in nödvändig hårdvara i tillräcklig mängd för att uppnå förslagets målsättningar. Som redan tagits upp under de generella reflektionerna ovan är stora delar av denna hårdvaruförsörjningskedja också beroende av stater utanför EU. För att uppnå ökad suveränitet krävs därför också att beroendet av dessa minskas. Detta kan i högre grad behöva beaktas i förslaget.

Otydlighet kring tredjeland

Användningen av molntjänstleverantörer från tredjeland medför utmaningar kopplade till säkerhet och suveränitet. Att använda molntjänster skapar ett beroende till leverantören, vilken i sin tur kan påverkas av aktuellt tredjeland. Enligt förslaget kan tjänstleverantör från tredjeland uppnå assurancesnivå 3. Samtidigt innebär kriterierna för assurancesnivå 3 att en tjänstleverantör ska vara *established* inom unionen samt att infrastruktur, tillgångar och personal ska vara placerade inom unionen. Här tycks finnas en otydlighet i hur tjänster från tredjeland ska bedömas.

Även om ett datacenter fysiskt befinner sig i Sverige eller EU kan tredjeland påverka molntjänstleverantören om leverantören lyder under deras lagar. Exempel på detta är amerikanska CLOUD Act där amerikanska myndigheter kan tvinga fram utlämnande av data från leverantörer som lyder under amerikansk jurisdiktion, oavsett var datan fysiskt lagras. Förslaget bör förtydliga att *measures in place* innefattar detta.

Ytterligare en risk är att ett tredjeland vid en geopolitisk kris med kort varsel kan etablera kontrollmekanismer, vilket kan innebära en osäkerhet kring tjänstens tillgänglighet i ett förändrat säkerhetsläge.

Sammantaget understryker detta behovet av sådan förmåga till kontinuerlig riskidentifiering och -hantering som lyfts tidigare i detta remissvar.

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av jurist Alexander Engvers. I den slutliga handläggningen har även chefsjurist Eva Liljefors, stabschef Niclas Karlsson, informationssäkerhetschef Andreas Sundberg, forskningsingenjör John Ziegenbein och handläggare Pär Eriksson deltagit.

Jens Mattsson

*Alexander Engvers*Sändlista:

Finansdepartementet

fi.remissvar@regeringskansliet.se med kopia till
fi.ofa.dis.remisser@regeringskansliet.seInternt FOI:

Registrator

ÖD-sekreterare

Stabschef

Chefsjurist

Avdelningschef FS