Svet
Evropske unije

Bruselj, 23. marec 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Datum:	22. marec 2021
Prejemnik:	delegacije
Zadeva:	Sklepi Sveta o strategiji EU za kibernetsko varnost v digitalnem desetletju – sklepi Sveta, ki jih je Svet odobril na seji 22. marca 2021

V prilogi vam pošiljamo Sklepe Sveta o strategiji EU za kibernetsko varnost v digitalnem desetletju, ki jih je Svet odobril na seji 22. marca 2021.

PRILOGA

Sklepi Sveta o strategiji EU za kibernetsko varnost v digitalnem desetletju

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],

– upravljanju interneta[2],

– Skupnem sporočilu Evropskemu parlamentu in Svetu z dne 20. novembra 2017: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“[3],

– krepitvi zmogljivosti in zmožnosti na področju kibernetske varnosti v EU[4],

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

– prihodnosti visoko digitalizirane Evrope po letu 2020 z naslovom „Krepitev digitalne in gospodarske konkurenčnosti v Uniji ter digitalna kohezija“[6],

– dopolnilnih prizadevanjih za krepitev odpornosti in preprečevanje hibridnih groženj[7],

– oblikovanju digitalne prihodnosti Evrope[8],

---

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

– digitalni diplomaciji[9],

– krepitvi odpornosti in preprečevanju hibridnih groženj, tudi dezinformacij v okviru pandemije COVID-19[10],

– kibernetski diplomaciji[11],

– usklajenem odzivu EU na velike kibernetske incidente in krize[12],

– okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“)[13],

– smernicah za krepitev zunanjih kibernetskih zmogljivosti EU[14],

– okrevanju, ki pospešuje prehod k bolj dinamični, odpornejši in bolj konkurenčni industriji[15],

– kibernetski varnosti povezanih naprav[16],

– krepitvi odpornosti evropskega sistema kibernetske varnosti ter spodbujanju konkurenčne in inovativne industrije kibernetske varnosti[17],

in na Resolucijo Sveta o šifriranju – varnost s pomočjo šifriranja in varnost kljub šifriranju[18],

---

9 12804/20.
10 14064/20.
11 6122/15 + COR 1.
12 10086/18.
13 10474/17.
14 10496/18.
15 13004/20.
16 13629/20.
17 14540/16.
18 13084/1/20 REV 1.

ter na izjavo držav članic z dne 15. oktobra 2020 „Graditev naslednje generacije računalništva v oblaku za podjetja in javni sektor v EU“,

OB OPOZARJANJU na sklepe Evropskega sveta o COVID-19, enotnem trgu, industrijski politiki in digitalni razsežnosti ter zunanjih odnosih z dne 1. in 2. oktobra 2020[19] in na sklepe Evropskega sveta o dezinformacijah in hibridnih grožnjah ter o novi strateški agendi 2019–2024 z dne 20. junija 2019[20],

OB OPOZARJANJU na Globalno strategijo za zunanjo in varnostno politiko Evropske unije: „Skupna vizija, enotno ukrepanje: močnejša Evropa“ z dne 28. junija 2016,

OB OPOZARJANJU na Sporočilo Evropske komisije o oblikovanju digitalne prihodnosti Evrope z dne 19. decembra 2020[21] in Sporočilo Komisije o strategiji EU za varnostno unijo z dne 24. julija 2020[22],

OB OPOZARJANJU na Skupno sporočilo Evropske komisije in visokega predstavnika o novi agendi EU-ZDA za globalne spremembe z dne 2. decembra 2020[23],

1. POUDARJA, da je kibernetska varnost bistvena za izgradnjo odporne, zelene in digitalne Evrope, ter POZDRAVLJA Skupno sporočilo Evropskemu parlamentu in Svetu z naslovom „Strategija EU za kibernetsko varnost v digitalnem desetletju“, v katerem je začrtan nov okvir za ukrepanje EU na področju „odpornosti, tehnološke neodvisnosti in vodilne vloge“, pa tudi za zaščito njenih državljanov, podjetij in institucij pred kibernetskimi incidenti in grožnjami, ob hkratni krepitvi zaupanja posameznikov in organizacij v sposobnost EU za spodbujanje varnih in zanesljivih omrežij in informacijskih sistemov, infrastrukture in povezljivosti, ter za spodbujanje in zaščito globalnega, odprtega, svobodnega, stabilnega in varnega kibernetskega prostora, ki temelji na človekovih pravicah, temeljnih svoboščinah, demokraciji in pravni državi.

---

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

2. PRIZNAVA, da je spričo pandemije COVID-19 povečana potreba po zaupanju v orodja in sisteme informacijske in komunikacijske tehnologije (IKT) ter njihovo varnost postavljena v ospredje našega vsakdanjega življenja. POUDARJA, da so kibernetska varnost ter svetovni in odprti internet bistveni za delovanje javne uprave in institucij na nacionalni ravni in ravni EU ter za našo družbo in gospodarstvo kot celoto.

3. POUDARJA, da je treba povečati ozaveščenost o kibernetskih vprašanjih na politični in strateški ravni odločanja, tako da se nosilcem odločanja zagotovijo ustrezno znanje in informacije, ter POUDARJA, da je treba izboljšati ozaveščenost širše javnosti in spodbujati kibernetsko higieno.

4. POZIVA k spodbujanju in varovanju temeljnih vrednot EU, kot so demokracija, pravna država, človekove pravice in temeljne svoboščine, vključno s pravico do svobode izražanja in obveščanja, pravico do svobode zbiranja in združevanja ter pravico do zasebnosti v kibernetskem prostoru. V zvezi s tem POZDRAVLJA nadaljnja vztrajna prizadevanja za zaščito zagovornikov človekovih pravic, civilne družbe in akademikov, ki se ukvarjajo z vprašanji, kot so kibernetska varnost, zasebnost podatkov, nadzor in spletna cenzura, in sicer z zagotavljanjem dodatnih praktičnih usmeritev, spodbujanjem najboljših praks in krepitvijo prizadevanj EU za preprečevanje kršitev in zlorab človekovih pravic ter zlorabe nastajajočih tehnologij, zlasti z uporabo diplomatskih ukrepov, kjer je to potrebno, in nadzorom nad izvozom takih tehnologij. V zvezi s tem POUDARJA pomen Akcijskega načrta EU za človekove pravice in demokracijo za obdobje 2020–2024 in njenih smernic o človekovih pravicah glede svobode izražanja na spletu in drugje.

5. IZPOSTAVLJA, da je doseganje strateške avtonomije ob hkratnem ohranjanju odprtega gospodarstva eden od ključnih ciljev Unije, da bo lahko sama določala svojo gospodarsko pot in interese. To vključuje krepitev sposobnosti sprejemanja samostojnih odločitev na področju kibernetske varnosti, da bi okrepili vodilno vlogo EU na digitalnem področju in njene strateške zmogljivosti. OPOZARJA, da to vključuje opredelitev in zmanjšanje strateških odvisnosti ter povečanje odpornosti v najobčutljivejših industrijskih ekosistemih in specifičnih območjih. IZPOSTAVLJA, da to lahko vključuje diverzifikacijo proizvodnih in dobavnih verig, spodbujanje in privabljanje naložb ter proizvodnje v Evropi, raziskovanje alternativnih rešitev in krožnih modelov ter spodbujanje širokega industrijskega sodelovanja med državami članicami.

6. Ob upoštevanju dejstva, da delovni sili primanjkuje digitalnih veščin in veščin na področju kibernetske varnosti, POUDARJA, da je treba zadostiti povpraševanju po usposobljeni delovni sili na področju digitalizacije in kibernetske varnosti, zlasti tako, da se na primer z izobraževanjem in usposabljanjem razvijajo, zadržijo in privabljajo najboljši talenti, da bi lahko digitalizirali našo družbo na kibernetsko varen način. SPODBUJA večjo udeležbo žensk in deklet v izobraževanju na področju naravoslovja, tehnologije, inženirstva in matematike (STEM) ter v poklicnem izpopolnjevanju in prekvalificiranju na področju IKT, kar zadeva digitalne veščine, kot enega od načinov za premostitev digitalnega razkoraka med spoloma.

7. 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 POUDARJA, da je zavezan mirnemu reševanju mednarodnih sporov v kibernetskem prostoru in da bi morala biti vsa diplomatska prizadevanja EU usmerjena predvsem v spodbujanje varnosti in stabilnosti v kibernetskem prostoru, in sicer s povečanim mednarodnim sodelovanjem, ter v zmanjšanje tveganja napačnega razumevanja, eskalacije in konfliktov, ki lahko izvirajo iz incidentov na področju informacijskih in komunikacijskih tehnologij, ter PODPIRA nadaljnji razvoj in operacionalizacijo ukrepov za krepitev zaupanja na regionalni in mednarodni ravni. PONAVLJA poziv Generalne skupščine Združenih narodov, sprejet soglasno, naj države članice ZN pri uporabi IKT upoštevajo priporočila iz poročil skupin vladnih strokovnjakov v okviru Združenih narodov, ter PONOVNO POTRJUJE uporabo mednarodnega prava v kibernetskem prostoru, zlasti Ustanovne listine ZN v celoti.

8. PONOVNO POUDARJA, da je nadaljnji razvoj norm in standardov v Uniji ključen za bistveno oblikovanje mednarodnih norm in standardov na področjih nastajajočih tehnologij ter tehnične in logične infrastrukture, ključne za splošno razpoložljivost in celovitost javnega jedra interneta, da bodo ti v skladu z univerzalnimi vrednotami in vrednotami EU ter bodo oblikovani z večdeležniškim pristopom. To bo zagotovilo, da bo internet ostal globalen, odprt, svoboden, stabilen in varen ter da se bodo pri uporabi in razvoju digitalnih tehnologij spoštovale človekove pravice ter da bo njihova uporaba zakonita, varna in etična. SE SEZNANJA s prihodnjo strategijo za standardizacijo in SE ZAVEZUJE k proaktivnemu in usklajenemu razširjanju za spodbujanje vodilne vloge EU in ciljev EU na mednarodni ravni, tudi v različnih mednarodnih organih za standardizacijo in s sodelovanjem s podobno mislečimi partnerji, civilno družbo, akademiki in zasebnim sektorjem.

9. ODLOČNO PODPIRA večdeležniški model za upravljanje interneta in kibernetsko varnost ter se zavezuje, da bo okrepil redne in strukturirane izmenjave z deležniki, vključno z zasebnim sektorjem, akademiki in civilno družbo v mednarodnih forumih, tudi v okviru pariškega poziva k zaupanju in varnosti v kibernetskem prostoru. SPODBUJA univerzalen, cenovno ugoden in enakopraven dostop do interneta, ki premošča digitalne vrzeli, ter zlasti okrepitev vloge žensk in deklet ter oseb v ranljivem ali marginaliziranem položaju tako pri oblikovanju politike kot pri uporabi interneta.

10. POUDARJA, da je treba kibernetsko varnost v prihodnjih letih vključiti v digitalne naložbe in pobude ter da je treba postopoma prispevati k ustvarjanju enakih konkurenčnih pogojev na področju kibernetske varnosti, in SE SEZNANJA z načrtom Komisije za povečanje javne porabe in spodbujanje zasebnih naložb na področju kibernetske varnosti. POUDARJA pomen malih in srednjih podjetij (MSP) v ekosistemu kibernetske varnosti in PRIZNAVA ustrezne finančne instrumente, ki so na voljo v večletnem finančnem okviru 2021–2027 ter v mehanizmu za okrevanje in odpornost in s katerimi se lahko podpre močna osredotočenost na kibernetsko varnost v okviru digitalne preobrazbe.

11. Z ZADOVOLJSTVOM PRIČAKUJE hitro izvajanje uredbe o Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost ter mreži nacionalnih koordinacijskih centrov (CCCN), vključno s hitro vzpostavitvijo in operacionalizacijo Evropskega strokovnega centra za kibernetsko varnost v Bukarešti. Hitro sprejetje njenega programa bo prispevalo k čim večjemu povečanju učinkov naložb za krepitev vodilne vloge Unije in strateške neodvisnosti na področju kibernetske varnosti ter podporo tehnološkim zmogljivostim in veščinam ter k povečanju globalne konkurenčnosti Unije s prispevki industrije in akademskih skupnosti na področju kibernetske varnosti, vključno z MSP in raziskovalnimi središči, ki bodo imeli koristi od bolj sistematičnega, vključujočega in strateškega sodelovanja, ob upoštevanju kohezije Unije in vseh njenih držav članic.

12. POZDRAVLJA delo, ki ga agencija ENISA trenutno opravlja v sodelovanju z državami članicami in zainteresiranimi deležniki, da bi EU zagotovila evropske certifikacijske sheme za proizvode, storitve in postopke IKT, ki bi morale prispevati k dvigu splošne ravni kibernetske varnosti na enotnem digitalnem trgu. V zvezi s tem Z ZANIMANJEM PRIČAKUJE tekoči delovni program Unije za razvoj certifikacijskih shem EU za kibernetsko varnost v okviru Akta o kibernetski varnosti. V zvezi s tem PRIZNAVA ključno vlogo EU pri razvoju standardov, ki lahko oblikujejo okolje kibernetske varnosti in prispevajo k zagotavljanju poštene konkurence v EU in na svetovni ravni, spodbujanju dostopa do trga in obravnavanju varnostnih tveganj, hkrati pa zagotavljajo uporabo zakonodajnega okvira EU.

13. POUDARJA, da je treba oceniti, ali je dolgoročno potrebna horizontalna zakonodaja, v kateri bi med drugim določili potrebne pogoje za dajanje na trg in obravnavali vse ustrezne vidike kibernetske varnosti povezanih naprav, kot so razpoložljivost, celovitost in zaupnost. V zvezi s tem POZDRAVLJA razpravo, v okviru katere bi preučili področje uporabe take zakonodaje in njene povezave s certifikacijskim okvirom za kibernetsko varnost, kot je opredeljen v aktu o kibernetski varnosti, da bi se dvignila raven varnosti znotraj enotnega digitalnega trga. POUDARJA, da bi bilo treba zahteve glede kibernetske varnosti opredeliti v skladu z ustrezno zakonodajo Unije, tudi certifikacijskim okvirom za kibernetsko varnost, novim zakonodajnim okvirom, uredbo o evropski standardizaciji in morebitno prihodnjo horizontalno zakonodajo, s čimer bi se izognili dvoumnosti in razdrobljenosti zakonodaje.

14. PRIZNAVA pomen celovitega in horizontalnega pristopa h kibernetski varnosti v Uniji, pri čemer je treba v celoti spoštovati pristojnosti in potrebe držav članic, pa tudi pomen stalne podpore za tehnično pomoč in sodelovanje za krepitev zmogljivosti držav članic. Ob upoštevanju razvoja okolja kibernetskih groženj SE SEZNANJA z novim predlogom direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, ki temelji na direktivi o varnosti omrežij in informacij, ter PONOVNO IZRAŽA podporo krepitvi in harmonizaciji nacionalnih okvirov kibernetske varnosti in trajnemu sodelovanju med državami članicami. Poleg tega POUDARJA, da je treba prilagoditi in uskladiti sektorsko zakonodajo na tem področju.

15. JE SEZNANJEN s predlogom Komisije, da bi se države članice podprlo pri vzpostavljanju in krepitvi centrov za varnostne operacije (SOC), tako da bi se vzpostavila mreža SOC po vsej EU, kar bi omogočilo nadaljnje spremljanje in predvidevanje znakov napadov na omrežja. V zvezi s tem PRIČAKUJE podrobne načrte Komisije za mrežo SOC, ob upoštevanju pristojnosti držav članic. OPOZARJA na prizadevanja držav članic, da bi ob podpori EU ustanovile sektorske, nacionalne in regionalne skupine za odzivanje na incidente na področju računalniške varnosti (CSIRT) ter nacionalne ali evropske centre za izmenjavo in analizo informacij (ISAC), ki bi bili del učinkovite mreže partnerstev na področju kibernetske varnosti v Uniji. SE Z ZANIMANJEM PRIPRAVLJA, da bo preučil, kako lahko ta mreža okrepi SOC ter izboljša njihovo dopolnjevanje in usklajevanje z obstoječimi mrežami in akterji (zlasti z mrežo skupin CSIRT), da bi spodbudili učinkovito, varno in zanesljivo kulturo izmenjave informacij. POUDARJA, da bo ta proces temeljil na delu, opravljenem v okviru pobud za umetno inteligenco in visokozmogljivostno računalništvo ter v evropskih vozliščih za digitalne inovacije.

16. JE SEZNANJEN z morebitnim razvojem sistema varne povezljivosti, ki bi temeljil na evropski infrastrukturi za kvantno komunikacijo (EuroQCI) in vladni satelitski komunikaciji Evropske unije (GOVSATCOM), ter PRIZNAVA, da bi moral vsak morebitni prihodnji razvoj temeljiti na trdnem okviru kibernetske varnosti in upoštevati celotno elektronsko komunikacijsko infrastrukturo, kot so vesoljska, kopenska in podmorska omrežja.

17. Z ZANIMANJEM PRIČAKUJE razprave s Komisijo, agencijo ENISA, dvema upravljavcema korenskih DNS strežnikov v EU in širšim krogom deležnikov, da bi ocenili, kakšna je vloga obeh upravljavcev korenskih DNS strežnikov v EU pri zagotavljanju, da bo internet ostal svetovno dostopen in nerazdrobljen. POZDRAVLJA nadaljnjo razpravo o nameri Komisije, da razvije alternativno evropsko storitev za dostop do svetovnega interneta („pobuda DNS4EU“), ki bo temeljila na preglednem modelu, skladnemu z najnovejšimi standardi in pravili glede varnosti, varstva podatkov ter vgrajene in privzete zasebnosti, da bi prispevali k večji odpornosti ter hkrati ohranili in izboljšali mednarodno povezljivost za vse države članice.

18. PRIZNAVA, da si morajo Komisija in države članice skupaj prizadevati za pospešeno uvajanje ključnih internetnih standardov, vključno z IPv6, in uveljavljenih standardov internetne varnosti, saj ti odločilno prispevajo k povečanju splošne ravni varnosti, odpornosti, odprtosti in interoperabilnosti svetovnega interneta ter hkrati večji konkurenčnosti industrije EU, zlasti upravljavcev internetne infrastrukture.

19. POUDARJA pomen usklajenega pristopa ter razvoja in izvajanja učinkovitih ukrepov na nacionalni ravni za okrepitev kibernetske varnosti omrežij 5G. PODPIRA naslednje korake, ki jih je treba sprejeti v zvezi s kibernetsko varnostjo omrežij 5G, kot so predstavljeni v dodatku k strategiji Evropske unije za kibernetsko varnost in temeljijo na rezultatih poročila o učinkih priporočila Komisije za varnost omrežij 5G, na primer v zvezi z opredelitvijo dolgoročnega in celostnega pristopa, ki zajema celotno vrednostno verigo in ekosistem 5G. Da bi dodatno okrepili usklajen pristop k varnosti omrežij 5G, POZIVA države članice, institucije EU in druge ustrezne deležnike, naj še naprej redno pregledujejo stanje, vključno z izmenjavo informacij in najboljših praks v okviru namenske delovne skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov v zvezi s kibernetsko varnostjo 5G, ter Svetu redno poročajo o doseženem napredku. Ob poudarjanju, da so države članice odgovorne za zaščito nacionalne varnosti, IZPOSTAVLJA, da je trdno zavezan uporabi in hitri dokončni izvedbi ukrepov EU v zvezi z naborom orodij 5G ter nadaljnjim prizadevanjem za zagotavljanje varnosti omrežij 5G in razvoj omrežij prihodnjih generacij. Tesno sodelovanje med državami članicami, Komisijo in agencijo ENISA na področju varnosti omrežij 5G bi lahko služilo kot zgled za druga vprašanja na področju kibernetske varnosti, pri čemer je treba spoštovati pristojnosti držav članic ter načeli subsidiarnosti in sorazmernosti.

20. PRIZNAVA pomen nadaljnjega vključevanja kibernetske varnosti v mehanizme EU za krizno odzivanje in njihovega preskušanja v okviru ustreznih vaj ter POUDARJA, kako pomembno je, da se v primeru obsežnih in čezmejnih kibernetskih incidentov in groženj okrepita sodelovanje in izmenjava informacij med različnimi kibernetskimi skupnostmi v EU ter medsebojno povežejo obstoječe pobude, strukture in postopki (kot so enotna ureditev EU za politično odzivanje na krize (IPCR), mreža CSIRT, skupina za sodelovanje na področju varnosti omrežij in informacijskih sistemov, organizacijska mreža za povezovanje v kibernetski krizi (CyCLONe), Evropski center za boj proti kibernetski kriminaliteti, Obveščevalni in situacijski center EU (EU INTCEN) in drugi ustrezni organi EU). OB UPOŠTEVANJU že doseženega napredka na tem področju PRIČAKUJE predlog Komisije o postopku, mejnikih in časovnem okviru za opredelitev skupne enote za kibernetsko varnost, ki bi prinesla dodano vrednost, jasno osredotočenost in racionalizacijo okvira EU za krizno upravljanje kibernetske varnosti, tudi tako, da bi se pregledno in postopno vzpostavila pripravljenost in skupno spremljanje razmer ter okrepila usklajeno odzivanje in izvajanje vaj, ob hkratnem preprečevanju podvajanja in prekrivanja ter ob spoštovanju pristojnosti držav članic.

21. POUDARJA pomen spodbujanja sodelovanja in izmenjave informacij med zadevnimi akterji na področju kibernetske varnosti in pristojnimi organi na področju varnosti in kazenskega pravosodja, npr. organi kazenskega pregona in pravosodnimi organi, pa tudi potrebo po razširitvi in izboljšanju zmogljivosti teh organov za preiskovanje in pregon kibernetske kriminalitete ter spodbujanju mednarodnih pogajanj in pravil EU o čezmejnem dostopu do elektronskih dokazov. Bistveno je, da ne glede na trenutno tehnološko okolje pristojni organi na področju varnosti in kazenskega pravosodja z zakonitim dostopom ohranijo pooblastila za opravljanje svojih nalog, kot je zakonsko določeno in dovoljeno. Taki zakoni, ki določajo izvršilna pooblastila, morajo vedno v celoti spoštovati predpisane postopke in druge zaščitne ukrepe ter temeljne pravice, zlasti pravico do spoštovanja zasebnega življenja in komunikacij ter pravico do varstva osebnih podatkov.

22. PONOVNO POTRJUJE svojo podporo razvoju, izvajanju in uporabi močnega šifriranja kot nujnega sredstva za zaščito temeljnih pravic in digitalne varnosti posameznikov, vlad, industrije in družbe, ter hkrati PRIZNAVA, da je treba zagotoviti, da bodo lahko pristojni organi na področju varnosti in kazenskega pravosodja, npr. organi kazenskega pregona in pravosodni organi, tako na spletu kot zunaj njega izvajali svoja zakonita pooblastila za zaščito naših družb in državljanov. Pristojnim organom je treba omogočiti zakonit in ciljno usmerjen dostop do podatkov, ob doslednem spoštovanju temeljnih pravic in ustrezne zakonodaje o varstvu podatkov, pri čemer je treba zagotoviti kibernetsko varnost. POUDARJA, da je treba pri vseh dejavnostih te interese skrbno uravnovesiti z načeli nujnosti, sorazmernosti in subsidiarnosti.

23. PODPIRA in PROMOVIRA Budimpeško konvencijo o kibernetski kriminaliteti in tekoče delo za pripravo Drugega dodatnega protokola k navedeni konvenciji. Poleg tega še naprej sodeluje v večstranskih izmenjavah o kibernetski kriminaliteti, med drugim tudi v okviru procesov, povezanih s Svetom Evrope, Uradom Združenih narodov za droge in kriminal (UNODC) in Komisijo za preprečevanje kriminala in kazensko pravosodje (CCPCJ), da bi se zagotovilo okrepljeno mednarodno sodelovanje v boju proti kibernetski kriminaliteti, vključno z izmenjavo najboljših praks in tehničnega znanja ter podporo za krepitev zmogljivosti, ob hkratnem spoštovanju, spodbujanju in varstvu človekovih pravic in temeljnih svoboščin.

24. Čeprav je nacionalna varnost še vedno v izključni pristojnosti vsake države članice, PRIZNAVA pomen strateškega sodelovanja na področju obveščevalnih podatkov v zvezi s kibernetskimi grožnjami in dejavnostmi ter POZIVA države članice, naj prek svojih pristojnih organov še naprej prispevajo k delu EU INTCEN kot središču za spremljanje razmer in ocene groženj v zvezi s kibernetskimi vprašanji v EU ter naj preučijo predlog o morebitni ustanovitvi delovne skupine držav članic za kibernetsko obveščevalno dejavnost, da bi se na podlagi obveščevalnih podatkov, ki jih prostovoljno prispevajo države članice, in brez poseganja v njihove pristojnosti okrepila namenska zmogljivost INTCEN na tem področju.

25. POUDARJA pomen trdnega in doslednega varnostnega okvira za zaščito vsega osebja, podatkov, komunikacijskih omrežij in informacijskih sistemov EU ter postopkov odločanja na podlagi celostnih, doslednih in homogenih pravil. To bi bilo treba doseči zlasti s krepitvijo odpornosti in izboljšanjem varnostne kulture EU zoper kibernetske grožnje ter s krepitvijo varnosti tajnih in netajnih omrežij EU, ob hkratnem zagotavljanju ustreznega upravljanja in razpoložljivosti zadostnih virov in zmogljivosti, tudi v povezavi s krepitvijo mandata skupine za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU). V zvezi s tem POZDRAVLJA trenutne razprave o oblikovanju skupnih pravil o informacijski varnosti pri čemer je treba ustrezno upoštevati varnostne predpise Sveta za varovanje tajnih podatkov EU, ter o določitvi skupnih zavezujočih pravil o kibernetski varnosti za vse institucije, organe in agencije EU.

26. ZAVEZUJE SE, da bo NA PODLAGI prizadevanj EU v okviru kibernetske diplomacije povečal uspešnost in učinkovitost zbirke orodij za kibernetsko diplomacijo, in Z ZANIMANJEM PRIČAKUJE poglobljene razprave o njenem področju uporabe in sami uporabi na podlagi izkušenj, pridobljenih pri dosedanji uporabi tega instrumenta. Te razprave bi morale prispevati k promoviranju varnosti na mednarodni ravni, in sicer s spodbujanjem dialoga in skupne vizije o vprašanjih kibernetske varnosti, krepitvijo preprečevanja, stabilnosti in sodelovanja, poglabljanjem zaupanja in krepitvijo izgradnje zmogljivosti, po potrebi pa tudi z uporabo omejevalnih ukrepov, da bi preprečevali zlonamerne kibernetske dejavnosti, uperjene zoper celovitost in varnost EU in njenih držav članic, odvračali od teh dejavnosti, jih preusmerili in se nanje odzivali, s čimer bi ob doslednem spoštovanju nacionalnih pristojnosti in pooblastil prispevali k mednarodni varnosti in stabilnosti ter utrdili stališče EU glede kibernetskih vprašanj. Posebno pozornost bi bilo treba nameniti zlasti preprečevanju in zatiranju kibernetskih napadov s sistemskimi učinki, ki bi lahko prizadeli naše dobavne verige, kritično infrastrukturo in bistvene storitve, demokratične institucije in procese ter ogrozili našo gospodarsko varnost, vključno s kibernetsko krajo intelektualne lastnine. Države članice in institucije EU bi morale dodatno razmisliti tudi o povezovanju med okvirom EU za krizno upravljanje kibernetske varnosti, naborom orodij za kibernetsko diplomacijo ter določbami člena 42(7) PEU in člena 222 PDEU, zlasti z delom na podlagi scenarijev, da bi oblikovali skupno razumevanje praktičnih načinov izvajanja člena 42(7) PEU.

27. PRIZNAVA pomen krepitve sodelovanja z mednarodnimi organizacijami in partnerskimi državami, da bi spodbudili skupno razumevanje okolja kibernetskih groženj, razvili dialoge in mehanizme sodelovanja, po potrebi opredelili skupne diplomatske odzive ter izboljšali izmenjavo informacij, tudi z izobraževanjem, usposabljanjem in vajami. Zlasti POUDARJA, da močno čezatlantsko partnerstvo na področju kibernetske varnosti prispeva k naši skupni varnosti, stabilnosti in blaginji, ter SE SEZNANJA z določbami o sodelovanju na področju kibernetske varnosti v okviru Sporazuma o trgovini in sodelovanju med EU in Združenim kraljestvom. 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 ponovno poudarja pomen okrepljenega, medsebojno dopolnjujočega in koristnega sodelovanja v okviru izobraževanja, usposabljanja, vaj in usklajenega odzivanja na zlonamerne kibernetske dejavnosti, ob doslednem spoštovanju avtonomije odločanja in postopkov obeh organizacij na podlagi načel preglednosti, vzajemnosti in vključenosti.

28. Z namenom prispevanja h globalnemu, odprtemu, svobodnemu, stabilnemu in varnemu kibernetskemu prostoru, ki je vse pomembnejši za nadaljnjo blaginjo, rast, varnost, dobrobit, povezljivost in integriteto naših družb, SE ZAVEZUJE, da bo še naprej sodeloval v postopkih določanja standardov v mednarodnih organizacijah, zlasti postopkih, povezanih s Prvim odborom ZN, ter promoviral in prispeval k priznavanju uporabe mednarodnega prava v kibernetskem prostoru in spoštovanju standardov, pravil in načel odgovornega ravnanja države v kibernetskem prostoru; med drugim bo promoviral hitro oblikovanje akcijskega programa za spodbujanje odgovornega ravnanja držav v kibernetskem prostoru kot konstruktivnega, vključujočega in sporazumnega nadaljnjega ukrepanja na podlagi trenutnih procesov skupine vladnih strokovnjakov in odprte delovne skupine v okviru ZN.

29. OPOZARJA, da je trdno zavezan učinkovitemu multilateralizmu in na pravilih temelječemu mednarodnemu redu, v središču katerega so Združeni narodi, ter je odločen okrepiti sodelovanje in usklajevanje z mednarodnimi in regionalnimi organizacijami, tj. sistemom ZN, Natom, Svetom Evrope, OVSE, OECD, Afriško unijo, Organizacijo ameriških držav, Združenjem držav jugovzhodne Azije (ASEAN), regionalnim forumom ASEAN, Svetom za sodelovanje v Zalivu in Ligo arabskih držav, kar zadeva razprave o vprašanjih, povezanih s kibernetsko varnostjo, ter nadaljevanje in širitev strukturiranih dialogov in posvetovanj EU o kibernetski varnosti s tretjimi državami. POUDARJA, da dejavno podpira ZN, zlasti v zvezi z Agendo 2030 in cilji trajnostnega razvoja, ter POZDRAVLJA časovni načrt generalnega sekretarja ZN za digitalno sodelovanje in agendo generalnega sekretarja ZN za razorožitev, ki spodbujata odgovornost in spoštovanje standardov v kibernetskem prostoru ter prispevata k preprečevanju in mirnemu reševanju konfliktov, ki izhajajo iz zlonamernih dejavnosti v kibernetskem prostoru. POZDRAVLJA predlog visokega predstavnika za zunanje zadeve in varnostno politiko o vzpostavitvi neformalne mreže EU za kibernetsko diplomacijo, da bi razvili sodelovanje in strokovno znanje EU in držav članic v zvezi z mednarodnimi kibernetskimi vprašanji in tako okrepili usklajeno komuniciranje.

30. Z ZANIMANJEM PRIČAKUJE prihodnji predlog za pregled okvira politike za kibernetsko obrambo in SE ZAVEZUJE, da si bo še naprej prizadeval za okrepitev kibernetske varnosti in kibernetske obrambe, da bi bili obe razsežnosti v celoti vključeni v širše področje varnosti in obrambe, zlasti v okviru dela v zvezi s strateškim kompasom. MENI, da bo prihodnja „vojaška vizija in strategija o kibernetskem prostoru kot področju delovanja“ prispevala k nadaljevanju teh razprav. POZDRAVLJA pobudo Evropske obrambne agencije (EDA) za spodbujanje sodelovanja med vojaškimi skupinami CERT in PODPIRA prizadevanja za okrepitev civilno-vojaških sinergij in usklajevanja na področju kibernetske obrambe in kibernetske varnosti, tudi kar zadeva vidike, povezane z vesoljem, med drugim v okviru namenskih projektov PESCO.

31. POZDRAVLJA predlog za oblikovanje agende EU za krepitev zunanjih kibernetskih zmogljivosti, predlog za ustanovitev odbora EU za izgradnjo kibernetskih zmogljivosti ter vzpostavitev in izvajanje omrežja EU za izgradnjo kibernetskih zmogljivosti (EU CyberNet), da bi povečali kibernetsko odpornost in zmogljivosti po vsem svetu. V zvezi s tem POZDRAVLJA sodelovanje z državami članicami, pa tudi partnerji iz javnega in zasebnega sektorja, zlasti s svetovnim forumom o kibernetskem strokovnem znanju (GFCE) in drugimi ustreznimi mednarodnimi organi, da bi se zagotovilo usklajevanje in preprečilo podvajanje. Zlasti SPODBUJA sodelovanje s partnerji na Zahodnem Balkanu ter v vzhodnem in južnem sosedstvu EU.

32. Za zagotovitev, da bi imele vse države možnost, da izkoristijo socialne, gospodarske in politične prednosti interneta in uporabe tehnologij, SE ZAVEZUJE, da bo partnerskim državam pomagal pri spopadanju z vse večjim izzivom zlonamernih kibernetskih dejavnosti, zlasti tistih, ki škodujejo razvoju njihovih gospodarstev in družb ter celovitosti in varnosti demokratičnih sistemov, tudi v skladu s prizadevanji na podlagi akcijskega načrta za evropsko demokracijo.

33. Za zagotovitev razvoja, izvajanja in spremljanja predlogov, predstavljenih v okviru strategije EU za kibernetsko varnost, in ob upoštevanju večletne narave nekaterih pobud SPODBUJA Komisijo in visokega predstavnika za zunanje zadeve in varnostno politiko, naj pripravita podroben načrt izvajanja, v katerem bodo določene prednostne naloge in časovni razpored načrtovanih ukrepov. SPREMLJAL BO napredek pri izvajanju teh sklepov na podlagi akcijskega načrta, ki ga bo Svet redno pregledoval in posodabljal v tesnem sodelovanju z Evropsko komisijo in visokim predstavnikom.