Vijeće
Europske unije

Bruxelles, 23. svibnja 2022.
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	23. svibnja 2022.
Za:	Delegacije
Predmet:	Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora – zaključci Vijeća koje je Vijeće odobrilo na sastanku 23. svibnja 2022.

Za delegacije se u prilogu nalaze Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje je Vijeće odobrilo na sastanku 23. svibnja 2022.

PRILOG

Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora

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”[1],

– Okvir za politiku kibernetičke obrane EU-a[2],

– svoje zaključke o upravljanju internetom[3],

– svoje zaključke o kibernetičkoj diplomaciji[4],

– svoje zaključke o jačanju europskog sustava kiberotpornosti i poticanju konkurentne i inovativne industrije kibersigurnosti[5],

– svoje zaključke od 20. studenoga 2017. o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a[6],

– svoje zaključke o okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („Alati za kiberdiplomaciju”)[7],

– svoje zaključke o koordiniranom odgovoru EU-a na kiberincidente i kiberkrize velikih razmjera[8],

– svoje zaključke o smjernicama za izgradnju vanjskih kiberkapaciteta EU-a[9],

---

1 Dok. 12109/13.
2 Dok. 15585/14.
3 Dok. 16200/14.
4 Dok. 6122/15 + COR 1.
5 Dok. 14540/16.
6 Dok. 14435/17 + COR 1.
7 Dok. 10474/17.
8 Dok. 10086/18.
9 Dok. 10496/18.

– Provedbenu odluku Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU-a za integrirani politički odgovor na krizu[10],

– svoje zaključke o izgradnji kapaciteta i sposobnosti u području kibersigurnosti u EU-u[11],

– svoje zaključke o važnosti mreža 5G za europsko gospodarstvo i potrebi za ublažavanjem sigurnosnih rizika povezanih s mrežama 5G[12],

– svoje zaključke o budućnosti visoko digitalizirane Europe nakon 2020.: „Poticanje digitalne i gospodarske konkurentnosti u cijeloj Uniji i digitalna kohezija”[13],

– svoje zaključke o dodatnim nastojanjima za jačanje otpornosti i suzbijanje hibridnih prijetnji[14],

– svoje zaključke o oblikovanju digitalne budućnosti Europe[15],

– svoje zaključke o kibersigurnosti povezanih uređaja[16],

– svoje zaključke o Strategiji EU-a za kibersigurnost za digitalno desetljeće[17],

– svoje zaključke o sigurnosti i obrani[18],

– svoje zaključke o istraživanju potencijala inicijative o Zajedničkoj jedinici za kibersigurnost – dopuna koordiniranog odgovora EU-a na kiberincidente i kiberkrize velikih razmjera[19],

– Strateški kompas za sigurnost i obranu – za Europsku uniju koja štiti svoje građane, vrijednosti i interese te doprinosi međunarodnom miru i sigurnosti[20],

---

10 SL L 320, 17.12.2018., str. 28–34.
11 Dok. 7737/19.
12 Dok. 14517/19.
13 Dok. 9596/19.
14 Dok. 14972/19.
15 Dok. 8711/20.
16 Dok. 13629/20.
17 Dok. 7290/21.
18 Dok. 8396/21.
19 Dok. 13048/21.
20 Dok. 7371/22.

1. NAGLAŠAVA da se zlonamjerno ponašanje i državnih i nedržavnih aktera u kiberprostoru posljednjih godina pojačalo, što uključuje i nagli i stalan rast zlonamjernih aktivnosti usmjerenih na kritičnu infrastrukturu, lance opskrbe i intelektualno vlasništvo EU-a i njegovih država članica, povećani rizik od učinaka prelijevanja te porast napada ucjenjivačkim softverom na naša poduzeća, organizacije i građane; NAPOMINJE da s povratkom politike moći neke zemlje sve više pokušavaju osporiti i ugroziti međunarodni poredak u kiberprostoru utemeljen na pravilima, pretvarajući kiberprostor, zajedno s otvorenim morem, zračnim prostorom i svemirom, u sve spornije područje; PREPOZNAJE da su kibernapadi velikih razmjera ili pokušaji ometanja ili uništavanja mrežnih i informacijskih sustava te ulaska u njih, koji uzrokuju sistemske učinke, postali sve češći, da bi mogli ugroziti našu gospodarsku sigurnost i utjecati na naše demokratske institucije i procese i da se njima pokazuje spremnost nekih aktera da ugroze međunarodnu sigurnost i stabilnost; ISTIČE da je ruska vojna agresija protiv Ukrajine pokazala da se ofenzivne kiberaktivnosti mogu provoditi kao sastavni dio hibridnih strategija koje kombiniraju zastrašivanje, destabilizaciju i gospodarske poremećaje;

2. PONAVLJA da je s obzirom na trenutačne geopolitičke promjene snaga naše Unije u jedinstvu, solidarnosti i odlučnosti te da će se provedbom Strateškog kompasa ojačati strateška autonomija EU-a i njegova sposobnost da surađuje s partnerima kako bi se zaštitile njegove vrijednosti i interesi, među ostalim u kiberdomeni; ISTIČE da će snažniji i sposobniji EU u području sigurnosti i obrane pozitivno doprinijeti globalnoj i transatlantskoj sigurnosti te da je komplementaran NATO-u, koji je i dalje temelj kolektivne obrane svojih članica; PONOVNO POTVRĐUJE namjeru EU-a da pojača potporu međunarodnom poretku utemeljenom na pravilima, u čijem su središtu Ujedinjeni narodi;

3. u skladu sa zaključcima Vijeća o Strategiji EU-a za kibersigurnost i sa Strateškim kompasom, PONOVNO ISTIČE potrebu za razvojem položaja Unije u pogledu kiberprostora jačanjem naše sposobnosti sprečavanja kibernapada putem izgradnje kapaciteta, razvoja sposobnosti, osposobljavanja, vježbi, veće otpornosti te odlučnim odgovorom na kibernapade usmjerene na EU i njegove države članice uz upotrebu svih dostupnih alata EU-a. To uključuje daljnje pokazivanje odlučnosti EU-a da pruži neposredne i dugoročne odgovore akterima koji predstavljaju prijetnju i koji nam nastoje uskratiti siguran i otvoren pristup kiberprostoru i utjecati na naše strateške interese, uključujući sigurnost naših partnera; u tom kontekstu NAGLAŠAVA da se položajem u pogledu kiberprostora nastoje kombinirati različite inicijative koje su dio djelovanja EU-a za konsolidaciju mira i stabilnosti u kiberprostoru te u cilju otvorenog, slobodnog, stabilnog i sigurnog kiberprostora, pri čemu se bolje koordiniraju kratkoročna, srednjoročna i dugoročna djelovanja za sprečavanje, suzbijanje i odvraćanje od kiberprijetnji i kibernapada i odgovor na njih te za iskorištavanje kibersposobnosti; NAGLAŠAVA da bi te elemente trebalo uključiti u položaj EU-a u pogledu kiberprostora, u skladu s pet funkcija EU-a u kiberdomeni, a to su: jačanje naše kiberotpornosti i sposobnosti za zaštitu; poboljšanje sveobuhvatnog upravljanja krizama utemeljenog na solidarnosti; promicanje naše vizije kiberprostora; jačanje suradnje s partnerskim zemljama i međunarodnim organizacijama; sprečavanje i obrana od kibernapada i odgovor na njih;

I. JAČANJE NAŠE KIBEROTPORNOSTI I SPOSOBNOSTI ZA ZAŠTITU

4. PONOVNO ISTIČE potrebu za povećanjem ukupne razine kibersigurnosti EU-a, SA ZANIMANJEM OČEKUJE brzo donošenje Nacrta direktive o mjerama za postizanje visoke zajedničke razine kibersigurnosti širom Unije (NIS), Nacrta uredbe o digitalnoj operativnoj otpornosti za financijski sektor (DORA) i Nacrta direktive o otpornosti ključnih subjekata (CER) te PRIMA NA ZNANJE Prijedlog uredbe o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije kako bi se potaknula Europska unija koja štiti svoje građane, javne usluge i poduzeća u kiberprostoru; POTIČE Komisiju da dovrši donošenje ključnih prijedloga za osiguravanje sigurnosti digitalnih infrastruktura, tehnologija i proizvoda kako bi se poslala jasna poruka o ambicijama EU-a u pogledu tih tema i omogućila potpora poduzećima kako bi se mogla suočiti s tim izazovom; POZIVA Komisiju da predloži zajedničke EU-ove kibersigurnosne zahtjeve za povezane uređaje i povezane procese i usluge putem Akta o kiberotpornosti, koji bi Komisija trebala predložiti prije kraja 2022., uzimajući u obzir potrebu za horizontalnim i cjelovitim pristupom koji obuhvaća cijeli životni vijek digitalnih proizvoda, kao i postojeće propise, posebno u području kibersigurnosti;

5. POZIVA relevantna tijela, kao što su Tijelo europskih regulatora za elektroničke komunikacije (BEREC), Agencija Europske unije za kibersigurnost (ENISA) i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava (NIS), zajedno s Europskom komisijom, da na temelju procjene rizika izrade preporuke državama članicama i Europskoj komisiji kako bi se ojačala otpornost komunikacijskih mreža i infrastruktura u Europskoj uniji, uključujući nastavak provedbe paketa mjera EU-a za 5G;

6. POZIVA EU i njegove države članice da pojačaju napore za povećanje ukupne razine kibersigurnosti, na primjer olakšavanjem pojave pouzdanih pružatelja kibersigurnosnih usluga, i NAGLAŠAVA da bi poticanje razvoja takvih pružatelja usluga trebalo biti prioritet industrijske politike EU-a u području kibersigurnosti; kako bi se bolje oduprlo kibernapadima s mogućim sistemskim učincima te na temelju iskustava iz postupanja s ranjivostima nakon napada na Solarwinds, Microsoft Exchange i Apache Log4J, POZIVA Komisiju da predloži mogućnosti za poticanje stvaranja pouzdane industrije kibersigurnosnih usluga, ojača kibersigurnost lanca opskrbe informacijske i komunikacijske tehnologije, pozabavi se mogućim učincima ranjivosti softvera za EU i njegove države članice, među ostalim s obzirom na predstojeći Akt o kiberotpornosti, i poboljša sposobnosti za otkrivanje kiberprijetnji i razmjenu informacija o njima u državama članicama i među njima;

7. PONOVNO ISTIČUĆI da su ulaganje u inovacije i bolje iskorištavanje civilne tehnologije ključni za jačanje naše tehnološke suverenosti, među ostalim u kiberdomeni, POZIVA Komisiju da brzo operacionalizira Europski centar za stručnost u području kibersigurnosti radi razvoja snažnog europskog istraživačkog, industrijskog i tehnološkog ekosustava u kiberpodručju, ISTIČE potrebu za poticanjem istraživanja i inovacija, većim ulaganjem u civilna i obrambena područja radi jačanja EU-ove obrambene tehnološke i industrijske baze (EDTIB) i razvojem kibersposobnosti EU-a i njegovih država članica, uključujući sposobnosti strateške potpore; NAGLAŠAVA važnost intenzivne upotrebe nove tehnologije, posebice kvantnog računalstva, umjetne inteligencije i velike količine podataka, kako bi se ostvarile komparativne prednosti, među ostalim u pogledu operacija odgovora na kibernapade;

8. PREPOZNAJUĆI da je jačanje naše kibersigurnosti način povećanja učinkovitosti i sigurnosti naših napora na kopnu, u zraku, na moru i u svemiru, NAGLAŠAVA važnost uključivanja pitanja kibersigurnosti u sve javne politike EU-a, uključujući sektorsko zakonodavstvo kojim se dopunjuje Direktiva NIS 2, i POZIVA Komisiju da istraži mogućnosti za povećanje kibersigurnosti u cijelom opskrbnom lancu EU-ove obrambene tehnološke i industrijske baze (EDTIB);

9. POTVRĐUJE da su osiguravanje odgovarajućih financijskih i ljudskih resursa za kibersigurnost i mjere usmjerene na stvaranje povoljnog okružja kako bi privatni sektor bio konkurentan ključni za razvoj položaja EU-a u pogledu kiberprostora te da bi se pitanje stabilnog i dugoročnog financiranja kibersigurnosti trebalo rješavati i na razini EU-a osmišljavanjem i provedbom horizontalnog mehanizma koji kombinira više izvora financiranja, uključujući trošak visokokvalificiranih ljudskih resursa; stoga POZIVA Komisiju da prije kraja 2022. istraži mogućnosti za takav mehanizam, o kojima se treba raspravljati u okviru relevantnih tijela Vijeća;

10. NAGLAŠAVA potrebu za jačanjem naših napora i povećanjem suradnje u borbi protiv međunarodnog kiberkriminaliteta, posebno ucjenjivačkog softvera, putem mehanizma EMPACT (Europska multidisciplinarna platforma za borbu protiv kaznenih djela), razmjenama među sektorima kibersigurnosti, kaznenog progona i diplomacije i jačanjem kapaciteta za kazneni progon u istragama i progonu kiberkriminaliteta; PONOVNO ISTIČE svoju predanost informiranju javnosti o kiberprijetnjama i mjerama poduzetima na nacionalnoj razini i razini EU-a protiv tih prijetnji uključivanjem civilnog društva, privatnog sektora i akademske zajednice, u cilju podizanja svijesti i poticanja odgovarajuće razine kiberzaštite i kiberhigijene; NAGLAŠAVA da je potrebno usredotočiti se na vještine i sposobnosti građana u području kibersigurnosti na razini EU-a i država članica te da je potrebno aktivno uključiti korisnike u njihovu vlastitu zaštitu;

II. **POBOLJŠANJE SVEOBUHVATNOG UPRAVLJANJA KRIZAMA UTEMELJENOG NA SOLIDARNOSTI**

11. na temelju godišnjih kibervježbi, drugih vježbi koje uključuju kiberdimenziju i vježbi u području kibersigurnosti EU CyCLES za 2022., NAGLAŠAVA važnost uspostave programa redovitih kibervježbi među zajednicama i na više razina kako bi se testirao i razvio unutarnji i vanjski odgovor EU-a na kiberincidente velikih razmjera, uz sudjelovanje Vijeća, ESVD-a, Komisije i relevantnih dionika kao što su ENISA i privatni sektor, pri čemu će se taj program razraditi i doprinijeti općoj politici EU-a u području vježbi; NAGLAŠAVA važnost daljnjeg razvoja vježbi Cyber Europe i BlueOlEx, kojima se kombinira odgovor na različitim razinama; PREPOZNAJE potrebu za evaluacijom i konsolidacijom postojećih vježbi i istraživanjem mogućnosti daljnjih vježbi u određenim segmentima kiberdomene, posebno vojne vježbe CERT-a i vježbe usmjerene na suradnju među institucijama, tijelima i agencijama EU-a u kriznim situacijama; POTVRĐUJE da će se položajem EU-a u pogledu kiberprostora ojačati naša sposobnost sprečavanja kibernapada putem različitih djelovanja, uključujući osposobljavanje, i stoga POZIVA države članice da poboljšaju civilno-vojnu suradnju u osposobljavanju u kiberpodručju i zajedničkim vježbama;

12. ISTIČE potrebu za daljnjim ispitivanjem i jačanjem operativne suradnje i zajedničke informiranosti o stanju među državama članicama, među ostalim putem uspostavljenih mreža kao što su mreža CSIRT-ova i Europska mreža organizacija za vezu za kiberkrize (EU-CyCLONe) kako bi se unaprijedila pripravnost EU-a za suočavanje s kiberincidentima velikih razmjera; ISTIČE važnost rada na razvoju zajedničkog jezika među državama članicama i s institucijama, tijelima i agencijama EU-a, koji je prilagođen za raspravu na političkoj razini, kako bi se poduprla uspostava konsolidirane procjene ozbiljnosti i učinka relevantnih kiberincidenata, kao i mogućih scenarija razvoja i potreba koje iz njih proizlaze, ako to bude prikladno; u tom pogledu ISTIČE potrebu za poboljšanjem komplementarnosti zajedničkih izvješća o procjeni stanja, uključujući izvješća mreže EU-CyCLONe o učinku i ozbiljnosti kiberincidenata velikih razmjera diljem država članica EU-a i procjene prijetnji koje provodi EU INTCEN u okviru alata EU-a za kiberdiplomaciju; POZIVA Komisiju, visokog predstavnika i Skupinu za suradnju u području sigurnosti mrežnih i informacijskih sustava da u koordinaciji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, do kraja 2022. provedu evaluaciju rizika i izrade scenarije rizika iz perspektive kibersigurnosti u situaciji prijetnje ili mogućeg napada na države članice ili partnerske zemlje te da ih predstave relevantnim tijelima Vijeća; NAGLAŠAVA potrebu za odgovarajućom i koordiniranom javnom komunikacijom o odgovoru EU-a na kiberincidente velikih razmjera;

13. u slučaju kiberincidenta velikih razmjera NAGLAŠAVA potrebu za jačanjem koordinacije i, prema potrebi, na temelju postignutog napretka i rada timova za brz odgovor na kiberincidente u okviru PESCO-a te na temelju rada mreže CSIRT-ova i mreže EU-CyCLONe, dobrovoljnog udruživanja kapaciteta za odgovor na incidente među državama članicama; PREPOZNAJE da bi razvoj veza s privatnim sektorom mogao povećati javne kapacitete, posebno u kontekstu nedostatka vještina diljem EU-a, te da bi utvrđivanje i koordinacija tih privatnih partnera mogli imati utjecaja u slučaju incidenata velikih razmjera; kako bi se u potpunosti pripremilo za suočavanje s kiberincidentima velikih razmjera, POZIVA Komisiju da do kraja trećeg tromjesečja 2022. predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibersigurnosti;

14. u skladu sa Strateškim kompasom, PONOVNO ISTIČE potrebu za ulaganjem u našu uzajamnu pomoć na temelju članka 42. stavka 7. Ugovora o Europskoj uniji, kao i u solidarnost na temelju članka 222. Ugovora o funkcioniranju Europske unije, posebno čestim vježbama; u tom okviru NAGLAŠAVA potrebu za daljnjim radom na pružanju i koordinaciji bilateralne civilne i/ili vojne potpore, među ostalim istraživanjem moguće potpore koju pruža EU na izričit zahtjev država članica te na utvrđivanju odgovarajućih mjera odgovora, među ostalim razvojem koordinirane komunikacijske strategije u kontekstu provedbe članka 42. stavka 7.; NAPOMINJE da bi to također trebalo uključivati istraživanje poveznica s postojećim mehanizmima EU-a za upravljanje krizama i Mehanizmom EU-a za civilnu zaštitu;

15. ISTIČE da će pojačan položaj EU-a u pogledu kiberprostora zahtijevati bolju sigurnu komunikaciju; u tu svrhu PONOVNO ISTIČE smjernice iz Strateškog kompasa u vezi s time i POZIVA Komisiju i druge relevantne institucije, tijela i agencije da do kraja 2022.izrade pregled postojećih alata za sigurnu komunikaciju u kiberpodručju o kojima treba raspravljati u okviru relevantnih tijela Vijeća i s relevantnim skupinama za suradnju, kao što su mreža CSIRT-ova i EU-CyCLONe;

III. PROMICANJE NAŠE VIZIJE KIBERPROSTORA

16. 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 predanost EU-a mirnom rješavanju međunarodnih sporova u kiberprostoru i primjeni međunarodnog prava, uključujući međunarodno pravo o ljudskim pravima i međunarodno humanitarno pravo, na djelovanja država u kiberprostoru; ISTIČE predanost EU-a i njegovih država članica djelovanju u skladu s dobrovoljnim, neobvezujućim normama odgovornog ponašanja država u kiberprostoru koje su dogovorile sve države članice UN-a; NAGLAŠAVA važnost otvorenog, slobodnog, globalnog, stabilnog i sigurnog kiberprostora u kojem se u potpunosti primjenjuju ljudska prava, temeljne slobode i vladavina prava kao potpora socijalnoj dobrobiti, gospodarskom rastu, prosperitetu i integritetu naših slobodnih i demokratskih društava te PONOVNO POTVRĐUJE predanost EU-a i njegovih država članica daljnjem promicanju tih vrijednosti i načela; u cilju razvoja kanala za konstruktivan, iskren i otvoren dijalog s ključnim dionicima u kiberprostoru, NAGLAŠAVA važnost toga da kiberpitanja, uključujući alate EU-a za kiberdiplomaciju, postanu sastavni dio pregovora o pristupanju Uniji te strateških i političkih dijaloga EU-a s međunarodnim partnerima i konkurentima te istodobno POZIVA visokog predstavnika da preispita postojeće bilateralne dijaloge o kiberprostoru i, prema potrebi, predloži pokretanje slične suradnje s dodatnim zemljama ili relevantnim međunarodnim organizacijama;

17. PODSJEĆA na važnost suradnje više dionika jer i drugi dionici snose odgovornost za kibersigurnost, posebno kad je riječ o provedbi preporuka i odluka donesenih na međunarodnim i regionalnim forumima; POZIVA EU i njegove države članice da nastave promicati naš model kiberprostora i interneta na temelju pristupa koji uključuje više dionika i putem inicijativa kao što su Pariški poziv za povjerenje i sigurnost u kiberprostoru i Deklaracija o budućnosti interneta, čime se naglasak stavlja na zajedničke koristi od stabilnosti u kiberprostoru i podiže globalna svijest o opasnostima vizije interneta koja je usmjerena na državu i autoritarna, te POZIVA EU i njegove države članice da dodatno ojačaju suradnju sa širom zajednicom dionika, među ostalim iskorištavanjem relevantnih projekata kao što su inicijativa EU-a za kiberdiplomaciju u okviru EU-ova instrumenta vanjske politike;

18. OBVEZUJE se kontinuirano sudjelovati u relevantnim međunarodnim organizacijama, posebno u postupcima povezanima s prvim i trećim odborom UN-a, naglašavajući pritom da se postojeće međunarodno pravo bez zadrške primjenjuje u kiberprostoru i u pogledu njega; NAGLAŠAVA važnost stalnih napora za očuvanje i promicanje okvira UN-a za odgovorno ponašanje država i ISTIČE da će EU i njegove države članice aktivno raditi na jačanju njegove provedbe, među ostalim uspostavom Programa djelovanja za poticanje odgovornog ponašanja država u kiberprostoru; NAGLAŠAVA da će EU i njegove države članice aktivno sudjelovati u pregovorima o budućoj konvenciji UN-a koja će tijelima kaznenog progona i pravosudnim tijelima služiti kao djelotvoran instrument u globalnoj borbi protiv kiberkriminaliteta, uzimajući u potpunosti u obzir postojeći okvir međunarodnih i regionalnih instrumenata u tom području, posebno Budimpeštansku konvenciju o kibernetičkom kriminalu; NAGLAŠAVA važnost daljnjeg podupiranja razvoja i operacionalizacije mjera za izgradnju povjerenja na regionalnoj i međunarodnoj razini te daljnjeg poticanja upotrebe postojećih mjera za razvoj povjerenja u okviru OESS-a, među ostalim u razdobljima međunarodnih napetosti;

19. PODSJEĆA da je proaktivan pristup koji se temelji na ljudskim pravima kako bi se osigurali međunarodni standardi u području tehnologija u nastajanju i temeljne internetske arhitekture u skladu s demokratskim vrijednostima i načelima ključan kako bi se osiguralo da internet ostane globalan, nefragmentiran i otvoren te PODUPIRE načelo da se upotrebom i razvojem tehnologija poštuju ljudska prava, da su usmjereni na privatnost te da je njihova upotreba zakonita, sigurna i etička; POTIČE visokog predstavnika i Komisiju da razviju stratešku viziju o tehničkim pitanjima u digitalnom području koja imaju posljedice na vanjsku politiku i koja bi mogla utjecati na stabilnost kiberprostora, a posebno interneta, među ostalim u relevantnim specijaliziranim međunarodnim organizacijama (Međunarodna unija za telekomunikacije itd.);

IV. JAČANJE MEĐUNARODNE SURADNJE S PARTNERSKIM ZEMLJAMA I MEĐUNARODNIM ORGANIZACIJAMA

20. ISTIČE potrebu za boljim povezivanjem strategije EU-a za izgradnju kiberkapaciteta s UN-ovim normama odgovornog ponašanja država u kiberprostoru, među ostalim razvojem prilagođenih programa suradnje i izgradnje kapaciteta kako bi se trećim zemljama pružila potpora u njihovim naporima u provedbi, a pritom i dalje proširili naši napori za promicanje Programa djelovanja UN-a za poticanje odgovornog ponašanja država u kiberprostoru; NAGLAŠAVA važnost potpunog uključivanja izgradnje kiberkapaciteta kao dijela ponude EU-a kao pružatelja sigurnosti, uz odgovarajuću koordinaciju napora između država članica i institucija, tijela i agencija EU-a, a posebno POZDRAVLJA suradnju među državama članicama, kao i s partnerima iz javnog i privatnog sektora, posebno putem mreže EU CyberNet (mreža EU-a za izgradnju kiberkapaciteta) i Globalnog foruma o kiberstručnosti (GFCE), kako bi se osigurala koordinacija i izbjeglo udvostručavanje;

POZIVA visokog predstavnika i Komisiju da do trećeg tromjesječja 2022. osnuju *odbor za izgradnju kiberkapaciteta* i da redovito razmjenjuju informacije u okviru Horizontalne radne skupine za kiberpitanja; POZIVA Komisiju i visokog predstavnika da dodatno mobiliziraju Instrument za susjedstvo, razvoj i međunarodnu suradnju (NDICI), Instrument pretpristupne pomoći (IPA III) i druge financijske instrumente, kao što su Europski instrument mirovne pomoći (EPF) i inicijativa Global Gateway, kako bi se poduprlo jačanje otpornosti naših partnera, njihove sposobnosti za utvrđivanje i suzbijanje kiberprijetnji te za istragu i kazneni progon kiberkriminaliteta te razvoj projekata suradnje, među ostalim posebno u kontekstu

krize, POTIČE suradnju s partnerima na zapadnom Balkanu i u istočnom i južnom susjedstvu EU-a te raspoređivanje stručnjaka EU-a i država članica kako bi pružili potporu u kiberkrizama, uzimajući u obzir postojeće pravne mandate;

21. NAGLAŠAVA da je potrebno pojačati napore za razvoj strukturiranog i otvorenog pristupa EU-a informiranju javnosti o tome kako promicati globalno zajedničko razumijevanje primjene međunarodnog prava u kiberprostoru, okvira UN-a za odgovorno ponašanje država u kiberprostoru, uključujući inicijativu za Program djelovanja za promicanje odgovornog ponašanja država u kiberprostoru, kao i o stajalištu EU-a i njegovih država članica u tekućim pregovorima o konvenciji UN-a o kiberkriminalitetu, te u okviru tih napora ZAHTIJEVA od visokog predstavnika da do kraja 2022. Vijeću predstavi plan informiranja; POTIČE visokog predstavnika i službe Komisije da u potpunosti i sustavno iskoriste 145 delegacije i da razviju redovitu, plodnu suradnju između njih i veleposlanstava država članica u trećim zemljama, pod okriljem predviđene mreže EU-a za kiberdiplomaciju; POZIVA visokog predstavnika da do trećeg tromjesečja 2022. uspostavi mrežu EU-a za kiberdiplomaciju, čime bi se doprinijelo razmjeni informacija, zajedničkim aktivnostima osposobljavanja osoblja EU-a i država članica, dosljednim naporima za izgradnju kapaciteta i jačanju provedbe okvira UN-a za odgovorno ponašanje država, kao i mjerama za izgradnju povjerenja među državama;

22. NAGLAŠAVA svoju predanost daljnjoj suradnji s međunarodnim organizacijama kako bi se unaprijedilo zajedničko razumijevanje okružja kiberprijetnji, razvili mehanizmi suradnje i proaktivno utvrdili zajednički diplomatski odgovori; PODSJEĆAJUĆI na ključna postignuća suradnje EU-a i NATO-a u području kibersigurnosti u okviru provedbe zajedničkih izjava iz Varšave iz 2016. i Bruxellesa iz 2018., uz potpuno poštovanje autonomije u donošenju odluka i postupaka obiju organizacija te na temelju načela transparentnosti, uzajamnosti i uključivosti, NAGLAŠAVA potrebu za daljnjim jačanjem kibersuradnje s NATO-om putem vježbi, razmjene informacija i razmjene među stručnjacima, među ostalim u pogledu razvoja sposobnosti, izgradnje kapaciteta partnera te misija i operacija, kao i u pogledu primjenjivosti međunarodnog prava i normi UN-a o odgovornom ponašanju država u kiberprostoru, te za daljnjim jačanjem mogućih koordiniranih odgovora na zlonamjerne kiberaktivnosti;

V. SPREČAVANJE I OBRANA OD KIBERNAPADA I ODGOVOR NA NJIH

23. PREPOZNAJE da je kiberprostor postao područje geopolitičkog natjecanja te stoga PONOVNO ISTIČE da EU mora moći brzo i odlučno odgovoriti na kibernapade, kao što su zlonamjerne kiberaktivnosti pod pokroviteljstvom države usmjerene na EU i njegove države članice, te stoga treba ojačati alate EU-a za kiberdiplomaciju i u potpunosti iskoristiti sve svoje instrumente, uključujući dostupne političke, gospodarske, diplomatske, pravne i strateške komunikacijske alate za sprečavanje i suzbijanje zlonamjernih kiberaktivnosti, odvraćanje od njih i odgovor na njih; ISTIČE da neprijateljski akteri trebaju biti svjesni da će se kibernapadi na države članice i institucije EU-a otkriti u ranoj fazi, brzo identificirati i da će se na njih odgovoriti svim potrebnim alatima i politikama; oslanjajući se posebno na elemente položaja u pogledu kiberprostora koji su u njemu sadržani i na pouke izvučene iz provedbe alata EU-a za kiberdiplomaciju od njegova početka te iz vježbe u području kibersigurnosti (EU CyCLES), POZIVA države članice i visokog predstavnika da uz potporu Komisije do kraja prvog tromjesečja 2023. rade na revidiranoj verziji provedbenih smjernica paketa alata EU-a za kiberdiplomaciju, posebno razmatranjem dodatnih mjera odgovora;

24. ISTIČE potrebu za održavanjem redovitih razmjena informacija o kiberprijetnjama u relevantnim tijelima i odborima Vijeća, uz redovitu suradnju s privatnim sektorom i na temelju procjene učinka i ozbiljnosti nedavnih incidenata, kako bi se povećala opća osviještenost i pripravnost za daljnje primjene alata EU-a za kiberdiplomaciju te razvili dodatni alati za potporu njegovoj provedbi; iako je nacionalna sigurnost i dalje isključiva odgovornost svake države članice, PRIMA NA ZNANJE potrebu za jačanjem razmjene obavještajnih podataka i informacija te suradnje među državama članicama, kao i s centrom EU INTCEN kako bi se na početku postupka donošenja odluka, među ostalim o pitanju pripisivanja odgovornosti, mogli razmjenjivati obavještajni podaci i tako omogućiti brz, učinkovit i utemeljen odgovor na zlonamjerne kiberaktivnosti usmjerene na EU i njegove partnere; PONOVNO ISTIČE važnost jačanja kapaciteta centra EU INTCEN u kiberdomeni, na temelju dobrovoljnih obavještajnih doprinosa iz država članica i ne dovodeći u pitanje njihove nadležnosti, te važnost razmatranja prijedloga o mogućem osnivanju radne skupine država članica za kiberobavještajne podatke;

25. POTVRĐUJUĆI da su izjave EU-a i mjere ograničavanja poduzete u okviru alata EU-a za kiberdiplomaciju poslale snažnu poruku da su zlonamjerne kiberaktivnosti koje predstavljaju vanjsku prijetnju EU-u, njegovim državama članicama i partnerima neprihvatljive i da tako doprinose sprečavanju, suzbijanju, odvraćanju od zlonamjernih kiberaktivnosti i odgovoru na njih, PONOVNO ISTIČE svoju predanost primjeni tih mjera u cilju podsjećanja na obveze koje se primjenjuju na kiberprostor na temelju međunarodnog prava, uključujući Povelju UN-a u cijelosti, i poticanju okvira UN-a za odgovorno ponašanje država u kiberprostoru, uključujući obvezu dužne pažnje svih država da svjesno ne dopuste da se njihovo državno područje upotrebljava za međunarodno protupravna djela upotrebom IKT-a, s ciljem daljnjeg razvoja i promicanja zajedničkog stajališta EU-a o primjeni međunarodnog prava u kiberprostoru; primjećujući da odgovarajuće i brze poruke ublažavaju rizike od eskalacije i mogu odvratiti napadače koji su usmjereni protiv europskih interesa, POZIVA visokog predstavnika da razvije i državama članicama podnese usklađenu komunikacijsku strategiju o upotrebi alata EU-a za kiberdiplomaciju;

26. POTIČE razvoj postupnih, ciljanih i trajnih pristupa i odgovora na zlonamjerne kiberaktivnosti upotrebom širokog raspona alata EU-a za kiberdiplomaciju, uključujući režim EU-a za kibersankcije, te predviđanjem dodatnih mjera; NAGLAŠAVA da je potrebno povećati mogućnost mobilizacije, na pojedinačnoj osnovi, svih dostupnih alata, unutarnjih i vanjskih, za sprečavanje, suzbijanje i odvraćanje od kibernapada i odgovor za njih, njihovom primjenom u brzom, učinkovitom, postupnom, ciljanom i održivom pristupu koji se temelji na dugoročnom strateškom angažmanu; POZIVA visokog predstavnika da u suradnji s Komisijom utvrdi moguće zajedničke odgovore EU-a na kibernapade, uključujući mogućnosti za sankcije, u cijelom spektru kako bi se pripremilo za poduzimanje brzih i učinkovitih djelovanja kada je to potrebno i za njihovo predstavljanje Vijeću do kraja prvog tromjesečja 2023.;

27. imajući u vidu da je kiberobrana prvenstveno u nacionalnoj nadležnosti, POTIČE države članice da dodatno razviju vlastite kapacitete za provođenje operacija kiberobrane, uključujući proaktivne mjere za zaštitu, otkrivanje i obranu od kibernapada te odvraćanje od njih, te po mogućnosti kao potporu drugim državama članicama i EU-u; svaka država članica potiče se da, prema potrebi, poveća svoje sposobnosti za pružanje i primanje pomoći i potpore; NAGLAŠAVA da bi daljnji razvoj tih sposobnosti trebao biti jedan od ključnih ciljeva predstojeće politike kiberobrane EU-a; NAPOMINJE da bi se u okviru politike kiberobrane EU-a trebalo voditi više računa o ulozi koju relevantne institucije i tijela EU-a mogu imati u povećanju suradnje među relevantnim akterima u području kiberobrane iz EU-a i država članica te u razvoju vlastitih kapaciteta, u skladu s njihovim mandatima; POZIVA visokog predstavnika da zajedno s Komisijom dopuni razvoj položaja EU-a u pogledu kiberprostora podnošenjem ambicioznog prijedloga za politiku kiberobrane EU-a u 2022., čime će se utrti put Vijeću za daljnji razvoj položaja EU-a u pogledu kiberprostora;

28. NAGLAŠAVA potrebu za povećanjem interoperabilnosti i razmjene informacija suradnjom među vojnim timovima za hitne računalne intervencije (MilCERT); POZIVA države članice da na temelju rada Europske obrambene agencije (EDA) uspostave mrežu MilCERT za razvoj suradnje i olakšavanje razmjene informacija, što bi također pomoglo u poticanju koordinacije s drugim kiberzajednicama, kao i mrežu vojnih zapovjednika za kiberobranu kako bi se ojačala strateška suradnja između zapovjedništva država članica EU-a za kiberobranu ili drugih odgovarajućih tijela; uspostavom tih mreža, zajedno s projektima u okviru PESCO-a u području kibersigurnosti, doprinijelo bi se jačanju kiberobrane na razini EU-a; naglašava važnost suradnje između predložene mreže milCERT i već postojeće civilne mreže (CSIRT-ovi) kako bi se poboljšale razmjena informacija i informiranost o stanju;

29. na temelju vojne vizije EU-a i strategije EU-a o kiberprostoru kao području operacija te primajući na znanje tekući razvoj vojnog koncepta kiberobrane za vojne operacije i misije pod vodstvom EU-a, PONOVNO ISTIČE potrebu za uključivanjem kiberdimenzije u planiranje i provođenje misija i operacija ZSOP-a, među ostalim jačanjem njihovih kibersposobnosti, te NAGLAŠAVA da će se time doprinijeti boljoj informiranosti o stanju u kiberprostoru na razini EU-a;

30. zaključno, PRIMA NA ZNANJE da će stajalište u pogledu kiberprostora biti korak prema uspostavi doktrine EU-a za djelovanje u kiberprostoru, na temelju povećane otpornosti, sposobnosti i mogućnosti odgovora, kao i zajedničkog stajališta o primjeni međunarodnog prava u kiberprostoru. Vijeće će u 2023. RAZMOTRITI napredak ostvaren u provedbi ovih zaključaka kako bi osiguralo daljnji razvoj stajališta EU-a u pogledu kiberprostora.