Vijeće
Europske unije

Bruxelles, 9. srpnja 2026.
(OR. en)

11711/26

CYBER 337
JAI 979
TELECOM 383
CSC 483
DATAPROTECT 234
RELEX 990
COSI 111
COPS 434

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	8. srpnja 2026.
Za:	Thérèse BLANCHET, glavna tajnica Vijeća Europske unije
Br. dok. Kom.:	COM(2026) 577 final
Predmet:	KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA Akcijski plan za kibernetičku sigurnost i umjetnu inteligenciju

Za delegacije se u prilogu nalazi dokument COM(2026) 577 final.

Priloženo: COM(2026) 577 final

EUROPSKA
KOMISIJA

Strasbourg, 7.7.2026.
COM(2026) 577 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA

Akcijski plan za kibernetičku sigurnost i umjetnu inteligenciju

1. Uvod

Pionirska umjetna inteligencija (UI) iz temelja mijenja kibernetičku sigurnost. Pionirski UI modeli (tj. najnapredniji UI modeli koji su dostupni ili su u razvoju) sve su sposobniji poboljšati pripravnost, otkrivanje prijetnji i odgovor na njih, što otvara **dosad neviđene mogućnosti za jačanje kibernetičke otpornosti**. Kako se te sposobnosti postupno budu povećavale[1], UI će timovima za kibernetičku sigurnost omogućiti da brže obavljaju znatno više zadaća, a organizacijama da učinkovitije odgovore na nove prijetnje. Osim toga, **napredne UI sposobnosti već su dostupne,** među ostalim zahvaljujući otvorenom kodu, **i mogu se koristiti za jačanje kibernetičke otpornosti EU-a**[2].

Umjetna inteligencija već je postala **jedno od glavnih obilježja prijetnji** te omogućuje automatiziranije, opsežnije i sofisticiranije kibernetičke napade, uključujući kibernetički kriminal[3]. Pionirske sposobnosti zasad ima tek malen broj UI modela i sustava (tj. modeli i sustavi koji mogu obavljati širok spektar zadaća i koji su trenutačno dosegnuli, gotovo dosegnuli ili premašili najvišu tehnološku razinu)[4]. Međutim, razlika u sposobnostima među modelima sve je manja jer se modeli otvorenog koda neprestano poboljšavaju. Zato će pionirske sposobnosti s vremenom vjerojatno postati dostupne sve širem krugu korisnika, pa tako i zlonamjernim akterima kao što su počinitelji kibernetičkog kriminala, koji bi ih mogli iskoristiti za složenije napade.

EU je spreman za taj novi svijet. Posljednjih godina uspostavio je pravne i operativne temelje za kibernetičku sigurnost u doba umjetne inteligencije. **UI akt** prvi je pravno obvezujući okvir u svijetu za upravljanje rizicima koji proizlaze iz UI sustava i modela. Obuhvaća i sistemske rizike najnaprednijih UI modela opće namjene, kao što je rizik od zloupotrebe u kibernetičkom prostoru[5]. **Aktom o kibernetičkoj otpornosti** (koji će se u cijelosti primjenjivati od kraja 2027.) štite se lanci opskrbe tako što se za softverske i hardverske proizvode na tržištu EU-a propisuju integrirana sigurnost i upravljanje ranjivostima tijekom životnog ciklusa[6]. UI akt i Akt o kibernetičkoj otpornosti zajedno doprinose sigurnom razvoju i održavanju UI modela i sustava te proizvoda s digitalnim elementima. Osim toga, **Direktiva NIS 2**[7], a za financijski sektor i **Akt o digitalnoj operativnoj otpornosti**[8], služe kao okvir za kibernetičku sigurnost kritičnih sektora koji se temelji na riziku. Ti zakonodavni akti čvrst su okvir koji, ako se učinkovito provodi, može odgovoriti i na tehnološki razvoj i na promjene prijetnji. **Akt o kibernetičkoj solidarnosti** dopunjuje taj okvir operativnim mehanizmima koji državama članicama pomažu da se pripreme na značajne i velike incidente te da ih otkriju i odgovore na

[1] Nedavno istraživanje Instituta Ujedinjene Kraljevine (AISI) za sigurnost umjetne inteligencije ukazuje na to da najnapredniji UI modeli u kontroliranim ispitivanjima kibernetičke sigurnosti bez ljudske pomoći uspijevaju izvršiti sve dugotrajnije zadatke. Procijenjeno trajanje izvršenih zadataka udvostručuje se svakih nekoliko mjeseci, a ne godina, dok najnoviji rezultati ukazuju na dodatno ubrzavanje tog trenda.

[2] *AI is changing the economics of vulnerability discovery. Defenders should adapt now*, CERT-EU, travanj 2026.

[3] ENISA, Izvješće ENISA-e o stanju kibernetičkih prijetnji za 2025., listopad 2025.

[4] Kako je definirano u članku 2. točki 4. predloženog Akta o razvoju računalstva u oblaku i umjetne inteligencije, COM(2026) 502 final.

[5] Uredba (EU) 2024/1689.

[6] Uredba (EU) 2024/2847.

[7] Direktiva (EU) 2022/2555, koja obuhvaća 11 sektora visoke kritičnosti (energetika, promet, bankarstvo, infrastruktura financijskog tržišta, zdravlje, voda za piće, otpadne vode, digitalna infrastruktura, upravljanje uslugama IKT-a, javna uprava i svemir) i sedam drugih kritičnih sektora (poštanske i kurirske usluge, gospodarenje otpadom, izrada, proizvodnja i distribucija kemikalija, proizvodnja, prerada i distribucija hrane, proizvodnja, pružatelji digitalnih usluga te istraživanje).

[8] Uredba (EU) 2022/2554.

njih[9]. Sve te mjere doprinose ciljevima **Strategije za Uniju pripravnosti**[10] i **strategije ProtectEU**[11].

Napredne kibernetičke sposobnosti koje omogućuje UI nužne su i za sigurnost Unije. Te sposobnosti već mogu znatno ojačati kibernetičku otpornost EU-a jer ih imaju razni modeli, uključujući otvorene modele. Međutim, pionirske sposobnosti uglavnom se razvijaju izvan EU-a, a o njihovoj dostupnosti često odlučuju strani akteri na netransparentan način. To znači da su znanje o tim sposobnostima i pristup njima važni za digitalnu otpornost, ali i za tehnološku suverenost Europe. Kako bi očuvao tu suverenost, EU se mora pobrinuti da uvođenje naprednih UI sposobnosti u području kibernetičke sigurnosti ne uzrokuje nove strateške ovisnosti. Osim toga, Europa mora ubrzati jačanje otpornosti kako bi držala korak s prijetnjama koje se ubrzano mijenjaju.

EU je već poduzeo **strateške korake za smanjenje ovisnosti o kritičnim tehnologijama i razvoj vlastitih kapaciteta**. U okviru programa Obzor Europa i Digitalna Europa već financira razvoj naprednih kibernetičkih sposobnosti koje omogućuje UI. Osim toga, Fond Europskog vijeća za inovacije postao je važan ulagač u duboku tehnologiju u Europi, među ostalim u *start-up* i *scale-up* poduzeća u području kibernetičke sigurnosti i UI tehnologija[12]. Nadalje, nedavno predloženim **Aktom o razvoju računalstva u oblaku i umjetne inteligencije**[13] povećali bi se kapaciteti podatkovnih centara u EU-u te njegova autonomija u području računalstva u oblaku i UI-ja. To bi olakšalo širu primjenu umjetne inteligencije, među ostalim u alatima i aplikacijama za kibernetičku sigurnost. Na taj bi se način EU mogao osloniti na vlastite ključne kapacitete u području računalstva u oblaku i umjetne inteligencije te smanjiti ovisnosti zbog kojih je izložen geopolitičkim i sigurnosnim rizicima. Prijedlog se temelji na **Strategiji za primjenu umjetne inteligencije** i **Akcijskom planu za kontinent umjetne inteligencije**, pri čemu se posebno uzima u obzir potreba za pokretanjem velikih pothvata koji će potaknuti razvoj i širu primjenu pionirske umjetne inteligencije.

Nakon što je postavio te čvrste temelje, **EU mora odlučnije odgovoriti na neposredna pitanja i iskoristiti mogućnosti koje UI donosi u kibernetičkoj sigurnosti**.

Ovaj akcijski plan **prva je ciljana mjera pomoći državama članicama i organizacijama u Uniji da se prilagode novoj stvarnosti**.

Prvo, kako bi se pionirska umjetna inteligencija primjenjivala sigurno i odgovorno, EU će ojačati kapacitete za njezinu evaluaciju prije stavljanja na raspolaganje, uključujući evaluaciju u području kibernetičke sigurnosti. Drugim riječima, uspostavit će rigorozan postupak vanjske evaluacije i vrhunske kapacitete za evaluaciju umjetne inteligencije. Osim toga, EU će europskim akterima olakšati pristup naprednim kibernetičkim sposobnostima koje omogućuje UI te podupirati testiranje dostupnih UI modela za primjene u kibernetičkoj sigurnosti.

Drugo, EU će učiniti više kako bi pomogao kritičnim sektorima i MSP-ovima da se pripreme za kibernetičke prijetnje koje omogućuje UI, među ostalim uspostavom temeljnih mjera kibernetičke sigurnosti. Pritom će se osloniti na sva dostupna UI rješenja i poticati njihovu primjenu radi povećanja kibernetičke otpornosti i uklanjanja najkritičnijih ranjivosti.

[9] Uredba (EU) 2025/38.
[10] JOIN(2025) 130 final.
[11] COM(2025) 148 final.
[12] Sifted, 20. ožujka 2026.: *Europe's most active deep tech investors in 2025*; Izvješće o učinku EIC-a za 2025.
[13] COM(2026) 502 final.

Treće, EU će ojačati europski ekosustav za razvoj i uvođenje rješenja koja se temelje na umjetnoj inteligenciji te nastaviti graditi vlastite kapacitete za razvoj pionirskih tehnologija. Za ostvarenje tog cilja bit će potrebna hitna i velika ulaganja u vlasnički kapital kako bi Europa izgradila vlastite kapacitete za pionirsku umjetnu inteligenciju i stvorila europska rješenja prilagođena vlastitim potrebama.

Naposljetku, EU će na ostvarivanju tih ciljeva surađivati s partnerima sličnih stavova kako bi potaknuo pouzdan i siguran globalni pristup pionirskoj umjetnoj inteligenciji i kibernetičkoj sigurnosti.

2. 1. stup: Sigurna, pristupačna i primjenjiva pionirska umjetna inteligencija u službi europske kibernetičke sigurnosti

Napredne kibernetičke sposobnosti koje omogućuje UI mogle bi se uskoro početi iskorištavati protiv naše kritične infrastrukture i društva. EU stoga prvenstveno mora što prije steći uvid u te sposobnosti, poboljšati tehničke kapacitete za procjenu rizika koje one donose, stvoriti uvjete za ispitivanje potencijala njihove primjene u kibernetičkoj sigurnosti te definirati jasnije načine na koje im se može pristupiti u legitimne kibernetičkosigurnosne svrhe u Europi. EU će s tim ciljem na temelju pravnog okvira uspostavljenog UI aktom proširiti europske kapacitete za evaluaciju modela prije njihova objavljivanja, potaknuti zajednički europski pristup pionirskoj umjetnoj inteligenciji i koordinirati testiranja kako bi se njezine mogućnosti u Europi mogle sigurno koristiti za potrebe kibernetičke sigurnosti.

2.1. Procjena i ublažavanje rizika pionirske umjetne inteligencije

UI aktom propisuju se zahtjevi za kibernetičku sigurnost **UI sustava**[14], a **od dobavljača najnaprednijih UI modela opće namjene zahtijeva se da procjenjuju i ublažavaju sistemske rizike**, među ostalim od zloupotrebe umjetne inteligencije u kibernetičkom području[15].

Komisija će od 2. kolovoza 2026. izvršavati nadzorne i provedbene ovlasti propisane UI aktom kako bi djelotvorno nadzirala UI sustave i UI modele opće namjene, uključujući modele koji predstavljaju sistemske rizike povezane s kibernetičkom sigurnošću[16]. U okviru tog nadzora procjenjivat će kako su dobavljači utvrdili rizike povezane sa sposobnostima modela i mjere koje su uveli kako bi ih ublažili. Zahtjevi će pritom ostati razmjerni sposobnostima predmetne tehnologije.

U izvršavanju nadzornih i provedbenih ovlasti Komisiji će pomoći **znanstveno povjerenstvo koje savjetuje njezin Ured za umjetnu inteligenciju**, **sigurni kanali za prijavljivanje** i **Kodeks dobre prakse za umjetnu inteligenciju opće namjene.**

[14] Na temelju Priloga III. UI aktu UI sustavi koji se koriste u kritičnoj infrastrukturi smatrat će se visokorizičnima i podlijegati posebnim odredbama, među ostalim onima o kibernetičkoj sigurnosti.

[15] Sistemski rizici definirani su UI aktom kao rizici specifični za sposobnosti visokog učinka UI modelâ opće namjene, koji imaju znatan utjecaj na tržište Unije zbog svojeg dosega ili zbog stvarnih ili razumno predvidljivih negativnih učinaka na javno zdravlje, sigurnost, javnu sigurnost, temeljna prava ili društvo u cjelini, a koji se mogu proširiti po cijelom vrijednosnom lancu (članak 3. točka 65.).

[16] Ako dobavljači UI modela opće namjene sa sistemskim rizikom ne poštuju odredbe o ublažavanju sistemskih rizika, Komisija na temelju svojih provedbenih ovlasti može zatražiti informacije o modelu ili pristup modelu radi evaluacije, naložiti mjere za ublažavanje rizika, a u krajnjem slučaju i izreći novčanu kaznu u iznosu do 3 % globalnog godišnjeg prometa ili od dobavljača zatražiti da ograniči stavljanje modela na raspolaganje na tržištu ili pak da ga povuče ili opozove.

2.2. Postizanje europske izvrsnosti u evaluaciji pionirske umjetne inteligencije prije stavljanja na raspolaganje

Kako bi se UI u područje kibernetičke sigurnosti u EU-u uveo sigurno i odgovorno, regulatorne mjere moraju se dopuniti **povećanim europskim kapacitetima za evaluaciju**. S razvojem UI sposobnosti i širenjem sistemskih rizika izvan kibernetičkog područja[17] vanjske evaluacije u praksi se pokazuju kao najbolji način da se zajamči sigurnost pionirske umjetne inteligencije u skladu s pristupima uspostavljenima u drugim industrijama izloženima riziku. U UI aktu ističe se i **važnost evaluacije prije uvođenja** koju provode treće strane kako bi se sistemski rizici prema potrebi procijenili i ublažili. Većina vodećih subjekata koji kao neovisne treće strane evaluiraju UI modele prije uvođenja zasad su poduzeća izvan EU-a. Budući da su te evaluacije sve važnije, dio potrebnog stručnog znanja i infrastrukture hitno treba uspostaviti u EU-u.

U skladu s tim EU treba proširiti bazu stručnog znanja kako bi stvorio pouzdan i konkurentan ekosustav vanjskih evaluatora naprednih UI sposobnosti i mjera ublažavanja rizika, što bi povećalo povjerenje u okvir EU-a za upravljanje umjetnom inteligencijom. Komisija će s tim ciljem predložiti **kriterije za vanjske evaluatore za potrebe Kodeksa dobre prakse za UI opće namjene i poticati razvoj šireg ekosustava evaluacija.** Pritom će, među ostalim, olakšavati sadržajnu razmjenu znanja među evaluatorima i relevantnim stručnjacima kako bi se unaprijedile metodologije za evaluaciju i pojasnili zahtjevi u pogledu kvalifikacija.

Vrhunski europski stručnjaci za kibernetičku sigurnost mogu Europi omogućiti da postane predvodnica u području **evaluacije UI modela, posebno za potrebe kibernetičke sigurnosti**. Zbog hitnosti situacije EU bi to stručno znanje trebao iskoristiti i ojačati, stoga će Komisija objaviti namjenski poziv za **uspostavu kapaciteta EU-a za evaluaciju UI modela koji mora obuhvaćati kibernetičku sigurnost.** Takav bi kapacitet uvelike potaknuo razvoj novog ekosustava u EU-u na temelju stručnog znanja i iskustva država članica o evaluaciji umjetne inteligencije. Doprinio bi i regulatornim aktivnostima koje Komisija provodi putem Ureda za umjetnu inteligenciju[18] jer bi omogućio da UI modele i mjere za ublažavanje rizika neovisno evaluiraju i europski subjekti. Budući da bi omogućio neovisnu evaluaciju sposobnosti modelâ i djelotvornosti mjera koje dobavljači modela provode kako bi ublažili rizike, pomogao bi im da upravljaju rizicima[19].

Taj europski kapacitet pomoći će dobavljačima UI modela opće namjene da ispune relevantne obveze iz UI akta i pridržavaju se Kodeksa dobre prakse za UI opće namjene[20]. S tim ciljem uspostavit će se pouzdan i rigorozan postupak vanjske evaluacije. Vrhunske sposobnosti evaluacije u EU-u doprinijet će i boljem razumijevanju potencijalnih sistemskih rizika u kibernetičkoj sigurnosti, biotehnologiji i drugim područjima te omogućiti rana upozorenja kad se utvrde rizici.

[17] Na primjer, biologija je jedno od područja u kojem se sposobnosti UI modela opće namjene kontinuirano razvijaju, a njihova bi zloupotreba mogla ugroziti javno zdravlje i javnu sigurnost.

[18] U poglavlju o sigurnosti i zaštiti Kodeksa dobre prakse za UI opće namjene od dobavljača se zahtijeva da evaluacije modela povjere i neovisnim vanjskim evaluatorima s odgovarajućim kvalifikacijama (Dodatak 3.5.). Ta će izvješća zatim poslužiti u regulatornim aktivnostima Ureda za umjetnu inteligenciju, kojem su dobavljači uz izvješće o modelu obvezni dostaviti i sva dostupna izvješća vanjskih evaluacija (mjera 7.4.).

[19] Evaluacije u okviru tog kapaciteta razlikovat će se od onih na platformi za testiranje iz odjeljka 2.4. Naime, platforma će se prvenstveno koristiti za testiranje primjene UI modela u kibernetičkoj sigurnosti, a u okviru kapaciteta procjenjivat će se i ublažavati sistemski rizici radi usklađenosti s Kodeksom dobre prakse.

[20] Taj kapacitet neće imati ulogu tijela za ocjenjivanje sukladnosti, već će svojim evaluacijama samo podupirati usklađenost.

2.3. Lakši pristup naprednim kibernetičkim sposobnostima koje omogućuje UI u EU-u

O pristupu pionirskoj umjetnoj inteligenciji s naprednim kibernetičkim sposobnostima sve češće samostalno odlučuju dobavljači, često izvan Europe. Neki od njih pritom radi upravljanja rizicima od zloupotrebe ograničavaju pristup primjenom **programa strukturiranog pristupa** (npr. postupno objavljivanje modela). Takva ograničenja mogu biti opravdana iz sigurnosnih razloga, no kriteriji koji se primjenjuju kako bi se utvrdilo koje će organizacije, uključujući poduzeća, dobiti pristup i način na koji se taj pristup odobrava često nisu transparentni. Zbog toga europski akteri, uključujući nadležna tijela i operatere kritične infrastrukture, možda neće moći pravodobno iskoristiti te UI sposobnosti da povećaju svoju otpornost.

Hitno je potreban koordiniran pristup na razini EU-a kako bi se relevantnim **europskim javnim i privatnim akterima** omogućio siguran i pravodoban pristup takvoj pionirskoj umjetnoj inteligenciji. EU će u tu svrhu poticati razvoj najsuvremenijeg postupka koji se temelji na riziku, ima jasne kriterije i uključuje djelotvorne mjere zaštite od zloupotrebe.

Komisija će u suradnji s Agencijom Europske unije za kibernetičku sigurnost (ENISA) razviti **Europski plan za strukturirani pristup naprednim UI sposobnostima za potrebe kibernetičke sigurnosti**. U tim smjernicama objasnit će se kako dobavljači UI rješenja s naprednim kibernetičkim sposobnostima mogu odobriti pristup europskim organizacijama, uključujući poduzeća, i tako im pomoći u ublažavanju kibernetičkih rizika.

Taj će dokument sadržavati **kriterije koje bi trebalo razmotriti** pri odobravanju pristupa UI rješenjima s naprednim kibernetičkim mogućnostima europskim akterima. Plan bi trebao obuhvaćati kriterije prilagođene različitim vrstama organizacija (npr. institucije EU-a, tijela država članica, operateri kritične infrastrukture, pružatelji kibernetičke sigurnosti i akteri u istraživanjima) te uključivati opis načina na koji bi te aktere trebalo utvrditi. Trebao bi sadržavati i sigurnosne kriterije kako pristup koji se na temelju njega odobri ne bi stvarao neopravdan rizik, kao i **mehanizam kojim bi se pojednostavnilo davanje pristupa** subjektima koji zadovoljavaju kriterije. Taj bi mehanizam ujedno trebao dobavljačima olakšati rano **informiranje** o planiranim programima pouzdanog pristupa te omogućiti razmjenu znanja među organizacijama EU-a kojima je odobren pristup određenom modelu ili sustavu.

Premda plan **dobavljačima neće nametnuti nove obveze**, bit će u skladu s ciljevima Kodeksa dobre prakse za umjetnu inteligenciju opće namjene jer će se u njemu utvrditi moguće sigurnosne mjere za ublažavanje rizika koje mogu dopuniti **upravljanje sistemskim rizicima** koje trebaju uvesti dobavljači UI modela opće namjene sa sistemskim rizikom[21][22]. Budući da će služiti kao **europski referentni okvir**, na njemu će se temeljiti daljnja međunarodna suradnja.

Plan bi trebao sadržavati i **izvanredne mjere u slučaju ograničenja ili ukidanja pristupa umjetnoj inteligenciji s naprednim kibernetičkim sposobnostima** kako bi se utvrdilo što EU treba učiniti ako dobavljač ili tijelo treće zemlje ograniči ili ukine pristup relevantnom modelu ili sustavu. Osim toga, kad je za opću upotrebu potreban pravodoban pristup pionirskoj umjetnoj inteligenciji, Komisija će u suradnji s državama članicama razmotriti mogućnost korištenja dostupnih instrumenata financiranja, uključujući zajedničku nabavu, kako bi se **zajednički ostvario pristup takvim modelima ili sustavima**.

[21] U skladu s člankom 55. stavkom 1. točkom (b) UI akta.

[22] Npr. u poglavlju o sigurnosti i zaštiti Kodeksa dobre prakse za umjetnu inteligenciju opće namjene kao primjer sigurnosne mjere za ublažavanje rizika u okviru mjere 5.1. spominje se „postupno odobravanje pristupa modelu”.

2.4. Testiranje umjetne inteligencije s naprednim kibernetičkim sposobnostima radi pravodobnog i sigurnog uvođenja u područje kibernetičke sigurnosti

Pristup sigurnoj i pouzdanoj pionirskoj umjetnoj inteligenciji mora biti popraćen testiranjem njezinih sposobnosti za upotrebu u operacijama kibernetičke sigurnosti, kao što su skeniranje ranjivosti, otklanjanje ranjivosti i odgovor na incidente. Kako bi se iskoristile njezine prednosti, operateri kritične infrastrukture i javna tijela prije uvođenja u osjetljiva okruženja moraju brzo utvrditi kako UI s naprednim kibernetičkim sposobnostima funkcionira u realnim uvjetima kibernetičke sigurnosti. Takva testiranja trebalo bi provoditi u **sigurnim i kontroliranim okruženjima**.

Kako bi se stvorile sinergije na europskoj razini, **ENISA** i **Zajednički istraživački centar Europske komisije (JRC)** u suradnji s drugim relevantnim službama Komisije i subjektima Unije, kao što su CERT-EU, Europol i sektorska tijela, te državama članicama uspostavit će **sigurnu platformu za testiranje primjene umjetne inteligencije u kibernetičkoj sigurnosti[23].** Sudionici će na platformi moći koristiti vlastite pristupne ključeve za modele na temelju zajedničkih pravila o sigurnosti i povjerljivosti, pri čemu će svaki sudionik snositi vlastite troškove, koristiti vlastite alate i odgovarati za svoje metode testiranja. ENISA bi u suradnji s JRC-om trebala upravljati pristupom platformi za testiranje i agregirati rezultate.

Na toj će se sigurnoj europskoj platformi moći i **testirati uvođenje kibernetičkih sposobnosti napredne umjetne inteligencije u sustave kritične infrastrukture** bez izlaganja stvarne infrastrukture riziku („**kibernetički poligoni**"[24]). Prednost će se dati **prilagodbi i proširenju postojećih kibernetičkih poligona** umjesto dupliciranja okruženja. Naime, novi kibernetički poligoni razvijat će se samo u sektorima u kojima takvih kapaciteta zasad nema, a poduzeća iz različitih sektora mogla bi poduprijeti tu inicijativu tako da preuzmu namjenske obveze u skladu s kojima bi postojeća okruženja stavila na raspolaganje za integraciju s platformom. Akteri iz industrije koji odluče sudjelovati mogli bi primati agregirane informacije dobivene relevantnim aktivnostima testiranja u skladu s primjenjivim pravilima o povjerljivosti.

To će okruženje služiti prvenstveno za testiranje umjetne inteligencije radi povećanja kibernetičke otpornosti, a ne za ocjenjivanje usklađenosti UI modela opće namjene s UI aktom[25]. Tako će se brže stjecati praktično iskustvo u primjeni umjetne inteligencije za kibernetičku otpornost, uključujući otkrivanje i trijažu prijetnji, obradu obavještajnih podataka o prijetnjama i odgovor na njih, kako bi se preduhitrili napadači. Kako bi zajamčila visoku razinu kibernetičke sigurnosti u cijeloj Uniji, **ENISA** će na temelju svojih saznanja objavljivati i ažurirati **smjernice i savjete o sigurnoj upotrebi dostupnih UI modela i sustava** za širi ekosustav.

Ključne aktivnosti:

- **1. ključna aktivnost – <u>Komisija</u> će poduprijeti uspostavu kapaciteta EU-a za evaluaciju UI modelâ koji mora obuhvaćati kibernetičku sigurnost (2027.).**

[23] Postojeća platforma kojom upravlja JRC mogla bi se nadograditi kako bi se na njoj mogla provoditi ta vrsta testiranja.

[24] Kibernetički poligoni su sigurna i kontrolirana okruženja koja simuliraju digitalne sustave, mreže ili infrastrukturu. Omogućuju testiranje u realnim uvjetima, a aktivnosti koje se u njima provode ne utječu na stvarne sustave ili usluge.

[25] Testiranjem umjetne inteligencije za potrebe kibernetičke otpornosti nastoji se utvrditi je li UI model ili sustav operativno prikladan za određeni zadatak kibernetičke sigurnosti. S druge strane, evaluacijom UI modela radi usklađivanja s UI aktom nastoje se procijeniti rizici koji proizlaze iz modela i djelotvornost mjera kojima ih je njegov dobavljač ublažio. Stoga se testiranje umjetne inteligencije za potrebe kibernetičke otpornosti razlikuje od evaluacije UI modela radi usklađivanja s UI aktom te zahtijeva drukčije vještine i resurse.

- **2. ključna aktivnost – <u>Komisija će u suradnji s ENISA-om</u> osmisliti Europski plan za strukturirani pristup naprednim UI sposobnostima za potrebe kibernetičke sigurnosti kako bi im europske organizacije mogle sigurno i pravodobno pristupiti (četvrto tromjesečje 2026.).**
- **3. ključna aktivnost – <u>ENISA i Zajednički istraživački centar Europske komisije (JRC)</u> razvit će sigurnu platformu za testiranje umjetne inteligencije s naprednim kibernetičkim sposobnostima za primjene u kibernetičkoj sigurnosti kako bi se potaknulo pravodobno i sigurno uvođenje UI rješenja u kibernetičku sigurnost (četvrto tromjesečje 2026.).**

3. 2. stup: Priprema kibernetičkog ekosustava EU-a za doba umjetne inteligencije

Budući da napredne UI kibernetičke sposobnosti postaju sve dostupnije i raširenije, EU mora biti spreman spriječiti njihovu moguću zloupotrebu protiv svojeg gospodarstva i društva, ali i sposoban sigurno ih koristiti za kibernetičku otpornost. Umjetna inteligencija može uvelike automatizirati otkrivanje ranjivosti i provoditi ga u znatno većem opsegu, no zahvaljujući njoj zlonamjernim akterima potrebno je sve manje stručnog znanja, vremena i resursa za sofisticirane napade. Prvi je i najhitniji zadatak EU-a ojačati vlastitu pripravnost i pomoći kritičnim sektorima da se prilagode tim prijetnjama. To znači da u operacije kibernetičke sigurnosti treba uključiti dostupna UI rješenja, uključujući sve dostupne UI modele, a posebno one otvorenog koda, te ubrzati utvrđivanje i otklanjanje najkritičnijih ranjivosti. ENISA ima jedinstvene preduvjete da europskom ekosustavu kibernetičke sigurnosti pomogne da zakorači u doba umjetne inteligencije.

3.1. Primjena temeljnih mjera kibernetičke sigurnosti EU-a i jačanje pripravnosti

U novom tehnološkom i sigurnosnom okruženju **temeljne mjere kibernetičke sigurnosti i pripravnost važnije su nego ikad prije** pa postojeće alate i instrumente EU-a za kibernetičku sigurnost treba iskoristiti u punoj mjeri.

Regulatorni okvir EU-a za kibernetičku sigurnost, prije svega **Direktiva NIS 2[26] i Akt o digitalnoj operativnoj otpornosti (DORA)**, čvrst je temelj za pripremu kritične infrastrukture na sve vrste rizika u pogledu kibernetičke sigurnosti, uključujući UI rizike. Stoga države članice moraju hitno prenijeti i provesti ta pravila, a u svojim nadzornim aktivnostima moraju uzeti u obzir rizike koje donosi napredni UI. Operateri u kritičnim sektorima i financijski subjekti također bi svoje okvire za upravljanje rizicima trebali preispitati i prilagoditi novoj stvarnosti i računati s češćim i opsežnijim kibernetičkim napadima koje omogućuje UI. Osim toga, trebali bi skratiti vrijeme potrebno za primjenu zakrpa, što podrazumijeva njihovo češće uvođenje i brzo uvođenje u složene sustave.

Kako bi dodatno ojačali pripravnost, subjekti bi trebali dosljedno provoditi **osnovne mjere kibernetičke higijene** te povećati sigurnost mreže i sustava (među ostalim primjenom pristupâ nultog povjerenja kad je to potrebno). Osim toga, trebali bi početi **koristiti već dostupne UI sposobnosti,** uključujući sposobnosti modela otvorenog koda, kako bi otkrili ranjivosti te poboljšali otkrivanje i sprečavanje kibernetičkih napada. Uz potporu CERT-EU-a i smjernica Međuinstitucijskog odbora za kibernetičku sigurnost (IICB) **subjekti Unije** u tome mogu

[26] Direktivom NIS 2 uspostavljeni su temelji za upravljanje rizicima u području kibernetičke sigurnosti s obzirom na to da se od ključnih i važnih subjekata u 18 kritičnih sektora zahtijeva da zaštite svoje mrežne i informacijske sustave te spriječe incidente i njihov učinak svedu na najmanju moguću mjeru.

predvoditi vlastitim primjerom i ojačati opću razinu kibernetičke sigurnosti Unije u skladu s Uredbom o kibernetičkoj sigurnosti subjekata Unije[27]. Osim toga, države članice uvelike se potiču da u potpunosti iskoriste mogućnosti pretvaranja usluga **pričuve EU-a za kibernetičku sigurnost** u usluge pripravnosti kako bi ojačale otpornost na kibernetičke prijetnje koje omogućuje UI, među ostalim skeniranjem ranjivosti, automatiziranim penetracijskim testiranjem i praćenjem rizika uz preporuke za primjenu zakrpa.

Nadalje, kako je navedeno u **Aktu o kibernetičkoj otpornosti**, koji će se u potpunosti primjenjivati od 11. prosinca 2027., i dalje su ključne razvojne prakse u skladu s načelom integrirane sigurnosti, sustavno upravljanje ranjivostima, pravodobne zakrpe i prakse sigurnog kodiranja, uključujući pristupe kojima se otklanjaju cijele kategorije ranjivosti, kao što je razvoj memorijski sigurnog softvera. Rizike za kibernetičku sigurnost specifične za UI, uključujući trovanje podataka i modela, neprijateljske napade i umetanje zlonamjernih uputa, također je potrebno pažljivo procijeniti i ublažiti u skladu s relevantnim odredbama UI akta.

Kako bi u tome pomogla, **ENISA** će u suradnji s europskim nadzornim tijelima i drugim relevantnim subjektima Unije objaviti i ažurirati **odgovarajuće smjernice, preporuke, savjete i primjere dobre prakse za zaštitu od prijetnji koje omogućuje UI[28] i sigurnu integraciju UI alata u kibernetičkosigurnosne operacije**. U takvim smjernicama i savjetima trebalo bi uzeti u obzir i potrebe MSP-ova, koji su najosjetljiviji na napade. Ta bi se nastojanja prema potrebi mogla ojačati i obogatiti sektorskim inicijativama i mehanizmima suradnje u područjima kao što su financije, promet, energetika, poljoprivredno-prehrambeni sektor, zdravstvo[29] i svemir.

Budući da će se tehnologije i povezani rizici nastaviti razvijati, za poboljšanje informiranosti o stanju bit će ključne aktivnosti relevantnih mreža Unije na horizontalnoj i sektorskoj razini koje omogućuju **zajedničko praćenje stanja i strukturiranu razmjenu informacija o prijetnjama kibernetičkoj sigurnosti koje omogućuje UI**. ENISA bi trebala razmotriti načine na koje može pomoći u suradnji s dobavljačima UI rješenja radi bolje razmjene obavještajnih podataka o prijetnjama.

Slično tomu, države članice trebale bi iskoristiti postojeće strukture na razini Unije u području kibernetičke sigurnosti kako bi **procijenile pripravnost kritične infrastrukture**. Pritom bi trebale surađivati ponajprije u okviru Skupine za suradnju NIS, a prema potrebi i s Odborom za umjetnu inteligenciju osnovanim na temelju UI akta.

3.2. Ubrzavanje primjene zakrpa: modernizacija upravljanja ranjivostima u doba otkrivanja ubrzanog umjetnom inteligencijom

Kako bi se pobrinuo za svoju kibernetičku sigurnost, EU prioritetno mora **otkloniti postojeće ranjivosti prije nego što se počnu masovno iskorištavati**. Budući da UI skraćuje vrijeme koje je zlonamjernim akterima potrebno da iskoriste ranjivosti, relevantni subjekti također moraju ubrzati svoju analizu i utvrđivanje prioriteta ranjivosti te ih otklanjati i uvoditi ispravke dovoljno brzo da spriječe njihovo iskorištavanje.

Postojeća postupanja s ranjivostima moraju se modernizirati kako bi ostala djelotvorna u doba otkrivanja ranjivosti uz pomoć umjetne inteligencije. ENISA bi se trebala pobrinuti

[27] Uredba (EU, Euratom) 2023/2841.

[28] Primjer takvih savjeta je objava na blogu CERT-EU-a: UI mijenja ekonomiku otkrivanja ranjivosti. Stručnjaci za kibernetičku sigurnost trebali bi se odmah prilagoditi, 21. travnja 2026.

[29] Europski akcijski plan za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite: COM(2025) 10 final.

da europska infrastruktura i usluge za upravljanje ranjivostima, uključujući Europsku bazu podataka o ranjivostima (EUVD) i jedinstvenu platformu za izvješćivanje u okviru akta CRA, odgovaraju potrebama doba u kojem UI pomaže u otkrivanju ranjivosti. Zajedno s državama članicama trebala bi povećati interoperabilnost platformi i baza podataka o ranjivostima na razini EU-a te nacionalnoj i globalnoj razini.

Budući da se broj prijavljenih ranjivosti povećava, proizvođači moraju odlučiti koje će nedostatke u linijama proizvoda najprije ispraviti, dok korisnici, posebno ključni i kritični važni subjekti, moraju odlučiti koja će ažuriranja prva uvesti, često uz ograničene resurse. Organizacije se moraju moći osloniti na jasne smjernice na razini EU-a utemeljene na riziku te usklađene s Aktom o kibernetičkoj otpornosti i Direktivom NIS 2 kako bi zakrpe primjenjivale ondje gdje su rizici najveći.

U okviru obveza na temelju Direktive NIS 2 **države članice trebale bi ažurirati i nacionalne politike koordiniranog otkrivanja ranjivosti (CVD)** kako bi obuhvatile iskorištavanje ranjivosti uz pomoć umjetne inteligencije. Skupina za suradnju NIS trebala bi revidirati svoje smjernice o provedbi CVD-a, a EU preispitati jesu li norme ISO/IEC na kojima se temelje okviri za CVD i dalje svrsishodne s obzirom na današnje prijetnje. Budući da se te prakse oblikuju na svjetskoj razini, neophodna je i međunarodna suradnja.

Naposljetku, zaštita kritične infrastrukture ne završava objavljivanjem utvrđenih ranjivosti ili objavljivanjem ispravaka. Veći je izazov **te ispravke doista i primijeniti**. Kako UI ubrzava otkrivanje ranjivosti, problemi sa zastojima u primjeni zakrpa postaju sve izraženiji. Države članice trebale bi uz potporu ENISA-e iskoristiti postojeće mreže, kao što je Skupina za suradnju NIS, kako bi riješile taj iznimno hitan problem.

3.3. Primjena u praksi: uklanjanje najvažnijih ranjivosti

Znanje koje stekne o tome kako UI može ojačati kibernetičku otpornost EU mora **primijeniti tamo gdje je to hitno potrebno**. Drugim riječima, brži pronalazak ranjivosti sâm po sebi nije dovoljan, već ih je potrebno i analizirati, ukloniti te koordinirati uvođenje ispravaka u velikom opsegu. **Mjere su najprije potrebne u području ključnog softvera otvorenog koda**, koji je iznimno raširen u sektorima s kritičnom infrastrukturom. Izvješća pokazuju da je otvoreni kod prisutan u 98 % ukupne kodne baze, pri čemu u prosjeku 80 % kodnih baza industrija s kritičnom infrastrukturom ima ranjivost visokog ili kritičnog rizika[30].

Strategija EU-a za otvoreni kod[31], objavljena u okviru Paketa za tehnološku suverenost, obuhvaća niz mjera za povećanje sigurnosti kritičnih komponenata otvorenog koda i potporu njihovu održavanju. Komisija će u tom kontekstu s ENISA-om, državama članicama[32] i zajednicama otvorenog koda pokrenuti provedbu pilot-mjera posebno usmjerenih na kibernetičku sigurnost i UI.

ENISA će u suradnji s Komisijom, državama članicama i zajednicama otvorenog koda ubrzati mapiranje kritičnih komponenata otvorenog koda predviđeno tom strategijom. Na temelju preliminarnog popisa sastavljenog u skladu s dogovorenim kriterijima pokrenut će **pilot-projekt Kampanje za otpornost kritičnog otvorenog koda** za komponente otvorenog koda relevantne za kritičnu infrastrukturu. Provedba instrumenta za održavanje otvorenog koda

[30] Blackduck, 2026. *Open Source Security and Risk Analysis Report*: npr. 87 % u zrakoplovno-svemirskoj industriji, zrakoplovstvu, automobilskoj industriji, prometu i logistici, 88 % u prerađivačkoj industriji, 88 % u zdravstvu, 89 % u energetici te 80 % u internetskoj i softverskoj infrastrukturi.

[31] COM(2026) 503 final.

[32] Prema potrebi posebno u koordinaciji s Konzorcijem za europsku digitalnu infrastrukturu za zajednička digitalna dobra (DC-EDIC).

temeljit će se na rezultatima te kampanje. Kampanja će se provoditi kao dobrovoljni program sponzorstva u okviru kojeg će se projekti otvorenog koda povezati s organizacijama koje su voljne blisko surađivati s održavateljima projekata kako bi im pomogle u održavanju i zaštiti. Sponzori mogu biti države članice, subjekti Unije (npr. CERT-EU), operateri kritične infrastrukture, proizvođači i drugi javni ili privatni subjekti koji mogu pomoći, primjerice tako što će održavateljima projekata otvorenog koda staviti na raspolaganje kvalificirano osoblje ili UI modele i alate. Države članice i drugi prihvatljivi korisnici mogu zatražiti pomoć privatnih pouzdanih dobavljača iz **pričuve EU-a za kibernetičku sigurnost** u skeniranju ranjivosti povezanih s ovisnostima o komponentama otvorenog koda u kritičnoj infrastrukturi. Osim toga, ENISA će izraditi **katalog UI usluga** za potporu primjeni zakrpa i uklanjanju ranjivosti otvorenog koda.

Program sponzorstva i katalog usluga održavateljima otvorenog koda omogućit će brži i djelotvorniji rad na smanjenju kibernetičkih rizika, koji se sve češće javljaju zbog razvoja UI modela. Inicijativa će ojačati postojeće upravljanje otvorenim kodom i povezane radne postupke te omogućiti testiranje šireg europskog pristupa uklanjanju ranjivosti uz pomoć umjetne inteligencije, čime će se dodatno poboljšati operativno znanje Unije. Rezultirat će povećanjem kibernetičke otpornosti u svim sektorima, uključujući kritičnu infrastrukturu i MSP-ove. Prva pilot-kampanja pokrenut će se 2026. Ako se pokaže uspješnom, njezin će se opseg proširiti, među ostalim u kontekstu Strategije za otvoreni kod.

Ključne aktivnosti:

- **4. ključna aktivnost – <u>ENISA će u suradnji s relevantnim subjektima Unije</u> izdavati smjernice, preporuke, savjete i primjere dobre prakse za zaštitu od prijetnji koje omogućuje UI i sigurnu integraciju umjetne inteligencije u operacije kibernetičke sigurnosti (od trećeg tromjesečja 2026.).**
- **5. ključna aktivnost – <u>Komisija, države članice, ENISA i industrija</u> surađivat će na prilagodbi postojećih praksi i alata za upravljanje ranjivostima potrebama doba umjetne inteligencije (od trećeg tromjesečja 2026.).**
- **6. ključna aktivnost – <u>ENISA će u suradnji s Komisijom, državama članicama, zajednicama otvorenog koda, subjektima Unije i industrijom</u> pokrenuti prvi pilot-projekt Kampanje za otpornost kritičnog otvorenog koda kako bi se ubrzala primjena zakrpa, među ostalim uz pomoć umjetne inteligencije (četvrto tromjesečje 2026.).**

4. 3. stup: Jačanje europskih UI kapaciteta u području kibernetičke sigurnosti

Budući da se u obrambenim i napadačkim kibernetičkim operacijama sve više koristi napredna umjetna inteligencija, sposobnost razvoja i uvođenja UI rješenja za kibernetičku sigurnost postaje strateški pokretač kibernetičke otpornosti i suvereniteta. EU se posebno u osjetljivim primjenama mora moći osloniti na suverene UI kapacitete koji zadovoljavaju nužne sigurnosne zahtjeve, među ostalim u području obrane. To znači da europskim dobavljačima, uključujući disruptivne inovatore, sad mora omogućiti da takvu naprednu umjetnu inteligenciju razviju, uvedu i skaliraju u Europi. Uz ulaganja u kibernetičku sigurnost i umjetnu inteligenciju EU mora uposliti svoj cjelokupni tehnološki ekosustav kako bi se zadovoljile najhitnije operativne potrebe u području kibernetičke sigurnosti, potaknula ulaganja u razvoj i primjenu sve naprednijih europskih UI sposobnosti te razvile vještine potrebne za njihovo uvođenje u svim sektorima.

4.1. Jačanje europskog ekosustava UI rješenja za kibernetičku sigurnost

Budući da se UI već koristi u zlonamjerne svrhe, organizacije moraju preduhitriti napadače i uvesti dostupna UI rješenja za kibernetičku sigurnost kako bi se zaštitila kritična infrastruktura u svim sektorima. EU mora potaknuti europsko tržište da takve alate stavi na raspolaganje dovoljno brzo i u potrebnim razmjerima te ubrzati njihovu primjenu u europskoj kritičnoj infrastrukturi.

EU već znatno ulaže u **istraživanje i razvoj domaćih naprednih UI tehnologija za kibernetičku sigurnost** te u kibernetičku sigurnost umjetne inteligencije, pri čemu posebno treba istaknuti 200 milijuna EUR koji su u tu svrhu predviđeni iz programa Obzor Europa i Digitalna Europa do kraja aktualnog višegodišnjeg financijskog okvira. Na primjer, krajem 2026. pokrenut će se tri vodeća projekta u okviru programa Obzor Europa za razvoj, treniranje i testiranje umjetne inteligencije za praćenje i otkrivanje kibernetičkih napada, odgovor na njih i samooporavak digitalnih procesa i sustava, uključujući neprijateljske UI napade, kao i za razvoj generativnih UI alata i tehnologija za kontinuirano praćenje, usklađenost i automatizirano otklanjanje ranjivosti. EU u okviru programa Obzor Europa, Fonda za unutarnju sigurnost, programa Digitalna Europa i CERIS-a financira i cijeli razvojni ciklus UI sposobnosti u području izvršavanja zakonodavstva, od istraživanja do testiranja i validacije te operativnog uvođenja. Osim toga, EU preko Europskog vijeća za inovacije (EIC), uključujući izravna ulaganja Fonda EIC-a, ulaže u europska poduzeća dubokih tehnologija u području kibernetičke sigurnosti i umjetne inteligencije. Ta će se ulaganja 2026. i 2027. proširiti i na relevantne tehnologije s dvojnom namjenom i strateške obrambene tehnologije[33]. Točnije, Komisija će do kraja 2026. omogućiti ulaganja iz Fonda EIC-a u tehnološka poduzeća koja se bave kibernetičkom sigurnošću i umjetnom inteligencijom. Ta ulaganja bit će dio paketa od 100 milijuna EUR za *start-up* i *scale-up* poduzeća koja razvijaju strateške obrambene tehnologije, a slična potpora nastavit će se i 2027. Prva ulaganja u rast strateških poduzeća iz Fonda za *scale-up* poduzeća u Europi provest će se već 2026. Nadovezujući se na Međunarodnu digitalnu strategiju EU-a, Unija i države članice iskoristit će i ponudu EU-a za tehnološki sektor kako bi podržale uvođenje umjetne inteligencije i softverskih rješenja.

Uz ta ulaganja Unija bi trebala nastojati dodatno **ubrzati razmjenu znanja o primjeni naprednih UI sposobnosti u području kibernetičke sigurnosti radi odgovora na kibernetičke napade velikih razmjera uz pomoć umjetne inteligencije**. EU danas raspolaže bogatim ekosustavom i bazom znanja u akademskoj zajednici, industriji i javnom sektoru. Međutim, UI rješenja za kibernetičku sigurnost i dalje su fragmentirana, ne testiraju se dovoljno u operativnim okruženjima i daleko su od široke primjene u svim sektorima[34]. Primjerice, automatizirano otklanjanje ranjivosti danas je jedno od glavnih operativnih uskih grla u području kibernetičke sigurnosti jer UI alati za otkrivanje ranjivosti napreduju brže od UI alata za njihovo uklanjanje, što dovodi do strukturne neravnoteže u korist napadača. Kako bi odgovorila na pozive da se suzbije prijetnja napadačke primjene umjetne inteligencije[35], Komisija će uz potporu Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti (ECCC) i u suradnji s ENISA-om pokrenuti namjenski **veliki pothvat EU-a za otklanjanje ranjivosti uz pomoć umjetne inteligencije**. U njemu će se okupiti europska poduzeća koja se bave kibernetičkom sigurnošću i umjetnom inteligencijom, istraživačke organizacije, operateri kritične infrastrukture i zajednice otvorenog koda kako bi zajedno doprinijeli razvoju UI sustava koji će timovima za kibernetičku sigurnost pomagati tijekom cijelog ciklusa otklanjanja ranjivosti. U okviru velikog pothvata povezat će se istraživanje i praktična primjena, što će omogućiti da se obećavajuća rješenja testiraju u realnim

[33] Fond EIC-a – Europsko vijeće za inovacije – Europska komisija.
[34] *Public Letter of Support for a European Grand Challenge in AI and Security – Google Docs*.
[35] *Idem*.

operativnim okruženjima i u konačnici stave na raspolaganje organizacijama u cijeloj Europi. Time će se ublažiti operativna uska grla koja onemogućuju pravodobno otklanjanje ranjivosti. Zainteresirane države članice bit će pozvane da podrže tu razmjenu znanja.

4.2. Razvoj europskih pionirskih kapaciteta

Postojeći UI modeli i sustavi sa sposobnostima u području kibernetičke sigurnosti već uvelike omogućuju provedbu operacija kibernetičke sigurnosti, no pionirske kibernetičke sposobnosti koje omogućuje UI imaju i dalekosežne posljedice za tehnološku suverenost, sigurnost i obranu Europe. EU stoga mora **razviti vlastite suverene pionirske UI sposobnosti opće namjene** kako bi smanjio rizik od novih ovisnosti o resursu koji je postao strateški ključan, a čiji se sve veći potencijal dvojne namjene proteže daleko izvan kibernetičke sigurnosti. To je širi međusektorski izazov za naše gospodarstvo i društvo, koji će Komisija nastaviti pomno pratiti kako bi prilagodila svoj odgovor u skladu s njegovim razvojem.

Komisija je već poduzela konkretne korake kako bi ključnim europskim akterima pomogla u razvoju sve naprednijih UI mogućnosti.

- Komisija je nedavno odabrala pobjednika velikog pothvata u području pionirske umjetne inteligencije, omogućila mu pristup računalnim kapacitetima EuroHPC-a i tako poduprla razvoj europskog naprednog UI modela otvorenog koda[36].
- Komisija u okviru programa Resurs za UI znanost u Europi (RAISE) financira mrežu laboratorija za pionirsku umjetnu inteligenciju kako bi se unaprijedila istraživanja i u tom području.
- U okviru programa Obzor Europa Komisija financira razvoj sigurne i zaštićene umjetne inteligencije do najnaprednije razine.
- Komisija će nastaviti surađivati s Francuskom i Njemačkom na uspostavi zajedničkog projekta („Europska inicijativa za pionirski UI”) usmjerenog na odvažne istraživačke i inovacijske pothvate, privlačenje talenata i lakše izdvajanje poduzeća (*spin-off*).
- Forum za pionirsku umjetnu inteligenciju Komisiji pruža tehničke savjete[37]

Ti početni koraci važni su temelji, no **ambicije i resurse sada je potrebno podići na sasvim novu razinu** kako bi se europske težnje u području pionirske umjetne inteligencije pretvorile u trajni suvereni kapacitet i konkurentsku prednost. Razvoj pionirske umjetne inteligencije zahtijeva dosad nezabilježenu količinu resursa, stoga se projekti u tom području moraju provoditi zajednički na razini Unije. U predloženom Aktu o razvoju računalstva u oblaku i umjetne inteligencije ti su projekti utvrđeni kao prioritetni te im se uz računalne resurse država članica dodjeljuju i računalni resursi Unije. **Postojeće UI tvornice i buduće UI gigatvornice** trebalo bi uključiti u suverenu europsku infrastrukturu za UI i kibernetičku sigurnost, koja bi obuhvaćala računalstvo, podatke i povezivost, kako bi se EU pozicionirao kao vodeći UI kontinent. Takva je povezivost preduvjet za pouzdanu razmjenu skupova podataka spremnih za primjenu umjetne inteligencije, povezivanje resursa preko granica, siguran rad kontroliranih okruženja te razvoj, testiranje, uvođenje i pristup otpornim, pouzdanim i visokoučinkovitim UI sposobnostima u području kibernetičke sigurnosti. Relevantne UI tvornice usmjerene na kibernetičku sigurnost trebale bi olakšati pristup visokokvalitetnim skupovima podataka spremnima za UI, od javnih podataka do povjerljivih industrijskih podataka[38] i podataka o

[36] Komisija odabrala konzorcij EUROPA kao pobjednika velikog pothvata u području pionirske umjetne inteligencije, projekta izgradnje europskog pionirskog UI modela s otvorenim kodom na sva 24 jezika EU-a | Izgradnja digitalne budućnosti Europe.

[37] Komisija traži stručnjake koji bi sudjelovali u Forumu za pionirsku umjetnu inteligenciju | Izgradnja digitalne budućnosti Europe.

[38] Pod uvjetom da se poštuju primjenjivi zakoni, uključujući pravo tržišnog natjecanja EU-a.

kibernetičkoj sigurnosti. Za to bi se trebale osloniti na pouzdane, sigurne i otporne mehanizme za razmjenu podataka, a njihovi podatkovni laboratoriji trebali bi olakšati razvoj i validaciju UI modela u kontroliranom i provjerljivom okruženju s jasno utvrđenom odgovornošću.

Komisija će u okviru Europskog fonda za konkurentnost poticati razvoj suverenih europskih UI sposobnosti za kibernetičku sigurnost, među ostalim za obranu, kako bi Europa mogla bolje zaštititi svoje strateške interese i smanjiti kritične ovisnosti. U tom će kontekstu s relevantnim agencijama, uključujući ENISA-u i Europsku obrambenu agenciju (EDA), i državama članicama osnovati posebnu radnu skupinu koja će se baviti ublažavanjem sigurnosnih rizika povezanih s uvođenjem pionirskih UI modela u obrambene sustave i kritične sustave s dvojnom namjenom.

Za razvoj suverenih pionirskih sposobnosti bit će potrebne **stotine milijardi eura ulaganja**, a javnim sredstvima moći će se pokriti samo dio tog iznosa. Zbog toga je potrebno hitno privući velika privatna ulaganja, posebno rizični i vlasnički kapital, kako bi se razvila i skalirala inovativna europska rješenja. Bez računalnih kapaciteta, modela i podatkovne infrastrukture Europa će ostati ranjiv korisnik pionirskih UI sustava razvijenih drugdje, koje drugi mogu iznenada isključiti, što bi imalo goleme posljedice za gospodarstvo i (kibernetičku) sigurnost. Izgradnja vlastitih europskih kapaciteta za pionirsku umjetnu inteligenciju mogla bi biti vrlo skupa, no cijena njihove neizgradnje mogla bi biti još veća i rasti iz godine u godinu kako se razlika u sposobnostima UI-ja bude povećavala.

U okviru Paketa za tehnološku suverenost od 3. lipnja 2026. Komisija je pokrenula **savjetovanja s državama članicama, Grupom EIB-a i drugim ključnim dionicima o prijedlogu uspostave novog europskog kapaciteta za vlasnički kapital**. Taj bi kapacitet upravljao portfeljem velikih vlasničkih ulaganja u napredne tehnologije i infrastrukturu ključne za našu tehnološku suverenost, uključujući digitalne tehnologije (npr. pionirska umjetna inteligencija), ali i tehnologije čiste energije, biotehnologiju, a potencijalno i obrambenu tehnologiju. Njegova bi glavna prednost bila stvaranje prijeko potrebnog „uporišta za zajednička ulaganja" u vlasnički kapital, što znači da bi privukao velika privatna ulaganja jer bi funkcionirao u sinergiji s financijskim instrumentima koji već postoje na razini EU-a, kao što je Fond za *scale-up* poduzeća u Europi, ili ulagao u njih. Taj novi instrument vlasničkog ulaganja u stratešku tehnologiju iz temelja bi promijenio sposobnost EU-a da osigura potrebna velika ulaganja u pionirsku umjetnu inteligenciju. Instrument InvestEU u okviru Europskog fonda za konkurentnost mogao bi postati važan mehanizam za velika strateška vlasnička ulaganja u naprednu tehnologiju i infrastrukturu.

4.3.Razvoj vještina u području kibernetičke sigurnosti za doba umjetne inteligencije

Za uspjeh Europe nije dovoljna samo tehnologija. Djelotvorna i sigurna primjena napredne umjetne inteligencije u operacijama kibernetičke sigurnosti ovisit će i o **dovoljnom broju kvalificiranih stručnjaka koji razumiju i znaju sigurno koristiti UI modele s naprednim kibernetičkim mogućnostima** i upravljati rizicima svojstvenima umjetnoj inteligenciji. Budući da će timovi za kibernetičku sigurnost u svoj rad sve više uključivati naprednu umjetnu inteligenciju, postojeći nedostatak stručnjaka i vještina mogao bi se dodatno pogoršati. EU stoga svoju radnu snagu u području kibernetičke sigurnosti mora osposobiti za primjenu umjetne inteligencije u tom području.

Akademija EU-a za vještine u području kibernetičke sigurnosti, u okviru koje se industrija, pružatelji usluga osposobljavanja i akademske ustanove okupljaju oko konkretnih obveza i partnerstava za osposobljavanje u području kibernetičke sigurnosti, odgovarajući je okvir za ispunjavanje te potrebe na razini Unije. Komisija će zajedno s državama članicama iskoristiti taj rastući ekosustav kako bi u okviru Akademije pokrenula namjensku mjeru za razvoj

programa osposobljavanja stručnjaka za kibernetičku sigurnost o upotrebi UI alata. Razmotrit će i moguće sinergije s budućom Akademijom za vještine u području umjetne inteligencije. Osim toga, ENISA će ažurirati **Europski okvir za vještine u području kibernetičke sigurnosti**, pri čemu će u postojeće stručne profile uvrstiti kompetencije povezane s umjetnom inteligencijom i prema potrebi definirati nove uloge.

Ključne aktivnosti:

- **7. ključna aktivnost – Komisija će uz potporu Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti i u suradnji s ENISA-om pokrenuti veliki pothvat EU-a kako bi pomogla u skaliranju europskih UI rješenja za kibernetičku sigurnost (četvrto tromjesečje 2026.).**
- **8. ključna aktivnost – Komisija će zajedno s državama članicama nastojati omogućiti pristup računalnim kapacitetima UI tvornica kako bi se na suverenoj računalnoj infrastrukturi ispitivali, trenirali i uvodili dostupni napredni i pionirski UI modeli za potrebe kibernetičke otpornosti.**
- **9. ključna aktivnost – Komisija će surađivati s državama članicama i industrijom (u okviru Akademije za vještine u području kibernetičke sigurnosti) na razvoju modula osposobljavanja stručnjaka za primjenu umjetne inteligencije u kibernetičkoj sigurnosti (četvrto tromjesečje 2026.).**

5. Suradnja s partnerima sličnih stavova na globalnom pristupu kibernetičkoj sigurnosti u doba umjetne inteligencije

Učinci umjetne inteligencije na kibernetičku sigurnost po svojoj su prirodi globalni jer su UI modeli i sustavi, lanci opskrbe softverom i ekosustavi otvorenog koda prekogranični. Objavljivanje UI modela s kibernetičkim sposobnostima razvijenog u jednoj jurisdikciji može imati ozbiljne posljedice za sigurnost kritične infrastrukture i poduzeća u cijelom svijetu. Vlade, međunarodne organizacije i industrija stoga su pred **zajedničkim izazovom za koji je međunarodna suradnja neophodna** jer samo tako mogu izbjeći fragmentaciju, potaknuti interoperabilnost među pouzdanim partnerima i udružiti snage radi ublažavanja rizika koje UI donosi za kibernetičku sigurnost.

EU bi trebao predvoditi oblikovanje globalnih praksi u području pouzdanog UI-ja i kibernetičke otpornosti, pri čemu bi se trebao osloniti na **regulatorni okvir Unije za UI i kibernetičku sigurnost**. Posebno je potrebna bliska suradnja partnera sličnih stavova kako bi pionirske UI mogućnosti ostale sigurne i dostupne za pouzdane primjene te kako bi se zlonamjerne aktere spriječilo da ih zloupotrebljavaju. Ovaj Akcijski plan ujedno je poziv našim međunarodnim partnerima da nam se pridruže kako bismo pojačali učinak predloženih mjera za sigurnost umjetne inteligencije i kibernetičku otpornost.

Komisija će te ciljeve posebno promicati u okviru bilateralnih i multilateralnih foruma. Nastavit će aktivno **promicati svoj pristup u skupini G-7**, među ostalim u okviru **radnih skupina za digitalnu i informacijsku tehnologiju te kibernetičku sigurnost**, kako bi se izgradilo zajedničko poimanje rizika koje napredne UI sposobnosti donose za kibernetičku sigurnost. Komisija će poticati suradnju skupine G-7 u području standarda i evaluacije tih modela. Osim toga, članice te skupine i druge međunarodne partnere poziva da se pridruže radu na povećanju sigurnosti softvera otvorenog koda i surađuju radi prilagodbe praksi upravljanja ranjivostima. EU će nastaviti aktivno djelovati i u okviru UN-a.

EU će na bilateralnoj razini produbiti komunikaciju s partnerskim zemljama o naprednoj umjetnoj inteligenciji i kibernetičkoj sigurnosti, među ostalim u okviru digitalnih partnerstava te dijaloga u digitalnom i kibernetičkom sektoru. Pritom će prema potrebi dati prednost ključnim područjima suradnje: evaluaciji modela, zaštiti kritične infrastrukture, smanjenju ranjivosti i poboljšanju kibernetičke otpornosti.

Osim toga, **Mreža za mjerenje, evaluaciju i znanost u području naprednog UI-ja, koju koordinira organizacija AISI iz UK-a** i koja blisko surađuje s institutima za sigurnost i zaštitu u partnerskim zemljama i **Komisijinim Uredom za umjetnu inteligenciju**, važna je platforma za razvoj zajedničkih metodologija za evaluaciju pionirskih UI modela, razmjenu primjera dobre prakse i pouzdanu međunarodnu suradnju u području sigurnosti i zaštite umjetne inteligencije.

Komisija će poticati i strukturirani dijalog između vlada i vodećih poduzeća za razvoj pionirske umjetne inteligencije kako bi se uskladili pristupi njezinoj sigurnosti, evaluaciji i odgovornom uvođenju.

Naposljetku, s obzirom na navedene posljedice za europsku i nacionalnu sigurnost EU će produbiti postojeću komunikaciju s **NATO-om** o mogućnostima i rizicima pionirskih UI kapaciteta u kibernetičkom području, među ostalim u okviru budućeg NATO-ova Centra izvrsnosti za umjetnu inteligenciju.

6. Zaključak

Ovaj Akcijski plan nadovezuje se na dugogodišnje koordinirano europsko djelovanje. Budući da će se napredne UI sposobnosti nastaviti sve brže razvijati i sa sobom donositi nove prilike i rizike, Komisija će redovito ocjenjivati provedbu Akcijskog plana i prema potrebi prilagođavati aktivnosti iz njega kako bi se pobrinula da djelotvorno doprinosi razvoju sigurnog i otpornog europskog ekosustava za doba umjetne inteligencije.