Mnenje Evropskega ekonomsko-socialnega odbora – Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov

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

(2019/C 159/10)

Poročevalec: **Antonio LONGO**

Soporočevalec: **Alberto MAZZOLA**

Zaprosilo	Evropski svet, 5. 10. 2018 Evropski parlament, 1. 10. 2018
Pravna podlaga	tretji odstavek člena 173 ter člena 188 in 304 Pogodbe o delovanju Evropske unije
Pristojnost	strokovna skupina za promet, energijo, infrastrukturo in informacijsko družbo
Datum sprejetja mnenja strokovne skupine	9. 1. 2019
Datum sprejetja na plenarnem zasedanju	23. 1. 2019
Plenarno zasedanje št.	540
Rezultat glasovanja (za/proti/vzdržani)	143/5/2

1. Sklepi in priporočila

1.1 Evropski ekonomsko-socialni odbor (EESO) odobrava pobudo Komisije in meni, da je bistvena za razvoj industrijske strategije za kibernetsko varnost ter da pomeni strateško potezo za dosego dobre in obširne digitalne neodvisnosti. Ta dejavnika sta nujna za okrepitev evropskih obrambnih mehanizmov pred novo kibernetsko vojno, ki lahko ogrozi politične, gospodarske in družbene sisteme.

1.2 EESO ugotavlja, da so vse strategije za kibernetsko varnost neločljivo povezane z ozaveščenostjo in varnim ravnanjem vseh uporabnikov.

1.3 EESO se strinja s splošnimi cilji predloga in se zaveda, da bodo posebni vidiki delovanja analizirani pozneje. Ker pa gre za uredbo, meni, da bi bilo treba vnaprej opredeliti občutljive vidike, povezane z upravljanjem, financiranjem in doseganjem vnaprej določenih ciljev. Pomembno je, da prihodnja mreža in center čim bolj temeljita na kibernetskem in strokovnem znanju držav članic in da niso vse pristojnosti skoncentrirane v novem centru. Preprečiti je treba tudi prekrivanje področja delovanja prihodnje mreže in centra z obstoječimi mehanizmi in organi sodelovanja.

1.4 EESO podpira razširitev sodelovanja na industrijo na podlagi trdnih zavez glede znanosti in naložb z njeno prihodnjo vključitvijo v upravni odbor. V primeru tristranskega sodelovanja med Evropsko komisijo, državami članicami in industrijo bi bilo treba prisotnost podjetij iz tretjih držav omejiti na tista, ki so že dolgo na evropskem ozemlju in se v celoti vključujejo v evropsko tehnološko in industrijsko bazo, če se zanje uporabljajo ustrezni mehanizmi pregledovanja in nadzora ter če spoštujejo načelo vzajemnosti in obveznost zaupnosti.

1.5 Za kibernetsko varnost si morajo skupaj prizadevati vse države članice, ki morajo zato sodelovati v upravnem odboru; načini za to se šele določijo. Njihov finančni prispevek bi se lahko črpal iz evropskih sredstev, dodeljenih vsaki državi članici.

1.6 V predlogu bi moralo biti bolje pojasnjeno, na kakšen način naj bi bil strokovni center vključen v usklajevanje financiranja iz programa za digitalno Evropo in programa Obzorje Evropa ter zlasti po katerih smernicah se bodo pripravljala in dodeljevala morebitna javna naročila. Ta vidik je ključnega pomena za preprečevanje podvajanj ali prekrivanj. Poleg tega je za povečanje finančnih sredstev priporočljivo razširiti sinergije z drugimi finančnimi instrumenti EU (npr. regionalnimi skladi, strukturnimi skladi, instrumentom za povezovanje Evrope, Evropskim obrambnim skladom, programom InvestEU itd.).

1.7 EESO meni, da je nujno treba opredeliti načine sodelovanja ter odnose med evropskim strokovnim centrom in nacionalnimi centri. Poleg tega je pomembno, da EU nacionalnim centrom zagotovi financiranje vsaj za upravne stroške, s čimer bi olajšali usklajevanje upravnih zadev in kompetenc, da se zmanjša obstoječa vrzel med evropskimi državami.

1.8 Odbor poudarja, da je človeški kapital pomemben, in želi, da bi lahko strokovni center v sodelovanju z univerzami, raziskovalnimi centri in visokošolskimi izobraževalnimi ustanovami promoviral izobraževanje in usposabljanje na ravni odličnosti, tudi s posebnimi univerzitetnimi in srednješolskimi učnimi programi. Hkrati je bistveno, da se zagotovi posebna podpora zagonskim podjetjem in MSP.

1.9 EESO meni, da je nujno treba bolje razjasniti področja pristojnosti ter ločnice med nalogami strokovnega centra in Agencije Evropske unije za varnost omrežij in informacij (ENISA), pri čemer je treba jasno opredeliti način sodelovanja in vzajemne podpore ter se izogniti prekrivanju pristojnosti in podvajanju prizadevanj. Podobne težave se pojavljajo pri drugih organih, ki se ukvarjajo s kibernetsko varnostjo, kot so agencija EDA, Europol ter CERT-EU. Priporočljivo bi bilo, da se uvedejo podobni mehanizmi za strukturirani dialog med različnimi subjekti.

2. **Sedanji okvir za kibernetsko varnost**

2.1 Kibernetska varnost je ena prednostnih tematik za EU, saj je nepogrešljiva pri obrambi ustanov, podjetij in državljanov, potrebna pa je tudi za ohranjanje demokracije. Med najbolj skrb zbujajočimi pojavi je eksponentna rast zlonamerne programske opreme, ki se širi po omrežju prek samodejnih sistemov. Leta 2007 je bilo takih primerov 130000, leta 2017 pa že 8 milijonov. Poleg tega je Unija neto uvoznica izdelkov in rešitev za kibernetsko varnost, kar povzroča težave pri gospodarski konkurenčnosti ter civilni in vojaški varnosti.

2.2 Čeprav ima EU na voljo pomembno strokovno znanje in izkušnje na področju kibernetske varnosti, so industrija, univerze in raziskovalni centri še vedno razdrobljeni, neusklajeni in brez skupne strategije razvoja, saj ustrezni sektorji, povezani s področjem kibernetske varnosti (npr. energija, vesolje, obramba, promet), niso dovolj podprti, prav tako pa niso izkoriščene niti sinergije med sektorji civilne in vojaške kibernetske varnosti.

2.3 Za spoprijemanje z vse večjimi izzivi je Evropska unija v letu 2013 pripravila strategijo za kibernetsko varnost za spodbujanje zanesljivega, varnega in odprtega kibernetskega okolja ([1]). Nato je v letu 2016 sprejela prve posebne ukrepe za varnost omrežij in informacijskih sistemov ([2]). To je privedlo do javno-zasebnega partnerstva na področju kibernetske varnosti.

2.4 V letu 2017 je bilo v sporočilu z naslovom Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU ([3]) ugotovljeno, da je treba zagotoviti ohranitev in razvoj pomembne ključne tehnološke zmogljivosti kibernetske varnosti za zavarovanje enotnega digitalnega trga ter zlasti za zaščito kritičnih omrežij in informacijskih sistemov ter zagotavljanje ključnih storitev kibernetske varnosti.

([1]) JOIN(2013) 1 final.
([2]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).
([3]) JOIN(2017) 450 final.

2.5 Zato mora biti Unija sposobna zaščititi svoja digitalna sredstva in procese ter konkurirati na svetovnem trgu kibernetske varnosti, dokler ni dosežena dobra in obširna digitalna neodvisnost ([4]).

3. Predlog Komisije

3.1 Cilj evropskega strokovnega centra bo lajšanje in pomoč pri koordiniranju dela mreže nacionalnih koordinacijskih centrov ter opravljanje vloge referenčne točke za strokovno skupnost za kibernetsko varnost ob hkratnem spodbujanju tehnološke agende na področju kibernetske varnosti in lajšanju dostopa do zbranega strokovnega znanja.

3.2 To bo opravljal zlasti z izvajanjem zadevnih delov programa za digitalno Evropo in programa Obzorje Evropa ter z dodeljevanjem nepovratnih sredstev in javnimi naročili. Glede na precejšnje naložbe v kibernetsko varnost drugod po svetu in glede na potrebo po usklajevanju in združevanju virov s tega področja v Evropi se predlaga, da ima strokovni center obliko evropskega partnerstva z dvojno pravno podlago, kar bo lajšalo skupne naložbe Unije, držav članic in/ali industrije.

3.3 Predlog predvideva, da države članice k ukrepom strokovnega centra in mreže prispevajo sorazmeren znesek. Finančni prispevek EU znaša približno 2 milijardi EUR iz programa za digitalno Evropo, znesek iz programa Obzorje Evropa je treba še določiti, skupni prispevek držav članic pa bo vsaj enak prispevku Unije.

3.4 Glavni organ odločanja je upravni odbor, v katerem sodelujejo vse države članice, glasovalno pravico pa imajo samo tiste, ki k strokovnemu centru finančno prispevajo. Sistem glasovanja v upravnem odboru sledi načelu dvojne večine, ki zahteva 75 % finančnih prispevkov in 75 % glasov. Komisija ima 50 % glasov. Strokovnemu centru pomaga industrijsko-znanstveni svetovalni odbor, ki zagotavlja reden dialog s podjetji, potrošniki in drugimi ustreznimi zainteresiranimi stranmi.

3.5 V tesnem sodelovanju z mrežo nacionalnih koordinacijskih centrov in strokovno skupnostjo za kibernetsko varnost bi bil strokovni center glavni izvedbeni organ za finančna sredstva EU, namenjena kibernetski varnosti v okviru predlaganih programov za digitalno Evropo in Obzorje Evropa.

3.6 Nacionalne koordinacijske centre morajo določiti države članice. Imeti bi morali tehnološko strokovno znanje s področja kibernetske varnosti ali pa neposreden dostop do takšnega znanja, zlasti na področjih, kot so kriptografija, varnostne storitve IKT, samodejno zaznavanje vdorov, varnost sistemov in omrežij, varnost programske opreme in aplikacij ter človeški in družbeni vidiki varnosti in zasebnosti. Prav tako bi morali imeti zmogljivost, da učinkovito sodelujejo in se usklajujejo z industrijo in javnim sektorjem, vključno z organi, imenovanimi v skladu z Direktivo (EU) 2016/1148.

4. Splošne ugotovitve

4.1 EESO odobrava pobudo Komisije in meni, da je strateškega pomena za razvoj kibernetske varnosti, kar je v skladu z odločitvijo, sprejeto na vrhu v Talinu septembra 2017. Tam so voditelji držav in vlad pozvali Unijo, naj postane „*do leta 2025 vodilna v svetu na področju kibernetske varnosti, da se zagotovijo zaupanje, gotovost in zaščita državljanov, potrošnikov in podjetij na spletu ter omogoči brezplačen in zakonsko urejen internet*“.

4.2 EESO poudarja, da smo pred pravo kibernetsko vojno, ki grozi, da bo oslabila politične, gospodarske in družbene sisteme z napadi na informacijske sisteme ustanov, kritično infrastrukturo (energetika, promet, banke, finančne ustanove itd.) in podjetja ter z vplivanjem na volilne in demokratične procese na splošno z ustvarjanjem lažnih novic ([5]). To pa zahteva veliko ozaveščenost ter odločen in pravočasen odziv. Zato je treba vzpostaviti jasno in dobro podprto industrijsko politiko za kibernetsko varnost kot nepogrešljiv in osnoven pogoj za dosego digitalne neodvisnosti. EESO meni, da bi delovni program moral dati prednost sektorjem, določenim v Direktivi (EU) 2016/1148, ki se uporablja za javna in zasebna podjetja, ki zagotavljajo osnovne storitve, zaradi njihovega pomena za družbo ([6]).

([4]) UL C 227, 28.6.2018, str. 86.
([5]) Informativno poročilo o vplivu na socialne in politične procese v EU in državah vzhodnega sosedstva prek medijev, Indrė Vareikytė, 2014.
([6]) UL C 227, 28.6.2018, str. 86.

4.3 EESO ugotavlja, da so vse strategije za kibernetsko varnost neločljivo povezane z ozaveščenostjo in varnim ravnanjem vseh uporabnikov. Zato morajo vsako tehnološko pobudo spremljati ustrezne kampanje za informiranje in ozaveščanje, da bi se ustvarila „kultura digitalne varnosti“ ([7]).

4.4 EESO se strinja s splošnimi cilji predloga in se zaveda, da bodo posebni vidiki delovanja analizirani pozneje. Ker pa gre za uredbo, meni, da bi bilo treba vnaprej opredeliti občutljive vidike, povezane z upravljanjem, financiranjem in doseganjem vnaprej določenih ciljev. Pomembno je, da prihodnja mreža in center čim bolj temeljita na kibernetskem in strokovnem znanju držav članic in da niso vse pristojnosti skoncentrirane v novem centru. Preprečiti je treba tudi prekrivanje področij delovanja prihodnje mreže in centra z obstoječimi mehanizmi in organi sodelovanja.

4.5 EESO opozarja, da je v svojem mnenju TEN/646 o uredbi o kibernetski varnosti ([8]) predlagal tristransko sodelovanje v obliki javno-zasebnega partnerstva med Evropsko komisijo, državami članicami in industrijo, vključno z malimi in srednjimi podjetji, medtem ko je trenutna struktura, katere pravno obliko je treba poglobiti, v bistvu javno-javno partnerstvo med Evropsko komisijo in državami članicami.

4.6 EESO podpira razširitev sodelovanja na industrijo na podlagi trdnih zavez glede znanosti in naložb z njeno prihodnjo vključitvijo v upravni odbor. Oblikovanje industrijsko-znanstvenega svetovalnega odbora morda ne bo zagotovilo rednega dialoga med podjetji, potrošniki in drugimi ustreznimi zainteresiranimi stranmi. V novem okviru, ki ga je oblikovala Evropska komisija, tudi ni jasno, kakšno vlogo bo imela Evropska organizacija za kibernetsko varnost, ki je bila ustanovljena junija 2016 na pobudo Evropske komisije in je njena nasprotna stran. Kapitala, ki ga ima ta organizacija glede omrežja in znanja, se ne bi smelo zanemariti.

4.6.1 V primeru tristranskega sodelovanja je pomembno pozornost nameniti vprašanju podjetij iz tretjih držav. EESO zlasti poudarja, da bi moralo tako sodelovanje temeljiti na trdnem mehanizmu za preprečevanje prisotnosti podjetij iz tretjih držav, ki bi lahko ogrozila varnost in avtonomijo Unije. Pri tem bi se morale uporabljati povezane določbe, opredeljene v evropskem programu za razvoj obrambne industrije ([9]).

4.6.2 EESO hkrati priznava, da bi lahko bila nekatera podjetja iz tretjih držav, ki so že dolgo na evropskem ozemlju in se v celoti vključujejo v evropsko tehnološko in industrijsko bazo, zelo koristna za projekte EU. Zato bi se jim lahko omogočil dostop do teh projektov, če bi države članice vzpostavile ustrezne mehanizme pregledovanja in nadzora teh podjetij ter če bi ta podjetja spoštovala načelo vzajemnosti in obveznost zaupnosti.

4.7 Za kibernetsko varnost si morajo skupaj prizadevati vse države članice, ki morajo zato sodelovati v upravnem odboru; načini za to se šele določijo. Pomembno je tudi, da vse države finančno in na ustrezen način prispevajo k pobudi Komisije. Njihov finančni prispevek bi se lahko črpal iz sredstev EU, dodeljenih vsaki državi članici.

4.8 EESO se strinja, da lahko vsaka država članica sama imenuje svojega predstavnika v upravnem odboru evropskega strokovnega centra. Priporoča jasno opredelitev profilov izobrazbe nacionalnih predstavnikov s kombinacijo strateškega in strokovnega znanja ter znanja v zvezi z vodenjem, upravljanjem in proračunom.

4.9 V predlogu bi moralo biti bolje pojasnjeno, na kakšen način naj bi bil strokovni center vključen v usklajevanje financiranja iz programa za digitalno Evropo in programa Obzorje Evropa, o katerem še vedno potekajo pogajanja, ter zlasti po katerih smernicah se bodo pripravljala in dodeljevala morebitna javna naročila. Ta vidik je ključnega pomena za preprečevanje podvajanj ali prekrivanj. Poleg tega je za povečanje finančnih sredstev priporočljivo razširiti sinergije z drugimi finančnimi instrumenti EU (npr. regionalnimi skladi, strukturnimi skladi, instrumentom za povezovanje Evrope, Evropskim obrambnim skladom, programom InvestEU itd.). EESO upa, da bo mreža nacionalnih koordinacijskih centrov vključena v upravljanje in koordinacijo sredstev.

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

4.10 EESO ugotavlja, da naj bi svetovalni odbor imel 16 članov in da niso določeni mehanizmi, s katerimi bi se vanj pritegnili predstavniki podjetij, univerz, raziskovalcev in potrošnikov. Po mnenju EESO bi bilo koristno in primerno zagotoviti, da člani svetovalnega odbora izstopajo z velikim poznavanjem tega področja in da uravnoteženo zastopajo različne vpletene sektorje.

4.11 EESO meni, da je treba opredeliti načine sodelovanja ter odnose med evropskim strokovnim centrom in nacionalnimi centri. Poleg tega je pomembno, da EU nacionalnim centrom zagotovi financiranje vsaj za upravne stroške, s čimer bi olajšali usklajevanje upravnih zadev in kompetenc, da se zmanjša obstoječa vrzel med evropskimi državami.

4.12 EESO v skladu s svojimi prejšnjimi mnenji ([10]) poudarja pomen usposabljanja človeških virov na ravni odličnosti na področju kibernetske varnosti, tudi v okviru posebnih srednješolskih, dodiplomskih in podiplomskih programov. Zagotoviti je treba ustrezno finančno podporo za mala, srednja in zagonska podjetja v tem sektorju ([11]), ki so ključna za razvoj vodilnih raziskovalnih dejavnosti.

4.13 EESO meni, da je nujno treba bolje razjasniti področja pristojnosti ter ločnice med nalogami strokovnega centra in agencije ENISA, pri čemer je treba jasno opredeliti način sodelovanja in vzajemne podpore ter se izogniti prekrivanju pristojnosti in podvajanju prizadevanj ([12]). Predlog uredbe predvideva prisotnost predstavnika agencije ENISA kot stalnega opazovalca v upravnem odboru, vendar pa to ne daje jamstva za strukturirani dialog med organoma. Podobne težave se pojavljajo pri drugih organih, ki se ukvarjajo s kibernetsko varnostjo, kot so agencija EDA, Europol in CERT-EU. V zvezi s tem je pomemben memorandum o soglasju, ki so ga maja 2018 podpisale agencija ENISA, agencija EDA, Europol in CERT-EU.

V Bruslju, 23. januarja 2019

Predsednik
Evropskega ekonomsko-socialnega odbora
Luca JAHIER

([10]) UL C 451, 16.12.2014, str. 25.
([11]) UL C 227, 28.6.2018, str. 86.
([12]) UL C 227, 28.6.2018, str. 86.