# Mnenje Evropskega ekonomsko-socialnega odbora – Skupno sporočilo Evropskemu parlamentu in Svetu – Politika EU na področju kibernetske obrambe

**(mnenje na lastno pobudo)**

(2023/C 293/04)

Poročevalec: **Anastasis YIAPANIS**

Soporočevalec: **Alberto MAZZOLA**

| | |
|---|---|
| Sklep plenarne skupščine | 20. 9. 2022 |
| Pravna podlaga | člen 52(2) Poslovnika |
| | mnenje na lastno pobudo |
| Pristojnost | posvetovalna komisija za spremembe v industriji (CCMI) |
| Datum sprejetja na seji strokovne skupine | 27. 3. 2023 |
| Datum sprejetja na plenarnem zasedanju | 14. 6. 2023 |
| Plenarno zasedanje št. | 579 |
| Rezultat glasovanja | |
| (za/proti/vzdržani) | 208/1/2 |

## 1. **Sklepi in priporočila**

1.1 Evropski ekonomsko-socialni odbor (EESO) podpira predlagano politiko EU za kibernetsko obrambo, vendar bi pričakoval, da bo imela organizirana civilna družba pomembnejšo vlogo pri pripravi teh predlogov. Trenutno EESO težko oceni, ali bodo prihodnje pobude, opisane v skupnem sporočilu, izvedene in ali bodo z njimi doseženi želeni rezultati. Institucije EU in države članice poziva, naj napovedane pobude obravnavajo prednostno, da bi dosegle hiter napredek.

1.2 EESO poudarja, da so potrebni dodatni ukrepi za izboljšanje zmožnosti EU za odkrivanje kibernetskih groženj, ter poziva, naj se financiranje raziskav in razvoja usmeri v razvoj vrhunskih zmogljivosti EU. Bistveno je sodelovanje med zasebnim in javnim sektorjem, ki ne sme biti enosmerno. EESO meni, da je potrebno usklajevanje na ravni EU, da bi odpravili razdrobljenost in zagotovili sodelovanje med državami članicami in njihove skupne naložbe.

1.3 EESO podpira ustanovitev centra EU za koordinacijo kibernetske obrambe in priporoča, naj se države članice zavežejo k stalni pripravljenosti za hitro odzivanje, ocenijo kibernetsko pripravljenost in učinkovitost mehanizmov EU za odzivanje na kibernetske krize s poudarkom na vojaških zmogljivostih in kritičnih sektorjih, kot so opredeljeni v Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta [1] (direktiva NIS 2). EESO podpira razširitev pristojnosti Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost (ECCC), da bi pripomogel k delu centra EU za koordinacijo kibernetske obrambe.

1.4 EESO meni, da bi bilo treba za povečanje strateške avtonomije in suverenosti Unije razviti dinamično platformo za preizkušanje in izmenjavo informacij v realnem času ali jo prevzeti iz realnega sektorja, da bi opredelili sedanje vrzeli v obstoječih zmogljivostih. Uporabljala bi se lahko tudi za izmenjavo dobrih praks, poročanje o kibernetskih incidentih in sestavo seznama EU vseh storilcev kibernetskih kaznivih dejanj.

---

[1] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333,27.12.2022, str. 80).

1.5 EESO poudarja, da se je treba bolje pripraviti na kibernetske napade, kakršni so ruski v Ukrajini, zlasti tiste, ki so usmerjeni v kritično infrastrukturo. Za učinkovito obvladovanje kriz, interoperabilnost in preprečevanje podvajanja prizadevanj in naložb je bistveno sodelovanje med civilnimi in vojaškimi ekosistemi, tudi s simuliranimi preizkusnimi kibernetskimi napadi.

1.6 EESO meni, da bi bilo treba pri naložbah v kibernetsko obrambo dati prednost zaščiti državljanov EU in kritične infrastrukture tudi z uporabo zaupanja vrednih ponudnikov strojne in programske opreme. Vztraja pri pravočasnih posodobitvah prednostnih nalog in naložb, o katerih se morajo dogovoriti EU in države članice ob sodelovanju ustreznih zasebnih deležnikov.

1.7 EU mora ohraniti in razviti zmogljivosti, ki so potrebne za zaščito njenega digitalnega gospodarstva, družbe, demokracije in kritičnih tehnologij, ter zagotavljati ključne storitve kibernetske varnosti. Za zagotovitev strateške avtonomije EU je bistveno, da se zmanjša odvisnost od tretjih držav. EESO meni, da je za EU bistvenega pomena, da sprejme srednjeročni pristop k avtonomiji, kar zadeva ključne tehnologije, in odločno zagovarja, naj raziskovalne in proizvodne zmogljivosti vzpostavijo podjetja s sedežem v EU, pri čemer naj se ustrezna evropska industrijska politika osredotoča na avtonomen kibernetski ekosistem.

1.8 Mala in srednja podjetja bi morala biti deležna ciljno usmerjene podpore in imeti dostop do financiranja programov, s katerimi bi se povečala njihova odpornost na kibernetske napade, pa tudi do pomoči, usposabljanja in priložnosti za izobraževanje o kibernetskih tveganjih in zaščiti pred njimi. EU bi morala zagotoviti mehanizem spodbud za postopno seznanjanje, namenjen malim in srednjim podjetjem, in za razvoj inovativnih malih in srednjih podjetij.

1.9 EESO podpira načrt za ustanovitev akademije za kibernetske veščine in poziva Evropsko komisijo, naj uskladi in financira obsežne programe usposabljanja ter poklicnega in strokovnega izobraževanja, ki bodo vključevali vse države članice in katerih namen bo usposobiti delovno silo za vse agencije in organizacije, ki bodo sodelovale pri kibernetski obrambi, pa tudi za zasebna civilna omrežja.

1.10 EESO meni, da je ozaveščanje državljanov o kibernetski varnosti bistveno za zmanjšanje izpostavljenosti kibernetskim napadom, ter poziva k učnim načrtom in programom vseživljenjskega učenja za izobraževanje o kibernetski varnosti, usmerjenim v izboljšanje kibernetskih veščin in znanja. Podpira vključevanje kibernetske varnosti v vse prihodnje javne politike EU in obveščanje splošne javnosti o kibernetskih grožnjah.

1.11 EESO meni, da se mora tesno sodelovanje z zaveznicami Nata na vojaških področjih osredotočati na polno usklajevanje in vzajemnost, skupne projekte za raziskave, razvoj in inovacije, izmenjavo dobrih praks, obsežne programe usposabljanja in simulacije kibernetskih napadov, katerih glavni cilj je povečati skupno zmogljivost za odzivanje.

1.12 EESO poziva visokega predstavnika, naj pregleda dvostranske dialoge o kibernetiki, ki potekajo, in sodeluje v dodatnih razpravah z drugimi državami in ustreznimi mednarodnimi organizacijami, da se vzpostavi svetovni okvir za spoštovanje mednarodnega prava v kibernetskem prostoru, z velikim poudarkom na vzajemnosti. EESO meni, da lahko EU prevzame vodilno vlogo v mednarodnih razpravah o prihodnosti kibernetske varnosti, zlasti v Organizaciji združenih narodov, saj ima trdne temelje v temeljnih demokratičnih svoboščinah.

1.13 EU bi se morala odločno zavzemati proti kakršnemu koli sistemu družbenega točkovanja državljanov. EESO poudarja, da ni prave demokracije brez pravega varstva osebnih podatkov, in meni, da je odgovorno in učinkovito ravnanje s podatki bistveno, da bi hiperpovezljivost postala konkurenčna prednost.

## 2. **Uvod in splošne ugotovitve**

2.1 Digitalizacija družb prinaša številne grožnje za kibernetsko varnost, ki jih povzročajo tehnološke posodobitve. V zadnjih letih sta se močno povečala število in izpopolnjenost kibernetskih napadov, ki ogrožajo varnost javnih in zasebnih subjektov. Naj gre za izsiljevalsko programje, zlonamerno programsko opremo, napade prek elektronskih naslovov, kršitve varstva podatkov, dezinformacije, porazdeljene napade za zavrnitev storitve ali druge oblike napadov, vsi pomenijo stalno in nenehno grožnjo za varnost EU kot celote.

2.2 EESO pozdravlja skupno sporočilo Politika EU za kibernetsko obrambo ([2]) in meni, da je treba ukrepati zdaj, nujno in usklajeno na ravni EU, pri tem pa vključiti civilne in vojaške ekosisteme kibernetskega prostora ter zagotoviti ustrezen naložbeni okvir za zmogljivosti kibernetske obrambe. Vendar ugotavlja, da je sporočilo zgolj izjava o odločenosti za ukrepanje in seznam prihodnjih pobud EU, ki bi jih bilo treba izpeljati, ter meni, da ni mogoče oceniti, ali bodo te prihodnje zaveze dejansko uresničene, saj bodo na končni izid akcijskega načrta EU za kibernetsko varnost seveda vplivala pogajanja med sozakonodajalcema.

2.3 Po ruskem napadu na satelitsko omrežje KA-SAT, zaradi katerega je bila motena komunikacija med ukrajinskimi vojaškimi silami, in nedavnem škandalu v zvezi z Éricom Léandrijem, ki so ga nekatera obrambna podjetja najela za kibernetsko vohunjenje v njihovem imenu, je kibernetska varnost na vrhu seznama varnostnih groženj v EU. Čeprav je splošna uredba o varstvu podatkov trden zakonodajni akt EU in je v veljavi že več let, je jasno, da so razpoložljivi podatki, katerih količina narašča, ranljivi in je tveganje, da bi tretje strani prešle mejo zakonitosti, vsak dan večje.

2.4 Glede na nadnacionalno naravo kibernetskih napadov je potrebno usklajevanje EU, da bi zmanjšali sedanjo razdrobljenost in zagotovili, da bodo države članice pripravljene na sodelovanje in skupne naložbe. To je zlasti pomembno za prihodnje primere, v katerih bi bila lahko tarča ena država članica, vse druge pa bi morale imeti možnost, da ji nemudoma zagotovijo podporo.

## 3. **Skupno ukrepanje za močnejšo kibernetsko obrambo**

3.1 EESO je seznanjen z napovedanimi ambicioznimi pobudami za ustanovitev centra EU za koordinacijo kibernetske obrambe, razvoj projekta CyDEf-X, ustanovitev skupin za hitro odzivanje na kibernetske grožnje, pripravo pobude EU za kibernetsko solidarnost ter preučitev razvoja sistemov certificiranja kibernetske varnosti za proizvode, storitve in procese IKT. EESO priporoča, naj se vse države članice zavežejo, da bodo stalno pripravljene na hiter odziv, pri čemer bo center EU za koordinacijo vključen v ocenjevanje in pripravo rednih poročil o kibernetski pripravljenosti držav članic in učinkovitosti evropskega mehanizma za odzivanje na kibernetske krize, osredotočal pa se bo na vojaške zmogljivosti in kritične sektorje, kakor so opredeljeni v direktivi o ukrepih za visoko skupno raven kibernetske varnosti v Uniji. Vsaka država članica bi morala imeti strokovnjake, posebej usposobljene za posredovanje v primeru kibernetskih incidentov, in redno preizkušati svojo zmogljivost za posredovanje v drugih državah članicah.

3.2 V sporočilu je naveden dolg seznam postopnih izboljšav, medtem ko bi EESO želel izrecen časovni načrt za izvajanje teh pobud z jasnim upravljanjem ter roki za predložitev in sprejetje. Poleg tega je EESO pričakoval, da bo imela organizirana civilna družba pomembnejšo vlogo pri pripravi teh predlogov.

3.3 EESO meni, da morajo države članice povečati svojo notranjo zmogljivost za boj proti kibernetskim grožnjam, obenem pa sodelovati v projektih za koordinacijo in izmenjavo informacij in dobrih praks z ustreznimi organi v drugih državah članicah. V vseh državah članicah so potrebne hitre naložbe v zmogljivosti kibernetske obrambe in pospešeno uvajanje tehnologije ([3]) ter skupno pripravljenost za odkrivanje kibernetskih napadov, okrevanje po njih in obrambo pred njimi. EESO meni, da bi bilo treba za podporo strateški avtonomiji Unije razviti ali iz zasebnega sektorja prevzeti dinamično platformo za preizkušanje in izmenjavo informacij v realnem času, ki bi se osredotočala na ugotavljanje, katerih zmogljivosti zdaj primanjkuje.

3.4 EESO se strinja, da bi morale v tej fazi vojaške operacije v kibernetskem prostoru ostati v izključni pristojnosti držav članic, ter podpira napovedano sodelovanje med vojaškimi skupinami za odzivanje na izredne računalniške razmere (milCERT), skupinami za odzivanje na incidente na področju računalniške varnosti (CSIRT) in skupino za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU).

3.5 V nedavno sprejeti direktivi o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in direktivi o odpornosti kritičnih subjektov ([4]) so že določene specifične nacionalne in sektorske obveznosti za okvir EU za kibernetsko obrambo. Potrebni so dodatni ukrepi za izboljšanje kolektivne zmogljivosti odkrivanja EU, zato EESO poziva k naložbam v raziskave in razvoj, da se razvijejo vrhunske zmogljivosti.

---

([2]) Sporočilo Komisije o politiki EU za kibernetsko obrambo.
([3]) Kot je pospeševalnik obrambnih inovacij za severnoatlantsko območje (DIANA) v okviru NATO.
([4]) Direktiva o odpornosti kritičnih subjektov.

4. **Zaščita obrambnega ekosistema EU**

4.1 EESO meni, da se je obrambni ekosistem spremenil zaradi zapletenosti in hitro razvijajočih se tehnoloških izzivov in da je kibernetska varnost postala skupna tema za vojaški in civilni sektor, pa tudi državljane EU. Sodelovanje med civilnimi in vojaškimi ekosistemi je zdaj pomembnejše kot kadar koli prej in bi moralo prinesti koristi v smislu učinkovitejšega obvladovanja kriz, pa tudi nenehnega napredka in interoperabilnosti, s čimer bi preprečili podvajanje in multipliciranje istih prizadevanj in naložb. Države članice bi morale biti pripravljene za izvajanje nacionalnih stresnih testov kritične infrastrukture, da bi ocenile in povečale odpornost na prihodnje kibernetske napade.

4.2 EESO meni, da bi morale biti naložbe v kibernetsko obrambo prednostno usmerjene v zaščito državljanov EU in kritične infrastrukture. Glede na hitrost digitalne preobrazbe in hitri razvoj področja groženj odločno poziva, da bi se morale EU in države članice dogovoriti o pravočasnem posodabljanju prednostnih nalog in naložb, pri tem pa se temeljito posvetovati z ustreznimi zasebnimi deležniki. Naprave, povezane v internet stvari, pogosto niso tako dobro zaščitene kot tradicionalne naprave in EESO poziva, naj se zagotovi minimalna raven varnosti prek platform za upravljanje identitete in dostopa. Ker je certificiranje ključna metoda za zagotavljanje višje ravni varnosti, EESO poziva tudi k novemu pristopu EU k certificiranju, ki bi bolj poudarjal varnost interneta stvari.

4.3 EU mora povečati svojo odpornost na kibernetske napade in jih učinkovito odvračati. Kritično infrastrukturo je treba tudi z obrambnimi sistemi EU zaščititi pred kibernetskimi napadi vseh vrst. EESO meni, da je za EU strateško pomembno, da ohrani in razvije bistvene zmogljivosti za zaščito svojega digitalnega gospodarstva, družbe in demokracije ter doseže polno digitalno suverenost, ki je edini način za zaščito kritičnih tehnologij in zagotavljanje učinkovitih ključnih storitev kibernetske varnosti. Za strateško avtonomijo EU je bistveno tudi zmanjšanje odvisnosti od tretjih držav. EESO meni, da bi bilo treba v proces vključiti sektorske agencije EU (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA itd.), ki bi pripravljale smernice za razvoj shem kibernetske varnosti.

4.4 Pandemija COVID-19 je pospešila digitalni prehod in tradicionalno delo preoblikovala v hibridno in/ali delo na daljavo, s tem pa ustvarila nove odnose med delodajalci in delojemalci ter nova pričakovanja, pa tudi nov pojav digitalnih nomadov, katerih število narašča. EESO je seznanjen s hitrimi spremembami na trgu dela, ki so povzročile sprejetje strukture ničelnega zaupanja v podjetjih z uporabo rešitev za upravljanje identitete in dostopa ter upravljanje privilegiranih dostopov. EESO meni, da tako upravljanje z viri podjetja prinaša nove rešitve, povezane s kibernetskimi grožnjami, in da je treba zasebni sektor podpreti pri krepitvi stopnje varnosti njihovih inovativnih digitalnih rešitev.

4.5 EESO izraža razočaranje v zvezi z navedbo Komisije, da bi se „[v] sodelovanju z državami članicami […] lahko pripravil izvedbeni načrt“, in meni, da je tak izvedbeni načrt nujen. Meni, da bi ga bilo treba pripraviti skupaj z državami članicami in čim prej izvesti. Zaskrbljen je, ker Komisija to jemlje zlahka, in poziva institucije EU in države članice, naj olajšajo hiter napredek v zvezi z napovedanimi pobudami.

5. **Vlaganje v zmogljivosti kibernetske obrambe**

5.1 Ker je tehnološki razvoj hiter, je postal kibernetski prostor najnovejša domena vojskovanja za vojskovanjem na kopnem, morju, v zraku in vesolju. Omogoča tudi veliko priložnosti za kazniva dejanja zlonamernih kibernetskih akterjev, od neodvisnih hekerjev do poklicnih zločincev in celo državnih akterjev.

5.2 Naložbe v raziskave in razvoj so ključne in EESO pozdravlja obstoječa namenska sredstva v okviru programa Digitalna Evropa, Evropskega obrambnega sklada, programa Obzorje Evropa in nacionalnih programov za okrevanje, vendar bi si želel več nadnacionalnih projektov, ki bi se osredotočali na sodelovanje in interoperabilnost med sistemi kibernetske obrambe v vseh državah članicah, ter več sinergij med instrumenti financiranja, zlasti za inovativna mala in srednja podjetja.

5.3 EESO ugotavlja, da je v skladu z napovedjo v strategiji EU za kibernetsko varnost iz leta 2020 rok za ustanovitev skupne kibernetske enote v letošnjem letu, in čaka novice o dokončanju tega procesa in pripravljenosti EU za odzivanje na obsežne kibernetske incidente. Pričakuje, da se bosta z njo izboljšali ozaveščenost glede položaja EU in splošna zmogljivost za odzivanje in okrevanje.

5.4 EESO podpira razširitev pristojnosti ECCC, da bi pripomogel k dejavnosti centra EU za koordinacijo kibernetske obrambe. Poleg tega bi lahko ta mreža podpirala evropsko digitalno suverenost z razvojem konkurenčne evropske industrijske baze za ključne tehnološke zmogljivosti, ki bi deloma temeljila na delu pogodbenih javno-zasebnih partnerstev. Javno-zasebna partnerstva so se izkazala kot najučinkovitejši pristop k izboljšanju kibernetske varnosti celotnega digitalnega ekosistema, vendar ne smejo biti enosmerna: tudi javne institucije morajo svoje podatke deliti z zasebnim sektorjem.

5.5 EESO ugotavlja, da mora EU za obravnavanje prihodnjih poskusov hekerskih napadov s kvantnih računalnikov nemudoma začeti vlagati v vrhunske tehnologije, kot je postkvantna kriptografija. Meni, da si mora Evropa srednjeročno prizadevati za avtonomijo, ter odločno poziva, naj raziskave in proizvodne zmogljivosti razvijajo podjetja s sedežem v EU. Po mnenju EESO bi bilo treba povečati vire EU za digitalne raziskave in inovacije ter podpreti naložbe izvajalcev in dobaviteljev v nove tehnične varnostne funkcije, tudi v povezavi z novimi trendi, kot sta razširjena resničnost in metaverzum. Zlasti je bistveno zgraditi evropsko porazdeljeno infrastrukturo oblaka, ki bo temeljila na evropskih pravilih s področij, kot sta shranjevanje in obdelava podatkov ([5]).

5.6 Mala in srednja podjetja bi morala biti deležna posebne pozornosti in imeti dostop do financiranja programov, s katerimi bi se povečala njihova odpornost na kibernetske napade, pa tudi do pomoči ter programov usposabljanja in izobraževanja, ki bi pripomogli k njihovemu razumevanju kibernetskih tveganj in načinih zaščite pred njimi. EU bi morala zagotoviti mehanizem spodbud za postopno seznanjanje, namenjen malim in srednjim podjetjem.

5.7 Komisija ocenjuje, da obstoječe pomanjkanje veščin na področju kibernetske varnosti zadeva pol milijona ljudi, in EESO pozdravlja predlog o ustanovitvi akademije za kibernetske veščine. Jasno je, da prizadevanja na ravni držav članic ne zadostujejo za zmanjšanje vrzeli v spretnostih, zato EESO predlaga, naj ob ustanovitvi te akademije Komisija izkoristi evropsko leto spretnosti ter usklajuje in financira obsežne programe usposabljanja ter poklicnega in strokovnega izobraževanja na ravni EU, ki bodo vključevali vse države članice ter bodo osredotočeni na usposabljanje delovne sile za vse agencije in organe, ki sodelujejo v kibernetski obrambi, pa tudi za zasebna civilna omrežja. Usposabljanje delovne sile je treba posebej poudariti, zlasti na področju naravoslovja, tehnologije, inženirstva in matematike.

5.8 Nadalje EESO meni, da je bistveno ozaveščati državljane o kibernetski varnosti, da bi se zmanjšala izpostavljenost kibernetskim napadom, zlasti osnovnim kibernetskim kaznivim dejanjem, katerih tarča je splošna javnost. Poziva k učnim načrtom za izobraževanje o kibernetski varnosti ter programom vseživljenjskega učenja o kibernetski varnosti, ki bodo osredotočeni na izboljšanje kibernetskih veščin ter seznanjanje državljanov, zlasti mlajše generacije, s kibernetsko varnostjo, da bi to področje zanje postalo privlačnejše. EESO podpira vključevanje premislekov o kibernetski varnosti v vse prihodnje javne politike EU in obveščanje splošne javnosti o kibernetskih grožnjah, vključno z brezplačnimi usposabljanji za vse, brezplačnimi informativnimi aplikacijami za mobilne telefone in komuniciranjem v času največje gledanosti televizije. Vzporedno s temi ukrepi je treba spodbujati širok kulturni napredek na vseh ravneh družbe k pristopu, usmerjenem v kibernetsko varnost.

5.9 EESO meni, da je nujno treba oceniti profile tveganja posameznih dobaviteljev in nato uvesti ustrezne omejitve za dobavitelje, ki štejejo za visoko tvegane, vključno s potrebnimi prepovedmi za ključna sredstva in aplikacije, ki so opredeljeni kot kritični in občutljivi v usklajeni oceni tveganja v EU, ter certificiranjem zaupanja vrednih ponudnikov strojne in programske opreme.

## 6. **Partnersko povezovanje za reševanje skupnih izzivov**

6.1 Stopnja pripravljenosti na prihodnje kibernetske napade se med državami članicami močno razlikuje. EESO meni, da bi moral biti takojšnji prvi korak vzpostavitev platforme za komuniciranje o dobrih praksah v EU, na kateri bi lahko najbolj kibernetsko napredne države članice svoje znanje delile z drugimi državami in jim olajšale takojšnjo uveljavitev teh praks. To bi pripomoglo k izboljšanju vzajemnega zaupanja med nacionalnimi subjekti. Drugič, EESO meni, da je potrebno tesnejše sodelovanje med državnimi in nedržavnimi akterji po vsej EU, da bi izboljšali kibernetsko varnost proizvodov in storitev na notranjem trgu. Predlaga tudi vzpostavitev skupne platforme EU za poročanje o kibernetskih incidentih, vključno s črnim seznamom vseh povzročiteljev kibernetske kriminalitete v EU.

([5]) Kot je francosko-nemška pobuda Gaia-X.

6.2 EESO meni, da se je treba pri tesnem sodelovanju z zaveznicami Nata na vojaškem področju osredotočati ne le na krepitev zmogljivosti in zgodnje odkrivanje, temveč tudi na skupne projekte raziskav, razvoja in inovacij, izmenjavo dobrih praks in izmenjave med strokovnjaki, velike programe usposabljanja in simulacije kibernetskih napadov. Glavni cilj bi moral biti, da se poveča skupna zmogljivost za odzivanje in ustvarijo sinergije za boj proti prihodnjim hibridnim grožnjam v skladu s skupnimi izjavami iz Varšave iz leta 2016 in iz Bruslja iz leta 2018. Pri sodelovanju med EU in Natom je na voljo še veliko poti, ki jih je mogoče izkoristiti, takojšen napredek pa lahko pomeni bistveno razliko pri zagotavljanju varnosti za evropske državljane in družbo.

6.3 EESO meni, da bi morale razprave na svetovni ravni in z mednarodnimi partnerji postati temelj za spodbujanje svetovnega in odprtega kibernetskega prostora, ki varuje človekove pravice, temeljne svoboščine in pravno državo, ter se osredotoča na pripravo zavezujočih mednarodnih standardov v sektorjih s hitrim digitalnim razvojem. Visokemu predstavniku predlaga, naj pregleda obstoječe dvostranske dialoge o kibernetiki in sodeluje v nadaljnjih pogajanjih z drugimi državami in ustreznimi mednarodnimi organizacijami, da bi spodbudil svetovni okvir za uporabo mednarodnega prava v kibernetskem prostoru, ki bi temeljil na strogih pogojih vzajemnosti.

6.4 Nazadnje EESO meni, da je EU najprimernejša za vodenje mednarodnih razprav o prihodnosti kibernetske varnosti, zlasti v okviru razprav v OZN, ker ima trdne temelje v osrednjih demokratičnih svoboščinah. EU mora sodelovati tudi v boju proti totalitarnim režimom, ki izvajajo spremljanje državljanov in kršijo njihove pravice in svoboščine, ter odločno nasprotovati kakršnemu koli sistemu družbenega točkovanja državljanov. EESO poudarja, da ni prave demokracije brez pravega varstva osebnih podatkov, in meni, da je odgovorno in učinkovito ravnanje s podatki bistveno, da bi hiperpovezljivost postala prednost.

V Bruslju, 14. junija 2023

*Predsednik*
*Evropskega ekonomsko-socialnega odbora*
Oliver RÖPKE