Mišljenje Europskog gospodarskog i socijalnog odbora o prijedlogu Uredbe Europskog parlamenta i Vijeća o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara

(COM(2018) 630 final — 2018/0328 (COD))

(2019/C 159/10)

Izvjestitelj: **Antonio LONGO**

Suizvjestitelj: **Alberto MAZZOLA**

Zahtjev za savjetovanje:	Europsko vijeće, 5.10.2018. Europski parlament, 1.10.2018.
Pravni temelj:	članak 173. stavak 3., članci 188. i 304. Ugovora o funkcioniranju Europske unije
Nadležna stručna skupina:	Stručna skupina za promet, energiju, infrastrukturu i informacijsko društvo
Datum usvajanja u Stručnoj skupini:	9.01.2019.
Datum usvajanja na plenarnom zasjedanju:	23.01.2019.
Plenarno zasjedanje br.:	540
Rezultat glasovanja (za/protiv/suzdržani):	143/5/2

1. Zaključci i preporuke

1.1. Europski gospodarski i socijalni odbor (EGSO) pozdravlja inicijativu Komisije i smatra da je ključna za razvoj industrijske strategije za kibersigurnost i strateški važna za postizanje snažne i široke digitalne autonomije. Ti su čimbenici nužni za jačanje europskih obrambenih mehanizama imajući u vidu kibernetički rat koji je u tijeku i koji bi mogao ugroziti političke, gospodarske i društvene sustave.

1.2. Odbor ističe da se svaka strategija za kibersigurnost treba temeljiti na općoj obaviještenosti i sigurnom ponašanju korisnika.

1.3. Odbor se slaže s općim ciljevima Prijedloga i svjestan je činjenice da će posebni aspekti funkcioniranja biti razrađeni u naknadnoj analizi. Međutim, s obzirom na to da je riječ o uredbi, smatra da je određene osjetljive aspekte povezane s upravljanjem, financiranjem i postizanjem zacrtanih ciljeva potrebno utvrditi unaprijed. Važno je da se buduća mreža i centar što više temelje na kiberkapacitetima i stručnom znanju država članica te da se u novom centru ne objedinjuju sve nadležnosti. Osim toga, valja spriječiti preklapanje djelatnosti buduće mreže i centra s postojećim mehanizmima i tijelima za suradnju.

1.4. EGSO podržava proširenje suradnje na sektor industrije na temelju čvrstih obveza na znanstvenom i investicijskom polju te njegovo uključivanje u Upravni odbor u budućnosti. U slučaju trostrane suradnje između Europske komisije, država članica i industrije, prisutnost poduzeća iz zemalja koje nisu članice EU-a trebala bi biti ograničena na poduzeća koja već dugo postoje na europskom tlu i potpuno su uključena u europsku tehnološku i industrijsku bazu, pod uvjetom da podliježu odgovarajućim mehanizmima praćenja i kontrole, kao i poštovanju načela uzajamnosti i obveza povjerljivosti.

1.5. Kibersigurnost treba biti zajednička obveza svih država članica koje stoga trebaju sudjelovati u Upravnom odboru na način koji je još potrebno definirati. Kad je riječ o financijskom doprinosu država članica, financijska sredstva iz europskih fondova mogla bi se dodijeliti svakoj od njih.

1.6. U Prijedlogu je potrebno pojasniti kako će Centar moći intervenirati u koordinaciji financiranja programa Digitalna Europa i Obzor Europa te, prije svega, u skladu s kojim će se smjernicama obavljati javna nabava i dodjeljivati javni ugovori. Taj je aspekt nužan kako bi se izbjegla udvostručavanja ili preklapanja. Osim toga, kako bi se povećala financijska omotnica, preporučuje se proširenje sinergija s drugim financijskim instrumentima EU-a (npr. regionalnim fondovima, strukturnim fondovima, CEF-om, ERF-om, InvestEU-om...).

1.7. EGSO smatra da je ključno utvrditi načine suradnje i odnose Europskog centra i nacionalnih centara. Nadalje, važno je da se nacionalni centri financiraju sredstvima EU-a, barem kad je riječ o administrativnim troškovima, te da se time olakša administrativna i stručna usklađenost kako bi se smanjio jaz među europskim državama.

1.8. Odbor ponovno ističe važnost ljudskog kapitala i nada se da će Centar za stručnost moći – u suradnji sa sveučilištima, istraživačkim centrima i centrima za visoko obrazovanje – promicati visokokvalitetno obrazovanje i osposobljavanje, među ostalim putem specifičnih obrazovnih programa na sveučilištima i visokim učilištima. Jednako tako, od ključne je važnosti predvidjeti posebnu potporu za novoosnovana te mala i srednja poduzeća.

1.9. EGSO smatra da je od presudne važnosti pojasniti područja nadležnosti i granice između mandata Centra i Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), pritom jasno utvrditi načine njihove suradnje i uzajamne potpore te izbjeći preklapanje nadležnosti i udvostručavanje napora. Slični problemi postoje u pogledu drugih tijela za kibersigurnost, kao što su EDA, Europol i CERT-EU te se preporučuje stvaranje mehanizama strukturiranog dijaloga među različitim tijelima.

2. Trenutačni okvir za kibersigurnost

2.1. Tema kibersigurnosti nalazi se na vrhu programa EU-a jer je riječ o bitnom čimbeniku za obranu institucija, poduzeća i građana, kao i nužnom sredstvu za održavanje demokracija. Među pojavama koje uzrokuju najveću zabrinutost je eksponencijalno povećanje širenja malicioznih softvera na internetu putem automatskih sustava, čija je učestalost porasla sa 130000 u 2007. godini na 8 milijuna u 2017. Nadalje, Unija je neto uvoznik proizvoda i rješenja za kibersigurnost, što dovodi do problema gospodarske konkurentnosti te civilne i vojne sigurnosti.

2.2. Iako EU posjeduje znatnu stručnost i iskustvo u području kibersigurnosti, industrija u tom sektoru, sveučilišta i istraživački centri i dalje su fragmentirani i neusklađeni te nemaju zajedničku razvojnu strategiju. Uzrok tome je činjenica da relevantni sektori kibersigurnosti (npr. energetika, svemir, obrana i promet) ne primaju dostatnu potporu te se ne iskorištavaju sinergije između sektora civilne i obrambene kibersigurnosti.

2.3. Kako bi odgovorio na sve veće izazove, EU je 2013. utvrdio strategiju kibersigurnosti u cilju promicanja pouzdanog, sigurnog i otvorenog kiberekosustava ([1]). Naknadno su 2016. donesene prve posebne mjere za sigurnost mrežnih i informacijskih sustava ([2]). To je dovelo do stvaranja javno-privatnog partnerstva („JPP") za kibersigurnost.

2.4. U komunikaciji iz 2017. naslovljenoj „Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a" ([3]) istaknuta je potreba da se u EU-u zajamči zadržavanje i razvoj bitnih tehnoloških sposobnosti u području kibersigurnosti u cilju zaštite jedinstvenog digitalnog tržišta, a osobito u cilju zaštite ključnih mrežnih i informacijskih sustava i pružanja ključnih kibersigurnosnih usluga.

([1]) JOIN(2013) 1 final.
([2]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).
([3]) JOIN(2017) 450 final.

2.5. Stoga Unija mora moći zaštititi svoje digitalne resurse i procese i natjecati se na globalnom tržištu kibersigurnosti kako bi postigla snažnu i široku digitalnu autonomiju ([4]).

3. **Prijedlozi Komisije**

3.1. Svrha Centra za stručnost (ili „Centar ”) bit će olakšavanje i koordinacija rada Mreže nacionalnih centara, poticanje Zajednice stručnjaka za kibersigurnost, provedba programa tehnološkog razvoja te olakšavanje pristupa tako prikupljenom znanju.

3.2. Centar za stručnost će to ponajprije činiti provedbom relevantnih dijelova programa Digitalna Europa i Obzor Europa dodjelom bespovratnih sredstava i obavljanjem nabave. S obzirom na znatna ulaganja u kibersigurnost drugdje u svijetu i potrebu za koordinacijom i udruživanjem financijskih sredstava u Europi, predlaže se da se Centar za stručnost strukturira kao europsko partnerstvo s dvostrukim pravnim temeljem jer će se time olakšati zajednička ulaganja Unije, država članica i/ili industrije.

3.3. Prijedlogom se zahtijeva od država članica da djelovanju Mreže i Centra za stručnost pridonesu odgovarajućim iznosom. Predviđena financijska omotnica EU-a iznosi oko 2 milijarde EUR u okviru programa Digitalna Europa, utvrđuje se iznos iz programa Obzor Europa i ukupni doprinos država članica u barem jednakim iznosima kao doprinos Zajednice.

3.4. Glavno tijelo za donošenje odluka bit će Upravni odbor u kojem će biti zastupljene sve države članice, ali pravo glasa imaju samo one koje financijski pridonose. Sustav glasovanja u skladu je s načelom dvostruke većine kojim se zahtijeva 75 % financijskog doprinosa i 75 % glasova. Komisija ima 50 % glasova. Centru pomaže Industrijski i znanstveni savjetodavni odbor kako bi se osigurao dijalog s poduzećima, potrošačima i drugim interesnim skupinama.

3.5. U bliskoj suradnji s Mrežom nacionalnih koordinacijskih centara i Zajednicom stručnjaka za kibersigurnost, Centar bi bio glavno provedbeno tijelo za financijska sredstva EU-a namijenjena za informacijsku sigurnost u okviru predloženih programa Digitalna Europa i Obzor Europa.

3.6. Države članice odabiru nacionalne koordinacijske centre. Centri bi na raspolaganju trebali imati tehnološke stručnjake za područje kibersigurnosti ili izravan pristup takvim stručnjacima, osobito u područjima šifriranja, sigurnosnih usluga IKT-a, automatskog otkrivanja neovlaštenih pristupa, sigurnosti sustava, mrežne sigurnosti, sigurnosti softvera i aplikacija ili ljudskih i društvenih aspekata sigurnosti i privatnosti. Trebali bi biti sposobni djelotvorno surađivati i koordinirati aktivnosti s industrijom, javnim sektorom, uključujući tijela određena na temelju Direktive (EU) 2016/1148.

4. **Opće napomene**

4.1. EGSO pozdravlja inicijativu Komisije i smatra je strateški važnom za razvoj kibersigurnosti u provedbi odluke donesene na sastanku na vrhu u Tallinnu u rujnu 2017. Tada su šefovi država i vlada pozvali Uniju da postane „globalna predvodnica u području kibersigurnosti do 2025. kako bismo osigurali povjerenje i zaštitu naših građana, potrošača i poduzeća na internetu te ostvarili slobodan i zakonom uređen internet”.

4.2. EGSO ponavlja da je u tijeku pravi kibernetički rat koji može ugroziti političke, gospodarske i društvene sustave napadom na informacijske sustave institucija, ključnu infrastrukturu (energetika, promet, banke i financijske institucije...) i poduzeća te utjecanjem putem lažnih vijesti na izborne i demokratske postupke općenito ([5]). Stoga je potrebno snažno poticati osviještenost te čvrsto i pravodobno reagirati. Stoga je nužno uspostaviti jasnu i dobro podržanu industrijsku strategiju za kibersigurnost kao osnovni preduvjet za postizanje digitalne autonomije. EGSO smatra da u planu rada prioritet trebaju imati područja utvrđena u Direktivi (EU) 2016/1148 koja se primjenjuje na poduzeća koja pružaju ključne usluge, javne ili privatne, zbog njihove važnosti za društvo ([6]).

([4]) SL C 227, 28.6.2018., str. 86.

([5]) Informativno izvješće „Upotreba medija u svrhu utjecanja na društvene i političke procese u EU-u i istočnim susjednim zemljama“, Vareikytė, 2014.

([6]) SL C 227, 28.6.2018., str. 86.

4.3. Odbor ističe da se svaka strategija za kibersigurnost treba temeljiti na općoj obaviještenosti i sigurnom ponašanju korisnika. Stoga sve tehnološke inicijative trebaju biti popraćene odgovarajućim kampanjama za obavješćivanje i podizanje svijesti kako bi se stvorila „kultura digitalne sigurnosti” ([7]).

4.4. Odbor se slaže s općim ciljevima Prijedloga i svjestan je činjenice da će posebni aspekti funkcioniranja biti razrađeni u naknadnoj analizi. Međutim, s obzirom na to da je riječ o uredbi, smatra da je određene osjetljive aspekte povezane s upravljanjem, financiranjem i postizanjem zacrtanih ciljeva potrebno utvrditi unaprijed. Važno je da se buduća mreža i centar što više temelje na kiberkapacitetima i stručnom znanju država članica te da se u novom centru ne objedinjuju sve nadležnosti. Osim toga, valja spriječiti preklapanje područja djelatnosti buduće mreže i centra s postojećim mehanizmima i tijelima za suradnju.

4.5. EGSO podsjeća na to da je u svojem mišljenju TEN/646 o Aktu o kibersigurnosti ([8]) predložio trostranu suradnju u okviru javno-privatnog partnerstva između Europske komisije, država članica i industrije (uključujući MSP-ove), dok se postojećom strukturom, čiji pravni oblik treba pobliže odrediti, zapravo predviđa javno-javno partnerstvo između Europske komisije i država članica.

4.6. EGSO podržava proširenje suradnje na sektor industrije na temelju čvrstih obveza na znanstvenom i investicijskom polju te njegovo uključivanje u Upravni odbor u budućnosti. EGSO podržava proširenje suradnje na sektor industrije na temelju čvrstih obveza na znanstvenom i investicijskom polju te njegovo uključivanje u Upravni odbor u budućnosti. Osnivanjem Industrijskog i znanstvenog savjetodavnog odbora neće se nužno zajamčiti dijalog s poduzećima, potrošačima i drugim interesnim skupinama. Nadalje, u novom kontekstu koji je izradila Komisija nije jasno kakvu će ulogu imati Europska organizacija za kibersigurnost (ECSO) uspostavljena u lipnju 2016. na poticaj Komisije kao njezina druga strana čiji mrežni kapital i znanje ne smiju biti rascjepkani.

4.6.1. U slučaju trostrane suradnje, važno je posvetiti pozornost slučaju poduzeća iz trećih zemalja. Točnije, EGSO ističe da se ta suradnja treba temeljiti na strogom mehanizmu za sprečavanje prisutnosti poduzeća iz zemalja koje nisu članice EU-a jer bi to moglo narušiti sigurnost i autonomiju Unije. Relevantne odredbe utvrđene u Europskom programu industrijskog razvoja u području obrane ([9]) trebale bi se primjenjivati i u tom kontekstu.

4.6.2. EGSO istodobno uviđa da bi neka poduzeća iz zemalja koje nisu članice EU-a, koja već dugo postoje na europskom tlu i potpuno su uključena u europsku tehnološku i industrijsku bazu, mogla biti vrlo korisna za projekte Zajednice te bi im trebala moći pristupiti pod uvjetom da države članice uspostave odgovarajuće mehanizme praćenja i kontrole tih poduzeća te da poštuju načelo uzajamnosti i obveze povjerljivosti.

4.7. Kibersigurnost treba biti zajednička obveza svih država članica koje stoga trebaju sudjelovati u Upravnom odboru na način koji je još potrebno definirati. Osim toga, važno je da sve države članice na odgovarajući način financijski pridonose inicijativi Komisije. Kad je riječ o financijskom doprinosu država članica, sredstva Zajednice mogu se dodijeliti svakoj od njih.

4.8. EGSO se slaže da svaka država članica treba biti slobodna imenovati vlastitog predstavnika u Upravnom odboru Europskog centra za stručnost. Odbor preporučuje jasno definiranje obrazovnih profila nacionalnih predstavnika pri čemu je potrebno strateške i tehnološke vještine dopuniti upravljačkim, administrativnim i proračunskim vještinama.

4.9. U Prijedlogu je potrebno pojasniti kako će Centar moći intervenirati u koordinaciji financiranja programa Digitalna Europa i Obzor Europa, o čemu se i dalje pregovara, te, prije svega, u skladu s kojim će se smjernicama obavljati javna nabava i dodjeljivati javni ugovori. Taj je aspekt nužan kako bi se izbjegla udvostručavanja ili preklapanja. Osim toga, kako bi se povećala financijska omotnica, preporučuje se proširenje sinergija s drugim financijskim instrumentima EU-a (npr. regionalnim fondovima, strukturnim fondovima, CEF-om, ERF-om, InvestEU-om…). Odbor se nada da će Mreža nacionalnih centara biti uključena u upravljanje i koordinaciju fondova.

([7]) SL C 227, 28.6.2018., str. 86.
([8]) SL C 227, 28.6.2018., str. 86.
([9]) COM(2017) 294.

4.10. EGSO napominje da bi Savjetodavni odbor trebao imati 16 članova te da se ne navode mehanizmi uz pomoć kojih bi se trebalo doprijeti do poslovnog sektora, sveučilišta, istraživačkog sektora i potrošača. Odbor smatra da bi bilo korisno i prikladno da članovi tog odbora posjeduju visoku razinu znanja na tom polju te da na uravnotežen način predstavljaju različite relevantne sektore.

4.11. EGSO smatra da je važno utvrditi načine suradnje i odnose Europskog centra i nacionalnih centara. Nadalje, važno je da se nacionalni centri financiraju sredstvima EU-a, barem kad je riječ o administrativnim troškovima, te da se time olakša administrativna i stručna usklađenost kako bi se smanjio jaz među europskim državama.

4.12. U skladu sa svojim prethodnim mišljenjima ([10]), EGSO ističe važnost osiguravanja visokokvalitetnog obrazovanja i osposobljavanja ljudskih resursa u području kibersigurnosti, među ostalim putem posebnih obrazovnih, sveučilišnih i poslijediplomskih programa. Osim toga, važno je pružiti i odgovarajuću financijsku potporu MSP-ovima te novoosnovanim poduzećima iz tog sektora ([11]) koji su ključni za razvoj suvremenih istraživanja.

4.13. EGSO smatra da je od presudne važnosti pojasniti područja nadležnosti i granice između mandata Centra i ENISA-e, a pritom jasno utvrditi načine njihove suradnje i uzajamne potpore te izbjeći preklapanje nadležnosti i udvostručavanje napora ([12]). Prijedlogom uredbe predviđa se prisutnost izaslanika Agencije Europske unije za mrežnu i informacijsku sigurnost kao stalnog promatrača u Upravnom odboru, ali njegova nazočnost ne jamči strukturirani dijalog između ta dva tijela. Slični problemi postoje u pogledu drugih tijela za kibersigurnost, kao što su EDA, Europol i CERT-EU. U tom je smislu zanimljiv memorandum o razumijevanju koji je potpisan u svibnju 2018. između ENISA-e, EDA-e, Europol-a i CERT-EU-a.

Bruxelles, 23. siječnja 2019.

Predsjednik
Europskog gospodarskog i socijalnog odbora
Luca JAHIER

([10]) SL C 451, 16.12. 2014., str. 25.
([11]) SL C 227, 28.6.2018., str. 86.
([12]) SL C 227, 28.6.2018., str. 86.