

Bruxelles, 20. listopada 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

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	19. listopada 2021.
Za:	Delegacije

Br. preth. dok.:	12534/21
Predmet:	Zaključci Vijeća o istraživanju potencijala inicijative o Zajedničkoj jedinici za kibersigurnost – dopuna koordiniranog odgovora EU-a na kiberincidente i kiberkrize velikih razmjera – zaključci Vijeća (19. listopada 2021.)

Za delegacije se u Prilogu nalaze Zaključci Vijeća o istraživanju potencijala inicijative o Zajedničkoj jedinici za kibersigurnost – dopuna koordiniranog odgovora EU-a na kiberincidente i kiberkrize velikih razmjera, kako ih je Vijeće usvojilo na sastanku održanom 19. listopada 2021.

**Zaključci Vijeća o istraživanju potencijala inicijative o Zajedničkoj jedinici za kibersigurnost
– dopuna koordiniranog odgovora EU-a na kiberincidente i kiberkrize velikih razmjera**

VIJEĆE EUROPSKE UNIJE,

PODSJEĆAJUĆI na:

- svoje zaključke o Strategiji EU-a za kibersigurnost za digitalno desetljeće¹,
- svoje zaključke o koordiniranom odgovoru EU-a na kiberincidente i kiberkrize velikih razmjera²,
- svoje zaključke o kibernetičkoj diplomaciji³,
- svoje zaključke o okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („Alati za kiberdiplomaciju”)⁴,
- svoje zaključke o sigurnosti i obrani⁵,
- okvir za politiku kibernetičke obrane EU-a⁶,
- svoje zaključke o oblikovanju digitalne budućnosti Europe⁷,
- Provedbenu odluku Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU-a za integrirani politički odgovor na krizu,

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

- svoje zaključke o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvratanje i obrana: jačanje kibersigurnosti EU-a⁸,
 - svoje zaključke o izgradnji kapaciteta i sposobnosti u području kibersigurnosti u EU-u⁹,
1. NAGLAŠAVA važnost kibersigurnosti za izgradnju otporne, zelene i digitalne Europe; ISTIČE da je kibersigurnost neophodna za blagostanje i sigurnost EU-a i njegovih država članica, njegovih građana, poduzeća i institucija, kao i za očuvanje integriteta naših slobodnih i demokratskih društava;
 2. PREPOZNAJE prekograničnu i međusektorsku prirodu mnogih prijetnji povezanih s kibersigurnošću te rizike i moguće posljedice kontinuiranih kampanji učinkovitijih, sofisticiranijih, preciznije ciljanih, složenijih, trajnijih i/ili raširenijih zlonamjernih kiberaktivnosti¹⁰. Zbog pandemije bolesti COVID-19 dodatno su razotkrivene ranjivosti naših društava te mogući razmjeri štete koju kiberincidenti velikih razmjera mogu nanijeti gospodarstvu, demokraciji, ključnim uslugama i kritičnoj infrastrukturi, osobito u zdravstvenom sektoru. Povećana je i važnost povezivosti i oslanjanja društva na pouzdane i sigurne mrežne i informacijske sustave kojima se može vjerovati. Naposljetku, naglašena je potreba za globalnim, otvorenim, slobodnim, stabilnim i sigurnim internetom, kao i za povjerenjem u proizvode, procese i usluge informacijske i komunikacijske tehnologije (IKT) te njihovu sigurnost, uključujući potrebu da se osigura otporan lanac opskrbe;

⁸ 14435/17 + COR 1.

⁹ 7737/19.

¹⁰ Izvješće ENISA-e o prijetnjama iz 2020.

3. PONOVRNO ISTIČE važnost kiberotpornosti i daljnjeg razvoja EU-ova okvira za upravljanje kibernsigurnosnim krizama¹¹ čiji je cilj učinkovit i pravodoban odgovor na razini EU-a na kiberincidente i kiberkrize velikih razmjera te njegova daljnjeg uključivanja u postojeće horizontalne i sektorske mehanizme EU-a za odgovor a krizu; ISTIČE ulogu Vijeća i aranžmana EU-a za integrirani politički odgovor na krizu (IPCR) u osiguravanju pravodobne koordinacije i odgovora na političkoj razini Unije na krize, koje imaju širok učinak ili političku važnost, bez obzira na to jesu li te krize nastale unutar Unije ili izvan nje; NAGLAŠAVA važnost redovitog ispitivanja takvih okvira i mehanizama;
4. PODSJEĆA da se aktivnosti na razini EU-a u pogledu kiberincidenata i kiberkriza velikih razmjera odvijaju u skladu s načelima supsidijarnosti, proporcionalnosti, komplementarnosti, izbjegavanja udvostručavanja i povjerljivosti; PONOVRNO ISTIČE da države članice imaju primarnu odgovornost za odgovor na kiberincidente i kiberkrize velikih razmjera koji utječu na njih; PODSJEĆA da je važno poštovati nadležnosti država članica i njihovu isključivu odgovornost za nacionalnu sigurnost, u skladu s člankom 4. stavkom 2. Ugovora o Europskoj uniji, među ostalim u području kibernsigurnosti;
5. istodobno PODSJEĆA na važnost poštovanja nadležnosti i mandatâ institucija, tijelâ i agencija EU-a. Visoki predstavnik, Komisija i druge institucije, tijela i agencije EU-a također imaju ključnu ulogu koja proizlazi iz prava Unije, među ostalim zbog mogućeg učinka kiberincidenata i kiberkriza velikih razmjera na jedinstveno tržište, kao i na funkcioniranje samih institucija, tijela i agencija EU-a;

¹¹ 10086/18.

6. ISTIČE da je potrebno izbjeći nepotrebno udvostručavanje te nastojati ostvariti komplementarnost i dodanu vrijednost u daljnjem razvoju EU-ova okvira za upravljanje kibersigurnosnim krizama i osigurati usklađenost s postojećim mehanizmima, inicijativama, mrežama, procesima i postupcima na nacionalnoj i europskoj razini; NAGLAŠAVA važnost pojednostavnjenja postojećih procesa i struktura kako bi se smanjila složenost te, u interesu kohezije u Uniji, poboljšala pristupačnost i sposobnost reakcije kad su posrijedi osobe koje traže pomoć i solidarnost;
7. PREPOZNAJE primjenjivost međunarodnog prava, uključujući Povelju Ujedinjenih naroda u cijelosti, međunarodno humanitarno pravo i pravo o ljudskim pravima u kiberprostoru te PROMIČE pridržavanje dobrovoljnih, neobvezujućih normi, pravila i načela odgovornog ponašanja država u kiberprostoru koje su potvrdile sve države članice EU-a;
8. POZDRAVLJA napredak ostvaren proteklih godina u okviru Vijeća, posebice u okviru Horizontalne radne skupine za kiberpitanja i drugih relevantnih radnih skupina Vijeća, kao i u uspostavi drugih inicijativa, mreža i mehanizama za suradnju i razmjenu informacija među državama članicama, posebno Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava (Skupina za suradnju NIS) i mreže timova za odgovor na računalne sigurnosne incidente (mreža CSIRT-ova), uspostavljenih Direktivom (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016., Mreže organizacija za vezu za kiberkrize (CyCLONe), kao i relevantnih projekata povezanih s kiberobranom pokrenutih u okviru stalne strukturirane suradnje (PESCO)¹², Zajedničke radne skupine za djelovanje protiv kiberkriminaliteta (J-CAT), Europske pravosudne mreže za kiberkriminalitet (ELCN), dobrovoljnih doprinosa država članica centru EU INTCEN te koordinacije i suradnje u kontekstu alatâ za kiberdiplomaciju;

¹² Osobito, projekt „Timovi za brz odgovor na kiberincidente i uzajamna pomoć u području kibersigurnosti” koji koordinira Litva, „Koordinacijski centar za kibernetičko i informacijsko područje” koji koordinira Njemačka i „Platforma za razmjenu informacija o odgovoru na kiberprijetnje i kiberincidente” koji koordinira Grčka.

9. PODSJEĆA na postojeće okvire za suradnju među institucijama, tijelima i agencijama EU-a, kao što su strukturirana suradnja između EINISA-e i CERT-EU-a te Memorandum o razumijevanju između ENISA-e, Europske obrambene agencije (EDA), Europolova Europskog centra za kiberkriminalitet (EC3) i CERT-EU-a; ISTIČE važnost kontinuirane redovite razmjene informacija s Vijećem o daljnjem razvoju tih okvira za suradnju;
10. NAGLAŠAVA važnost jačanja suradnje i razmjene informacija među različitim kiberzajednicama unutar EU-a i država članica na svim potrebnim razinama, tehničkoj, operativnoj i strateškoj/političkoj, te povezivanja postojećih mehanizama, mreža, struktura, procesa i postupaka za upravljanje krizom ako se time podupire i poboljšava suočavanje s kiberincidentima i kiberkrizama velikih razmjera;
11. PREPOZNAJE napredak koji je skupina država članica ostvarila u razvoju zajedničkog operativnog kiberkapaciteta „Timovi za brz odgovor na kiberincidente” u okviru PESCO-a čiji je cilj produbljivanje dobrovoljne suradnje u kiberpodručju putem uzajamne pomoći, među ostalim kao odgovor na kiberincidente i kiberkrize velikih razmjera;
12. PREPOZNAJE iskustvo zajednice za kazneni progon i njezinu sposobnost da reagira u svakom trenutku u području operativne suradnje i sigurne razmjene informacija o velikim prekograničnim kibernapadima u okviru Protokola EU-a za odgovor tijela kaznenog progona EU-a na krizne situacije;

13. PREPOZNAJE kontinuiranu provedbu okvira za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („alati za kiberdiplomaciju”); PODSJEĆA da svaka država članica može na pojedinačnoj osnovi donijeti vlastitu suverenu odluku u pogledu pripisivanja zlonamjerne kiberaktivnosti; PODSJEĆA da bi se mjere poduzete u okviru zajedničkog diplomatskog odgovora EU-a na zlonamjerne kiberaktivnosti trebale temeljiti na zajedničkoj informiranosti o stanju dogovorenoj među državama članicama. EU INTCEN ima ključnu ulogu kao središte za pružanje informiranosti o stanju i procjene prijetnji u vezi s kiberpitanjima za EU, na temelju dobrovoljnih obavještajnih doprinosa država članica i ne dovodeći u pitanje njihove nadležnosti;
14. PONOVO ISTIČE važnost uzajamne pomoći i solidarnosti, u skladu s člankom 42. stavkom 7. Ugovora o Europskoj uniji i člankom 222. Ugovora o funkcioniranju Europske unije, te POZIVA na daljnje vježbe s kiberdimenzijom; PODSJEĆA na potrebu da se razmotri povezivanje EU-ova okvira za upravljanje kibersigurnosnim krizama, alatâ za kiberdiplomaciju i odredaba navedenih članaka u slučaju kiberincidenta ili kiberkrize velikih razmjera; dodatno PODSJEĆA da se obvezama za države članice koje proizlaze iz članka 42. stavka 7. Ugovora o Europskoj uniji ne dovodi u pitanje posebna priroda sigurnosne i obrambene politike određenih država članica; također PODSJEĆA na to da NATO i dalje predstavlja temelj kolektivne obrane za države koje su njegove članice;
15. PRIMA NA ZNANJE suradnju EU-a i NATO-a u području kibersigurnosti i obrane, uključujući razmjenu informacija između CERT-EU-a i NATO-ove službe za odgovor na računalne incidente (NCIRC), uz potpuno poštovanje načela transparentnosti, uzajamnosti i uključivosti te autonomije obiju organizacija u donošenju odluka;

16. PREPOZNAJE važnost suradnje, prema potrebi, s privatnim sektorom u pogledu razmjene informacija i pružanja relevantnog stručnog znanja, kao i pouzdanih rješenja i usluga, među ostalim u podupiranju odgovora i jačanju informiranosti o stanju među različitim kiberzajednicama;
17. ISTIČE važnost sigurnih komunikacijskih kanala za razmjenu povjerljivih i osjetljivih informacija; NAGLAŠAVA potrebu za daljnjim napretkom;

u tom pogledu, i imajući na umu navedeno:

18. PRIMA NA ZNANJE Preporuku Komisije o uspostavi Zajedničke jedinice za kibersigurnost, kao inicijative koju treba razmotriti u daljnjem razvoju EU-ova okvira za upravljanje kibersigurnosnim krizama¹³;
19. POZIVA EU i njegove države članice da nastave ulagati napore prema sveobuhvatnijem i učinkovitijem EU-ovu okviru za upravljanje kibersigurnosnim krizama, nadovezujući se na postojeće mehanizme i na napredak koji je već ostvaren, te da uzmu u obzir potencijal inicijative za Zajedničku jedinicu za kibersigurnost da dopuni te mehanizme, pri čemu se primjenjuje postupni pristup; ISTIČE da je postupan, transparentan i uključiv proces nužan za jačanje povjerenja te je stoga ključan za daljnji razvoj EU-ova okvira za upravljanje kibersigurnosnim krizama. U tom procesu trebalo bi poštovati postojeće uloge, nadležnosti i mandate država članica i institucija, tijela i agencija EU-a, kao i načela navedena u ovim zaključcima, uključujući proporcionalnost, supsidijarnost, uključivost, komplementarnost, izbjegavanje udvostručavanja i povjerljivost informacija; istodobno ISTIČE da je svako moguće sudjelovanje država članica u Zajedničkoj jedinici za kibersigurnost ili doprinos toj jedinici dobrovoljno;

¹³ C(2021) 4520 final (11155/21 i 11155/21 ADD 1).

20. ISTIČE da je potrebno uspostaviti odgovarajuće metode rada i upravljanje kako bi se omogućilo sudjelovanje svih država članica u raspravama, razvoju i učinkovitim postupcima donošenja odluka u vezi s EU-ovim okvirom za upravljanje kibersigurnosnim krizama, među ostalim o mogućoj inicijativi za Zajedničku jedinicu za kibersigurnost; POZIVA na poštovanje ovlasti Vijeća na temelju Ugovorâ i načela lojalne suradnje;
21. ISTIČE važnost utvrđivanja i uključivanja svih relevantnih kiberzajednica unutar EU-a i njegovih država članica, uzimajući istodobno u obzir njihove različite uloge i odgovornosti u različitim vrstama kiberincidenata i kiberkriza velikih razmjera; ISTIČE ključnu ulogu Vijeća, posebice putem Horizontalne radne skupine za kiberpitanja, u oblikovanju politika i koordinacijskoj funkciji u pogledu daljnjeg razvoja EU-ova okvira za upravljanje kibersigurnosnim krizama; stoga POZIVA države članice, Komisiju, Europsku službu za vanjsko djelovanje (ESVD), EU INTCEN, CERT-EU, ENISA-u, Europol (EC3), Eurojust (EJCN), Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC) te predstavnike iz mreže CSIRT-ova, mreže CyCLONe, Skupine za suradnju NIS, EDA-e i relevantnih projekata u okviru PESCO-a, kao i druge moguće dionike, da sudjeluju u ovom procesu. Mogla bi se dodatno ispitati moguća radna skupina, kako je predložena u preporuci Komisije, koja bi služila kao privremeni forum u kojem bi se okupljali predstavnici svih relevantnih kiberzajednica u državama članicama i unutar EU-a, pri čemu bi se osigurala odgovarajuća zastupljenost svih država članica i djelovalo bi se pod političkim vodstvom Vijeća. Takva radna skupina trebala bi redovito izvješćivati o svojim aktivnostima i Vijeću podnositi moguće prijedloge radi rasprava, odobrenja i daljnjih smjernica. Osim toga, mogli bi se uspostaviti drugi oblici dijaloga unutar zajednica i među njima, među ostalim putem radionica, seminara, zajedničkog osposobljavanja i vježbi;

22. ISTIČE ulogu Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC) i Mreže nacionalnih koordinacijskih centara u odnosu na potencijalnu Zajedničku jedinicu za kibersigurnost, posebice s obzirom na njezinu ulogu u znatnom povećanju Unijinih tehnoloških kapaciteta, tehnoloških rješenja, sposobnosti i vještina u području kibersigurnosti;
23. POZIVA EU i njegove države članice da se uključe u daljnji razvoj EU-ova okvira za upravljanje kibersigurnosnim krizama, među ostalim istraživanjem potencijala inicijative za Zajedničku jedinicu za kibersigurnost, utvrđivanjem i određivanjem procesa, uključujući ključne etape i vremenski okvir, te pojašnjavanjem ciljeva i mogućih uloga i odgovornosti; NAGLAŠAVA potrebu da se prioritetno konsolidiraju postojeće mreže i interakcije unutar svake zajednice, kao i da se utvrdi temeljit pregled mogućih nedostataka i potreba u pogledu razmjene informacija unutar kiberzajednica i među njima te unutar europskih institucija, tijela i agencija i među njima, te da se zatim postigne dogovor o mogućim primarnim ciljevima i prioritetima potencijalne Zajedničke jedinice za kibersigurnost; ne dovodeći u pitanje ishod, ISTIČE potrebu da se naglasak stavi na utvrđivanje potreba u pogledu razmjene informacija kako bi se izgradila zajednička informiranost o stanju među svim relevantnim zajednicama. Pri utvrđivanju nedostataka i potreba u pogledu razmjene informacija, uključujući moguću upotrebu virtualnih platformi, dužnu pažnju trebalo bi i dalje posvećivati sigurnim komunikacijskim kanalima za razmjenu klasificiranih i osjetljivih informacija, istodobno ISTIČUĆI važnost korištenja već postojećom infrastrukturom. Uvođenjem postupnog pristupa namjerava se izgraditi povjerenje i temelj za moguće daljnje korake povezane s poboljšanjem pripravnosti i operativne suradnje; PREPOZNAJE da bi različiti ciljevi mogli opravdati različita rješenja i sudjelovanje različitog skupa predstavnika relevantnih kiberzajednica unutar EU-a i njegovih država članica;

24. POZIVA na daljnje razmatranje u vezi s pravnom osnovom za potencijalnu Zajedničku jedinicu za kibersigurnost tijekom cijelog procesa, uključujući procjenu zadaća i uloga u odnosu na one dodijeljene ENISA-i u preporuci s obzirom na članak 7. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019.; POZIVA na daljnje razmatranje pojedinačnih elemenata Preporuke o Zajedničkoj jedinici za kibersigurnost, među ostalim u pogledu ideje o timovima EU-a za brzu reakciju u području kibersigurnosti i plana EU-a za odgovor na kiberincidente i kiberkrize; NAGLAŠAVA da potencijalna Zajednička jedinica za kibersigurnost mora poštovati nadležnosti, mandate i pravne ovlasti svojih mogućih budućih sudionika;
25. POZIVA EU i njegove države članice da razmotre potencijal inicijative za Zajedničku jedinicu za kibersigurnost, među ostalim i iz perspektive institucija, tijela i agencija EU-a, kako bi se nadopunili aktualni naponi na razini država članica; POZDRAVLJA namjeru Komisije da ojača otpornost relevantnih institucija, tijela i agencija EU-a budućim prijedlogom uredbe o zajedničkim obvezujućim pravilima o kibersigurnosti za institucije, tijela i agencije EU-a;
26. kao zaključak, PONOVRNO POTVRĐUJE svoju predanost jačanju kiberotpornosti i daljnjem razvoju EU-ova okvira za upravljanje kibersigurnosnim krizama i REDOVITO ĆE PRATITI napredak i pružati dodatne smjernice za dopunu tog okvira.
-