

Bruselj, 8. oktober 2021
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

DOPIS O TOČKI POD „I/A“

Pošiljatelj:	Generalni sekretariat Sveta
Prejemnik:	Odbor stalnih predstavnikov (2. del)/Svet
Zadeva:	Sklepi Sveta o preučitvi potenciala pobude za skupno kibernetško enoto – dopolnjevanje usklajenega odziva EU na velike kibernetške incidente in krize – odobritev

1. Komisija je 23. junija 2021 objavila priporočilo o vzpostavitvi skupne kibernetške enote¹ za obravnavanje naraščajočega števila hudih kibernetških incidentov, ki vplivajo na javne storitve ter življenje podjetij in državljanov po vsej Evropski uniji.
2. Komisija je priporočilo predstavila na seji Horizontalne delovne skupine za kibernetška vprašanja 28. junija 2021. Med slovenskim predsedovanjem so na sejah Horizontalne delovne skupine za kibernetška vprašanja 7. in 14. julija 2021 potekale nadaljnje razprave, da bi se zbrala mnenja držav članic o priporočilu Komisije.

¹ C(2021) 4520 final (11155/21 in 11155/21 ADD1).

3. Predsedstvo je na neformalni videokonferenci Horizontalne delovne skupine za kibernetika vprašanja 23. julija 2021 predstavilo prvi osnutek sklepov Sveta o preučitvi potenciala pobude za skupno kibernetiko enoto – dopolnjevanje usklajenega odziva EU na velike kibernetike incidente in krize². O tem osnutku sklepov je Horizontalna delovna skupina za kibernetika vprašanja podrobneje razpravljala na sejah 8. in 29. septembra 2021.
4. Horizontalna delovna skupina za kibernetika vprašanja je na seji 6. oktobra 2021 dosegla dogovor o priloženem osnutku sklepov Sveta.
5. Glede na navedeno naj Odbor stalnih predstavnikov priloženi osnutek sklepov Sveta predloži Svetu in mu predlaga, da te sklepe sprejme kot točko pod „A“ dnevnega reda.

² 10975/21.

**Osnutek sklepov Sveta o preučitvi potenciala pobude za skupno kibernetško enoto –
dopolnjevanje usklajenega odziva EU na velike kibernetške incidente in krize**

SVET EVROPSKE UNIJE –

OB OPOZARJANJU na svoje sklepe:

- o strategiji EU za kibernetško varnost v digitalnem desetletju³,
- o usklajenem odzivu EU na velike kibernetške incidente in krize⁴,
- o kibernetški diplomaciji⁵,
- o okviru za skupen diplomatski odziv EU na zlonamerne kibernetške dejavnosti („zbirka orodij za kibernetško diplomacijo“)⁶,
- o varnosti in obrambi⁷,
- o okviru EU za politiko kibernetške obrambe⁸,
- o oblikovanju digitalne prihodnosti Evrope⁹,
- Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize,

³ 7290/21.
⁴ 10086/18.
⁵ 6122/15 + COR 1.
⁶ 10474/17.
⁷ 8396/21.
⁸ 15585/14.
⁹ 8711/20.

- o Skupnem sporočilu Evropskemu parlamentu in Svetu: „Odpornost, odvracanje in obramba: okrepitev kibernetске varnosti za EU“¹⁰,
 - o krepitvi zmogljivosti in zmožnosti na področju kibernetске varnosti v EU¹¹,
1. OPOZARJA na pomen kibernetске varnosti pri vzpostavljanju odporne, digitalne in zelene Evrope. POUDARJA, da je kibernetска varnost nepogrešljiva za blaginjo in varnost EU ter njenih držav članic, državljanov, podjetij in institucij ter za ohranjanje integritete naših svobodnih in demokratičnih družb.
 2. Se ZAVEDA čezmejnega in medsektorskega značaja mnogih kibernetских groženj ter tveganj in možnih posledic kontinuiranih kampanj z bolj učinkovitimi, izpopolnjenimi, ciljno usmerjenimi, kompleksnimi, trdovratnimi in/ali vsesplošnimi zlonamernimi kibernetскими dejavnostmi¹². Pandemija COVID-19 je naše družbe še dodatno izpostavila nevarnostim škode, ki jo veliki kibernetски incidenti lahko povzročijo gospodarstvu, demokraciji, osnovnim storitvam in kritični infrastrukturi, zlasti v zdravstvenem sektorju. Povečala sta se tudi pomen povezljivosti in odvisnost družbe od zanesljivih in varnih omrežij ter informacijskih sistemov. Naposled pa se je tudi izkazalo, da potrebujemo globalen, odprt, brezplačen, stabilen in varen internet ter da moramo zaupati izdelkom, procesom in storitvam informacijske in komunikacijske tehnologije, ki morajo biti varni, poleg tega pa je treba zagotoviti odporne dobavne verige.

¹⁰ 14435/17 + COR 1.

¹¹ 7737/19.

¹² Poročilo agencije ENISA o naravi groženj, 2020.

3. Ponovno OPOZARJA na pomen kibernetске odpornosti in nadaljnega razvoja okvira EU za krizno upravljanje kibernetске varnosti¹³, katerega cilj je učinkovit in pravočasen odziv na velike kibernetске incidente in krize na ravni EU, ter njegovega nadaljnega vključevanja v obstoječe horizontalne in sektorske mehanizme EU za odzivanje na krize. POUDARJA vlogo Sveta in enotne ureditve za politično odzivanje na krize (IPCR) pri zagotavljanju pravočasnega usklajevanja in odziva na politični ravni Unije na krize, ki imajo daljnosežne učinke ali politično težo in ne glede na to, ali izvirajo iz Unije ali zunaj nje. OPOZARJA, da je treba take okvire in mehanizme preizkušati na rednih vajah.
4. OPOZARJA, da dejavnosti na ravni EU glede velikih kibernetских incidentov in kriz potekajo v skladu z načeli subsidiarnosti, sorazmernosti, dopolnjevanja, izogibanja podvajanju in zaupnosti. Ponovno POUDARJA, da je odzivanje na velike kibernetске incidente in krize, ki so jih utrpele, predvsem naloga držav članic. OPOZARJA, da je treba spoštovati pristojnost in izključno odgovornost držav članic za nacionalno varnost v skladu s členom 4(2) Pogodbe o Evropski uniji, tudi na področju kibernetске varnosti.
5. Hkrati OPOZARJA, da je treba spoštovati pristojnost in pooblastila institucij, organov in agencij EU. Visoki predstavnik, Komisija ter druge institucije, organi in agencije EU imajo prav tako bistveno vlogo, utemeljeno v pravu Unije, saj imajo lahko veliki kibernetски incidenti in krize posledice tudi za enotni trg ter za delovanje samih institucij, organov in agencij EU.

¹³ 10086/18.

6. POUDARJA, da se je treba pri nadaljnjem razvoju okvira EU za krizno upravljanje kibernetске varnosti izogibati nepotrebnemu podvajanju ter si prizadevati za dopolnjevanje in dodano vrednost, poleg tega pa mora biti okvir usklajen z obstoječimi mehanizmi, pobudami, mrežami, procesi in postopki na nacionalni in evropski ravni. OPOZARJA na pomen racionalizacije in zmanjšanja zapletenosti obstoječih procesov in struktur, zaradi potrebe po koheziji v Uniji pa tudi izboljšati dostopnost in odzivnost za tiste, ki iščejo pomoč in solidarnost.
7. PRIZNAVA veljavnost mednarodnega prava, vključno s celotno Ustanovno listino Združenih narodov, mednarodnega humanitarnega prava in prava človekovih pravic v kibernetском prostoru, ter SPODBUJA spoštovanje prostovoljnih, nezavezujočih norm, pravil in načel odgovornega ravnanja držav v kibernetском prostoru, ki so jih podprle vse države članice ZN.
8. POZDRAVLJA napredek, ki je bil v zadnjih letih dosežen v Svetu, zlasti v Horizontalni delovni skupini za kibernetска vprašanja in drugih ustreznih delovnih skupinah Sveta, pa tudi pri oblikovanju drugih pobud, mrež in mehanizmov za sodelovanje in izmenjavo informacij med državami članicami, zlasti Skupine za sodelovanje na področju varnosti omrežij in informacij ter mreže skupin CSIRT, vzpostavljenih z Direktivo (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016, organizacijske mreže za povezovanje v kibernetски krizi (CyCLONe) ter ustreznih projektov v zvezi s kibernetско obrambo v okviru stalnega strukturnega sodelovanja (PESCO)¹⁴, skupne projektne skupine za kibernetски kriminal (J-CAT), Evropske pravosodne mreže za kibernetско kriminaliteto in prostovoljnih prispevkov držav članic za Obveščevalni in situacijski center EU (EU INTCEN), pa tudi pri usklajevanju in sodelovanju pri zbirki orodij za kibernetско diplomacijo.

¹⁴ Zlasti „enot za hitro odzivanje na kibernetске grožnje in medsebojne pomoči na področju kibernetске varnosti“, ki jih usklajuje Litva, „centra za usklajevanje na kibernetском in informacijskem področju“, ki ga usklajuje Nemčija, in „platforme za izmenjavo informacij v zvezi s kibernetскими grožnjami in odzivanjem na incidente“, ki jo usklajuje Grčija.

9. OPOZARJA na obstoječe okvire za sodelovanje med institucijami, organi in agencijami EU, kot je strukturirano sodelovanje med agencijo ENISA in skupino CERT-EU, ter na memorandum o soglasju med agencijo ENISA, Evropsko obrambno agencijo (EDA), Europolovim centrom za boj proti kibernetiski kriminaliteti (EC3) in skupino CERT-EU. OPOZARJA, da je potrebna redna izmenjava informacij s Svetom o nadaljnjem razvoju teh okvirov sodelovanja.
10. POUDARJA, da je treba okrepiti sodelovanje in izmenjavo informacij med različnimi kibernetiskimi skupnostmi v EU in njenih državah članicah na vseh potrebnih ravneh – tehnični, operativni in strateški/politični – ter povezati obstoječe mehanizme, omrežja, strukture, procese in postopke kriznega upravljanja, kadar to pomaga pri obvladovanju velikih kibernetiskih incidentov in kriz in ga izboljšuje.
11. JE SEZNANJEN z napredkom skupine držav članic pri oblikovanju skupnih operativnih kibernetiskih zmogljivosti „enot za hitro odzivanje na kibernetiske grožnje“ v okviru PESCO, katerih cilj je poglobiti prostovoljno sodelovanje na kibernetiskem področju prek medsebojne pomoči, vključno z odzivom na velike kibernetiske incidente in krize.
12. PRIZNAVA izkušnje in zmožnost stalnega odzivanja (24 ur na dan in vse dni v tednu) skupnosti organov kazenskega pregona na področju operativnega sodelovanja in varne izmenjave informacij v primeru večjih čezmejnih kibernetiskih napadov prek protokola EU za odzivanje organov kazenskega pregona na izredne razmere.

13. UGOTAVLJA, da se okvir za skupen diplomatski odziv EU na zlonamerne kibernetike dejavnosti („zbirka orodij za kibernetiko diplomacijo“) še naprej izvaja. OPOZARJA, da lahko vsaka država članica sama za vsak primer posebej sprejme suvereno odločitev v zvezi s pripisovanjem odgovornosti za zlonamerne kibernetike dejavnosti. OPOZARJA, da bi morali ukrepi, sprejeti v okviru skupnega diplomatskega odziva EU na zlonamerne kibernetike dejavnosti, temeljiti na skupnem situacijskem zavedanju, usklajenem med državami članicami. Obveščevalni in situacijski center EU (EU INTCEN) ima osrednjo vlogo kot središče za spremljanje razmer in ocene groženj v zvezi s kibernetiskimi vprašanji v EU na podlagi prostovoljnih obveščevalnih prispevkov držav članic in brez poseganja v njihove pristojnosti.
14. PONOVRNO POUDARJA pomen vzajemne pomoči in solidarnosti v skladu s členom 42(7) Pogodbe o Evropski uniji in členom 222 Pogodbe o delovanju Evropske unije ter POZIVA k nadaljnjim vajam s kibernetiko razsežnostjo. OPOZARJA, da je treba razmisliti o povezovanju med okvirom EU za krizno upravljanje kibernetike varnosti, naborom orodij za kibernetiko diplomacijo in določbami navedenih členov v primeru velikega kibernetikega incidenta ali krize. OPOZARJA, da obveznosti držav članic, ki izhajajo iz člena 42(7) Pogodbe o Evropski uniji, ne posegajo v posebno naravo varnostne in obrambne politike posameznih držav članic. OPOZARJA tudi, da Nato ostaja temelj kolektivne obrambe držav, ki so njegove članice.
15. JE SEZNANJEN s sodelovanjem med EU in Natom na področju kibernetike varnosti in obrambe, vključno z izmenjavo informacij med CERT-EU in zmogljivostjo Nata za odzivanje na računalniške incidente (NCIRC), ob polnem spoštovanju načel preglednosti, vzajemnosti in vključenosti ter avtonomije odločanja obeh organizacij.

16. SE ZAVEDA pomena sodelovanja – po potrebi – z zasebnim sektorjem v smislu izmenjave informacij in zagotavljanja ustreznega strokovnega znanja ter zanesljivih rešitev in storitev, na primer tudi pri podpiranju odzivanja na incidente in krepitvi situacijskega zavedanja med različnimi kibernetскими skupnostmi.
17. POUDARJA pomen varnih komunikacijskih kanalov za izmenjavo tajnih in občutljivih informacij. OPOZARJA, da je potreben nadaljnji napredek.

V zvezi s tem in ob upoštevanju navedenega:

18. PRIZNAVA, da je priporočilo Komisije o vzpostavitvi skupne kibernetске enote pobuda, ki bi jo bilo treba upoštevati pri nadaljnjem razvoju okvira EU za krizno upravljanje kibernetске varnosti¹⁵.
19. POZIVA EU in njene države članice, naj si še naprej prizadevajo za celovitejši in učinkovitejši okvir EU za krizno upravljanje kibernetске varnosti na podlagi obstoječih mehanizmov in že doseženega napredka ter pri tem upoštevajo potencial pobude za skupno kibernetско enoto, ki bi lahko – če bi k temu pristopili postopno – te mehanizme dopolnjevala. POUDARJA, da je postopen, pregleden in vključujoč proces bistvenega pomena za krepitev zaupanja ter je zato ključnega pomena za nadaljnji razvoj okvira EU za krizno upravljanje kibernetске varnosti. Pri tem procesu bi bilo treba upoštevati obstoječe vloge, pristojnosti in pooblastila držav članic ter institucij, organov in agencij EU, pa tudi načela iz teh sklepov, vključno s sorazmernostjo, subsidiarnostjo, vključevalnostjo, dopolnjevanjem, izogibanjem podvajanju in zaupnostjo informacij. Hkrati POUDARJA, da je vsakršno sodelovanje v morebitni skupni kibernetскими enoti ali prispevek držav članic k njej prostovoljne narave.

¹⁵ C(2021)4520 final (11155/21 in 11155/21 ADD1).

20. POUDARJA, da je treba uvesti ustrezne delovne metode in upravljanje, da bi lahko vse države članice sodelovale v razpravah in dejanskih postopkih odločanja o okviru EU za krizno upravljanje kibernetске varnosti ter pri njegovem razvoju, vključno z morebitno pobudo za skupno kibernetско enoto. POZIVA k spoštovanju pristojnosti Sveta v skladu s Pogodbama in načelom lojalnega sodelovanja.
21. OPOZARJA, da je treba identificirati in vključiti vse relevantne kibernetске skupnosti v EU in njenih državah članicah ter pri tem upoštevati različne vloge in odgovornosti, ki jih imajo v različnih vrstah velikih kibernetских incidentov in kriz. POUDARJA ključno vlogo Sveta, zlasti prek Horizontalne delovne skupine za kibernetска vprašanja (HWPCI), pri oblikovanju politik in usklajevanju nadaljnega razvoja okvira EU za krizno upravljanje kibernetске varnosti. Zato POZIVA države članice, Komisijo, Evropsko službo za zunanje delovanje (ESZD), EU INTCEN, CERT-EU, ENISA, Europol (EC3), Eurojust (EJCN), Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetско varnost (ECCC) ter predstavnike mreže skupin CSIRT, mreže CyCLONE, Skupine za sodelovanje na področju varnosti omrežij in informacij, EDA in relevantnih projektov v okviru PESCO ter druge morebitne deležnike, naj sodelujejo v tem procesu. Lahko bi podrobneje preučili možnost vzpostavitve delovne skupine, predlagane v priporočilu Komisije, ki bi – ob zagotovitvi ustrezne zastopanosti vseh držav članic in v skladu s političnimi smernicami Sveta – delovala kot začasni forum, ki bi združeval predstavnike vseh zadevnih kibernetских skupnosti v državah članicah in v EU. Taka delovna skupina bi morala redno poročati o svojih dejavnostih in Svetu predložiti morebitne predloge za razpravo, potrditev in nadaljnje smernice. Poleg tega bi lahko vzpostavili tudi druge oblike dialoga znotraj skupnosti in med njimi, vključno z delavnicami in seminarji ter skupnimi usposabljanji in vajami.

22. POUDARJA vlogo Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetško varnost (ECCC) ter mreže nacionalnih koordinacijskih centrov pri morebitni skupni enoti za kibernetško varnost, zlasti glede na vlogo, ki naj bi jo slednja imela, tj. da znatno poveča tehnološke zmogljivosti, tehnološke rešitve, zmogljivosti in veščine Unije na področju kibernetške varnosti.
23. POZIVA EU in njene države članice k sodelovanju pri nadaljnjem razvoju okvira EU za krizno upravljanje kibernetške varnosti, med drugim tako, da preučijo potencial pobude skupne kibernetške enote, določijo in opredelijo postopek, vključno z mejniki in časovnim načrtom, ter pojasnijo cilje in morebitne vloge in odgovornosti. POUDARJA, da je treba v prvi vrsti utrditi obstoječe mreže in interakcije znotraj posameznih skupnosti ter opraviti natančen pregled morebitnih vrzeli pri izmenjavi informacij v posameznih kibernetških skupnostih in med njimi, pa tudi v evropskih institucijah, organih in agencijah in med njimi, ter potreb na tem področju, nato pa se dogovoriti o možnih primarnih ciljih in prednostnih nalogah morebitne skupne kibernetške enote. Brez poseganja v zadevni izid POUDARJA, da se je treba osredotočiti na opredelitev potreb po izmenjavi informacij, da bi vzpostavili skupno situacijsko zavedanje med vsemi zadevnimi skupnostmi. Pri ugotavljanju vrzeli pri izmenjavi informacij in potreb na tem področju, vključno z morebitno uporabo virtualnih platform, bi bilo treba še naprej namenjati ustrezno pozornost varnim komunikacijskim kanalom za izmenjavo tajnih in občutljivih informacij, ob tem pa POUDARJATI, da je treba uporabljati že obstoječo infrastrukturo. Z uvedbo postopnega pristopa naj bi vzpostavili zaupanje in podlago za morebitne nadaljnje korake pri krepitvi pripravljenosti in operativnega sodelovanja. SE ZAVEDA, da bi lahko različni cilji upravičevali različne rešitve in sodelovanje različnih skupin predstavnikov zadevnih kibernetških skupnosti v EU in njenih državah članicah.

24. POZIVA k nadaljnemu razmisleku o pravni podlagi za morebitno skupno enoto za kibernetško varnost v celotnem procesu, vključno z oceno nalog in vlog glede na naloge in vloge, dodeljene agenciji ENISA v priporočilu ob upoštevanju člena 7 Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019. POZIVA k nadaljnemu razmisleku o posameznih elementih priporočila o skupni kibernetški enoti, tudi v zvezi z zamislijo o skupinah EU za hiter odziv na področju kibernetške varnosti ter načrtom odzivanja EU na kibernetške incidente in krize. POUDARJA, da mora morebitna skupna enota za kibernetško varnost spoštovati pristojnosti, mandate in pravna pooblastila morebitnih prihodnjih udeležencev.
25. POZIVA EU in njene države članice, naj preučijo potencial pobude skupne kibernetške enote, tudi z vidika institucij, organov in agencij EU, da bi dopolnili aktualna prizadevanja na ravni držav članic. POZDRAVLJA namero Komisije, da okrepi odpornost ustreznih institucij, organov in agencij EU s prihodnjim predlogom uredbe o skupnih zavezujočih pravilih o kibernetški varnosti za institucije, organe in agencije EU.
26. Na koncu PONOVRNO POUDARJA, da je zavezan krepitvi kibernetške odpornosti in nadaljnemu razvoju okvira EU za krizno upravljanje kibernetške varnosti, ter BO REDNO SPREMLJAL napredek in zagotavljal nadaljnje smernice za dopolnitev navedenega okvira.
-