

Een veiligheidsbarrière voor kunstmatige intelligentie volledig opbouwen

De gezonde en ordelijke ontwikkeling van kunstmatige intelligentie bevorderen

Chen Yixin

Partijsecretaris van het Ministerie van Staatsveiligheid, minister

Op dit moment leidt kunstmatige intelligentie de nieuwe ronde van wetenschappelijke en technologische revolutie en industriële verandering steeds verder de diepte in. Het gebied van kunstmatige intelligentie is reeds het belangrijkste strijdtoneel van de mondiale technologische concurrentie en een nieuw spoor van de strategische wedijver tussen grote mogendheden geworden.

Het Centraal Comité van de Communistische Partij van China hecht grote waarde aan de ontwikkeling van kunstmatige intelligentie. Secretaris-generaal Xi Jinping heeft een reeks belangrijke aanwijzingen gegeven en benadrukt dat men "de wetenschappelijke en technologische innovatie, industriële ontwikkeling en toepassingsgerichte benutting van kunstmatige intelligentie volledig moet bevorderen, het toezicht- en governancestelsel voor kunstmatige intelligentie moet verbeteren en stevig de initiatiefpositie in de ontwikkeling en governance van kunstmatige intelligentie in handen moet houden".

Wij moeten de geest van de belangrijke aanwijzingen van secretaris-generaal Xi Jinping diepgaand bestuderen en begrijpen, onwankelbaar het alomvattende nationale veiligheidsconcept uitvoeren, de opbouw van een systeem voor preventie en beheersing van veiligheidsrisico's van kunstmatige intelligentie versnellen en met een hoog niveau van veiligheid en zeer efficiënte governance de gezonde en ordelijke ontwikkeling van de kunstmatige intelligentie van ons land bevorderen.

De fundamentele leidraad voor het verbeteren van de governance van kunstmatige intelligentie stevig vasthouden

Sinds het 18e Partijcongres heeft secretaris-generaal Xi Jinping vanuit het strategische niveau van "het bevorderen van China's sprongsgewijze wetenschappelijke en technologische ontwikkeling, industriële optimalisering en opwaardering en de algehele sprong van de productiekrachten" en van "het verkrijgen van het initiatief in de mondiale technologische concurrentie" een reeks belangrijke uiteenzettingen gedaan over het verbeteren van de governance van kunstmatige intelligentie.

Wij moeten deze volledig, nauwkeurig en alomvattend bestuderen en begrijpen en vooral de volgende acht aspecten goed vatten.

Ten eerste: de strategische positionering van kunstmatige intelligentie.

Kunstmatige intelligentie is een strategische technologie die deze ronde van wetenschappelijke en technologische revolutie en industriële verandering leidt. Zij heeft een zeer sterk uitstraling- en aandrijfeffect, het effect van de "leidende wilde gans". Wie de ontwikkelingskansen van kunstmatige intelligentie en andere nieuwe economieën kan grijpen, heeft de polsslag van het tijdperk goed gevoeld. Daarom moet kunstmatige intelligentie als strategische industrie worden behandeld en in het geheel van de nationale ontwikkeling worden geïntegreerd.

Ten tweede: het ontwikkelingsbeleid voor kunstmatige intelligentie.

De voordelen van China's nieuwe systeem voor het mobiliseren van nationale krachten moeten volledig worden benut. Men moet vasthouden aan zelfstandigheid en zelfverbetering en de toepassingsoriëntatie benadrukken. Innovatie moet als eerste drijvende kracht worden genomen en veiligheid als ondergrens worden geëist. De top-level planning moet worden verbeterd en de werkorganisatie versterkt, om de alomvattende kracht van China's kunstmatige intelligentie als geheel en systematisch naar een hoger niveau te brengen.

Ten derde: de waardegerichtheid van kunstmatige intelligentie.

Men moet het welzijn van de gehele mensheid voor ogen houden en de kunstmatige intelligentie in een nuttige, veilige en rechtvaardige richting gezond en ordelijk laten ontwikkelen. Het vervullen van de wens van het volk naar een beter leven moet als uitgangspunt van technologische innovatie worden genomen. Kunstmatige intelligentie moet nauw worden verbonden met het waarborgen en verbeteren van het levensonderhoud van de bevolking en moet de pijnpunten en moeilijke problemen oplossen op gebieden van het levensonderhoud van de bevolking zoals onderwijs, medische zorg, ouderenzorg en transport.

Ten vierde: het governanceconcept voor kunstmatige intelligentie.

Ontwikkeling en veiligheid moeten gecoördineerd worden. Men moet de formulering en verbetering van relevante wetten en voorschriften, beleids- en institutionele systemen, toepassingsnormen en ethische richtlijnen versnellen. Er moeten systemen voor technische monitoring, vroegtijdige risicowaarschuwing en noodrespons worden opgebouwd. Het onderzoek naar en de preventie van potentiële risico's van de ontwikkeling van kunstmatige intelligentie moeten worden versterkt, om de belangen van het volk en de nationale veiligheid te beschermen.

Ten vijfde: de belangrijkste taken voor kunstmatige intelligentie.

Fundamenteel onderzoek moet voortdurend worden versterkt. De krachten moeten worden geconcentreerd om kerntechnologieën zoals geavanceerde chips en basissoftware te doorbreken en een autonoom beheersbaar, gecoördineerd functionerend systeem van basis-hardware en -software voor kunstmatige intelligentie op te bouwen. De diepe integratie van wetenschappelijke en technologische innovatie op het gebied van kunstmatige intelligentie met industriële innovatie moet worden bevorderd en nieuwe sporen voor de ontwikkeling van strategische opkomende industrieën en toekomstige industrieën moeten worden geopend.

Ten zesde: de praktische versterking door kunstmatige intelligentie.

De "AI+"-actie moet volledig worden uitgevoerd. Kunstmatige intelligentie moet een verandering in het paradigma van wetenschappelijk onderzoek leiden. De combinatie van kunstmatige intelligentie met industriële ontwikkeling, culturele opbouw, waarborging van het levensonderhoud van de bevolking en maatschappelijk bestuur moet worden versterkt. Men moet de dominante positie in de toepassingen van de AI-industrie veroveren en alle sectoren van industrie en maatschappij volledig met AI versterken.

Ten zevende: de ondersteuning en waarborgen voor kunstmatige intelligentie.

De aanleg van infrastructuur voor rekenkracht moet gecoördineerd worden bevorderd. De ontwikkeling en benutting van databronnen en het openstellen en delen ervan moeten worden verdiept, om de voordelen van China's omvang van data en marktomvang vrij te maken. Beleidsmaatregelen op het gebied van intellectueel eigendom, financiën en belastingen, overheidsaankopen en dergelijke moeten alomvattend worden ingezet. De waarborgen voor wetenschappelijk onderzoek en het beoordelingsmechanisme voor talent moeten worden verbeterd en hooggekwalificeerd talent moet worden opgeleid.

Ten achtste: internationale samenwerking op het gebied van kunstmatige intelligentie.

Kunstmatige intelligentie zou een internationaal publiek goed moeten zijn dat de gehele mensheid ten goede komt. Internationale samenwerking moet breed worden ontplooid, ontwikkelingslanden van het mondiale Zuiden moeten worden geholpen hun technologische capaciteitsopbouw te versterken en de mondiale intelligentiekloof moet worden gedicht. Alle partijen moeten worden bevorderd om de aansluiting en coördinatie van ontwikkelingsstrategieën, governance-regels en technische standaarden te versterken, teneinde zo spoedig mogelijk een mondiaal governancekader en standaardnormen met brede consensus te vormen.

De reeks belangrijke uiteenzettingen van secretaris-generaal Xi Jinping is strategisch vooruitziend, diepgaand van gedachte en rijk aan inhoud en biedt een fundamentele leidraad voor het verbeteren van de governance van kunstmatige intelligentie. Wij moeten de daarin vervatte kernbetekenis, geestelijke essentie en praktische vereisten diepgaand begrijpen en deze bewust doorvoeren in alle aspecten en het volledige proces van het verbeteren van de governance van kunstmatige intelligentie.

De risico's en uitdagingen die de ontwikkeling van kunstmatige intelligentie met zich meebrengt volledig onderkennen

Kunstmatige intelligentie is de kernmotor van de nieuwe ronde van wetenschappelijke en technologische revolutie en industriële verandering. Zij dringt momenteel met ongekende snelheid, breedte en diepte door in alle lagen van de menselijke samenleving en hervormt diepgaand de mondiale economische structuur, machtsverhoudingen, innovatieparadigma's en de logica van maatschappelijk bestuur.

Wij moeten zowel de kansen zien en het initiatief grijpen, als de risico's onderkennen en de ondergrens bewaken.

Ten eerste: een systematische invloed op de politieke veiligheidsomgeving.

Per juni 2026 bedroeg de omvang van de gebruikers van kunstmatige-intelligentieproducten in ons land meer dan 500 miljoen personen en overschreed het dagelijkse aantal token-aanroepen 140 biljoen. AI-toepassingen zijn snel en volledig uitgerold.

Allerlei vijandige krachten en personen met bijbedoelingen misbruiken generatieve AI-technologieën zoals deepfake-audio en -video, door AI gegenereerde tekst en afbeeldingen en "intelligente internetlegers" om tegen lage kosten en op grote schaal politieke geruchten te fabriceren, schadelijke informatie te verspreiden en tegenstellingen en vijandige emoties aan te wakkeren. Zij voeren tegen ons een publieke-opiniestrijd en cognitieve oorlog, hetgeen rechtstreeks onze politieke veiligheid, systeemveiligheid en ideologische veiligheid bedreigt.

Ten tweede: een ontwrichtende upgrade van de situatie op het gebied van cyberaanvallen en cyberverdediging.

Gesymboliseerd door de onlangs door Amerikaanse technologiebedrijven gelanceerde grote modellen "Mythos" (Claude Mythos) en "Cyber" (GPT-5.5-Cyber), verhoogt AI-technologie momenteel aanzienlijk de efficiëntie van het opsporen van kwetsbaarheden in netwerken, de efficiëntie van de ontwikkeling van kwaadaardige software en het niveau van bewapening.

Cyberaanvallen en cyberverdediging zijn een nieuwe fase binnengegaan van industriële productie van kwetsbaarheden, volledig geautomatiseerde aanval en verdediging en AI-tegen-AI. Sommige landen en organisaties beschikken over het vermogen om snel en in grote aantallen kwetsbaarheden

op te sporen, automatisch aanvalsroutes aan elkaar te koppelen en complexe hackertaken te voltooien. Dit verlaagt de technische drempel en de kosten voor het uitvoeren van cyberaanvallen aanzienlijk en brengt ernstige risico's en verborgen gevaren met zich mee voor de kritieke informatie-infrastructuur van ons land.

Ten derde: een grootschalige vergroting van het risico op diefstal en het uitlekken van geheimen.

Buitenlandse spionage- en inlichtingenorganen maken intensief gebruik van technologieën zoals intelligente webcrawlers, intelligente datamining en intelligente profielanalyse om op grote schaal belangrijke nationale gegevens, bedrijfsgeheimen, persoonlijke privacy van burgers en andere gevoelige informatie en gegevens te verzamelen en te verkrijgen.

Sommige binnenlandse gebruikers beschikken over onvoldoende veiligheidsbewustzijn en gebruiken buitenlandse AI-producten om gevoelige informatie te verwerken en gegevens naar het buitenland uit te voeren, waardoor op grote schaal gegevens uit het binnenland naar buiten lekken.

Ook open-source AI-agenttools zoals "Lobster" ("龙虾"), die in de eerste helft van 2026 sterk populair werden en buiten de oorspronkelijke kring bekendheid verwierven, kennen volgens de tekst structurele problemen, zoals het op afstand kunnen worden overgenomen van apparaatbeheermachtigingen en het lekken van gevoelige gebruikersinformatie.

Ten vierde: een monopolistische versterking van de onevenwichtige technologische ontwikkeling.

Bepaalde landen maken gebruik van hun opgebouwde voordelen op het gebied van fundamentele AI-theorie, modelarchitectuur en kernrekenkracht en gebruiken, onder het voorwendsel van "het handhaven van nationale veiligheid", middelen zoals het opstellen van entiteitenlijsten, het uitvoeren van technologische controles, het monopoliseren van industriestandaarden en het opbouwen van gesloten ecosystemen om relevante landen streng te beperken in het invoeren van geavanceerde technologische apparatuur en het verbeteren van hun vermogen tot wetenschappelijke en technologische innovatie.

Hierdoor worden de mondiale industriële en toeleveringsketens voor kunstmatige intelligentie uiteengereten en wordt de onevenwichtige ontwikkeling van de mondiale intelligente industrie versterkt.

Ten vijfde: een structurele schok voor het systeem van maatschappelijk bestuur.

De toepassing van kunstmatige intelligentie brengt grote hoeveelheden onzekere factoren met zich mee voor maatschappelijk bestuur en de openbare orde. Algoritmische "black boxes" en "datavergiftiging" kunnen bestaande maatschappelijke vooroordelen versterken.

Misbruik van persoonlijke informatie tijdens het gebruik van gegevens kan een vertrouwenscrisis onder gebruikers veroorzaken. Automatische besluitvorming door systemen veroorzaakt problemen met betrekking tot de toewijzing van verantwoordelijkheid.

In het bijzonder heeft de snelle ontwikkeling van kunstmatige intelligentie de traditionele kaders voor technologisch bestuur doorbroken, waardoor bestaande wettelijke normen, ethische beginselen en governance-mechanismen in de praktijk herhaaldelijk achterlopen en het moeilijk is effectieve institutionele beperkingen en toezichtsystemen te vormen.

Ten zesde: een fundamentele verandering in de vorm van militaire strijd.

AI-technologie stuwt de vorm van oorlogvoering momenteel het tijdperk van intelligentisering binnen. Wie via algoritmen een fijnmaziger waarneming, nauwkeuriger beoordeling en preciezere aanval kan realiseren, kan het initiatief op het slagveld in handen krijgen.

In het conflict tussen de Verenigde Staten, Israël en Iran heeft de militarisering van AI volgens de tekst geleid tot intelligente integratie van inlichtingen, intelligente ondersteuning van besluitvorming, intelligente doelidentificatie, intelligente ondersteuning van daadwerkelijke gevechtsoperaties en intelligente vormgeving van cognitie.

Kunstmatige intelligentie verandert volgens Chen daarmee van een "ondersteunende bijrol" op het slagveld in een "sleutelrol".

Belangrijkste maatregelen om de governance van kunstmatige intelligentie systematisch te bevorderen

Geconfronteerd met de complexe risico's en uitdagingen die voortkomen uit de snelle iteratieve ontwikkeling van AI-technologie moeten wij de reeks belangrijke uiteenzettingen van secretaris-generaal Xi Jinping als fundamentele leidraad nemen, de hervormingsmaatregelen uit het 15e Vijfjarenplan met betrekking tot de bevordering van de modernisering van het nationale veiligheidsstelsel en de nationale veiligheids capaciteit volledig uitvoeren, de governance capaciteit op het gebied van kunstmatige intelligentie versneld verbeteren en veiligheidsrisico's op het gebied van kunstmatige intelligentie effectief voorkomen en oplossen.

Ten eerste: vasthouden aan de alomvattende leiding van de Partij.

De Xi Jinping-Gedachte over het socialisme met Chinese kenmerken voor het nieuwe tijdperk moet diepgaand worden bestudeerd en uitgevoerd, in het bijzonder de belangrijke gedachte van secretaris-generaal Xi Jinping over het uitbouwen van China tot een sterke cybermacht.

Men moet vasthouden aan het beheer van het internet door de Partij en het beheer van data door de Partij, AI-governance opnemen in de algemene inrichting van de opbouw van een sterke cybermacht en een digitaal China, de top-level planning versterken, het governancekader verbeteren en de juiste richting vasthouden.

De voordelen van de leiding van de Partij moeten worden omgezet in governance-effectiviteit voor kunstmatige intelligentie en AI moet in een opwaartse, goede richting worden geleid, zodat zij stabiel en ver vooruit kan gaan.

Ten tweede: de gezamenlijke kracht van het systeem verhogen.

Het brede veiligheidsconcept moet stevig worden gevestigd. AI-veiligheid moet diepgaand worden geïntegreerd in het veiligheidswerk van andere belangrijke gebieden. De voordelen van China's nieuwe systeem voor het mobiliseren van nationale krachten moeten volledig worden benut.

Er moeten samenwerkingsmechanismen tussen verschillende gebieden en departementen worden opgezet en verbeterd. Het bijeenbrengen en delen van capaciteiten op het gebied van databronnen, platforminfrastructuur en dergelijke moet systematisch worden versterkt.

De mechanismen voor werkoverleg, gecoördineerde samenwerking, besluitvormingsadvies, risicobeoordeling en veiligheidsbeoordeling moeten voortdurend worden geoptimaliseerd. De verbetering van relevante rechtsstelsels, strategische systemen, beleidssystemen en risicopreventie- en controlesystemen moet gecoördineerd worden bevorderd, zodat een alomvattende kracht voor het handhaven van AI-veiligheid ontstaat.

Ten derde: risicoperceptie en vroegtijdige waarschuwing versterken.

Er moet een AI-veiligheidstoezichtplatform worden opgezet en verbeterd. Technische instrumenten voor evaluatie en beoordeling en dreigingsanalyse moeten voortdurend worden uitgebreid. Monitoring en vroegtijdige waarschuwing van veiligheidsrisico's moeten worden versterkt.

Onderzoek naar belangrijke kwesties zoals de ontwikkelingstendensen van AI moet worden verdiept. Potentiële risico's die door opkomende technologieën worden veroorzaakt moeten wetenschappelijk worden beoordeeld. Relevante patronen, ontwikkelingen en trends moeten nauwkeurig worden begrepen. Kwetsbaarheden en verborgen gevaren moeten tijdig worden gedicht.

Regelmatig moeten richtlijnen voor het voorkomen van veiligheidsrisico's worden gepubliceerd om sectorbedrijven, overheidsdepartementen en andere betrokken partijen begeleiding te bieden.

Ten vierde: wetenschappelijke en technologische innovatie intensiveren.

Onderzoek naar fundamentele principes op het gebied van kunstmatige intelligentie en naar sleuteltechnologieën zoals rekenkrachtchips, ontwikkelframeworks en toepassingssoftware moet worden versterkt.

De aanleg van nationale en lokale databronnenpools, het netwerk voor "Oostelijke data, westelijke rekenkracht" en andere AI-infrastructuur moet worden versneld.

Overheden, ondernemingen, wetenschappelijke onderzoeksinstituten en andere partijen moeten worden aangemoedigd en geleid om de samenwerking te versterken en gezamenlijk, via samenwerking tussen industrie, onderwijs en onderzoek, een ecosysteem voor kunstmatige intelligentie op te bouwen.

Er moet voor worden gezorgd dat sleuteltechnologieën zelfstandig beheersbaar zijn, dat de technologische soevereiniteit stevig in eigen handen wordt gehouden en dat innovatie en empowerment enerzijds en veiligheidsgovernance anderzijds in een gezonde wisselwerking en gecoördineerd naast elkaar vooruitgaan.

Ten vijfde: het systeem van juridische waarborgen verbeteren.

De Cybersecurity Law van de Volksrepubliek China en de Counter-Espionage Law van de Volksrepubliek China moeten volledig worden uitgevoerd. De invoering van specifieke wetten en voorschriften voor onderzoek en ontwikkeling, toepassing en toezicht op AI-technologie moet worden versneld.

Rond prominente problemen zoals algoritmische veiligheid, gegevensbescherming, ethische normen en privacyrechten moet een volledig regel- en standardsysteem voor toezicht worden opgebouwd dat de volledige keten bestrijkt van technologisch onderzoek en ontwikkeling, toepassing in de praktijk, risicopreventie en -beheersing tot het achteraf vaststellen van verantwoordelijkheid.

Het toezicht- en handhavingmechanisme moet worden verbeterd. De wettelijke verantwoordelijkheid van toezichthoudende sectoren, AI-ondernemingen en andere betrokken partijen moet worden vastgelegd en activiteiten die AI gebruiken voor het stelen van gegevens, het vervaardigen en verspreiden van schadelijke informatie en dergelijke illegale en criminele activiteiten moeten overeenkomstig de wet worden bestraft.

Ten zesde: de vormen van voorlichting en mobilisatie vernieuwen.

De belangrijke momenten van de Nationale Dag voor Onderwijs over Nationale Veiligheid op 15 april, de Nationale Cybersecurityweek en dergelijke moeten worden aangegrepen.

Via traditionele media en kanalen van nieuwe-mediaplatforms moet krachtig publiciteit worden gegeven aan de belangrijke uiteenzettingen van secretaris-generaal Xi Jinping over AI-governance. Beleidsvoorlichting, uitleg van wetten, analyse van gevallen en waarschuwingen voor risico's moeten grondig worden uitgevoerd.

Ook moeten de praktijken van bepaalde landen die technologische barrières opwerpen en AI gebruiken om tegen ons infiltratie en diefstal van geheimen uit te voeren krachtig aan de kaak worden gesteld en moet worden tegengegaan dat China wordt belastend en zwartgemaakt, onderdrukt en ingeperkt.

Ten zevende: de resultaten van internationale samenwerking verdiepen.

Uitgaande van een mondiale visie op veiligheidsgovernance gebaseerd op gezamenlijk overleg, gezamenlijke opbouw en gezamenlijk delen, moet internationale samenwerking op het gebied van wetenschappelijke en technologische innovatie worden verdiept.

Hegemonisme, technologische barrières en gesloten en uitsluitende praktijken moeten resoluut worden bestreden. Er moet een eerlijk en open internationaal systeem van AI-regels worden opgebouwd. Technologische uitwisseling en het open delen van resultaten moeten worden bevorderd. Inclusieve en evenwichtige ontwikkeling moet worden bevorderd en de digitale en intelligente kloof moet worden gedicht.

Kunstmatige intelligentie moet worden geleid om de bevolking en de wereld beter ten goede te komen.

Oorspronkelijke titel: 全面筑牢人工智能安全屏障 推动人工智能健康有序发展

Bron: 《中国网信》, nummer 8, 2026

Auteur: 陈一新 (Chen Yixin), partijsecretaris van het Ministerie van Staatsveiligheid en minister.