Svet
Evropske unije

Bruselj, 10. december 2019
(OR. en)

14972/19

HYBRID 56	**EDUC 478**
DISINFO 18	**AUDIO 118**
AG 68	**DIGIT 179**
PE 257	**INF 332**
DATAPROTECT 300	**COSI 252**
JAI 1307	**CSDP/PSDC 575**
CYBER 328	**COPS 360**
JAIEX 177	**POLMIL 129**
FREMP 176	**IPCR 23**
RELEX 1147	**PROCIV 100**
CULT 141	**CSC 294**

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Prejemnik:	delegacije
Zadeva:	Dopolnilna prizadevanja za krepitev odpornosti in preprečevanje hibridnih groženj – sklepi Sveta (10. december 2019)

V prilogi vam pošiljamo sklepe Sveta o dopolnilnih prizadevanjih za krepitev odpornosti in preprečevanje hibridnih groženj, ki so bili sprejeti na 3739. seji Sveta 10. decembra 2019.

PRILOGA

Sklepi Sveta o dopolnilnih prizadevanjih za krepitev odpornosti in preprečevanje hibridnih groženj

1. Svet se sklicuje na relevantne sklepe Evropskega sveta[1] in Sveta[2] ter je še naprej zavezan krepitvi odpornosti Unije in njenih držav članic proti večplastnim in stalno spreminjajočim se hibridnim grožnjam ter krepitvi sodelovanja z namenom odkrivanja, preprečevanja in odvračanja teh groženj.

2. Svet priznava napredek, ki je bil v skladu z ustreznimi sklepi Sveta dosežen pri izvajanju skupnega okvira o preprečevanju hibridnih groženj (2016), skupnega sporočila o povečanju odpornosti in krepitvi zmogljivosti za obravnavanje hibridnih groženj (2018) in akcijskega načrta proti dezinformacijam (2018).

3. Za odvračanje hibridnih groženj so v prvi vrsti odgovorne države članice. Prizadevanja na ravni EU so dopolnilna in ne posegajo v izključno pristojnost držav članic za vprašanja nacionalne varnosti. Da bi našli ustrezen odgovor na hibridne grožnje, potrebujemo celovit vsevladni in vsedružbeni pristop k varnosti z bolj strateško usmerjenimi, usklajenimi in povezanimi prizadevanji vseh relevantnih političnih sektorjev. Vsevladni pristop moramo upoštevati in uporabiti tudi na ravni EU.

4. Svet v teh sklepih predstavlja prednostne naloge v zvezi z zaščito naših družb, državljank in državljanov, svoboščin ter varnosti naše Unije pred hibridnimi grožnjami v okviru izvajanja nove strateške agende za obdobje 2019–2024 s spodbujanjem celovitega pristopa k varnosti z boljšim usklajevanjem, obsežnejšimi viri in večjimi tehnološkimi zmogljivostmi, pri čemer se opira na pomembno delo, ki je bilo že opravljeno v različnih političnih sektorjih, tudi v okviru sodelovanja EU na področju varnosti in obrambe.

---

[1] Zlasti sklepe Evropskega sveta iz junija 2019, marca 2019, decembra 2018, oktobra 2018, junija 2018, marca 2018, junija 2015 in marca 2015.

[2] Zlasti ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19 in ST 7928/16.

5. V prizadevanjih za zaščito naših demokratičnih institucij pred hibridnimi grožnjami je treba vedno spoštovati temeljne pravice, vključno z varstvom osebnih podatkov, svobodo izražanja in obveščanja ter svobodo združevanja, ki so zagotovljene z Listino Evropske unije o temeljnih pravicah.

6. EU in njene države članice bi morale še naprej razvijati, usposabljati in izvajati zmogljivosti za odkrivanje, analizo virov in odzivanje na hibridne dejavnosti ter podpirati dolgoročno krepitev odpornosti držav članic ter institucij, organov in agencij EU na hibridne grožnje, pri tem pa v celoti izkoristiti obstoječe instrumente, ki so za to primerni. Svet poudarja, da je treba na podlagi ugotovitev in izkušenj, pridobljenih pri izvajanju preteklih projektov, posodobiti operativni protokol EU za preprečevanje hibridnih groženj.

7. Svet poudarja, da je treba za obrambo svetovnega reda, ki temelji na pravilih, še naprej sodelovati z mednarodnimi organizacijami, kot so ZN, OVSE in Svet Evrope, ter sestavami, kot je G7, tudi v okviru preprečevanja hibridnih groženj, vključno s krepitvijo zaupanja in drugimi ustreznimi ukrepi.

8. Svet poudarja, da je EU zavezana nadaljnjemu tesnemu in za vse strani koristnemu sodelovanju pri krepitvi odpornosti in preprečevanju hibridnih groženj, z vsemi relevantnimi partnerskimi državami, zlasti v sosedstvu EU.

9. Svet poziva k nadaljnjim vztrajnim prizadevanjem, da bi pospešili napredek pri izvajanju vseh ukrepov za preprečevanje hibridnih groženj v okviru skupnega svežnja predlogov za udejanjanje skupnih izjav o sodelovanju med EU in Natom, tudi na področju spremljanja razmer, strateškega komuniciranja, preprečevanja kriz in odzivanja nanje ter krepitve odpornosti. V zvezi s tem ponovno poudarja, da je treba še naprej krepiti politični dialog o preprečevanju hibridnih groženj ter da so potrebne redne vzporedne in usklajene vaje (PACE), pri katerih morajo sodelovati vse države članice EU in zaveznice iz Nata, ter poziva k pravočasnemu dokončanju novega načrta za vzporedne in usklajene vaje. Svet poudarja, da je treba upoštevati ugotovitve, in izpostavlja pomen neovirane, vključujoče in nediskriminatorne izmenjave informacij.

Poleg tega izpostavlja dragocene prispevke Evropskega centra odličnosti za preprečevanje hibridnih groženj iz Helsinkov in ta center spodbuja k sodelovanju z ustreznimi centri odličnosti zveze NATO. Pozdravlja tudi redne in strukturirane izmenjave osebja, vključno s sodelovanjem med hibridno fuzijsko celico Obveščevalnega in situacijskega centra EU (INTCEN) in celico zveze Nato za hibridno analizo.

10. Svet priznava trud, ki so ga države članice v sodelovanju s Komisijo in Evropsko službo za zunanje delovanje (ESZD) vložile v izvedbo raziskave o hibridnem tveganju, ki je predvidena v Ukrepu 1 iz skupnega okvira o preprečevanju hibridnih groženj (2016), ter poziva k nadaljevanju dela in morebitni reviziji raziskave o hibridnem tveganju, da bi odpravili šibke točke.

Povezano sodelovanje za krepitev odpornosti in preprečevanje hibridnih groženj

11. Pri razvoju in uporabi novih in nastajajočih tehnologij, vključno z umetno inteligenco in tehnikami zbiranja podatkov, bi bilo treba za zmanjšanje splošnih tveganj ustrezno upoštevati nove možnosti za krepitev odpornosti ter morebitne šibke točke in domino učinke v okviru odvračanja hibridnih groženj, tudi pri strateškem načrtovanju okvirnega programa za raziskave in inovacije.

12. Svet ugotavlja, da so zlonamerne kibernetske dejavnosti lahko del hibridnih groženj, in v zvezi s tem izpostavlja pomen zbirke orodij EU za kibernetsko diplomacijo.

13. Povezava med hibridnimi grožnjami in ekonomsko varnostjo je pomemben element, ki bi ga bilo treba upoštevati in za katerega so še naprej v prvi vrsti odgovorne države članice.

14. Za krepitev odpornosti in odvračanje hibridnih groženj bi bilo treba zagotoviti učinkovito uporabo novih instrumentov, kot je mehanizem iz uredbe EU o pregledu neposrednih tujih naložb, zato je treba priskrbeti sredstva za prepoznavanje in obravnavo neposrednih tujih naložb, ki bi lahko vplivale na varnost ali javni red.

15. Svet poziva Komisijo, naj odpornost proti hibridnim grožnjam vključi v proces ocene učinka ustreznih prihodnjih zakonodajnih predlogov, vključno s prihodnjimi okvirnimi programi za raziskave in inovacije.

16. Svet izpostavlja pomen rednih simulacij in na scenarijih temelječih razprav o odvračanju hibridnih groženj na ministrski in drugih ravneh ter vključitve hibridnih elementov v druge ustrezne dejavnosti usposabljanja EU na vseh ravneh, ob podpori držav članic in ustreznih organov, zlasti Evropskega centra odličnosti za odvračanje hibridnih groženj, če je to primerno.

17. Da bi EU v prihodnje povezano sodelovala pri krepitvi odpornosti in odvračanju hibridnih groženj, Svet poziva Komisijo in visokega predstavnika, naj za pripravo novih pobud pripravita celovit pregled, v katerem bodo upoštevani do sedaj sprejeti ukrepi in relevantni dokumenti.

Povezava med notranjo in zunanjo varnostjo

18. Organi pregona, civilna zaščita in drugi ustrezni organi bi morali še naprej krepiti svojo pripravljenost za preprečevanje in odvračanje hibridnih groženj. Sodelovanje med ustreznimi nacionalnimi organi ter institucijami, organi in agencijami EU v okviru povezave med notranjo in zunanjo varnostjo na podlagi njihovih zadevnih pooblastil je treba nenehno izboljševati in ga izpostavljati, hkrati pa je treba povečati sinergije in preprečiti podvajanje prizadevanj, tudi s horizontalnimi delovnimi metodami, prostovoljno izmenjavo informacij ter medsektorskim usposabljanjem in projekti. Zato bi bilo treba dodatno oceniti podporno vlogo in prispevke ustreznih mehanizmov EU in agencij EU — v okviru njihovih mandatov in ob upoštevanju obstoječih proračunskih omejitev.

19. Institucije in organi EU bi morali skupaj z državami članicami nadalje razviti uporabo ustreznih mehanizmov in instrumentov EU, vključno z enotno ureditvijo za politično odzivanje na krize (IPCR), mehanizmom Unije na področju civilne zaščite in njegovim Centrom za usklajevanje nujnega odziva (ERCC), in na ta način podpreti odziv držav članic na medsektorske in čezmejne grožnje.

20. Svet priznava možnost, da se države članice pri reševanju hudih kriz, ki so posledica hibridnih dejavnosti, sklicujejo na solidarnostno klavzulo (člen 222 PDEU).

Situacijsko zavedanje in analiza obveščevalnih podatkov

21. Sodelovanje EU pri krepitvi odpornosti in preprečevanju hibridnih groženj morata spremljati ocena ogroženosti, ki se redno posodablja, in celostno situacijsko zavedanje, ki ju morata ob upoštevanju pristojnosti držav članic pripraviti EU INTCEN in njegova hibridna fuzijska celica, da se okrepijo zmožnosti EU in njenih držav članic za odkrivanje, preprečevanje in onemogočanje hibridnih dejavnosti ter odzivanje nanje. Svet meni, da bi bilo treba delo hibridne fuzijske celice EU dodatno okrepiti in pri tem upoštevati ustrezno raven virov, vključno s strokovnim znanjem.

22. Svet opozarja na svoje sklepe o preprečevanju hibridnih groženj z dne 19. aprila 2016, v katerih poziva k uporabi instrumentov EU za preprečevanje hibridnih groženj Uniji, njenim državam članicam in partnerjem ter boj proti njim. Svet poudarja, da je treba še naprej razvijati obstoječe funkcije situacijskega zavedanja držav članic in EU, pri čemer je treba upoštevati vire groženj, ter bolje uporabiti analizo obveščevalnih podatkov EU INTCEN in njene hibridne fuzijske celice, predvsem pri procesih oblikovanja politik EU in kriznega upravljanja na področju preprečevanja hibridnih groženj.

23. Svet meni, da bi lahko misije in operacije SVOP, če in kolikor je potrebno, veliko doprinesle k opredelitvi in analizi kazalnikov morebitnih hibridnih dejavnosti tretjih strani, vključno z dezinformacijami, katerih namen je diskreditirati in ovirati delovanje EU in njenih držav članic, ter priznava, da bi bilo koristno nadalje preučiti možnost, da se ta doprinos še poveča.

Zaščita kritične infrastrukture

24. Zaščita nacionalnih in evropskih kritičnih infrastruktur, funkcij in storitev, ki so bistvene za pravilno delovanje držav, gospodarstev in družb, je glavna prednostna naloga, tudi v okviru krepitve odpornosti proti hibridnim grožnjam, ki zahteva vsevladni in vsedružbeni pristop. Pri tem je treba upoštevati veliko medsebojno odvisnost različnih kritičnih funkcij in storitev, tudi finančnih, ključno vlogo zasebnega sektorja, spreminjajoče se varnostno okolje in nova tveganja, tako v fizičnem smislu kot v kibernetskem prostoru.

25. Ob tem bi bilo treba poleg pravnih, regulativnih in nadzornih zahtev EU, ki urejajo operativno odpornost in neprekinjeno poslovanje, spodbujati tudi sklepanje dogovorov z lastniki v zasebnem sektorju ter upravljavci infrastrukture in storitev, da se zagotovi neprekinjenost kritičnih storitev in dostop do njih, ne samo v primerih višje sile, in sicer tako, da se zagotovi sprejemljiva raven pripravljenosti za odzivanje na vse ustrezne grožnje ter prožnost za obravnavanje dogodkov s hudimi posledicami, a majhno verjetnostjo, da se zgodijo, blažitev njihovih posledic in okrevanje po njih.

26. Svet poudarja, da je odgovornost za zaščito kritične infrastrukture predvsem v nacionalni pristojnosti, vendar pa visoka stopnja čezmejne in medsektorske soodvisnosti zahteva koordinirana ali, kjer je to potrebno, usklajena prizadevanja na ravni EU, tudi za neprekinjeno delovanje notranjega trga.

27. Svet na podlagi ocene izvajanja Direktive (2008/114/ES) o ugotavljanju in določanju evropske kritične infrastrukture, ki je bila opravljena julija 2019, poziva Komisijo, naj se v začetku novega zakonodajnega cikla z državami članicami posvetuje o morebitnem predlogu za revizijo direktive, vključno z morebitnimi dodatnimi ukrepi za izboljšanje zaščite in odpornosti kritične infrastrukture v EU, ob upoštevanju velike soodvisnosti kritičnih funkcij in storitev.

28. Svet poziva Komisijo, naj še naprej sodeluje z državami članicami in po potrebi pripravi nezavezujoče dogovore o sodelovanju med državami članicami, ki imajo skupno kritično infrastrukturo.

29. Svet priznava, da je direktiva o varnosti omrežij in informacijskih sistemov pomembna za to, da upravljavci v kritičnih sektorjih razvijejo kulturo obvladovanja tveganj in varnosti, ter za nacionalne zmogljivosti in strategije, ki zagotavljajo visoko raven varnosti omrežij in informacijskih sistemov na njihovem ozemlju, tudi v okviru hibridnih groženj. Svet poziva države članice, Komisijo in Agencijo Evropske unije za kibernetsko varnost (ENISA), naj na vseh ustreznih ravneh še naprej krepijo sodelovanje na podlagi priporočila Komisije o usklajenem odzivu na velike kibernetske incidente in krize (načrt).

Preprečevanje dezinformacij ter zagotavljanje svobodnih in poštenih volitev

30. Svet pozdravlja poročilo o izvajanju akcijskega načrta proti dezinformacijam in priznava, da je neprekinjeno izvajanje akcijskega načrta še vedno v središču prizadevanj EU. Svet poudarja, da je treba redno pregledovati in po potrebi posodabljati akcijski načrt, da se zagotovi učinkovit dolgoročni pristop.

31. Svet poudarja, da je treba delo oddelka ESZD za strateško komuniciranje in predvsem tri projektne skupine (vzhod, Zahodni Balkan, jug) podpreti z zadostnimi viri, ki bi omogočala dolgoročno načrtovanje, izvajanje in ocenjevanje. Vse tri projektne skupine bi morale biti zmožne stalno odkrivati, analizirati in preprečevati dejavnosti dezinformiranja tujih državnih in zunanjih nedržavnih akterjev. Poleg tega bi morale projektne skupine še naprej prispevati k učinkovitemu in na dejstvih temelječemu pozitivnemu sporočanju ter promociji načel, vrednot in politik Unije v vzhodni in južni soseščini EU ter na Zahodnem Balkanu, pa tudi krepiti splošno medijsko okolje in civilno družbo v teh regijah. Svet poziva ESZD, naj oceni potrebe in možnosti za okrepitev njenega strateškega komuniciranja na drugih geografskih območjih, kot je podsaharska Afrika, hkrati pa ohrani potrebne zmogljivosti za izvajanje obstoječih nalog strateškega komuniciranja.

32. Svet se zaveda, da je pri obravnavi izzivov, ki jih predstavlja dezinformiranje, vključno z vmešavanjem, usmerjenim v spodkopavanje svobodnih in poštenih evropskih volitev, potreben celosten pristop na vseh ravneh s kar najboljšim izkoriščanjem vseh razpoložljivih spletnih in drugih orodij. Ta pristop mora vključevati tudi spremljanje in analizo dezinformacij in manipulativnih vplivov, izvrševanje evropskih pravil o varstvu podatkov, uporabo zaščitnih volilnih ukrepov, prizadevanja za krepitev pluralnih medijev, profesionalno novinarstvo in medijsko pismenost ter ozaveščanje med državljani. Svet priporoča, da se še bolj uveljavi aktivna neodvisna vseevropska mreža oseb, ki preverjajo dejstva, in raziskovalcev, ki razkrivajo dezinformacije. Svet priznava pomen vloge civilne družbe, akademskih krogov in zasebnega sektorja v boju proti dezinformacijam in krepitvi odpornosti.

33. Svet se zaveda potenciala sistema hitrega opozarjanja v boju proti dezinformacijam, predvsem pri vmešavanju v volitve. Komisijo in ESZD poziva, naj skupaj z državami članicami še naprej razvijata ta sistem, da bi ga nadgradili v celovito platformo, v okviru katere bi države članice in institucije EU krepile sodelovanje, usklajevanje in izmenjavo informacij, na primer o izsledkih raziskav in analiz, najboljših praksah in komunikacijskih produktih, s čimer bi v okviru različnih evropskih in nacionalnih prizadevanj podprli boj proti dezinformacijskim kampanjam.

34. Svet priznava koristnost ukrepov in priporočil, ki jih je Komisija predstavila 12. septembra 2018 v okviru volilnega svežnja za izvedbo evropskih volitev. Svet spodbuja Komisijo in države članice, naj preučijo možnosti za nadaljevanje dejavnosti evropskih mrež za volilno sodelovanje v podporo izmenjavi informacij in najboljših praks. Svet pozdravlja prizadevanja Komisije, da bi ob upoštevanju nacionalnih pristojnosti na tem področju vključila vse zadevne interesne skupine in podprla širok niz ukrepov, kot je uresničevanje projekta o kibernetski varnosti evropskih volitev (EU ELEx19).

35. Svet priznava, da je treba še naprej sodelovati s platformami družbenih medijev, da bi dosegli višje standarde odgovornosti, preglednosti in odgovornosti pri preprečevanju dezinformacij. Poleg tega bi bilo treba zagotoviti neoviran dostop do anonimiziranih podatkov, ki jih zagotavljajo ponudniki platform družbenih medijev za akademske raziskave, da se olajšajo politike, ki temeljijo na dokazih. Svet poziva Komisijo, naj predstavi pobude za nadaljnje ukrepanje proti dezinformacijam na spletnih platformah. Te pobude bi morale temeljiti na oceni izvajanja kodeksa ravnanja glede dezinformacij, pri kateri bi se morali upoštevati analitično delo in poročila akademskih krogov in organizacij civilne družbe, poročilo o spremljanju kodeksa, ki ga pripravlja Skupina evropskih regulatorjev za avdiovizualne medijske storitve, ter izkušnje, pridobljene v okviru volitev v Evropski parlament maja 2019. V zvezi s tem Svet poziva Komisijo, naj preuči načine, vključno z morebitnimi mehanizmi spoštovanja pravil na spletnih platformah, da bi se še bolj spodbudilo izvajanje kodeksa ravnanja, predvsem z vključitvijo neodvisne ocene izpolnjevanja zavez podpisnic.

Varnost institucij, organov in agencij EU

36. Varnost osebja, institucij, organov in agencij EU pred hibridnimi grožnjami in drugimi zlonamernimi dejavnostmi je skupni interes EU in njenih držav članic. Svet poziva institucije, organe in agencije EU, naj ob podpori držav članic na podlagi celovite ocene nevarnosti zagotovijo zmogljivosti Unije za zaščito njene integritete in okrepijo varnost informacijskih in komunikacijskih omrežij EU ter postopkov odločanja pred vsakovrstnimi zlonamernimi dejavnostmi. V ta namen bi morali institucije, organi in agencije ob podpori držav članic v skladu z mandatom Evropskega sveta iz junija 2019 pripraviti in izvajati celovit sklop ukrepov za zagotavljanje varnosti. Svet poudarja pomen zagotavljanja interoperabilnosti infrastrukture IT Evropske unije pri izmenjavi tajnih podatkov med institucijami, organi, agencijami in državami članicami EU.