Vijeće
Europske unije

Bruxelles, 9. ožujka 2021.
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

NAPOMENA O TOČKI „I/A”

Od:	Glavno tajništvo Vijeća
Za:	Odbor stalnih predstavnika / Vijeće
Predmet:	Nacrt zaključaka Vijeća o Strategiji EU-a za kibersigurnost za digitalno desetljeće

1. Komisija i Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku 16. prosinca 2020. objavili su zajedničku komunikaciju Europskom parlamentu i Vijeću naslovljenu „Strategija EU-a za kibersigurnost za digitalno desetljeće”[1]. Novom strategijom za kibersigurnost nastoji se ojačati kolektivna otpornost Europe na kiberprijetnje te osigurati da svi građani, građanke i poduzeća mogu u potpunosti iskoristiti pouzdane i vjerodostojne usluge i digitalne alate.

[1] Dok. 14133/20.

2. Komisija i ESVD predstavili su zajedničku komunikaciju na neformalnoj videokonferenciji Horizontalne radne skupine za kiberpitanja 17. prosinca 2020. i 12. siječnja 2021. Na neformalnoj videokonferenciji Horizontalne radne skupine za kiberpitanja 17. prosinca 2020. predstojeće portugalsko predsjedništvo najavilo je svoju namjeru da pripremi Nacrt zaključaka Vijeća o Strategiji EU-a za kibersigurnost za digitalno desetljeće.

3. Predsjedništvo je prvi nacrt zaključaka Vijeća predstavilo 2. veljače 2021. na neformalnoj videokonferenciji Horizontalne radne skupine za kiberpitanja. O tim se zaključcima naknadno raspravljalo na neformalnim videokonferencijama Horizontalne radne skupine za kiberpitanja 9. i 19. veljače 2021. te 1. i 9. ožujka 2021.

4. Budući da nacrt zaključaka sadržava i upućivanje na obrambene politike EU-a (točka 30.), Skupina za političko-vojna pitanja raspravljala je o relevantnoj točki na sastanku 10. veljače 2021.

5. Različite točke odnose se na zajedničku vanjsku i sigurnosnu politiku (točke 1., 4., 7., 8., 9., 20., 23., 24., 26., 27., 28., 29., 30., 31., 32. i 33.) te su stoga podnesene Političkom i sigurnosnom odboru koji ih je podržao na sastanku 4. ožujka 2021.

6. Na neformalnoj videokonferenciji 9. ožujka 2021. Horizontalna radna skupina za kiberpitanja postigla je dogovor o nacrtu zaključaka Vijeća kako je naveden u dokumentu 6722/21.

7. S obzirom na navedeno, Odbor stalnih predstavnika poziva se da Vijeću podnese nacrt zaključaka Vijeća, kako je naveden u Prilogu, te da predloži Vijeću da kao točku „A” dnevnog reda usvoji nacrt zaključaka.

PRILOG

Nacrt zaključaka Vijeća o Strategiji EU-a za kibersigurnost za digitalno desetljeće

VIJEĆE EUROPSKE UNIJE,

PODSJEĆAJUĆI na svoje zaključke o:

– Zajedničkoj komunikaciji Europskom parlamentu i Vijeću od 25. lipnja 2013. o Strategiji Europske unije za kibersigurnost naslovljenoj „Otvoren, siguran i zaštićen kiberprostor”[2],

– upravljanju internetom[3],

– Zajedničkoj komunikaciji Europskom parlamentu i Vijeću od 20. studenoga 2017. naslovljenoj „Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a”[4],

– izgradnji kapaciteta i sposobnosti u području kibersigurnosti u EU-u[5],

– važnosti mreža 5G za europsko gospodarstvo i potrebi za ublažavanjem sigurnosnih rizika povezanih s mrežama 5G[6],

– budućnosti visoko digitalizirane Europe nakon 2020.: „Poticanje digitalne i gospodarske konkurentnosti u cijeloj Uniji i digitalna kohezija”[7],

– dodatnim nastojanjima za jačanje otpornosti i suzbijanje hibridnih prijetnji[8],

– oblikovanju digitalne budućnosti Europe[9],

---

2 Dok. 12109/13.
3 Dok. 16200/14.
4 Dok. 14435/17 + COR 1.
5 Dok. 7737/19.
6 Dok. 14517/19.
7 Dok. 9596/19.
8 Dok. 14972/20.
9 Dok. 8711/20.

– digitalnoj diplomaciji[10],

– jačanju otpornosti i suzbijanju hibridnih prijetnji, uključujući dezinformacije u kontekstu pandemije bolesti COVID-19[11],

– kibernetičkoj diplomaciji[12]

– koordiniranom odgovoru EU-a na kiberincidente i kiberkrize velikih razmjera[13],

– okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („Alati za kiberdiplomaciju”)[14],

– smjernicama za izgradnju vanjskih kiberkapaciteta EU-a[15],

– oporavku kojim se pospješuje prijelaz prema dinamičnijoj, otpornijoj i konkurentnijoj europskoj industriji[16],

– kibersigurnosti povezanih uređaja[17],

jačanju europskog sustava kiberotpornosti i poticanju konkurentne i inovativne industrije kibersigurnosti[18],

– i na Rezoluciju Vijeća o sigurnosti s pomoću šifriranja i sigurnosti unatoč šifriranju[19]

---

10 Dok. 12804/20.
11 Dok. 14064/20.
12 Dok. 6122/15 + COR 1.
13 Dok. 10086/18.
14 Dok. 10474/17.
15 Dok. 10496/18.
16 Dok. 13004/20.
17 Dok. 13629/20.
18 Dok. 14540/16.
19 Dok. 13084/1/20 REV 1.

– te deklaraciju država članica od 15. listopada 2020. o izgradnji nove generacije oblaka za poslovni i javni sektor u Europskoj uniji,

PODSJEĆAJUĆI na zaključke Europskog vijeća o bolesti COVID-19, jedinstvenom tržištu, industrijskoj politici, digitalnim i vanjskim odnosima od 1. i 2. listopada 2020.[20] te zaključke o dezinformacijama i hibridnim prijetnjama i na Novi strateški program za razdoblje 2019.–2024. od 20. lipnja 2019.[21],

PODSJEĆAJUĆI na Globalnu strategiju za vanjsku i sigurnosnu politiku Europske unije od 28. lipnja 2016. naslovljenu „Zajednička vizija, zajedničko djelovanje: jača Europa”,

PODSJEĆAJUĆI na Komunikaciju Europske komisije od 19. prosinca 2020. naslovljenu „Izgradnja digitalne budućnosti Europe”[22] i Komunikaciju Europske komisije od 24. srpnja 2020. o strategiji EU-a za sigurnosnu uniju[23],

PODSJEĆAJUĆI na Zajedničku komunikaciju Europske komisije i Visokog predstavnika od 2. prosinca 2020. o novoj strategiji EU-a i SAD-a za globalne promjene[24],

1. NAGLAŠAVA činjenicu da je kibersigurnost ključna za izgradnju otporne, zelene i digitalne Europe te POZDRAVLJA Zajedničku komunikaciju Europskom parlamentu i Vijeću naslovljenu „Strategija EU-a za kibersigurnost za digitalno desetljeće” u kojoj se iznosi novi okvir za djelovanje EU-a u područjima „otpornosti, tehnološke suverenosti i vodstva”, kao i za zaštitu njegovih građana, poduzeća i institucija od kiberincidenata i kiberprijetnji, uz istodobno jačanje povjerenja pojedinaca i organizacija u sposobnost EU-a da promiče sigurne i pouzdane mrežne i informacijske sustave, infrastrukturu i povezivost te promiče i štiti globalan, otvoren, slobodan, stabilan i zaštićen kiberprostor koji se zasniva na ljudskim pravima, temeljnim slobodama, demokraciji i vladavini prava.

---

20 Dok. EUCO 13/20.
21 Dok. EUCO 9/19.
22 19.2.2020. COM(2020) 67 final.
23 24.7.2020. COM(2020) 605 final.
24 2.12.2020. JOIN(2020) 22 final.

2. UVIĐA da je uslijed pandemije bolesti COVID-19 povećana potreba za povjerenjem u alate i sustave informacijske i komunikacijske tehnologije (IKT) i njihovom sigurnosti postala prioritet u našem svakodnevnom životu. ISTIČE da su kibersigurnost te globalni i otvoreni internet ključni za funkcioniranje javne uprave i institucija na nacionalnoj razini i razini EU-a te za naše društvo i gospodarstvo u cjelini.

3. ISTIČE potrebu za većim podizanjem svijesti o kiberpitanjima na političkoj i strateškoj razini donošenja odluka pružanjem relevantnog znanja i informacija donositeljima odluka te ISTIČE potrebu za podizanjem svijesti šire javnosti i promicanjem kiberhigijene.

4. POZIVA na promicanje i zaštitu temeljnih vrijednosti EU-a, kao što su demokracija, vladavina prava, ljudska prava i temeljne slobode, uključujući pravo na slobodu izražavanja i informiranja, pravo na slobodu okupljanja i udruživanja te pravo na privatnost u kiberprostoru. U tom pogledu POZDRAVLJA ulaganje dodatnih kontinuiranih napora u zaštitu boraca za ljudska prava, civilnog društva i akademske zajednice koji se bave pitanjima kao što su kibersigurnost, privatnost podataka, nadzor i cenzura na internetu pružanjem dodatnih praktičnih smjernica, promicanjem najboljih praksi i jačanjem napora koje EU ulaže u sprečavanje kršenja i povreda ljudskih prava te zlouporabe tehnologija u nastajanju, prije svega primjenom diplomatskih mjera kada je to potrebno, kao i kontrolom izvoza takvih tehnologija. U tom kontekstu NAGLAŠAVA važnost Akcijskog plana EU-a za ljudska prava i demokraciju za razdoblje 2020.–2024. i njegovih smjernica o ljudskim pravima koje se odnose na slobodu izražavanja na internetu i izvan njega.
5. ISTIČE da je postizanje strateške autonomije uz očuvanje otvorenoga gospodarstva ključan cilj Unije kako bi ona sama odredila svoj gospodarski put i interese. Time je obuhvaćeno jačanje sposobnosti donošenja autonomnih odluka u području kibersigurnosti s ciljem jačanja digitalnog vodstva EU-a i njegovih strateških kapaciteta. PODSJEĆA na to da to uključuje utvrđivanje i smanjenje strateških ovisnosti i povećanje otpornosti u najosjetljivijim industrijskim ekosustavima i posebnim područjima. NAGLAŠAVA da to može uključivati diversifikaciju proizvodnih i opskrbnih lanaca, poticanje i privlačenje ulaganja i proizvodnje u Europi, istraživanje alternativnih rješenja i kružnih modela te promicanje široke industrijske suradnje među državama članicama.

6. Imajući na umu nedostatak radne snage s digitalnim vještinama i vještinama u području kibersigurnosti, ISTIČE važnost zadovoljavanja potražnje za osposobljenom radnom snagom u području digitalne tehnologije i kibersigurnosti, posebno razvojem, zadržavanjem i privlačenjem najtalentiranijih osoba, primjerice obrazovanjem i osposobljavanjem, kako bi se naše društvo moglo digitalizirati na kibersiguran način. POTIČE veće sudjelovanje žena i djevojčica u obrazovanju u području znanosti, tehnologije, inženjerstva i matematike („STEM") te usavršavanju i prekvalifikaciji u digitalnim vještinama kao jednom od sredstava za premošćivanje rodnog digitalnog jaza;

7. PODSJEĆA na to da je cilj zajedničkog i sveobuhvatnog pristupa EU-a kiberdiplomaciji doprinijeti sprečavanju sukoba, ublažavanju kibersigurnosnih prijetnji i većoj stabilnosti u međunarodnim odnosima. U tom kontekstu PONOVNO POTVRĐUJE svoju predanost rješavanju međunarodnih sporova u kiberprostoru mirnim sredstvima i da bi svi diplomatski napori EU-a trebali prvenstveno biti usmjereni na promicanje sigurnosti i stabilnosti u kiberprostoru povećanom međunarodnom suradnjom te na smanjenje rizika od pogrešnih predodžbi, eskalacije i sukoba koji mogu proizaći iz incidenata u području IKT-a te PODUPIRE daljnji razvoj i operacionalizaciju mjera za izgradnju povjerenja na regionalnoj i međunarodnoj razini. PONOVNO ISTIČE poziv Opće skupštine Ujedinjenih naroda, dogovoren konsenzusom, da se države članice UN-a vode preporukama iz izvješćâ Skupine vladinih stručnjaka UN-a u području informacija i telekomunikacija u kontekstu međunarodne sigurnosti (UNGGE) pri uporabi IKT-a te PONOVNO POTVRĐUJE primjenu međunarodnog prava u kiberprostoru, a posebno cjelokupne Povelje UN-a.

8. PONOVNO POTVRĐUJE da je daljnji razvoj normi i standarda unutar Unije ključan kako bismo mogli u znatnoj mjeri oblikovati međunarodne norme i standarde u područjima tehnologija u nastajanju te tehničke i logičke infrastrukture ključnih za opću dostupnost i integritet javne jezgre interneta, kako bi bili u skladu s univerzalnim vrijednostima i vrijednostima EU-a te višedioničkim pristupom. Time će se osigurati da internet ostane globalan, otvoren, slobodan, stabilan i siguran te da se pri upotrebi i razvoju digitalnih tehnologija poštuju ljudska prava i da njihova upotreba bude zakonita, sigurna i etična. PRIMA NA ZNANJE predstojeću strategiju za normizaciju i PREUZIMA OBVEZU proaktivne i koordinirane komunikacije s ciljem promicanja vodstva i ciljeva EU-a na međunarodnoj razini, među ostalim u raznim međunarodnim tijelima za normizaciju i u suradnji s partnerima istomišljenicima, civilnim društvom, akademskom zajednicom i privatnim sektorom.

9. SNAŽNO PODUPIRE višedionički model kibersigurnosti i upravljanja internetom te preuzima obvezu jačanja redovitih i strukturiranih razmjena s dionicima, uključujući privatni sektor, akademsku zajednicu i civilno društvo u međunarodnim forumima, među ostalim u kontekstu pariškoga poziva za povjerenje i sigurnost u kiberprostoru. u razvoju politika i pri korištenju internetom PROMIČE univerzalan, cjenovno pristupačan i jednak pristup internetu premošćivanjem digitalnog jaza, a posebno osnaživanje žena, djevojčica i osoba u ranjivim ili marginaliziranim situacijama.

10. NAGLAŠAVA potrebu za uključivanjem kibersigurnosti u digitalna ulaganja i inicijative u nadolazećim godinama te potrebu za tim da se postupno sve više doprinosi jednakim uvjetima u području kibersigurnosti te PRIMA NA ZNANJE plan Komisije za povećanje javne potrošnje i poticanje privatnih ulaganja u području kibersigurnosti. NAGLAŠAVA važnost malih i srednjih poduzeća (MSP) u ekosustavu kibersigurnosti i PREPOZNAJE relevantne financijske instrumente dostupne za potporu snažnoj usmjerenosti na kibersigurnost u okviru digitalne transformacije u višegodišnjem financijskom okviru (VFO) za razdoblje 2021. – 2027., kao i u Mehanizmu za oporavak i otpornost.

11. SA ZADOVOLJSTVOM OČEKUJE brzu provedbu Uredbe o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara, uključujući brzu uspostavu i operacionalizaciju Europskog centra za stručnost u području kibersigurnosti u Bukureštu. Brzim usvajanjem njezina programa doprinijet će se maksimalnom povećanju učinaka ulaganja radi jačanja vodstva i strateške autonomije Unije u području kibersigurnosti i potpore tehnološkim kapacitetima i vještinama te povećanja globalne konkurentnosti Unije uz doprinos industrije i akademske zajednice u području kibersigurnosti, uključujući MSP-ove i istraživačke centre, koji će imati koristi od sustavnije i uključivije strateške suradnje, uzimajući u obzir koheziju Unije i svih njezinih država članica.

12. POZDRAVLJA rad koji ENISA trenutačno obavlja u suradnji s državama članicama i zainteresiranim dionicima, kako bi se EU-u pružili programi certifikacije za IKT proizvode, usluge i procese kojima bi se trebalo doprinijeti povećanju opće razine kibersigurnosti na digitalnom jedinstvenom tržištu. U tom kontekstu SA ZADOVOLJSTVOM OČEKUJE kontinuirani program rada Unije s ciljem razvoja programâ kibersigurnosne certifikacije EU-a u okviru Akta o kibersigurnosti. U tom kontekstu PRIMA NA ZNANJE ključnu ulogu EU-a u razvoju standarda kojima se može oblikovati kibersigurnosno okružje i kojima se doprinosi osiguravanju poštenog tržišnog natjecanja u EU-u i na globalnoj razini, promicanju pristupa tržištu i uklanjanju sigurnosnih rizika uz istodobno osiguravanje primjenjivosti zakonodavnog okvira EU-a.

13. PONOVNO ISTIČE važnost procjene potrebe za horizontalnim zakonodavstvom, među ostalim kojim se utvrđuju nužni uvjeti za stavljanje na tržište, kako bi se dugoročno odgovorilo na sve relevantne aspekte kibersigurnosti povezanih uređaja, kao što su dostupnost, cjelovitost i povjerljivost. U tom pogledu POZDRAVLJA raspravu usmjerenu na razmatranje područja primjene takvog zakonodavstva i njegovih poveznica s okvirom za kibersigurnosnu certifikaciju, kako je definiran u Aktu o kibersigurnosti, s ciljem podizanja razine sigurnosti unutar digitalnog jedinstvenog tržišta. ISTIČE da bi kibersigurnosne zahtjeve trebalo definirati u skladu s relevantnim zakonodavstvom Unije, uključujući Akt o kibersigurnosti, novi zakonodavni okvir, Uredbu o europskoj normizaciji i moguće buduće horizontalno zakonodavstvo, kako bi se izbjegle nejasnoće i rascjepkanost zakonodavstva.

14. PRIMA NA ZNANJE važnost sveobuhvatnog i horizontalnog pristupa kibersigurnosti u Uniji, uz potpuno poštovanje nadležnosti i potreba država članica, kao i važnost stalne potpore tehničkoj pomoći i suradnje za izgradnju kapaciteta država članica. Uzimajući u obzir razvoj okružja kiberprijetnji, PRIMA NA ZNANJE novi Prijedlog direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije koji se nadovezuje na Direktivu o sigurnosti mrežnih i informacijskih sustava i ponovno ističe svoju potporu jačanju i usklađivanju nacionalnih okvira za kibersigurnost i stalnoj suradnji među državama članicama. Nadalje, NAGLAŠAVA potrebu za usklađivanjem i oblikovanjem sektorskog zakonodavstva u tom području.

15. PRIMA NA ZNANJE prijedlog Komisije da se državama članicama pruži potpora u uspostavi i jačanju centara za sigurnosne operacije (SOC) kako bi se diljem EU-a izgradila mreža centara za sigurnosne operacije, radi daljnjeg praćenja i predviđanja signala napada na mreže. U tom kontekstu OČEKUJE detaljne planove Komisije u vezi s mrežom centara za sigurnosne operacije, poštujući pritom nadležnosti država članica. PODSJEĆA na napore koje su države članice, uz potporu EU-a, poduzele kako bi uspostavile sektorske, nacionalne i regionalne timove za odgovor na računalne sigurnosne incidente (CSIRT) i nacionalne ili europske centre za razmjenu i analizu informacija (ISAC) kao dio djelotvorne mreže kibersigurnosnih partnerstava u Uniji. SA ZANIMANJEM OČEKUJE istraživanje potencijala te mreže za jačanje centara za sigurnosne operacije, kao i njihove komplementarnosti i koordinacije s postojećim mrežama i dionicima (posebno s mrežom timova za odgovor na računalne sigurnosne incidente) kako bi se promicala učinkovita, sigurna i pouzdana kultura razmjene informacija. NAGLAŠAVA da će se taj proces temeljiti na radu koji se obavlja u kontekstu inicijativa za umjetnu inteligenciju i računalstvo visokih performansi te na radu europskih centara za digitalne inovacije.

16. PRIMA NA ZNANJE mogući razvoj sigurnog sustava povezivosti koji se temelji na europskoj kvantnoj komunikacijskoj infrastrukturi (EuroQCI) i državnim satelitskim komunikacijama Europske unije (GOVSATCOM) te UVIĐA da bi se svaki mogući budući razvoj trebao temeljiti na snažnom kibersigurnosnom okviru i uzeti u obzir cjelokupnu infrastrukturu elektroničkih komunikacija kao što su svemirski, kopneni i podmorski mrežni sustavi.

17. SA ZANIMANJEM OČEKUJE rasprave s Komisijom, ENISA-om, dvama operaterima korijenskih DNS poslužitelja iz EU-a i širom zajednicom dionika kako bi se ocijenila uloga tih operatera u osiguravanju toga da internet i dalje bude globalno dostupan i nefragmentiran. POZDRAVLJA daljnju raspravu o namjeri Komisije da razvije alternativnu europsku uslugu za pristup globalnom internetu (inicijativa DNS4EU), koja se temelji na transparentnom modelu koji je u skladu s najnovijim standardima i pravilima u pogledu sigurnosti te tehničke i integrirane zaštite podataka i privatnosti, kako bi se doprinijelo većoj otpornosti, uz istodobno održavanje i poboljšanje međunarodne povezivosti za sve države članice.

18. UVIĐA potrebu za zajedničkim naporima Komisije i država članica da se ubrza prihvaćanje ključnih internetskih standarda, uključujući IPv6 i dobro poznatih standarda internetske sigurnosti, s obzirom na to da su važni za povećanje ukupne razine sigurnosti, otpornosti, otvorenosti i interoperabilnosti globalnog interneta, uz istodobno povećanje konkurentnosti industrije EU-a, posebno operatera internetske infrastrukture.

19. Naglašava važnost koordiniranog pristupa, kao i razvoja i provedbe djelotvornih mjera na nacionalnoj razini za jačanje kibersigurnosti 5G mreža. PODRŽAVA predstojeće korake koje treba poduzeti u pogledu kibersigurnosti 5G mreža, kako je predstavljeno u dodatku strategiji EU-a za kibersigurnost i na temelju rezultata izvješća o učincima preporuke Komisije o sigurnosti 5G mreža, na primjer u pogledu utvrđivanja dugoročnog i sveobuhvatnog pristupa koji se odnosi na cijeli vrijednosni lanac i ekosustav 5G tehnologije. S ciljem daljnjeg jačanja koordiniranog pristupa sigurnosti 5G mreža, POTIČE države članice, institucije EU-a i druge relevantne dionike da nastave sa svojim periodičnim pregledom stanja, zajedno s razmjenom informacija i najboljih praksi u okviru namjenske radne skupine za kibersigurnost 5G tehnologije u Skupini za suradnju u području sigurnosti mrežnih i informacijskih sustava te da redovito izvješćuju Vijeće o postignutom napretku. Iako ističe odgovornost država članica za zaštitu nacionalne sigurnosti, NAGLAŠAVA svoju snažnu predanost primjeni i brzom dovršetku provedbe paketa mjera EU-a za 5G te daljnjim naporima za jamčenje sigurnosti 5G mreža i razvoja budućih generacija mreža. Bliska suradnja između država članica, Komisije i ENISA-e u području sigurnosti 5G mreža mogla bi poslužiti kao primjer za druga pitanja u području kibersigurnosti, uz istodobno poštovanje nadležnosti država članica te načela supsidijarnosti i proporcionalnosti.

20. UVAŽAVA važnost daljnje integracije kibersigurnosti u mehanizme EU-a za odgovor na krize i njihova testiranja u relevantnim vježbama te ISTIČE važnost jačanja suradnje i razmjene informacija među različitim kiberzajednicama unutar EU-a te povezivanja postojećih inicijativa, struktura i postupaka (kao što su integrirani politički odgovor na krizu (IPCR), mreža timova za odgovor na računalne sigurnosne incidente (CSIRT), Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, mreža organizacija za vezu za kiberkrize (CyCLONe), Europski centar za kiberkriminalitet, Obavještajni i situacijski centar EU-a (EU INTCEN) i druga relevantna tijela EU-a) u slučaju velikih i prekograničnih kiberincidenata i prijetnji. UZIMAJUĆI U OBZIR napredak koji je već postignut u tom području, OČEKUJE prijedlog Komisije o postupku, ključnim etapama i vremenskom okviru za utvrđivanje zajedničke jedinice za kibersigurnost (JCU) s ciljem pružanja dodane vrijednosti, jasnog usmjerenja i pojednostavnjenja EU-ova okvira za upravljanje kibersigurnosnim krizama, među ostalim pripravnošću, zajedničkom informiranošću o stanju, jačanjem koordiniranog odgovora i vježbi na transparentan i postupan način, uz izbjegavanje udvostručavanja i preklapanja te uz poštovanje nadležnosti država članica.

21. ISTIČE važnost promicanja suradnje i razmjene informacija između relevantnih aktera u području kibersigurnosti i nadležnih tijela u području sigurnosti i kaznenog pravosuđa, npr. tijela za izvršavanje zakonodavstva i pravosudnih tijela, kao i potrebu za proširenjem i poboljšanjem kapaciteta tih tijela za istragu i kazneni progon kiberkriminaliteta te za poticanjem međunarodnih pregovora i pravila EU-a o prekograničnom pristupu elektroničkim dokazima. Ključno je da se zakonitim pristupom za obavljanje zadaća očuvaju ovlasti nadležnih tijela u području sigurnosti i kaznenog pravosuđa, kako je to propisano i dopušteno zakonom, neovisno o trenutačnom tehnološkom okružju. Takvi zakoni kojima se predviđaju izvršne ovlasti moraju uvijek u potpunosti poštovati zakonito postupanje i druge zaštitne mjere, kao i temeljna prava, a osobito pravo na poštovanje privatnog života i komuniciranja te pravo na zaštitu osobnih podataka.

22. PONOVNO POTVRĐUJE svoju potporu razvoju, provedbi i upotrebi snažnog šifriranja kao nužnog sredstva za zaštitu temeljnih prava i digitalne sigurnosti pojedinaca, vlada, industrije i društva te istodobno POTVRĐUJE potrebu da se osigura sposobnost nadležnih tijela u području sigurnosti i kaznenog pravosuđa, npr. tijela za izvršavanje zakonodavstva i pravosudnih tijela da izvršavaju svoje zakonite ovlasti na internetu i izvan njega, kako bi zaštitila naša društva i građane. Nadležnim tijelima mora biti omogućen zakonit i ciljan pristup podacima, uz puno poštovanje temeljnih prava i relevantnih zakona o zaštiti podataka te istodobno očuvanje kibersigurnosti. NAGLAŠAVA da se svim poduzetim djelovanjima treba pažljivo uspostaviti ravnoteža između interesa i načela nužnosti, proporcionalnosti i supsidijarnosti.

23. PODUPIRE i PROMIČE Budimpeštansku konvenciju o kiberkriminalitetu i tekući rad na Drugom dodatnom protokolu toj konvenciji. Osim toga, nastavlja sudjelovati u multilateralnim razmjenama u području kiberkriminaliteta, među ostalim u postupcima povezanima s Vijećem Europe, Uredom Ujedinjenih naroda za droge i kriminal (UNODC) i Komisijom za sprečavanje kriminala i kazneno pravosuđe (CCPCJ), kako bi se osigurala pojačana međunarodna suradnja u borbi protiv kiberkriminaliteta, uključujući razmjenu najboljih praksi i tehničkog znanja te podupiranje izgradnje kapaciteta, uz istodobno poštovanje, promicanje i zaštitu ljudskih prava i temeljnih sloboda.

24. Iako je nacionalna sigurnost i dalje isključiva odgovornost svake države članice, UVAŽAVA važnost strateške obavještajne suradnje u vezi s kiberprijetnjama i kiberaktivnostima te POZIVA države članice da putem svojih nadležnih tijela nastave doprinositi radu centra EU INTCEN kao središta za informiranost o stanju i procjene prijetnji u vezi s kiberpitanjima za EU i razmotre prijedlog o mogućoj uspostavi radne skupine država članica za kiberobavještajne podatke kako bi se ojačali namjenski kapaciteti INTCEN-a u tom području, na temelju dobrovoljnih obavještajnih doprinosa država članica i ne dovodeći u pitanje njihove nadležnosti.

25. NAGLAŠAVA važnost snažnog i dosljednog sigurnosnog okvira za zaštitu cjelokupnog osoblja, podataka, komunikacijskih mreža, informacijskih sustava te postupaka donošenja odluka EU-a koji se temelji na sveobuhvatnim, dosljednim i homogenim pravilima. To bi se posebno trebalo postići jačanjem otpornosti i poboljšanjem kulture sigurnosti EU-a protiv kiberprijetnji te jačanjem sigurnosti klasificiranih i neklasificiranih mreža EU-a uz istodobno osiguravanje odgovarajućeg upravljanja i raspoloživosti dostatnih resursa i kapaciteta, među ostalim u kontekstu jačanja mandata tima CERT-EU. U tom kontekstu POZDRAVLJA tekuće rasprave o uspostavi zajedničkih pravila o informacijskoj sigurnosti, uzimajući u obzir sigurnosna pravila Vijeća za zaštitu klasificiranih podataka EU-a, kao i definiranje zajedničkih obvezujućih pravila o kibersigurnosti za sve institucije, tijela i agencije EU-a.

26. NADOVEZUJUĆI SE NA napore EU-a u području kiberdiplomacije, PREUZIMA OBVEZU povećanja djelotvornosti i učinkovitosti alata za kiberdiplomaciju i SA ZANIMANJEM OČEKUJE produbljivanje rasprava o njegovu području primjene i upotrebi na temelju dosadašnjih iskustava stečenih u primjeni tog instrumenta. Tim bi se raspravama trebalo doprinijeti promicanju sigurnosti na međunarodnoj razini poticanjem dijaloga i njegovanjem zajedničke vizije kibersigurnosnih pitanja, jačanjem prevencije, stabilnosti, suradnje i jačanjem izgradnje povjerenja i kapaciteta te, prema potrebi, primjenom mjera ograničavanja kako bi se spriječile i obeshrabrile zlonamjerne kiberaktivnosti usmjerene na integritet i sigurnost EU-a i njegovih država članica te se od njih odvraćalo i na njih odgovorilo, čime bi se doprinijelo međunarodnoj sigurnosti i stabilnosti te konsolidirala razina kibersigurnosti EU-a, uz potpuno poštovanje nacionalnih nadležnosti i ovlasti. Posebnu pozornost prije svega trebalo bi posvetiti sprečavanju i suzbijanju kibernapada sa sistemskim učincima koji bi mogli utjecati na naše opskrbne lance, ključnu infrastrukturu i osnovne usluge, demokratske institucije i procese te ugroziti našu gospodarsku sigurnost, uključujući krađu intelektualnog vlasništva omogućenu kibertehnologijama. Države članice i institucije EU-a trebale bi također dodatno razmotriti povezivanje EU-ova okvira za upravljanje kibersigurnosnim krizama, alata za kiberdiplomaciju i odredaba članka 42. stavka 7. UEU-a i članka 222. UFEU-a, posebno putem rada temeljenog na scenarijima kako bi se izgradilo zajedničko razumijevanje praktičnih načina provedbe članka 42. stavka 7. UEU-a.

27. UVAŽAVA važnost jačanja suradnje s međunarodnim organizacijama i partnerskim zemljama kako bi se unaprijedilo zajedničko razumijevanje okružja kiberprijetnji, razvili dijalozi i mehanizmi suradnje, prema potrebi utvrdili zajednički diplomatski odgovori te poboljšala razmjena informacija, među ostalim obrazovanjem, osposobljavanjem i vježbama. Posebno ISTIČE da snažno transatlantsko partnerstvo u području kibersigurnosti doprinosi našoj zajedničkoj sigurnosti, stabilnosti i blagostanju te PRIMA NA ZNANJE odredbe o suradnji u području kibersigurnosti u okviru Sporazuma o trgovini i suradnji između EU-a i Ujedinjene Kraljevine. PODSJEĆAJUĆI NA ključna postignuća suradnje EU-a i NATO-a u području kibersigurnosti u okviru provedbe zajedničkih izjava iz Varšave 2016. i Bruxellesa 2018., ponovno ističe važnost pojačane, uzajamno ojačavajuće i korisne suradnje putem obrazovanja, osposobljavanja, vježbi i koordiniranog odgovora na zlonamjerne kiberaktivnosti, uz potpuno poštovanje samostalnosti u donošenju odluka i postupaka obiju organizacija, na temelju načela transparentnosti, uzajamnosti i uključivosti.

28. Kako bi se doprinijelo globalnom, otvorenom, slobodnom, stabilnom i sigurnom kiberprostoru, koji je sve važniji za trajni prosperitet, rast, sigurnost, povezivost i integritet naših društava, OBVEZUJE SE kontinuirano sudjelovati u postupcima utvrđivanja normi u međunarodnim organizacijama, posebno u postupcima povezanima s prvim odborom UN-a, promičući uvažavanje primjene međunarodnog prava u kiberprostoru i pridržavanje normi, pravila i načela odgovornog ponašanja država u kiberprostoru te im doprinoseći, među ostalim promicanjem brze izrade Akcijskog programa za unapređenje odgovornog ponašanja država u kiberprostoru, kao konstruktivnog i uključivog daljnjeg postupanja koje se temelji na konsenzusu u pogledu tekućih postupaka Skupine vladinih stručnjaka UN-a u području informacija i telekomunikacija u kontekstu međunarodne sigurnosti (UNGGE) i otvorene radne skupine (OEWG).

29. PODSJEĆA NA svoju snažnu predanost djelotvornom multilateralizmu i globalnom poretku utemeljenom na pravilima s Ujedinjenim narodima u središtu i odlučnost da ojača suradnju i koordinaciju s međunarodnim i regionalnim organizacijama, odnosno sa sustavom UN-a, NATO-om, Vijećem Europe, OESS-om, OECD-om, Afričkom unijom, Organizacijom američkih država (OAD), Udruženjem država jugoistočne Azije (ASEAN), Regionalnim forumom ASEAN-a, Vijećem za suradnju u Zaljevu (GCC) i Ligom arapskih država u pogledu rasprava o pitanjima povezanima s kibersigurnošću, kao i nastavka i širenja strukturiranih kiberdijaloga i savjetovanja EU-a s trećim zemljama. NAGLAŠAVA svoju aktivnu potporu UN-u, posebno u pogledu njegova Programa 2030., uključujući ciljeve održivog razvoja, te POZDRAVLJA Plan za digitalnu suradnju glavnog tajnika UN-a i Program glavnog tajnika UN-a za razoružanje kojima se potiče odgovornost i poštovanje normi u kiberprostoru te doprinosi sprečavanju i mirnom rješavanju sukoba koji proizlaze iz zlonamjernih aktivnosti u kiberprostoru. POZDRAVLJA prijedlog da Visoki predstavnik za vanjske poslove i sigurnosnu politiku uspostavi neformalnu mrežu EU-a za kiberdiplomaciju s ciljem razvoja suradnje i stručnog znanja EU-a i država članica u vezi s međunarodnim kiberpitanjima kako bi se ojačala koordinirana komunikacija.

30. SA ZANIMANJEM OČEKUJE predstojeći prijedlog preispitivanja okvira za politiku kiberobrane i OBVEZUJE SE da će i dalje ulagati napore u jačanje dimenzija kibersigurnosti i kiberobrane kako bi se osigurala njihova potpuna integracija u šire područje sigurnosti i obrane, posebno u kontekstu rada na Strateškom kompasu. SMATRA da će se predstojećom „Vojnom vizijom i strategijom o kiberprostoru kao području operacija” doprinijeti napretku tih rasprava. POZDRAVLJA inicijativu Europske obrambene agencije (EDA) za poticanje suradnje među vojnim CERT-ovima i PODUPIRE napore uložene u jačanje civilno-vojnih sinergija i koordinacije u području kiberobrane i kibersigurnosti, među ostalim u pogledu aspekata povezanih sa svemirom, među ostalim putem namjenskih projekata u okviru PESCO-a.

31. POZDRAVLJA prijedlog za razvoj programa EU-a za izgradnju vanjskih kiberkapaciteta, prijedlog za osnivanje odbora za izgradnju kiberkapaciteta EU-a te uspostavu i provedbu mreže za izgradnju kiberkapaciteta EU-a (EU CyberNet) kako bi se povećali kiberotpornost i kapaciteti diljem svijeta. U tom kontekstu POZDRAVLJA suradnju s državama članicama, kao i s partnerima iz javnog i privatnog sektora, posebno Globalnim forumom o kiberstručnosti (GFCE) i drugim relevantnim međunarodnim tijelima, kako bi se osigurala koordinacija i izbjeglo udvostručavanje. Posebno POTIČE suradnju s partnerima na zapadnom Balkanu te u istočnom i južnom susjedstvu EU-a.

32. Kako bi se osiguralo da sve zemlje mogu uživati društvene, gospodarske i političke prednosti interneta i upotrebe tehnologija, OBVEZUJE SE pomagati partnerskim zemljama u rješavanju sve većeg izazova zlonamjernih kiberaktivnosti, posebno onih koje štete razvoju njihovih gospodarstava, društava te integriteta i sigurnosti demokratskih sustava, među ostalim u skladu s naporima u okviru Akcijskog plana za europsku demokraciju.

33. Kako bi se osigurali razvoj, provedba i praćenje prijedloga predstavljenih u strategiji EU-a za kibersigurnost te uzimajući u obzir višegodišnju narav nekih inicijativa, POTIČE Komisiju i Visokog predstavnika za vanjske poslove i sigurnosnu politiku da izrade detaljan provedbeni plan u kojem se utvrđuju prioriteti i raspored planiranih djelovanja. PRATIT ĆE napredak u provedbi ovih zaključaka akcijskim planom koji će Vijeće redovito preispitivati i ažurirati u bliskoj suradnji s Europskom komisijom i Visokim predstavnikom.