Svet
Evropske unije

Bruselj, 20. oktober 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	19. oktober 2021
Prejemnik:	delegacije
Št. predh. dok.:	12534/21
Zadeva:	Sklepi Sveta o preučitvi potenciala pobude za skupno kibernetsko enoto – dopolnjevanje usklajenega odziva EU na velike kibernetske incidente in krize – sklepi Sveta (19. oktober 2021)

V prilogi vam pošiljamo sklepe Sveta o preučitvi potenciala pobude za skupno kibernetsko enoto – dopolnjevanje usklajenega odziva EU na velike kibernetske incidente in krize, ki jih je Svet sprejel na seji 19. oktobra 2021.

PRILOGA

Sklepi Sveta o preučitvi potenciala pobude za skupno kibernetsko enoto – dopolnjevanje usklajenega odziva EU na velike kibernetske incidente in krize

SVET EVROPSKE UNIJE –

OB OPOZARJANJU na svoje sklepe:

– o strategiji EU za kibernetsko varnost v digitalnem desetletju[1],

– o usklajenem odzivu EU na velike kibernetske incidente in krize[2],

– o kibernetski diplomaciji[3],

– o okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“)[4],

– o varnosti in obrambi[5],

– o okviru EU za politiko kibernetske obrambe[6],

– o oblikovanju digitalne prihodnosti Evrope[7],

– Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– o Skupnem sporočilu Evropskemu parlamentu in Svetu: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“[8],

– o krepitvi zmogljivosti in zmožnosti na področju kibernetske varnosti v EU[9],

1. OPOZARJA na pomen kibernetske varnosti pri vzpostavljanju odporne, digitalne in zelene Evrope. POUDARJA, da je kibernetska 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 kibernetskih groženj ter tveganj in možnih posledic kontinuiranih kampanj z bolj učinkovitimi, izpopolnjenimi, ciljno usmerjenimi, kompleksnimi, trdovratnimi in/ali vsesplošnimi zlonamernimi kibernetskimi dejavnostmi[10]. Pandemija COVID-19 je naše družbe še dodatno izpostavila nevarnostim škode, ki jo veliki kibernetski 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.

---

8 14435/17 + COR 1.
9 7737/19.
10 Poročilo agencije ENISA o naravi groženj, 2020.

3. Ponovno OPOZARJA na pomen kibernetske odpornosti in nadaljnjega razvoja okvira EU za krizno upravljanje kibernetske varnosti[11], katerega cilj je učinkovit in pravočasen odziv na velike kibernetske incidente in krize na ravni EU, ter njegovega nadaljnjega 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 kibernetskih incidentov in kriz potekajo v skladu z načeli subsidiarnosti, sorazmernosti, dopolnjevanja, izogibanja podvajanju in zaupnosti. Ponovno POUDARJA, da je odzivanje na velike kibernetske 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 kibernetske 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 kibernetski incidenti in krize posledice tudi za enotni trg ter za delovanje samih institucij, organov in agencij EU.

[11] 10086/18.

6. POUDARJA, da se je treba pri nadaljnjem razvoju okvira EU za krizno upravljanje kibernetske 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 kibernetskem prostoru, ter SPODBUJA spoštovanje prostovoljnih, nezavezujočih norm, pravil in načel odgovornega ravnanja držav v kibernetskem 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 kibernetska 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 kibernetski krizi (CyCLONe) ter ustreznih projektov v zvezi s kibernetsko obrambo v okviru stalnega strukturnega sodelovanja (PESCO)[12], skupne projektne skupine za kibernetski kriminal (J-CAT), Evropske pravosodne mreže za kibernetsko kriminaliteto in prostovoljnih prispevkov držav članic za Obveščevalni in situacijski center EU (EU INTCEN), pa tudi pri usklajevanju in sodelovanju pri zbirki orodij za kibernetsko diplomacijo.

[12] Zlasti „enot za hitro odzivanje na kibernetske grožnje in medsebojne pomoči na področju kibernetske varnosti“, ki jih usklajuje Litva, „centra za usklajevanje na kibernetskem in informacijskem področju“, ki ga usklajuje Nemčija, in „platforme za izmenjavo informacij v zvezi s kibernetskimi 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 kibernetski 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 kibernetskimi 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 kibernetskih incidentov in kriz in ga izboljšuje.

11. JE SEZNANJEN z napredkom skupine držav članic pri oblikovanju skupnih operativnih kibernetskih zmogljivosti „enot za hitro odzivanje na kibernetske grožnje“ v okviru PESCO, katerih cilj je poglobiti prostovoljno sodelovanje na kibernetskem področju prek medsebojne pomoči, vključno z odzivom na velike kibernetske 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 kibernetskih napadov prek protokola EU za odzivanje organov kazenskega pregona na izredne razmere.

13. UGOTAVLJA, da se okvir za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko 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 kibernetske dejavnosti. OPOZARJA, da bi morali ukrepi, sprejeti v okviru skupnega diplomatskega odziva EU na zlonamerne kibernetske 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 kibernetskimi vprašanji v EU na podlagi prostovoljnih obveščevalnih prispevkov držav članic in brez poseganja v njihove pristojnosti.

14. PONOVNO 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 kibernetsko razsežnostjo. OPOZARJA, da je treba razmisliti o povezovanju med okvirom EU za krizno upravljanje kibernetske varnosti, naborom orodij za kibernetsko diplomacijo in določbami navedenih členov v primeru velikega kibernetskega 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 kibernetske 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 kibernetskimi 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 kibernetske enote pobuda, ki bi jo bilo treba upoštevati pri nadaljnjem razvoju okvira EU za krizno upravljanje kibernetske varnosti[13].

19. POZIVA EU in njene države članice, naj si še naprej prizadevajo za celovitejši in učinkovitejši okvir EU za krizno upravljanje kibernetske varnosti na podlagi obstoječih mehanizmov in že doseženega napredka ter pri tem upoštevajo potencial pobude za skupno kibernetsko 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 kibernetske 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 kibernetski enoti ali prispevek držav članic k njej prostovoljne narave.

[13] 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 kibernetske varnosti ter pri njegovem razvoju, vključno z morebitno pobudo za skupno kibernetsko enoto. POZIVA k spoštovanju pristojnosti Sveta v skladu s Pogodbama in načelom lojalnega sodelovanja.

21. OPOZARJA, da je treba identificirati in vključiti vse relevantne kibernetske skupnosti v EU in njenih državah članicah ter pri tem upoštevati različne vloge in odgovornosti, ki jih imajo v različnih vrstah velikih kibernetskih incidentov in kriz. POUDARJA ključno vlogo Sveta, zlasti prek Horizontalne delovne skupine za kibernetska vprašanja (HWPCI), pri oblikovanju politik in usklajevanju nadaljnjega razvoja okvira EU za krizno upravljanje kibernetske 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 kibernetsko 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 kibernetskih 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 kibernetsko varnost (ECCC) ter mreže nacionalnih koordinacijskih centrov pri morebitni skupni enoti za kibernetsko 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 kibernetske varnosti.

23. POZIVA EU in njene države članice k sodelovanju pri nadaljnjem razvoju okvira EU za krizno upravljanje kibernetske varnosti, med drugim tako, da preučijo potencial pobude skupne kibernetske 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 kibernetskih 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 kibernetske 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 kibernetskih skupnosti v EU in njenih državah članicah.

24. POZIVA k nadaljnjemu razmisleku o pravni podlagi za morebitno skupno enoto za kibernetsko 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 nadaljnjemu razmisleku o posameznih elementih priporočila o skupni kibernetski enoti, tudi v zvezi z zamislijo o skupinah EU za hiter odziv na področju kibernetske varnosti ter načrtom odzivanja EU na kibernetske incidente in krize. POUDARJA, da mora morebitna skupna enota za kibernetsko varnost spoštovati pristojnosti, mandate in pravna pooblastila morebitnih prihodnjih udeležencev.

25. POZIVA EU in njene države članice, naj preučijo potencial pobude skupne kibernetske 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 kibernetski varnosti za institucije, organe in agencije EU.

26. Na koncu PONOVNO POUDARJA, da je zavezan krepitvi kibernetske odpornosti in nadaljnjemu razvoju okvira EU za krizno upravljanje kibernetske varnosti, ter BO REDNO SPREMLJAL napredek in zagotavljal nadaljnje smernice za dopolnitev navedenega okvira.