



2023/2113

11.10.2023

KOMMISSIONENS REKOMMENDATION (EU) 2023/2113

av den 3 oktober 2023

om kritisk teknik för EU:s ekonomiska säkerhet för vidare riskbedömning med medlemsstaterna

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 292, och

av följande skäl:

- (1) Kommissionen och den höga representanten har konstaterat att med ökande geopolitiska spänningar och en global ekonomisk integration som är djupare än någonsin tidigare kan vissa ekonomiska flöden och verksamheter utgöra en risk för vår säkerhet, och antog ett gemensamt meddelande om en europeisk strategi ⁽¹⁾ för ekonomisk säkerhet.
- (2) Den europeiska strategin för ekonomisk säkerhet vilar på tre pelare: främjande av EU:s ekonomiska bas och konkurrenskraft, skydd mot risker, och partnerskap med så många länder som möjligt som delar våra farhågor och intressen.
- (3) Som en del av denna ram, och mot bakgrund av riskerna som vissa ekonomiska beroendeförhållanden och den tekniska utvecklingen kan innebära, behöver EU ta en nykter blick på riskerna för den ekonomiska säkerheten och utvecklingen över tid.
- (4) Riskerna bör kartläggas och bedömas tillsammans med EU:s medlemsstater, och synpunkter från privata intressenter bör beaktas inom ramen för en dynamisk och kontinuerlig process.
- (5) Den europeiska strategin för ekonomisk säkerhet har fastställt följande fyra omfattande och icke uttömmande riskkategorier för ytterligare bedömning: leveranskedjornas resiliens, inbegripet energisäkerhet, fysisk säkerhet och cybersäkerhet för kritisk infrastruktur, teknisk säkerhet och teknikläckage, och användning av ekonomiskt beroende eller ekonomiskt tvång som vapen.
- (6) I det gemensamma meddelandet gjorde kommissionen åtagandet att bedöma riskerna för teknisk säkerhet och teknikläckage på grundval av en förteckning över strategisk teknik som är kritisk för den ekonomiska säkerheten, och när det gäller de känsligaste riskerna föreslå en förteckning över kritisk teknik för riskbedömning tillsammans med medlemsstaterna före slutet av 2023.
- (7) För att välja ut teknikområden med de känsligaste riskerna föreslås i det gemensamma meddelandet tre snävt definierade och proaktiva kriterier för ytterligare bedömning: teknikens möjliggörande och omdanande karaktär, risken för civil-militär fusion, och risken för att tekniken missbrukas för kränkningar av de mänskliga rättigheterna.
- (8) Kriteriet möjliggörande och omdanande karaktär tittar på teknikens potential och betydelse för att avsevärt öka prestanda och effektivitet och/eller radikala förändringar för sektorer, kapaciteter etc.
- (9) Kriteriet risk för civil-militär fusion tittar på teknikens betydelse för både den civila och den militära sektorn och dess potential att leda till framsteg på båda områdena, liksom risken för användning av viss teknik för att äventyra fred och säkerhet.

⁽¹⁾ JOIN(2023) 20 final.

- (10) Kriteriet risken för att tekniken missbrukas för kränkningar av de mänskliga rättigheterna tittar på teknikens potential att missbrukas för att kränka mänskliga rättigheter, däribland inskränka grundläggande friheter.
- (11) Efter en första intern analys har kommissionen upprättat en förteckning över tio kritiska teknikområden för EU:s ekonomiska säkerhet. Förteckningen tar hänsyn till det arbete som gjorts i enlighet med handlingsplanen för synergieffekter mellan civil industri, försvarsindustri och rymdindustri ⁽²⁾. Det är ett levande dokument som kan ändras och uppdateras i takt med den tekniska utvecklingen.
- (12) På grundval av tre snävt definierade och proaktiva urvalskriterier för vidare bedömning fastställs i meddelandet fyra kritiska teknikområden i förteckningen som med största sannolikhet innebär de känsligaste och mest omedelbara riskerna för ekonomisk säkerhet och teknickläckage, nämligen avancerade halvledare, artificiell intelligens, kvantteknik och bioteknik. Teknikområdena bör högprioriteras för en gemensam riskbedömning tillsammans med medlemsstaterna före årets slut. Efter sonderingsarbetet med medlemsstaterna kan den gemensamma bedömningen fokusera på undergrupper inom de fyra teknikkategorierna.
- (13) Förteckningen speglar kommissionens bedömning av vilka av dessa teknikområden som troligtvis innebär de känsligaste och mest omedelbara riskerna för teknisk säkerhet och teknickläckage. Detta kan ligga till grund för senare beslut om ytterligare åtgärder. Kommissionen kommer att föra en öppen dialog med medlemsstaterna om en lämplig tidsplan och räckvidden för ytterligare bedömning av risker, och bland annat ta hänsyn till tidsfaktorns betydelse för riskutvecklingen. Kommissionen välkomnar en diskussion i god tid om de här delarna av strategin för ekonomisk säkerhet i rådet, mot bakgrund av de övergripande politiska överläggningarna och riktlinjerna med anledning av det gemensamma meddelandet. Kommissionen kan komma att lägga fram ytterligare initiativ på området våren 2024, mot bakgrund av dialogen och de första erfarenheterna av den inledande bedömningen, liksom ytterligare synpunkter på förteckningen över teknikområden. När kommissionen tillsammans med medlemsstaterna fattar beslut om förslag till ytterligare riskbedömning för ett eller flera teknikområden eller tekniska undergrupper i förteckningen, kommer kommissionen att beakta pågående och planerade främjande åtgärder och partnerskap. I allmänhet kommer kommissionen att ha i åtanke att åtgärder som vidtas för att stärka EU:s konkurrenskraft på relevanta områden kan bidra till att minska vissa tekniskrisker.
- (14) Syftet med riskbedömningen bör vara att kartlägga och analysera sårbarheter i systemet utifrån deras tänkbara inverkan på EU:s ekonomiska säkerhet och sannolikheten för att de negativa konsekvenserna förverkligas. För att strukturera den framtida riskbedömningen tillsammans med medlemsstaterna har kommissionen utarbetat några vägledande principer.
- (15) Denna rekommendation föregriper inte resultatet av riskbedömningen. Endast resultatet av detaljerade bedömningar av risknivån och riskernas art kan ligga till grund för fortsatta diskussioner om behovet av precisa och proportionerliga främjande åtgärder, skyddsåtgärder eller partnerskap för något av dessa kritiska teknikområden eller tekniska undergrupper. Medlemsstaterna och kommissionen kan använda sig av uppgifterna för att utforma framtida politiska åtgärder, däribland skyddsåtgärder, främjande åtgärder eller partnerskap på nationell nivå, EU-nivå eller internationell nivå, vilka bör stå i proportion till risknivån och vara precisa till omfattningen. Inga slutsatser kan därför dras i nuläget om specifika instrument i EU:s eller medlemsstaternas verktygslådor för främjande åtgärder, skyddsåtgärder och partnerskap med andra för att öka den ekonomiska säkerheten.
- (16) Alla eventuella åtgärder som kan vidtas kommer att vara proportionerliga och riktade mot själva riskerna med varje kritiskt teknikområde eller relevant teknik. Alla genomförandeåtgärder syftar till att öka unionens styrka på dessa områden och utformas så att de minskar negativa spridningseffekter till marknaden eller ekonomin. Utvärderingarna bör särskilt bidra till att utveckla unionens politik till stöd för innovation och industriell utveckling för de berörda teknikerna, inbegripet genom internationella initiativ.

⁽²⁾ COM(2021) 70 final

HÄRIGENOM REKOMMENDERAS FÖLJANDE:

1. Av de tio kritiska teknikområden som nämns i förteckningen rekommenderas i ett första skede att medlemsstaterna tillsammans med kommissionen före slutet av 2023 utvärderar följande fyra teknikområden som är mest sannolika att utgöra de känsligaste och mest omedelbara riskerna med avseende på teknisk säkerhet och teknikläckage.

- a) Avancerad halvledarteknik

Halvledare, mikroelektronik och fotonik är avgörande komponenter i elektroniska apparater på kritiska områden som kommunikation, datorsystem, energi, hälsa, transport och försvars- och rymdsystem och -tillämpningar. På grund av deras möjliggörande och omdanande karaktär och deras användning för civila och militära syften är det viktigt att fortsätta spela en ledande roll för att bygga och vidareutveckla denna teknik.

- b) Teknik för artificiell intelligens

AI (mjukvara), högpresterande datorsystem, molntjänster, kantdatorsystem och dataanalys har många tillämpningar med dubbla användningsområden och är avgörande för att behandla stora mängder data och fatta beslut på grundval av denna datadrivna analys. Dessa teknikområden har enorm omvälvande potential i det avseendet.

- c) Kvantteknik

Kvantteknik har en enorm potential att förändra en rad civila och militära sektorer genom att möjliggöra ny teknik och nya system som utnyttjar kvantmekanikens egenskaper. Det går i nuläget inte att fullt ut bedöma vilka konsekvenser dagens och framtidens kvantteknik kan få.

- d) Bioteknik

Bioteknik har en avsevärd möjliggörande och omdanande karaktär inom områden som jordbruk, miljö, hälso- och sjukvård, biovetenskap, livsmedelskedjor och biotillverkning. Viss bioteknik, som genetisk ingenjörskonst som används på patogener eller skadliga föreningar som bildas vid genetisk modifiering av mikroorganismer, kan ha en säkerhets-/militär dimension, särskilt om den missbrukas.

2. Kommissionen uppmanar medlemsstaterna att föra en öppen dialog om en lämplig tidsplan och räckvidd för gemensamma riskbedömningar för andra teknikområden eller tekniska undergrupper i förteckningen, med tanke på den snabbt föränderliga geopolitiska miljön och de olika graderna av sannolikhet att teknikområdena i förteckningen innebär de känsligaste och mest omedelbara riskerna för teknisk säkerhet och teknikläckage.

3. För att strukturera den gemensamma riskbedömningen har följande vägledande principer använts:

- a) Kartlägga och analysera sårbarheter utifrån deras potentiella inverkan på EU:s ekonomiska säkerhet och sannolikheten att de negativa konsekvenserna förverkligas. Analysen bör kartlägga de viktigaste hoten och aktörerna som utgör ett hot, och bör vid behov beakta geopolitiska faktorer för att bedöma sannolikheten för negativa följdverkningar. Analysen bör också beakta bland annat teknikens värdekedja, riskutvecklingen och relevant teknisk utveckling, inbegripet befintliga och förväntade framtida flaskhalsar och kartlägga EU:s ställning på varje teknikområde, däribland viktiga aktörer och inslag för EU:s ledande ställning. Den globala interkonnekтивiteten hos teknikens ekosystem, inbegripet inom forskning och teknikens leveranskedja.
- b) I sonderingsfasen av den gemensamma bedömningen bör hänsyn tas till om den detaljerade bedömningen ska fokusera på de mest relevanta tekniska undergrupperna.
- c) Bedömningen av risker kommer inte att vara landspecifik.

- d) Risker med potential att påverka hela EU prioriteras.
 - e) Synergieffekter och komplementaritet skapas med befintliga analyser på EU-nivå och nationell nivå och kan användas i bedömningen av riskbedömningsprocessen.
 - f) Synpunkter från den privata sektorn beaktas.
- 4. Den gemensamma riskbedömningen kommer på begäran av medlemsstaterna eller privata intressenter att beläggas med sekretess. Slutresultatet av den gemensamma riskbedömningen kommer att sekretessklassas på lämpligt sätt.
 - 5. Bedömningen bör genomföras av medlemsstaterna och kommissionen med hjälp av befintliga forum, och vid behov nya forum, med relevant sakkunskap, utifrån behoven på varje kritiskt teknikområde.
 - 6. Kommissionen kommer att fortsätta följa den tekniska utvecklingen och vid behov föreslå att annan teknik läggs till denna rekommendation för framtida bedömning.

Utfärdad i Strasbourg den 3 oktober 2023.

På kommissionens vägnar
Thierry BRETON
Ledamot av kommissionen

BILAGA

Förteckning över tio kritiska teknikområden för EU:s ekonomiska säkerhet

	Teknikområde	Teknik*
<i>* Förteckningen innehåller områden som troligtvis kommer att stå i centrum för riskbedömning men är inte uttömmande</i>		
1.	AVANCERAD HALVLEDARTEKNIK	— Mikroelektronik, inbegripet processorer — Fotonikteknik (inbegripet högenergilasertechnik) — Högfrekvenshalvledare — Utrustning för tillverkning av halvledare i särskilt avancerade nod-storlekar
2.	AI-TEKNIK	— Högpresterande datorsystem — Moln- och kantdatorsystem — Dataanalysteknik — Datorseende, bearbetning av språk, objektigenkänning
3	KVANTTEKNIK	— Kvantdatorteknik — Kvantkryptografi — Kvantkommunikation — Kvantsensorteknik och -radar
4	BIOTEKNIK	— Teknik för genetisk modifiering — Nya genomiska metoder — Gendrivare — Syntetisk biologi
5	AVANCERAD KONNEKTIVITET, NAVIGATION OCH DIGITAL TEKNIK	— Säker digital kommunikation och konnektivitet, som RAN (Radio Access Network) och Open RAN och 6G — Cybersäkerhetsteknik, inbegripet cyberövervakning, säkerhets- och intrångssystem, digital kriminalteknik — Sakernas internet och virtuell verklighet — Distribuerad databasteknik och teknik för digital identitet — Väglednings-, navigations- och kontrollteknik, inbegripet relaterad flygelektronik och marin positionsbestämning
6	AVANCERAD SENSORTEKNIK	— Elektrooptiska, radarbaserade, kemiska, biologiska, strålningsbaserade och distribuerade sensorsystem — Magnetometrar, magnetiska gradiometrar — Sensorer för elektriska undervattensfält — Gravimetrar och gradiometrar
7	RYMD- OCH FRAMDRIVNINGSTEKNIK	— Särskild rymdfokuserad teknik, från komponent- till systemnivå — Teknik för rymdövervakning och jordobservation — Positionsbestämning, navigering och tidsbestämning (PNT) — Säker kommunikation, inbegripet satellit i jordnära omloppsbana (LEO) — Framdrivningsteknik, inbegripet hypersonisk teknik och komponenter för militär användning

Teknikområde		Teknik*
		* Förteckningen innehåller områden som troligtvis kommer att stå i centrum för riskbedömning men är inte uttömmande
8	ENERGITEKNIK	— Kärnfusionsteknik, kärnreaktorer och elproduktion, radiologisk omvandlings-, anriknings- och återvinningsteknik — Väte och nya bränslen — Nettonollteknik, inbegripet fotocellteknik — Smarta nät och energilagring, batterier
9	ROBOTAR OCH AUTONOMA SYSTEM	— Drönare och fordon (för luft-, land-, yt- och undervattenstransport) — Robotar och robotkontrollerade precisionssystem — Exoskelett — AI-baserade system
10	AVANCERAD MATERIAL-, TILLVERKNINGS- OCH ÅTERVINNINGSTEKNIK	— Teknik för nanomaterial, intelligenta material, avancerade keramiska material, stealth-material, inbyggd säkerhet och hållbarhet hos material — Additiv tillverkning, inbegripet på fältet — Digitalstyrd mikroprecisionstillverkning och småskaliga lasermaskiner/-svetsar — Teknik för utvinning, bearbetning och återvinning av kritiska råvaror (inbegripet hydrometallurgisk återvinning, biolakning, nanoteknikbaserad filtrering, elektrokemisk bearbetning och svart massa).