Svet
Evropske unije

Bruselj, 23. maj 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	

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	23. maj 2022
Prejemnik:	delegacije
Zadeva:	Sklepi Sveta o vzpostavitvi stališča Evropske unije glede kibernetskih vprašanj – sklepi, ki jih je Svet odobril na seji 23. maja 2022

V prilogi vam pošiljamo Sklepe Sveta o vzpostavitvi stališča Evropske unije glede kibernetskih vprašanj, ki jih je Svet odobril na seji 23. maja 2022.

PRILOGA

Sklepi Sveta o vzpostavitvi stališča Evropske unije glede kibernetskih vprašanj

SVET EVROPSKE UNIJE –

OB OPOZARJANJU na svoje sklepe o:

– Skupnem sporočilu Evropskemu parlamentu in Svetu z dne 25. junija 2013 „Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor“[1],

– okviru EU za politiko kibernetske obrambe[2],

– upravljanju interneta[3],

– kibernetski diplomaciji[4],

– krepitvi odpornosti evropskega sistema kibernetske varnosti ter spodbujanju konkurenčne in inovativne industrije kibernetske varnosti[5],

– Skupnem sporočilu Evropskemu parlamentu in Svetu z dne 20. novembra 2017: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“[6],

– okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“)[7],

– usklajenem odzivu EU na velike kibernetske incidente in krize[8],

– smernicah za krepitev zunanjih kibernetskih zmogljivosti EU[9],

– Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize[10],

---

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

– krepitvi zmogljivosti in zmožnosti na področju kibernetske varnosti v EU[11],

– pomenu omrežij 5G za evropsko gospodarstvo in dejstvu, da je treba zmanjšati varnostna tveganja, povezana z njimi[12],

– prihodnosti visoko digitalizirane Evrope po letu 2020 z naslovom „Krepitev digitalne in gospodarske konkurenčnosti v Uniji ter digitalna kohezija“[13],

– dopolnilnih prizadevanjih za krepitev odpornosti in preprečevanje hibridnih groženj[14],

– oblikovanju digitalne prihodnosti Evrope[15],

– kibernetski varnosti povezanih naprav[16],

– strategiji EU za kibernetsko varnost v digitalnem desetletju[17],

– varnosti in obrambi[18],

– preučitvi potenciala pobude za skupno kibernetsko enoto – dopolnjevanje usklajenega odziva EU na velike kibernetske incidente in krize[19],

– Strateški kompas za varnost in obrambo – Za Evropsko unijo, ki varuje svoje državljane in državljanke, vrednote in interese ter prispeva k mednarodnemu miru in varnosti[20],

---

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

1. POUDARJA, da se je zlonamerno ravnanje državnih in tudi nedržavnih akterjev v kibernetskem prostoru v zadnjih letih okrepilo, vključno z velikim in nenehnim porastom zlonamernih dejavnosti, uperjenih proti kritični infrastrukturi, dobavnim verigam in intelektualni lastnini EU in njenih držav članic, povečanim tveganjem učinkov prelivanja in vedno pogostejšimi napadi z izsiljevalskim programjem na naša podjetja, organizacije in državljane ter državljanke. UGOTAVLJA, da ob vračanju politike moči nekatere države vedno bolj skušajo izpodbijati in spodkopavati na pravilih temelječ mednarodni red v kibernetskem prostoru, s čimer postaja kibernetsko področje poleg odprtega morja, zračnega prostora in vesolja vse bolj sporno področje. PRIZNAVA, da vedno pogostejši veliki kibernetski napadi ali poskusi vdora, motenja ali uničevanja omrežij in informacijskih sistemov s sistemskimi učinki lahko ogrozijo našo gospodarsko varnost in vplivajo na naše demokratične institucije in procese, kažejo pa tudi na pripravljenost nekaterih akterjev, da ogrozijo mednarodno varnost in stabilnost. POUDARJA, da je vojaška agresija Rusije proti Ukrajini pokazala, da se ofenzivne kibernetske dejavnosti lahko izvajajo kot sestavni del hibridnih strategij, ki združujejo ustrahovanje, destabilizacijo in gospodarske motnje.

2. PONAVLJA, da je ob trenutnih geopolitičnih premikih moč naše Unije v enotnosti, solidarnosti in odločenosti ter da bo izvajanje strateškega kompasa okrepilo strateško avtonomijo EU in njeno sposobnost sodelovanja s partnerji pri zaščiti njenih vrednot in interesov, tudi na kibernetskem področju. POUDARJA, da bo močnejša in sposobnejša EU na področju varnosti in obrambe pozitivno prispevala k svetovni in čezatlantski varnosti ter dopolnjevala NATO, ki ostaja temelj kolektivne obrambe svojih članic. PONOVNO POTRJUJE, da EU namerava okrepiti podporo na pravilih temelječemu mednarodnemu redu, v središču katerega so Združeni narodi.

3. V skladu s sklepi Sveta o strategiji EU za kibernetsko varnost in strateškim kompasom VZTRAJA, da je treba oblikovati stališče Unije glede kibernetskih vprašanj tako, da se z uporabo vseh razpoložljivih orodij EU okrepi naša sposobnost preprečevanja kibernetskih napadov, in sicer s krepitvijo zmogljivosti in razvojem zmožnosti, usposabljanjem, vajami, okrepljeno odpornostjo ter odločnim odzivanjem na kibernetske napade zoper EU in njene države članice. Poleg tega bo EU akterjem groženj, ki si prizadevajo, da bi nam onemogočili varen in odprt dostop do kibernetskega prostora ter vplivali na naše strateške interese, vključno z varnostjo naših partnerjev, nadalje pokazala, da je odločena zagotoviti takojšnje in dolgoročne odzive. V zvezi s tem POUDARJA, da je cilj stališča glede kibernetskih vprašanj združiti različne pobude, ki prispevajo k ukrepom EU za utrjevanje miru in stabilnosti v kibernetskem prostoru ter v prid odprtemu, svobodnemu, globalnemu, stabilnemu in varnemu kibernetskemu prostoru, obenem pa bolje usklajevati kratkoročne, srednjeročne in dolgoročne ukrepe za preprečevanje kibernetskih groženj in napadov, odvračanje od njih in odzivanje nanje ter izkoristiti kibernetske zmožnosti. POUDARJA, da bi ti elementi morali biti vključeni v stališče EU glede kibernetskih vprašanj glede na pet funkcij EU na kibernetskem področju, in sicer okrepitev naše kibernetske odpornosti in zmogljivosti za zaščito; okrepitev solidarnostnega in celovitega kriznega upravljanja; spodbujanje naše vizije kibernetskega prostora; okrepitev sodelovanja s partnerskimi državami in mednarodnimi organizacijami; preprečevanje kibernetskih napadov, zaščito pred njimi in odzivanje nanje.

I. OKREPITEV NAŠE KIBERNETSKE ODPORNOSTI IN ZMOGLJIVOSTI ZA ZAŠČITO

4. PONOVNO POUDARJA, da je treba zvišati splošno raven kibernetske varnosti v EU, Z ZANIMANJEM PRIČAKUJE hitro sprejetje osnutka direktive o ukrepih za doseganje visoke skupne ravni kibernetske varnosti v Uniji, osnutka uredbe o digitalni operativni odpornosti za finančni sektor (DORA), osnutka direktive o odpornosti kritičnih subjektov in SE SEZNANJA s predlogom uredbe o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije, da bi spodbujali Evropsko unijo, ki ščiti svoje državljane in državljanke, javne storitve in podjetja v kibernetskem prostoru. SPODBUJA Komisijo, naj dokončno sprejme ključne predloge za zagotovitev varnosti digitalne infrastrukture, tehnologij, proizvodov in storitev, da bi poslala jasno sporočilo o ambicijah EU na teh področjih in omogočila podporo podjetjem, da bi bila kos tem izzivom. POZIVA Komisijo, naj v aktu o kibernetski odpornosti predlaga skupne zahteve EU glede kibernetske varnosti za povezane naprave ter z njimi povezane procese in storitve; akt naj bi Komisija predlagala pred koncem leta 2022, pri tem pa upoštevala potrebo po horizontalnem in celostnem pristopu, ki zajema celoten življenjski cikel digitalnih proizvodov, pa tudi obstoječe predpise, zlasti na področju kibernetske varnosti.

5. POZIVA ustrezne organe, kot so Organ evropskih regulatorjev za elektronske komunikacije (BEREC), Agencija Evropske unije za kibernetsko varnost (ENISA) in Skupina za sodelovanje na področju varnosti omrežij in informacij (NIS), ter Evropsko komisijo, naj na podlagi ocene tveganja oblikujejo priporočila za države članice in Evropsko komisijo, da bi okrepili odpornost komunikacijskih omrežij in infrastruktur v Evropski uniji, vključno z nadaljnjim izvajanjem nabora orodij EU za 5G.

6. POZIVA EU in njene države članice, naj okrepijo prizadevanja za dvig splošne ravni kibernetske varnosti, na primer s spodbujanjem razvoja zaupanja vrednih ponudnikov storitev kibernetske varnosti, in POUDARJA, da bi moralo biti spodbujanje razvoja takšnih ponudnikov prioriteta industrijske politike EU na področju kibernetske varnosti. Za boljšo odpornost na kibernetske napade z morebitnimi sistemskimi učinki in boj proti njim ter ob opiranju na izkušnje z odpravljanjem šibkih točk Solarwinds, Microsoft Exchange in Apache Log4J POZIVA Komisijo, naj predlaga možnosti za spodbujanje razvoja zaupanja vredne industrije storitev kibernetske varnosti, okrepitev kibernetske varnosti dobavne verige IKT, obravnavo morebitnih učinkov šibkih točk v programski opremi za EU in njene države članice, tudi ob upoštevanju prihodnjega akta o kibernetski odpornosti, ter izboljšanje zmožnosti za odkrivanje kibernetskih groženj in skupne uporabe teh zmožnosti v državah članicah in med njimi.

7. Ponovno POUDARJA, da so naložbe v inovacije in boljša uporaba civilne tehnologije ključnega pomena za krepitev naše tehnološke suverenosti, tudi na kibernetskem področju, POZIVA Komisijo, naj hitro operacionalizira Evropski kompetenčni center za kibernetsko varnost, da bi razvili močan evropski kibernetski raziskovalni, industrijski in tehnološki ekosistem, POUDARJA, da je treba okrepiti raziskave in inovacije, več vlagati v civilna in obrambna področja, da bi okrepili tehnološko in industrijsko bazo evropske obrambe (EDTIB) ter razvili kibernetske zmožnosti EU in njenih držav članic, vključno z zmožnostmi za strateško podporo. POUDARJA, da je pomembno, da se intenzivno uporabljajo nove tehnologije, zlasti kvantno računalništvo, umetna inteligenca in velepodatki, da bi dosegli primerjalne prednosti, tudi v smislu odzivanja na kibernetske napade.

8. OB PRIZNAVANJU, da je krepitev naše kibernetske varnosti eden od načinov za povečanje učinkovitosti in varnosti naših prizadevanj na kopnem, v zraku, na morju in v vesolju, POUDARJA pomen vključevanja vidikov kibernetske varnosti v vse javne politike EU, tudi v sektorsko zakonodajo, ki dopolnjuje direktivo NIS 2, in POZIVA Komisijo, naj preuči možnosti za povečanje kibernetske varnosti v celotni dobavni verigi tehnološke in industrijske baze evropske obrambe (EDITB).

9. PRIZNAVA, da je za razvoj stališča EU glede kibernetskih vprašanj bistveno zagotoviti ustrezne finančne in človeške vire za kibernetsko varnost in ukrepe za ustvarjanje ugodnega okolja za konkurenčnost zasebnega sektorja ter da bi bilo treba vprašanje stabilnega in dolgoročnega financiranja kibernetske varnosti obravnavati tudi na ravni EU z oblikovanjem in izvajanjem horizontalnega mehanizma, ki bi združeval več virov financiranja, tudi za stroške visoko kvalificiranih človeških virov. Zato POZIVA Komisijo, naj do konca leta 2022 preuči možnosti za tak mehanizem, o katerem bodo razpravljala ustrezna telesa Sveta.

10. POUDARJA, da je treba okrepiti naša prizadevanja in sodelovanje v boju proti mednarodni kibernetski kriminaliteti, zlasti proti izsiljevalskemu programju, v okviru mehanizma EMPACT (Evropska večdisciplinarna platforma proti grožnjam kriminala), z izmenjavami med sektorjem kibernetske varnosti, organi kazenskega pregona in diplomatskim sektorjem ter s krepitvijo zmogljivosti organov kazenskega pregona pri preiskovanju in pregonu kibernetske kriminalitete. PONAVLJA svojo zavezo, da bo javnost obveščal o kibernetskih grožnjah in ukrepih, sprejetih proti tem grožnjam na nacionalni ravni in ravni EU, ob vključevanju civilne družbe, zasebnega sektorja in akademskih krogov, da bi povečali ozaveščenost in spodbudili ustrezno raven kibernetske zaščite in kibernetske higiene. POUDARJA, da se je treba osredotočiti na spretnosti in znanje ter sposobnosti državljanov in državljank na področju kibernetske varnosti na ravni EU in držav članic ter da je treba uporabnike dejavno vključiti v njihovo lastno zaščito.

II. **OKREPITEV SOLIDARNOSTNEGA IN CELOVITEGA KRIZNEGA UPRAVLJANJA**

11. Glede na izkušnje iz letnih vaj na področju kibernetske varnosti, drugih vaj, ki vključujejo kibernetsko razsežnost, in vaje EU CyCLES 2022 POUDARJA, da je treba ob sodelovanju Sveta, ESZD, Komisije in ustreznih deležnikov, kot sta ENISA in zasebni sektor, pripraviti program rednih kibernetskih vaj na več ravneh in na katerih sodelujejo različne skupnosti, da bi preizkusili in razvili notranji in zunanji odziv EU na velike kibernetske incidente, pri čemer bo ta program usklajen s splošno politiko EU v zvezi z vajami in bo prispeval k njej. POUDARJA pomen nadaljnjega razvoja vaj Cyber Europe in BlueOLEx, ki združujejo odzive na različnih ravneh. PRIZNAVA, da je treba oceniti in konsolidirati obstoječe vaje ter preučiti možnost še drugih vaj v posebnih segmentih kibernetskega področja, zlasti vojaške vaje CERT in vaje s poudarkom na kriznem sodelovanju med institucijami, organi in agencijami EU. PRIZNAVA, da bo stališče Unije glede kibernetskih vprašanj z različnimi ukrepi, tudi usposabljanjem, okrepilo našo sposobnost preprečevanja kibernetskih napadov, in zato POZIVA države članice, naj okrepijo civilno-vojaško sodelovanje pri kibernetskem usposabljanju in skupnih vajah.

12. POUDARJA, da je treba dodatno preskusiti in okrepiti operativno sodelovanje in skupno situacijsko zavedanje med državami članicami, tudi prek vzpostavljenih mrež, kot sta mreža skupin CSIRT in organizacijska mreža za povezovanje v kibernetski krizi (EU CyCLONe), da bi izboljšali pripravljenost EU za odziv na velike kibernetske incidente. POUDARJA, da si je treba prizadevati za razvoj skupnega jezika med državami članicami in institucijami, organi in agencijami EU, prilagojenega razpravi na politični ravni, da bi podprli pripravo konsolidirane ocene resnosti in učinka zadevnih kibernetskih incidentov ter morebitnih scenarijev razvoja in iz njih izhajajočih potreb, kot je ustrezno. V zvezi s tem POUDARJA, da je treba izboljšati dopolnjevanje poročil o skupnem situacijskem zavedanju, tudi poročil EU CyCLONe o učinku in resnosti velikih kibernetskih incidentov v državah članicah EU ter ocen groženj, ki jih v okviru zbirke orodij EU za kibernetsko diplomacijo pripravlja EU INTCEN. POZIVA Komisijo, visokega predstavnika in Skupino za sodelovanje na področju varnosti omrežij in informacij, naj v sodelovanju z ustreznimi civilnimi in vojaškimi organi in agencijami ter vzpostavljenimi mrežami, tudi EU CyCLONe, do konca leta 2022 izvedejo oceno tveganja in pripravijo scenarije tveganja z vidika kibernetske varnosti v zvezi z grožnjami ali morebitnimi napadi na države članice ali partnerske države ter jih predložijo ustreznim organom Sveta. POUDARJA, da je treba javnost ustrezno in usklajeno obveščati o odzivu EU na velike kibernetske incidente.

13. POUDARJA, da je treba pri velikih kibernetskih incidentih okrepiti usklajevanje in po potrebi nadgraditi napredek in delo, ki so ga opravile skupine za hitro odzivanje na kibernetske grožnje v okviru PESCO, ter se opreti na delo mreže skupin CSIRT in EU CyCLONe ter prostovoljno združevanje naših zmogljivosti za odzivanje na incidente med državami članicami. PRIZNAVA, da bi povezovanje z zasebnim sektorjem lahko okrepilo javne zmogljivosti, zlasti v zvezi s pomanjkanjem znanj in spretnosti po vsej EU, ter da bi opredelitev in usklajevanje teh zasebnih partnerjev lahko bila pomemben dejavnik pri odzivu na velike kibernetske incidente. Da bi se v celoti pripravili na velike kibernetske incidente, POZIVA Komisijo, naj do konca tretjega četrtletja 2022 predstavi predlog o novem skladu za nujno odzivanje na kibernetske grožnje.

14. V skladu s strateškim kompasom VZTRAJA, da je treba vlagati v našo medsebojno pomoč v skladu s členom 42(7) Pogodbe o Evropski uniji in v solidarnost iz člena 222 Pogodbe o delovanju Evropske unije, zlasti s pogostimi vajami. V tem okviru POUDARJA, da je potrebno nadaljnje delo v zvezi z zagotavljanjem in usklajevanjem dvostranske civilne in/ali vojaške podpore, tudi s preučitvijo morebitne podpore, ki jo EU zagotovi na izrecno zahtevo držav članic, ter v zvezi z opredelitvijo ustreznih odzivnih ukrepov, tudi z razvojem usklajene komunikacijske strategije, v okviru izvajanja člena 42(7). UGOTAVLJA, da bi pri tem morali preučiti tudi povezave z obstoječimi mehanizmi EU za krizno upravljanje in mehanizmom EU na področju civilne zaščite.

15. POUDARJA, da bo za okrepljeno stališče EU glede kibernetskih vprašanj potrebna še varnejša komunikacija. V ta namen PONOVNO IZPOSTAVLJA tozadevne smernice iz strateškega kompasa ter POZIVA Komisijo in druge ustrezne institucije, organe in agencije, naj do konca leta 2022 pripravijo pregled obstoječih orodij za varno komunikacijo na kibernetskem področju, o katerem bodo razpravljali ustrezna telesa Sveta in ustrezne skupine za sodelovanje, na primer mreža skupin CSIRT in EU CyCLONe.

III. SPODBUJANJE NAŠE VIZIJE KIBERNETSKEGA PROSTORA

16. OPOZARJA, da je cilj skupnega in celostnega pristopa EU h kibernetski diplomaciji prispevati k preprečevanju konfliktov, zmanjšanju kibernetskih groženj in večji stabilnosti v mednarodnih odnosih. V zvezi s tem PONOVNO POTRJUJE, da je EU zavezana mirnemu reševanju mednarodnih sporov v kibernetskem prostoru in temu, da se za ukrepe držav v kibernetskem prostoru uporablja mednarodno pravo, vključno z mednarodnim pravom o človekovih pravicah in mednarodnim humanitarnim pravom. POUDARJA zavezo EU in njenih držav članic, da bodo delovale v skladu s prostovoljnimi, nezavezujočimi standardi odgovornega ravnanja držav v kibernetskem prostoru, o katerih so se dogovorile vse države članice ZN. POUDARJA pomen odprtega, svobodnega, globalnega, stabilnega in varnega kibernetskega prostora, v katerem se človekove pravice, temeljne svoboščine in vladavina prava v celoti uporabljajo v prid socialni blaginji, gospodarski rasti, blaginji in integriteti naših svobodnih in demokratičnih družb, ter PONOVNO POTRJUJE zavezo EU in njenih držav članic, da bodo še naprej spodbujale te vrednote in načela. Da bi razvili kanale za konstruktiven, odkrit in odprt dialog s ključnimi deležniki v kibernetskem prostoru, POUDARJA, kako pomembno je, da kibernetska vprašanja, vključno z zbirko orodij EU za kibernetsko diplomacijo, postanejo sestavni del pristopnih pogajanj Unije ter strateškega in političnega dialoga EU z mednarodnimi partnerji, pa tudi konkurenti, ter hkrati POZIVA visokega predstavnika, naj pregleda obstoječe dvostranske dialoge o kibernetskih vprašanjih in po potrebi predlaga začetek podobnega sodelovanja še z drugimi državami ali ustreznimi mednarodnimi organizacijami.

17. OPOZARJA na pomen večdeležniškega sodelovanja, saj so za kibernetsko varnost odgovorni tudi drugi deležniki, zlasti pri izvajanju priporočil in odločitev, sprejetih v mednarodnih in regionalnih forumih. POZIVA EU in njene države članice, naj še naprej spodbujajo naš model kibernetskega prostora in interneta, ki temelji na večdeležniškem pristopu, in sicer prek pobud, kot sta pariški poziv k zaupanju in varnosti v kibernetskem prostoru in deklaracija o prihodnosti interneta, pri čemer naj poudarijo skupne koristi stabilnosti v kibernetskem prostoru in povečajo globalno ozaveščenost o nevarnostih državno usmerjene in avtoritarne vizije interneta, ter POZIVA EU in njene države članice, naj dodatno okrepijo sodelovanje z večdeležniško skupnostjo, tudi z uporabo ustreznih projektov, kot je pobuda EU za kibernetsko diplomacijo v okviru instrumenta zunanje politike EU.

18. SE ZAVEZUJE k stalnemu sodelovanju v ustreznih mednarodnih organizacijah, zlasti v postopkih, povezanih s Prvim in Tretjim odborom ZN, pri čemer poudarja, da se v kibernetskem prostoru in v zvezi z njim brez pridržkov uporablja veljavno mednarodno pravo. OPOZARJA, da si je treba še naprej prizadevati za ohranitev in spodbujanje okvira ZN za odgovorno ravnanje držav, in POUDARJA, da si bodo EU in njene države članice dejavno prizadevale za okrepitev njegovega izvajanja, tudi z vzpostavitvijo akcijskega programa za spodbujanje odgovornega ravnanja držav v kibernetskem prostoru. POUDARJA, da bodo EU in njene države članice dejavno sodelovale pri pogajanjih o prihodnji konvenciji ZN, ki bi bila učinkovit instrument za organe kazenskega pregona in pravosodne organe v svetovnem boju proti kibernetski kriminaliteti, pri čemer bodo v celoti upoštevale obstoječi okvir mednarodnih in regionalnih instrumentov na tem področju, zlasti Budimpeško konvencijo o kibernetski kriminaliteti. IZPOSTAVLJA pomen nadaljnje podpore razvoju in operacionalizaciji ukrepov za krepitev zaupanja na regionalni in mednarodni ravni ter nadaljnjega spodbujanja uporabe obstoječih kibernetskih ukrepov za krepitev zaupanja v okviru OVSE, tudi v času mednarodnih napetosti.

19. OPOZARJA, da je proaktiven, na človekovih pravicah temelječ pristop za zagotavljanje mednarodnih standardov na področjih nastajajočih tehnologij in osrednje internetne arhitekture v skladu z demokratičnimi vrednotami in načeli bistvenega pomena za zagotovitev, da internet ostane globalen, nerazdrobljen in odprt, ter PODPIRA načelo, da se pri uporabi in razvoju tehnologij spoštujejo človekove pravice in zasebnost ter da je njihova uporaba zakonita, varna in etična. SPODBUJA visokega predstavnika in Komisijo, naj razvijeta strateško vizijo o tehničnih vprašanjih na digitalnem področju, ki vplivajo na zunanjo politiko in bi lahko vplivala na stabilnost kibernetskega prostora in zlasti interneta, tudi v ustreznih specializiranih mednarodnih organizacijah (Mednarodna telekomunikacijska zveza itd.).

IV. OKREPITEV SODELOVANJA S PARTNERSKIMI DRŽAVAMI IN MEDNARODNIMI ORGANIZACIJAMI

20. POUDARJA, da je treba strategijo EU za krepitev kibernetskih zmogljivosti bolje povezati s standardi ZN za odgovorno ravnanje držav v kibernetskem prostoru, tudi z razvojem prilagojenih programov sodelovanja in krepitve zmogljivosti za podporo tretjim državam pri njihovih prizadevanjih za izvajanje, pri tem pa nadaljevati in razširiti naša prizadevanja za spodbujanje akcijskega programa ZN za izboljšanje odgovornega ravnanja držav v kibernetskem prostoru. POUDARJA pomen popolne vključitve krepitve kibernetskih zmogljivosti v okviru ponudbe EU kot zagotovljalca varnosti, in sicer z ustreznim usklajevanjem prizadevanj med državami članicami ter institucijami, organi in agencijami EU, ter zlasti POZDRAVLJA sodelovanje med državami članicami, pa tudi s partnerji iz javnega in zasebnega sektorja, zlasti prek EU CyberNet (omrežje EU za izgradnjo kibernetskih zmogljivosti) in svetovnega foruma o kibernetskem strokovnem znanju (GFCE), da se zagotovi usklajevanje in prepreči podvajanje.

POZIVA visokega predstavnika in Komisijo, naj do tretjega četrtletja 2022 ustanovita *odbor za izgradnjo kibernetskih zmogljivosti* in redno izmenjujeta mnenja v Horizontalni delovni skupini za kibernetska vprašanja. POZIVA Komisijo in visokega predstavnika, naj še naprej uporabljata instrument za sosedstvo ter razvojno in mednarodno sodelovanje (NDICI), instrument za predpristopno pomoč (IPA III) in druga finančna orodja, kot sta evropski mirovni instrument (EPF) in pobuda Global Gateway, da bi podprli krepitev odpornosti naših partnerjev, njihovih zmogljivosti za prepoznavanje in obravnavanje kibernetskih groženj ter

za preiskovanje in pregon kibernetske kriminalitete ter razvoj projektov sodelovanja, tudi v okviru krize, in zlasti SPODBUJA sodelovanje s partnerji na Zahodnem Balkanu ter v vzhodnem in južnem sosedstvu EU ter napotitev strokovnjakov iz EU in držav članic, ki bodo nudili podporo v kibernetskih krizah, z upoštevanjem obstoječih pravnih pooblastil.

21. POUDARJA, da je treba okrepiti prizadevanja za razvoj strukturiranega in odprtega pristopa EU za ozaveščanje o tem, kako spodbujati globalno skupno razumevanje uporabe mednarodnega prava v kibernetskem prostoru, okvira ZN za odgovorno ravnanje držav v kibernetskem prostoru, vključno s pobudo za akcijski program za spodbujanje odgovornega ravnanja držav v kibernetskem prostoru, ter stališča EU in njenih držav članic v potekajočih pogajanjih o konvenciji ZN o kibernetski kriminaliteti, in POZIVA visokega predstavnika, naj v okviru teh prizadevanj Svetu do konca leta 2022 predstavi načrt ozaveščanja. SPODBUJA visokega predstavnika in službe Komisije, naj se v celoti in sistematično poslužujejo 145 delegacij ter razvijejo redno in plodno sodelovanje med njimi in veleposlaništvi držav članic v tretjih državah pod okriljem predvidene mreže EU za kibernetsko diplomacijo. POZIVA visokega predstavnika, naj do tretjega četrtletja 2022 vzpostavi mrežo EU za kibernetsko diplomacijo, ki bo prispevala k izmenjavi informacij, skupnim dejavnostim usposabljanja za osebje EU in držav članic, usklajenim prizadevanjem za izgradnjo zmogljivosti in krepitvi izvajanja okvira ZN za odgovorno ravnanje držav ter ukrepom za krepitev zaupanja med državami.

22. POUDARJA svojo zavezanost nadaljnjemu sodelovanju z mednarodnimi organizacijami in partnerskimi državami, da bi izboljšali skupno razumevanje okolja kibernetskih groženj, razvili mehanizme sodelovanja in proaktivno opredelili skupne diplomatske odzive. OB OPOZARJANJU na ključne dosežke sodelovanja med EU in Natom na področju kibernetske varnosti v okviru izvajanja skupne izjave iz Varšave iz leta 2016 in skupne izjave iz Bruslja iz leta 2018, ob doslednem spoštovanju avtonomije odločanja in postopkov obeh organizacij ter na podlagi načel preglednosti, vzajemnosti in vključenosti, POUDARJA, da je treba dodatno okrepiti kibernetsko sodelovanje z Natom, in sicer z vajami, izmenjavo informacij in izmenjavo med strokovnjaki, tudi kar zadeva razvoj zmožnosti, krepitev zmogljivosti za partnerje ter misije in operacije, pa tudi uporabo mednarodnega prava in standardov ZN za odgovorno ravnanje držav v kibernetskem prostoru ter morebitne usklajene odzive na zlonamerne kibernetske dejavnosti.

V. PREPREČEVANJE KIBERNETSKIH NAPADOV, ZAŠČITA PRED NJIMI IN ODZIVANJE NANJE

23. PRIZNAVA, da je kibernetski prostor postal prizorišče geopolitičnega tekmovanja, in zato PONOVNO POUDARJA, da mora biti EU sposobna hitrega in odločnega odziva na kibernetske napade, kot so zlonamerne kibernetske dejavnosti, ki jih spodbuja država in so usmerjene proti EU in njenim državam članicam, zato mora okrepiti zbirko orodij EU za kibernetsko diplomacijo in v celoti izkoristiti vse svoje instrumente, vključno z razpoložljivimi političnimi, gospodarskimi, diplomatskimi, pravnimi in strateškimi komunikacijskimi orodji za preprečevanje zlonamernih kibernetskih dejavnosti, odvračanje od njih in odzivanje nanje. POUDARJA, da se morajo sovražni akterji zavedati, da bodo kibernetski napadi na države članice in institucije EU odkriti zgodaj, da bodo hitro prepoznani in da se bomo nanje odzvali z vsemi potrebnimi orodji in politikami. Države članice in visokega predstavnika POZIVA, naj si ob podpori Komisije do konca prvega četrtletja 2023 prizadevajo pripraviti revidirano različico izvedbenih smernic iz zbirke orodij EU za kibernetsko diplomacijo, zlasti s preučitvijo dodatnih ukrepov za odzivanje, pri tem pa naj se opirajo zlasti na elemente stališča glede kibernetskih vprašanj, vsebovane v zbirki orodij EU za kibernetsko diplomacijo, in izkušnje, pridobljene z njenim izvajanjem vse od njene vzpostavitve, ter izkušnje, pridobljene z izvajanjem vaje EU CyCLES.

24. POUDARJA, da je v ustreznih telesih in odborih Sveta treba redno razpravljati o okolju kibernetskih groženj, pri čemer je treba tudi redno sodelovati z zasebnim sektorjem in izhajati iz ocene učinka in resnosti nedavnih incidentov, da bi povečali splošno ozaveščenost in pripravljenost za nadaljnjo uporabo zbirke orodij EU za kibernetsko diplomacijo ter razvili dodatna orodja za podporo njenemu izvajanju. Čeprav nacionalna varnost ostaja v izključni pristojnosti vsake države članice, UGOTAVLJA, da je treba okrepiti izmenjavo obveščevalnih podatkov in informacij ter sodelovanje med državami članicami ter z EU INTCEN, da bi lahko izmenjali obveščevalne podatke na začetku postopka odločanja, vključno z vprašanjem dodelitve, ter tako omogočili hiter, učinkovit in utemeljen odziv na zlonamerne kibernetske dejavnosti, usmerjene proti EU in njenim partnerjem. PONOVNO POUDARJA, kako pomembno je okrepiti zmogljivosti EU INTCEN na kibernetskem področju, in sicer na podlagi prostovoljnih obveščevalnih prispevkov držav članic in brez poseganja v njihove pristojnosti, ter preučiti predlog o morebitni ustanovitvi delovne skupine držav članic za kibernetsko obveščevalno dejavnost.

25. OB PRIZNAVANJU, da so izjave EU in omejevalni ukrepi, sprejeti v okviru zbirke orodij EU za kibernetsko diplomacijo, poslali jasno sporočilo, da so zlonamerne kibernetske dejavnosti, ki predstavljajo zunanjo grožnjo EU, njenim državam članicam in partnerjem, nesprejemljive, ter s tem prispevajo k preprečevanju zlonamernih kibernetskih dejavnosti, odvračanju od njih in odzivanju nanje; PONOVNO POUDARJA svojo zavezo, da te ukrepe uporabi, da bi opozoril na obveznosti, ki veljajo za kibernetski prostor v skladu z mednarodnim pravom, vključno s celotno Ustanovno listino ZN, in spodbujal okvir ZN za odgovorno ravnanje držav v kibernetskem prostoru, vključno z obveznostjo potrebne skrbnosti za vse države, da zavestno ne dovolijo uporabe svojega ozemlja za mednarodno nezakonita dejanja z uporabo IKT, z namenom nadaljnjega razvoja in spodbujanja skupnega stališča EU o uporabi mednarodnega prava v kibernetskem prostoru. Ob ugotavljanju, da ustrezna in hitra sporočila zmanjšujejo tveganje stopnjevanja in lahko odvrnejo napadalce, ki so izbrali cilje evropskega interesa, POZIVA visokega predstavnika, naj razvije usklajeno komunikacijsko strategijo o uporabi zbirke orodij EU za kibernetsko diplomacijo in jo predloži državam članicam.

26. SPODBUJA razvoj postopnih, ciljno usmerjenih in trajnih pristopov in odzivov na zlonamerne kibernetske dejavnosti z uporabo širokega nabora orodij, ki jih zagotavlja zbirka orodij EU za kibernetsko diplomacijo, vključno z režimom sankcij EU na kibernetskem področju, in s predvidevanjem dodatnih ukrepov. POUDARJA, da je treba povečati možnost, da se za vsak primer posebej uporabijo vsa razpoložljiva notranja in zunanja orodja za preprečevanje kibernetskih napadov, odvračanje od njih in odzivanje nanje, in sicer s hitrim, učinkovitim, postopnim, ciljno usmerjenim in trajnim pristopom, ki temelji na dolgoročnem strateškem sodelovanju. POZIVA visokega predstavnika, naj v sodelovanju s Komisijo opredeli celoten spekter možnih skupnih odzivov EU na kibernetske napade, vključno z možnostmi sankcij, da bi bili pripravljeni na hitro in učinkovito ukrepanje, kadar je to potrebno, ter jih do konca prvega četrtletja 2023 predstavi Svetu.

27. Ob ugotavljanju, da je kibernetska obramba predvsem v nacionalni pristojnosti, SPODBUJA države članice, naj še naprej razvijajo lastne zmožnosti za izvajanje operacij kibernetske obrambe, vključno s proaktivnimi ukrepi za zaščito in obrambo pred kibernetskimi napadi, njihovo odkrivanje ter odvračanje od njih, ter po možnosti v podporo drugim državam članicam in EU. Vsaka država članica naj po potrebi okrepi svoje sposobnosti za zagotavljanje in prejemanje pomoči in podpore. POUDARJA, da bi moral biti nadaljnji razvoj teh zmožnosti eden od ključnih ciljev prihodnje politike EU za kibernetsko obrambo. UGOTAVLJA, da bi bilo treba v politiki EU za kibernetsko obrambo več pozornosti nameniti vlogi, ki jo lahko imajo ustrezne institucije in organi EU pri krepitvi sodelovanja med ustreznimi akterji EU in držav članic na področju kibernetske obrambe, ter razvoju lastnih zmogljivosti v skladu z njihovimi mandati. POZIVA visokega predstavnika in Komisijo, naj oblikovanje stališča EU glede kibernetskih vprašanj dopolnita s predložitvijo ambicioznega predloga za politiko EU na področju kibernetske obrambe v letu 2022, ki bo Svetu omogočil nadaljnje oblikovanje stališča EU glede kibernetskih vprašanj.

28. OPOZARJA, da je treba v okviru sodelovanja med vojaškimi skupinami za odzivanje na računalniške grožnje (milCERT) povečati interoperabilnost in izmenjavo informacij. POZIVA države članice, naj na podlagi dela Evropske obrambne agencije vzpostavijo mrežo milCERT za razvoj sodelovanja in lažjo izmenjavo informacij, kar bi pripomoglo tudi k usklajevanju z drugimi kibernetskimi skupnostmi, pa tudi mrežo vojaških kibernetskih poveljnikov, da bi okrepili strateško sodelovanje med poveljstvi za kibernetsko obrambo ali drugimi ustreznimi organi držav članic EU. Vzpostavitev teh mrež bi skupaj s kibernetskimi projekti PESCO prispevala k okrepljeni kibernetski obrambi na ravni EU. POUDARJA pomen sodelovanja med predlagano mrežo milCERT in že obstoječo civilno mrežo (CSIRT), da bi izboljšali izmenjavo informacij in situacijsko zavedanje.

29. Na podlagi vojaške vizije in strategije EU za kibernetski prostor kot področja operacij in ob upoštevanju trenutnega razvoja vojaškega koncepta kibernetske obrambe za vojaške operacije in misije pod vodstvom EU PONOVNO POUDARJA, da je treba kibernetsko razsežnost vključiti v načrtovanje in izvajanje misij in operacij v okviru SVOP, tudi s krepitvijo njihovih kibernetskih zmožnosti, ter POUDARJA, da bo to prispevalo k boljšemu kibernetskemu situacijskemu zavedanju na ravni EU.

30. V zaključku UGOTAVLJA, da bo stališče glede kibernetskih vprašanj korak k oblikovanju doktrine EU za ukrepanje v kibernetskem prostoru, ki bo temeljila na večji odpornosti, zmogljivosti in možnosti odzivanja, ter skupnega stališča o uporabi mednarodnega prava v kibernetskem prostoru. Svet BO v letu 2023 OCENIL napredek, dosežen pri izvajanju teh sklepov, da bi zagotovili nadaljnje oblikovanje stališča EU glede kibernetskih vprašanj.