Mišljenje Europskog gospodarskog i socijalnog odbora o Zajednička Komunikacija Europskom parlamentu i Vijeću: Politika kiberobrane EU-a

(samoinicijativno mišljenje)

(2023/C 293/04)

Izvjestitelj: **Anastasis YIAPANIS**

Suizvjestitelj: **Alberto MAZZOLA**

Odluka Plenarne skupštine:	20.9.2022.
Pravna osnova:	pravilo 52. stavak 2. Poslovnika
	(samoinicijativno mišljenje)
Nadležno tijelo:	Savjetodavno povjerenstvo za industrijske promjene (CCMI)
Datum usvajanja u Stručnoj skupini:	27.3.2023.
Datum usvajanja na plenarnom zasjedanju:	14.6.2023.
Plenarno zasjedanje br.:	579
Rezultat glasanja	
(za/protiv/suzdržani):	208/1/2

1. **Zaključci i preporuke**

1.1. Europski gospodarski i socijalni odbor (EGSO) podržava predloženu politiku kiberobrane EU-a, ali je očekivao da će se organizacijama civilnog društva omogućiti istaknutija uloga u razradi predmetnih prijedloga. Odboru je u ovom trenutku teško procijeniti hoće li se buduće inicijative navedene u zajedničkoj komunikaciji provesti i hoće li se njima ostvariti željeni rezultati. Odbor poziva institucije EU-a i države članice da odrede prioritete među najavljenim inicijativama i brzo porade na njihovom promicanju.

1.2. EGSO naglašava da su potrebne dodatne mjere za poboljšanje sposobnosti EU-a za otkrivanje kiberprijetnji te poziva na usmjeravanje financijskih sredstava za istraživanje i razvoj u razvoj najsuvremenijih sposobnosti EU-a. Suradnja privatnog i javnog sektora od presudne je važnosti i ne smije biti jednosmjerna. EGSO smatra da je nužna koordinacija na razini EU-a kako bi se riješio problem rascjepkanosti i zajamčila suradnja i zajednička ulaganja država članica.

1.3. EGSO podržava osnivanje Koordinacijskog centra EU-a za kiberobranu i preporučuje da se države članice obvežu na brzi odgovor 24 sata dnevno i sedam dana u tjednu te da ocijene kiberspremnost i uspješnost mehanizama EU-a za odgovor na kiberkrize, uz naglasak na vojnim sposobnostima i ključnim sektorima utvrđenim u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća [1] (Direktiva NIS 2). Odbor podržava proširenje mandata Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC) kako bi on pomagao Koordinacijskom centru EU-a za kiberobranu u njegovu radu.

1.4. Kako bi se povećala strateška autonomija i suverenost Unije u području kibersigurnosti, EGSO smatra da bi trebalo razviti dinamičnu platformu za testiranje i razmjenu informacija u stvarnom vremenu ili preuzeti postojeću iz privatnog sektora kako bi se utvrdili nedostaci u postojećim sposobnostima. Ta se platforma može upotrebljavati i za razmjenu najboljih praksi, prijavljivanje incidenata u području kibersigurnosti i izradu EU-ova sveobuhvatnog popisa kiberkriminalaca.

---

[1] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

1.5. EGSO ističe potrebu za boljom pripremom za kibernapade kao što su ruski napadi u Ukrajini, koji su posebno usmjereni na kritičnu infrastrukturu. Suradnja između civilnih i vojnih ekosustava ključna je za učinkovito upravljanje krizama, interoperabilnost i izbjegavanje udvostručavanja napora i ulaganja, što se među ostalim može postići simuliranim testnim kibernapadima.

1.6. EGSO smatra da bi pri ulaganjima u kiberobranu trebalo dati prednost zaštiti građana EU-a i kritične infrastrukture, među ostalim i korištenjem usluga pouzdanih dobavljača hardvera i softvera. Ustraje na pravodobnom ažuriranju prioriteta i ulaganja o kojima se trebaju dogovoriti EU i države članice, uz sudjelovanje relevantnih privatnih dionika.

1.7. EU mora zadržati i razviti potrebne kapacitete kako bi osigurao svoje digitalno gospodarstvo, društvo, demokraciju i ključne tehnologije te pružio ključne usluge kibersigurnosti. Kako bi se osigurala strateška autonomija EU-a, ključno je smanjiti ovisnosti o trećim zemljama. EGSO smatra da je od ključne važnosti da EU usvoji srednjoročni pristup usmjeren na ostvarenje autonomije u području ključnih tehnologija i snažno se zalaže za to da poduzeća sa sjedištem u EU-u uspostave istraživačke i proizvodne objekte, uz odgovarajuću europsku industrijsku politiku usmjerenu na autonomni ekosustav u kiberprostoru.

1.8. MSP-ovi bi trebali dobivati ciljanu potporu i imati pristup programima financiranja kojima se povećava njihova otpornost na kibernapade, kao i mogućnostima pomoći, osposobljavanja i obrazovanja o kiberrizicima i načinima zaštite od njih. EU bi trebao osigurati mehanizam kojim bi se poticali postupno upoznavanje MSP-ova s tom temom i razvoj inovativnih MSP-ova.

1.9. EGSO podržava plan o osnivanju Akademije za vještine u području kibersigurnosti i traži od Europske komisije da koordinira i financira opsežne programe obuke i strukovnog obrazovanja i osposobljavanja u koje će biti uključene sve države članice i kojima će cilj biti stvaranje kvalificirane radne snage za sve agencije i organizacije uključene u kiberobranu, kao i za privatne civilne mreže.

1.10. Odbor smatra da je podizanje razine osviještenosti građana o kibersigurnosti ključno za smanjenje izloženosti kibernapadima te poziva na obrazovne programe u području kibersigurnosti i programe cjeloživotnog osposobljavanja koji će biti usmjereni na poboljšanje vještina i znanja u području kibersigurnosti. EGSO podržava uključivanje kibersigurnosti u sve buduće javne politike EU-a i informiranje šire javnosti o kiberprijetnjama.

1.11. EGSO smatra da je obvezna snažna suradnja sa saveznicima u NATO-u u vojnim područjima s naglaskom na potpunoj koordinaciji i reciprocitetu, zajedničkim projektima istraživanja, razvoja i inovacija, razmjeni najboljih praksi te opsežnim programima osposobljavanja i simulacijama kibernapada, pri čemu glavni cilj mora biti proširenje zajedničkih kapaciteta za odgovor.

1.12. Odbor poziva Visokog predstavnika da ispita trenutačne bilateralne kiberdijaloge i uključi se u dodatne rasprave s drugim zemljama i relevantnim međunarodnim organizacijama kako bi se uspostavio globalni okvir za poštovanje međunarodnog prava u kiberprostoru, sa snažnim naglaskom na uzajamnosti. Odbor smatra da je EU u dobrom položaju da preuzme vodeću ulogu u međunarodnim raspravama o budućnosti kibersigurnosti, posebno u okviru Ujedinjenih naroda, jer čvrsto počiva na temeljnim demokratskim slobodama.

1.13. EU bi se trebao odlučno usprotiviti bilo kakvom sustavu društvenog ocjenjivanja građana. EGSO jasno ističe da istinska demokracija nije moguća bez djelotvorne zaštite osobnih podataka i smatra da je odgovorno i učinkovito upravljanje podacima ključno kako bi se hiperpovezivost pretvorila u konkurentsku prednost.

2. **Uvod i opće napomene**

2.1. Digitalna ekspanzija društava popraćena je velikim brojem kibersigurnosnih prijetnji koje nastaju zbog nadogradnji tehnologije. Kibernapadi su proteklih nekoliko godina postali sve brojniji i sve sofisticiraniji, zbog čega je ugrožena sigurnost kako javnih tako i privatnih subjekata. Ucjenjivački softver, zlonamjerni programi, napadi e-poštom, povrede podataka, dezinformacije, distribuirani napadi uskraćivanjem usluga ili drugi oblici napada stalna su i trajna prijetnja sigurnosti EU-a u cjelini.

2.2. EGSO pozdravlja Zajedničku Komunikaciju o politici kiberobrane EU-a ([2]) i smatra da je sada vrijeme za hitno i koordinirano djelovanje na razini EU-a u koje moraju biti uključeni i civilni i vojni ekosustavi u kiberprostoru i kojim se mora zajamčiti odgovarajući okvir za ulaganja u sposobnosti za kiberobranu. Međutim, Odbor napominje da se u toj komunikaciji samo konstatira odlučnost za djelovanje i navodi popis budućih inicijativa EU-a koje bi trebale biti uspješne te smatra da nije moguće procijeniti hoće li se te buduće obveze zaista ispuniti jer će budući pregovori između suzakonodavaca naravno utjecati na konačni ishod akcijskog plana EU-a za kibersigurnost.

2.3. Kibersigurnost se nametnula kao jedna od najvažnijih sigurnosnih prijetnji u EU-u zbog ruskog napada na satelitsku mrežu KA-SAT koji je omeo komunikaciju između ukrajinskih vojnih snaga i nedavnog skandala u kojem su neka poduzeća koja djeluju u sektoru obrane angažirala Érica Léandrija kao svojeg kiberšpijuna. Iako je Opća uredba o zaštiti podataka solidan zakonodavni akt EU-a koji je na snazi nekoliko godina, jasno je da je sve veća količina dostupnih podataka osjetljiva i rizik da bi treće strane mogle prijeći granicu zakonitosti svaki dan postaje sve veći.

2.4. S obzirom na transnacionalnu prirodu kibernapada, potrebna je koordinacija na razini EU-a kako bi se smanjila trenutačna rascjepkanost i kako bi države članice bile spremne surađivati i zajednički ulagati. To je posebno važno za buduće slučajeve u kojima bi jedna država članica mogla biti napadnuta, a sve ostale trebale bi imati priliku pružiti joj neposrednu potporu.

3. **Zajedničko djelovanje za snažniju kiberobranu**

3.1. Odbor prima na znanje najavljene ambiciozne inicijative za uspostavu Koordinacijskog centra EU-a za kiberobranu, razvoj projekta CyDEf-X, osnivanje timova za brzu reakciju u području kibersigurnosti, razvoj inicijative EU-a za kibersolidarnost i istraživanje razvoja programa kibersigurnosne certifikacije za IKT proizvode, usluge i procese. EGSO preporučuje da se sve države članice obvežu da će biti spremne pružiti brz odgovor 24 sata dnevno sedam dana u tjednu, pri čemu bi Koordinacijski centar EU-a sudjelovao u procjeni i izradi redovitih izvješća o kiberspremnosti država članica i djelotvornosti europskog mehanizma za odgovor na kiberkrize, s naglaskom na vojnim sposobnostima i ključnim sektorima utvrđenima u Direktivi NIS 2. Svaka država članica trebala bi imati stručnjake koji su posebno osposobljeni za intervenciju u slučaju kiberincidenata te bi trebala redovito ispitivati njihovu sposobnost intervencije u drugim državama članicama.

3.2. Iako se u Komunikaciji navodi dug popis postupnih poboljšanja, EGSO je očekivao jasan plan za provedbu tih inicijativa, s jasnim upravljanjem i rokovima za podnošenje i usvajanje. Nadalje, Odbor je očekivao da će organizacijama civilnog društva biti omogućena istaknutija uloga u razvoju tih prijedloga.

3.3. EGSO smatra da države članice moraju jačati svoje interne kapacitete za suzbijanje kiberprijetnji i ujedno sudjelovati u projektima suradnje i razmjenjivati informacije i najbolje prakse posredstvom sličnih tijela u drugim državama članicama. Potrebni su ubrzana primjena tehnologija ([3]) i brza ulaganja u sposobnosti za kiberobranu u svim državama članicama, kao i u zajedničku pripravnost za otkrivanje kibernapada te oporavak i obranu od njih. Odbor smatra da se za potporu autonomiji Unije u području kibersigurnosti mora razviti dinamična platforma za testiranje i razmjenu informacija u stvarnom vremenu ili preuzeti postojeća iz privatnog sektora kako bi se utvrdili nedostaci u postojećim sposobnostima.

3.4. EGSO se slaže s mišljenjem da bi vojne operacije u kiberprostoru u ovoj fazi trebale ostati u isključivoj nadležnosti država članica te podržava najavljenu suradnju vojnih timova EU-a za hitne računalne intervencije (vojnih CERT-ova), timova za odgovor na računalne sigurnosne incidente (CSIRT-ova) i tima za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU).

3.5. Nedavno donesenom Direktivom NIS 2 i Direktivom o otpornosti kritičnih subjekata (CER) ([4]) već su uspostavljene posebne nacionalne i sektorske obveze za okvir EU-a za kiberobranu. Potrebno je daljnje djelovanje kako bi se poboljšao zajednički kapacitet EU-a za otkrivanje te EGSO poziva na ulaganje u istraživanje i razvoj radi razvoja najsuvremenijih sposobnosti EU-a.

([2]) Komunikacija Komisije o politici kiberobrane EU-a.
([3]) Kao što je NATO-ov Akcelerator za inovacije u području obrane za Sjevernoatlantsku inicijativu (DIANA).
([4]) Direktiva CER.

4. **Osiguravanje obrambenog ekosustava EU-a**

4.1. EGSO smatra da se obrambeni ekosustav promijenio uslijed inherentnih složenosti i tehnoloških izazova koji se brzo razvijaju te da je kibersigurnost postala zajednička tema za vojni i civilni sektor, kao i za građane EU-a. Suradnja civilnih i vojnih ekosustava sada je važnija nego ikad i trebala bi donijeti koristi u smislu djelotvornijeg upravljanja krizama i kontinuiranog napretka i interoperabilnosti, uz izbjegavanje udvostručavanja ili umnožavanja istih napora i ulaganja. Države članice trebale bi biti spremne provoditi nacionalna testiranja otpornosti kritične infrastrukture kako bi se procijenila i povećala otpornost na buduće kibernapade.

4.2. EGSO smatra da ulaganja u kiberobranu moraju biti prvenstveno usmjerena na zaštitu građana EU-a i kritične infrastrukture. S obzirom na brz tempo digitalne transformacije i brz razvoj okruženja u kojem se javljaju prijetnje, Odbor odlučno poziva EU i države članice da postignu dogovor o pravodobnom ažuriranju prioriteta i ulaganja, uz opsežno savjetovanje s relevantnim privatnim dionicima. Uređaji povezani s internetom stvari (IoT) često nisu tako dobro zaštićeni kao tradicionalni uređaji i EGSO poziva na to da se putem platformi za upravljanje identitetom i pristupom zajamči minimalna razina sigurnosti. Osim toga, s obzirom na to da je certificiranje ključna metoda kojom se pruža viša razina sigurnosti, Odbor poziva na veći naglasak na sigurnosti interneta stvari u novom pristupu EU-a certificiranju.

4.3. EU mora izgraditi otpornost na kibernapade i uspostaviti djelotvorno odvraćanje kiberprijetnji. Kritična infrastruktura mora biti zaštićena od svih vrsta kibernapada, uključujući napade koji se izvršavaju u okviru obrambenih sustava EU-a. Odbor smatra da je u strateškom interesu EU-a zajamčiti da Unija zadrži i razvije ključne kapacitete kako bi zaštitila svoje digitalno gospodarstvo, društvo i demokraciju te postigla potpunu digitalnu suverenost kao jedini način zaštite ključnih tehnologija i pružanja djelotvornih ključnih usluga u području kibersigurnosti. Smanjenje ovisnosti o trećim zemljama ključno je i za stratešku autonomiju EU-a. EGSO smatra da bi sektorske agencije EU-a (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA itd.) trebale sudjelovati u tom procesu i pružati smjernice za razvoj programa kibersigurnosti.

4.4. Digitalna tranzicija ubrzala se uslijed pandemije bolesti COVID-19, a tradicionalni rad pretvorio se u hibridni način rada i/ili rad na daljinu, što je dovelo do razvoja novih radnih odnosa i očekivanja te nove klase digitalnih nomada, čiji se broj povećava. EGSO prima na znanje brze promjene na tržištu rada koje su navele poduzeća na usvajanje arhitekture „Zero Trust" putem rješenjâ za IAM (upravljanje pristupom identitetu) i PAM (privilegirano upravljanje pristupom). Odbor smatra da ta vrsta upravljanja resursima poduzeća donosi nova rješenja za kiberprijetnje te smatra da je potrebno pružiti potporu nastojanjima privatnog sektora usmjerenima na jačanje razine sigurnosti inovativnih digitalnih rješenja.

4.5. EGSO je prilično razočaran izjavom Komisije da bi se plan provedbe mogao uspostaviti u suradnji s državama članicama i smatra takav plan provedbe obveznim. Smatra da bi ga trebalo izraditi zajednički s državama članicama i što prije provesti. Odbor je zabrinut zbog Komisijina labavog stava te potiče institucije EU-a i države članice da olakšaju brz napredak najavljenih inicijativa.

5. **Ulaganje u kapacitete kiberobrane**

5.1. Kiberprostor je zbog brzog razvoja tehnologije postao najnovije područje ratovanja, nakon kopna, mora, zraka i svemira. Osim toga, u njemu su se otvorile velike mogućnosti za kriminal koji provode razni zlonamjerni akteri u kiberprostoru, od neovisnih hakera do profesionalnih kriminalaca, pa čak i državnih aktera.

5.2. Ulaganje u istraživanje i razvoj od ključne je važnosti i EGSO pozdravlja postojeće namjenske fondove u okviru programa Digitalna Europa, Europskog fonda za obranu, programa Obzor Europa i nacionalnih programa oporavka. Međutim, Odbor smatra da je potrebno više transnacionalnih projekata usmjerenih na suradnju i interoperabilnost sustava za kiberobranu u svim državama članicama, kao i više sinergija među instrumentima financiranja, posebice onih namijenjenih inovativnim MSP-ovima.

5.3. Kako je najavljeno u strategiji EU-a za kibersigurnost iz 2020., Odbor napominje da rok za osnivanje Zajedničke jedinice za kibersigurnost istječe ove godine te čeka vijesti o dovršetku tog procesa i pripravnosti EU-a za odgovor na kiberincidente velikih razmjera. EGSO očekuje da će se time poboljšati informiranost EU-a o stanju te sveukupni kapacitet za odgovor i oporavak.

5.4. Odbor podržava proširenje mandata ECCC-a kako bi on pomagao Koordinacijskom centru EU-a za kiberobranu u njegovu radu. Osim toga, ta bi mreža mogla doprinijeti europskoj digitalnoj suverenosti razvojem konkurentne europske industrijske baze za ključne tehnološke sposobnosti, koja bi se djelomično temeljila na aktivnostima razvijenim u okviru ugovornih javno-privatnih partnerstava. Javno-privatna partnerstva pokazala su se najučinkovitijim pristupom poboljšanju kibersigurnosti cijelog digitalnog ekosustava, ali ona ne mogu biti jednosmjerna: javne institucije također moraju dijeliti svoje podatke s privatnim sektorom.

5.5. EGSO napominje da EU mora odmah ulagati u najsuvremenije tehnologije kao što je post-kvantna kriptografija kako bi se odgovorilo na buduće pokušaje hakiranja koji se provode s pomoću kvantnih računala. Smatra da Europa mora obvezno zauzeti srednjoročni pristup autonomiji i snažno se zalaže za to da poduzeća sa sjedištem u EU-u razvijaju istraživačke i proizvodne pogone. EGSO smatra da je važno povećati resurse EU-a za digitalno istraživanje i inovacije te poduprijeti ulaganja operatera i dobavljača u nove funkcionalnosti tehničke sigurnosti, što se odnosi i na nove trendove kao što su proširena stvarnost i metaverzum. Posebno je važno izgraditi europsku distribuiranu infrastrukturu oblaka koja se temelji na europskim pravilima o temama kao što su pohrana i obrada podataka ([5]).

5.6. MSP-ovima bi trebalo pridati posebnu pozornost i omogućiti im pristup programima financiranja kojima se jača njihova pripravnost na kibernapade, kao i programima pomoći, osposobljavanja i obrazovanja koji će im pomoći da razumiju kiberrizike i načine kako se zaštititi od njih. EU bi trebao pružiti mehanizam poticaja kojim se potiče postupno upoznavanje za MSP-ove.

5.7. Komisija procjenjuje da u području kibersigurnosti trenutačno nedostaje pola milijuna stručnjaka s potrebnim vještinama, a EGSO pozdravlja prijedlog o osnivanju Akademije za vještine u području kibersigurnosti. Jasno je da napori na razini država članica nisu dovoljni da bi se smanjio taj nedostatak vještina, pa Odbor predlaže da Komisija uz pokretanje Akademije iskoristi prilike koje nudi Europska godina vještina te koordinira i financira opsežne programe osposobljavanja i programe strukovnog obrazovanja i osposobljavanja na razini EU-a u kojima bi sudjelovale sve države članice i u kojima bi se naglasak stavio na osiguravanje kvalificirane radne snage za sve agencije i tijela uključena u kiberobranu, kao i za privatne civilne mreže. Poseban naglasak mora se staviti na osposobljavanje radne snage, posebno u područjima znanosti, tehnologije, inženjerstva i matematike (STEM).

5.8. Nadalje, EGSO smatra da je ključno podići razinu osviještenosti građana o kibersigurnosti kako bi se smanjila izloženost kibernapadima, posebno osnovnom kiberkriminalu usmjerenom na opću populaciju. Odbor poziva na uvođenje obrazovnih programa u području kibersigurnosti i cjeloživotnih programa osposobljavanja u području kibersigurnosti koji će biti usmjereni na poboljšanje vještina u području kibersigurnosti i povećanje osviještenosti o kibersigurnosti i njezine privlačnosti za građane, posebno mladu generaciju. EGSO se zalaže za uključivanje promišljanja o kibersigurnosti u sve buduće javne politike EU-a i informiranje šire javnosti o kiberprijetnjama, među ostalim putem besplatnih programa osposobljavanja za stanovništvo u cjelini, besplatnih informativnih aplikacija za mobilne telefone i informacija u udarnim televizijskim terminima. Usporedo s tim mjerama mora se promicati širok kulturni napredak na svim razinama društva prema pristupu „usmjerenom na kibersigurnost”.

5.9. EGSO smatra da je ključno procijeniti profil rizičnosti dobavljača i primijeniti relevantna ograničenja na dobavljače koji se smatraju visokorizičnima, uključujući potrebne zabrane za ključnu imovinu i aplikacije koje su u koordiniranim procjenama rizika na razini EU-a definirane kao kritične i osjetljive, kao i certificiranje pouzdanih pružatelja hardvera i softvera.

6. **Sklapanje partnerstava za rješavanje zajedničkih pitanja**

6.1. Države članice uvelike se razlikuju po razini pripravnosti na buduće kibernapade. EGSO smatra da je neposredni prvi korak uspostava platforme za komunikaciju o najboljim praksama unutar EU-a gdje će države članice koje su najnaprednije u području kibersigurnosti moći podijeliti svoje znanje s drugim zemljama i olakšati njegovo neposredno prihvaćanje. Time bi se doprinijelo poboljšanju uzajamnog povjerenja među nacionalnim subjektima. Kao drugo, Odbor smatra da je potrebna snažnija suradnja između državnih i nedržavnih aktera diljem EU-a kako bi se poboljšala kibersigurnost proizvoda i usluga na unutarnjem tržištu. EGSO također predlaže stvaranje zajedničke platforme EU-a za prijavljivanje kiberincidenata, uključujući crnu listu svih subjekata koji se bave kiberkriminalom u EU-u.

([5]) Npr. francusko-njemačka inicijativa Gaia-X.

6.2. EGSO smatra da snažna suradnja s našim saveznicima u NATO-u u vojnom području mora biti usmjerena na izgradnju kapaciteta i rano otkrivanje, ali i na zajedničke projekte istraživanja, razvoja i inovacija, razmjenu najboljih praksi i razmjene među stručnjacima, opsežne programe osposobljavanja i simulacije kibernapada. Glavni bi cilj trebao biti proširenje zajedničkog kapaciteta za odgovor i stvaranje sinergija za suzbijanje budućih hibridnih prijetnji nakon zajedničkih izjava iz Varšave (2016.) i Bruxellesa (2018.). U okviru suradnje EU-a i NATO-a postoji još mnogo mogućnosti koje se mogu iskoristiti, a trenutan napredak može znatno pridonijeti sigurnosti naših građana i društava.

6.3. Odbor smatra da bi se u raspravama na globalnoj razini i s našim međunarodnim partnerima trebali postaviti temelji za promicanje globalnog i otvorenog kiberprostora u kojem su zaštićena ljudska prava, temeljne slobode i vladavina prava, a naglasak se stavlja na razvoj obvezujućih međunarodnih standarda u sektorima u kojima vlada brz digitalni razvoj. Odbor savjetuje Visokom predstavniku da ispita postojeće bilateralne kiberdijaloge i uključi se u daljnje pregovore s drugim zemljama i relevantnim međunarodnim organizacijama s ciljem promicanja globalnog okvira za primjenu međunarodnog prava u kiberprostoru na temelju strogog uvjeta uzajamnosti.

6.4. Naposljetku, Odbor smatra da je EU u najboljem položaju da povede međunarodne rasprave o budućnosti kibersigurnosti, posebno u okviru rasprava koje se vode u UN-u, jer čvrsto počiva na temeljnim demokratskim slobodama. EU se mora uključiti i u borbu protiv totalitarnih režima koji prate podatke građana i krše njihova prava i slobode te bi se trebao snažno suprotstaviti bilo kakvom sustavu društvenog ocjenjivanja građana. EGSO jasno ističe da stvarna demokracija nije moguća bez djelotvorne zaštite osobnih podataka i smatra da je odgovorno i učinkovito upravljanje podacima ključno kako bi se hiperpovezivost pretvorila u prednost.

Bruxelles, 14. lipnja 2023.

Predsjednik
Europskog gospodarskog i socijalnog odbora
Oliver RÖPKE