



Bruxelles, 10. prosinca 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

ISHOD POSTUPAKA

Od: Glavno tajništvo Vijeća

Za: Delegacije

Predmet: Dodatna nastojanja za jačanje otpornosti i suzbijanje hibridnih prijetnji
– zaključci Vijeća (10. prosinca 2019.)

Za delegacije se u prilogu nalaze Zaključci Vijeća o dodatnim nastojanjima za jačanje otpornosti i suzbijanje hibridnih prijetnji doneseni na 3739. sastanku Vijeća održanome 10. prosinca 2019.

Zaključci Vijeća o dodatnim nastojanjima za jačanje otpornosti i suzbijanje hibridnih prijetnji

1. Vijeće podsjeća na relevantne zaključke Europskog vijeća¹ i Vijeća² te izražava svoju trajnu predanost jačanju otpornosti Unije i njezinih država članica na višedimenzionalne i sve složenije hibridne prijetnje te poboljšanju suradnje u otkrivanju, sprečavanju i suzbijanju tih prijetnji.
2. Vijeće prepoznaje napredak u provedbi Zajedničkog okvira za suzbijanje hibridnih prijetnji (2016.) i Zajedničke komunikacije o jačanju otpornosti i poboljšanju sposobnosti za borbu protiv hibridnih prijetnji (2018.), kao i Akcijskog plana za borbu protiv dezinformiranja (2018.), u skladu s relevantnim zaključcima Vijeća.
3. Primarnu odgovornost za suzbijanje hibridnih prijetnji snose države članice. Naponi na razini EU-a komplementarne su prirode i ne dovode u pitanje isključivu odgovornost država članica u pitanjima nacionalne sigurnosti. Za suočavanje s hibridnim prijetnjama potreban je sveobuhvatan pristup koji uključuje sve razine vlasti i cijelo društvo te koji djeluje u svim relevantnim sektorima politike, s više strateškog promišljanja, usklađenosti i dosljednosti. Važno je da se pristup koji uključuje sve razine vlasti prati i primjenjuje i na razini EU-a.
4. Vijeće u ovim zaključcima utvrđuje prioritete u vezi sa zaštitom naših društava, građana i sloboda te sigurnosti naše Unije od hibridnih prijetnji u kontekstu provedbe novog strateškog programa za razdoblje 2019. – 2024., promicanjem sveobuhvatnog pristupa sigurnosti s boljom koordinacijom, resursima i tehnološkim kapacitetima, oslanjajući se na važan rad koji je obavljen u različitim sektorima politike, među ostalim u okviru suradnje EU-a u području sigurnosti i obrane.

¹ Konkretno, zaključci Europskog vijeća iz lipnja 2019., ožujka 2019., prosinca 2018., listopada 2018., lipnja 2018., ožujka 2018., lipnja 2015. i ožujka 2015.

² Konkretno, ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16.

5. Pri ulaganju napora u zaštitu naših demokratskih institucija od hibridnih prijetnji uvijek se moraju poštovati temeljna prava, među ostalim zaštita osobnih podataka, sloboda izražavanja i informiranja te sloboda udruživanja, kako je utvrđeno u Povelji o temeljnim pravima.

6. EU i njegove države članice trebali bi nastaviti s razvijanjem, osposobljavanjem i korištenjem kapaciteta za otkrivanje izvora hibridnih aktivnosti, analizu tih aktivnosti i odgovor na njih te podupirati jačanje dugoročne otpornosti svojih država članica i institucija, tijela i agencija EU-a na hibridne prijetnje, uz potpuno iskorištavanje postojećih odgovarajućih instrumenata. Vijeće ističe potrebu za ažuriranjem operativnog protokola EU-a za suzbijanje hibridnih prijetnji na temelju utvrđenih i naučenih lekcija iz dosadašnjeg rada.

7. Vijeće ističe stalnu potrebu za suradnjom s međunarodnim organizacijama kao što su UN, OESS i Vijeće Europe te formatima kao što je skupina G7, radi zaštite globalnog poretka utemeljenog na pravilima, među ostalim u kontekstu suzbijanja hibridnih prijetnji, pa i putem izgradnje povjerenja i drugih relevantnih mjera.

8. Vijeće naglašava predanost EU-a nastavku bliske i međusobno osnažujuće suradnje u pogledu jačanja otpornosti i suzbijanja hibridnih prijetnji sa svim relevantnim partnerskim zemljama, posebno u susjedstvu EU-a, te pružanju potpore tim zemljama s tim u vezi.

9. Vijeće poziva na daljnje i kontinuirane napore za daljnji napredak u provedbi svih mjera povezanih sa suzbijanjem hibridnih prijetnji u okviru zajedničkog niza prijedloga za provedbu zajedničkih izjava o suradnji EU-a i NATO-a, među ostalim u područjima informiranosti o stanju, strateške komunikacije, sprječavanja kriza i odgovora na krize te jačanja otpornosti. U tom kontekstu ponovno ističe potrebu za daljnjim jačanjem političkog dijaloga o suzbijanju hibridnih prijetnji, kao i za redovitim usporednim i koordiniranim vježbama (PACE) uz sudjelovanje svih država članica EU-a i saveznika NATO-a te poziva na pravodobno dovršenje novog plana za PACE. Vijeće naglašava da je potrebno uzeti u obzir stečena iskustva i važnost neometane razmjene informacija na uključiv i nediskriminirajuć način.

Nadalje, Vijeće ističe vrijedne doprinose Europskog centra izvrsnosti za suzbijanje hibridnih prijetnji u Helsinkiju i potiče njegovu suradnju s relevantnim centrima izvrsnosti NATO-a. Također pozdravlja redovite i strukturirane razmjene osoblja, uključujući suradnju između jedinice za otkrivanje hibridnih prijetnji Obavještajnog i situacijskog centra EU-a (INTCEN) te odjela NATO-a za analizu hibridnih prijetnji.

10. Vijeće prima na znanje napore koje su države članice, u suradnji s Komisijom i Europskom službom za vanjsko djelovanje (ESVD), poduzele u provedbi istraživanja o hibridnom riziku predviđenima mjerom 1. zajedničkog okvira za suzbijanje hibridnih prijetnji (2016.) te poziva na nastavak rada i moguću reviziju istraživanja o hibridnom riziku kako bi se uspješnije otklonili nedostaci.

Usklađeno djelovanje na jačanju otpornosti i suzbijanju hibridnih prijetnji

11. Pri razvijanju i primjeni novih tehnologija i tehnologija u nastajanju, među ostalim umjetne inteligencije i tehnika prikupljanja podataka, na odgovarajući bi način trebalo uzeti u obzir nove mogućnosti za jačanje otpornosti te potencijalne nedostatke i kaskadne učinke u kontekstu suzbijanja hibridnih prijetnji, kako bi se umanjili ukupni rizici, među ostalim u strateškom planiranju postupka u pogledu Okvirnog programa za istraživanja i inovacije.

12. Vijeće napominje da zlonamjerne kiberaktivnosti mogu biti dio hibridnih prijetnji te u tom kontekstu ističe važnost alata EU-a za kiberdiplomaciju.

13. Povezanost hibridnih prijetnji i gospodarske sigurnosti važan je element koji treba uzeti u obzir te koji je i nadalje prvenstveno odgovornost država članica.

14. Nove instrumente, kao što je mehanizam u okviru Uredbe EU-a o provjeri izravnih stranih ulaganja, trebalo bi učinkovito upotrebljavati za jačanje otpornosti i suzbijanje hibridnih prijetnji osiguravanjem sredstava za utvrđivanje i rješavanje izravnih stranih ulaganja koja mogu utjecati na sigurnost ili javni poredak.

15. Vijeće poziva Komisiju da u postupak procjene učinka uključi otpornost na hibridne prijetnje za relevantne buduće zakonodavne prijedloge, uključujući buduće okvirne programe za istraživanja i inovacije.

16. Vijeće ističe važnost redovitih vježbi i rasprava na temelju scenarija o suzbijanju hibridnih prijetnji na ministarskoj i drugim razinama, kao i o uključivanje hibridnih elemenata u druge relevantne aktivnosti osposobljavanja i vježbi EU-a na svim različitim razinama, ako je potrebno uz potporu država članica i nadležnih tijela, posebno Europskog centra izvrsnosti za suzbijanje hibridnih prijetnji.

17. Kako bi se osigurala usklađenost sljedećih koraka suradnje EU-a u pogledu jačanja otpornosti i suzbijanja hibridnih prijetnji, Vijeće poziva Komisiju i Visokog predstavnika da izrade pregled kojim bi se u obzir uzele dosad poduzete mjere i relevantni dokumenti doneseni na sveobuhvatan način, s ciljem mogućih novih inicijativa.

Povezanost unutarnje i vanjske sigurnosti

18. Tijela kaznenog progona, civilne zaštite i druga relevantna tijela trebala bi nastaviti s razvijanjem svoje spremnosti za sprečavanje i suzbijanje hibridnih prijetnji. Suradnju među relevantnim nacionalnim tijelima, kao i institucijama, tijelima i agencijama EU-a potrebno je, na temelju njihovih mandata, stalno poboljšavati i uključivati u rad iz područja povezanosti unutarnje i vanjske sigurnosti uz istodobno povećanje sinergija i izbjegavanje udvostručivanja napora, među ostalim i s pomoću horizontalnih metoda rada, dobrovoljne razmjene informacija te osposobljavanja i vježbi u različitim sektorima. U tu bi svrhu trebalo dodatno procijeniti potporne uloge i doprinose relevantnih mehanizama i agencija EU-a, u okviru njihovih mandata te poštujući postojeća proračunska ograničenja.

19. Relevantne institucije i tijela EU-a trebale bi, zajedno s državama članicama, dodatno razraditi primjenu odgovarajućih mehanizama i instrumenata za potporu državama članicama u odgovorima na međusektorske i prekogranične prijetnje, uključujući aranžmane za integrirani politički odgovor na krizu (IPCR), Mehanizam Unije za civilnu zaštitu (UCPM) i njezin Koordinacijski centar za odgovor na krizne situacije (ERCC).

20. Vijeće potvrđuje mogućnost da se države članice pri rješavanju ozbiljnih kriza koje su posljedica hibridne aktivnosti pozovu na klauzulu solidarnosti (članak 222. UFEU-a).

Informiranost o stanju i analiza obavještajnih podataka

21. Suradnja EU-a u području jačanja otpornosti i suzbijanja hibridnih prijetnji treba se temeljiti na redovito ažuriranoj procjeni prijetnji i informiranosti o stanju. Njih bi trebali razviti EU INTCEN i njegova jedinica za otkrivanje hibridnih prijetnji s ciljem unaprjeđivanja kapaciteta EU-a i njegovih država članica za otkrivanje, sprečavanje i ometanje hibridnih aktivnosti te odgovor na njih, uz poštovanje nadležnosti država članica. Vijeće smatra da bi rad jedinice EU-a za otkrivanje hibridnih prijetnji trebalo dodatno poboljšati, uzimajući u obzir odgovarajuću razinu resursa, uključujući stručno znanje.

22. Vijeće podsjeća na svoje zaključke o suzbijanju hibridnih prijetnji od 19. travnja 2016. u kojima poziva na mobilizaciju instrumenata EU-a za sprečavanje i suzbijanje hibridnih prijetnji Uniji i njezinim državama članicama te partnerima. Vijeće ističe potrebu za daljnjim razvojem postojećih funkcija država članica i EU-a u pogledu informiranosti o stanju, uzimajući u obzir izvore prijetnji, te za boljim iskorištavanjem obavještajne analize EU INTCEN -a i njegove jedinice za otkrivanje hibridnih prijetnji, posebno u postupku donošenja politika i upravljanja krizama u suzbijanju hibridnih prijetnji.

23. Vijeće prima na znanje važan doprinos koji misije i operacije ZSOP-a mogu, prema potrebi, osigurati pri utvrđivanju i analizi pokazatelja mogućih hibridnih aktivnosti trećih strana, uključujući dezinformacije kojima se nastoji diskreditirati i otežati djelovanje EU-a i njegovih država članica, te uviđa vrijednost daljnjeg istraživanja mogućnosti razvoja tog doprinosa.

Zaštita kritične infrastrukture

24. Za zaštitu nacionalnih i europskih ključnih infrastruktura, kao i funkcija i usluga kritičnih za dobro funkcioniranje države, gospodarstva i društva, koja je ključan prioritet, među ostalim u kontekstu jačanja otpornosti na hibridne prijetnje, potreban je pristup koji uključuje sve razine vlasti i cijelo društvo. U okviru tog rada treba uzeti u obzir snažnu međuovisnost različitih ključnih funkcija i usluga, uključujući financijske usluge, ključnu ulogu privatnog sektora, promjenjivo sigurnosno okruženje i nove rizike, i u području fizičkoga i u kibernetičkom području.

25. Nadalje, uz pravne, regulatorne i nadzorne zahtjeve potrebne za operativnu otpornost i kontinuitet poslovanja, trebalo bi promicati aranžmane s vlasnicima iz privatnog sektora te operatorima infrastruktura i usluga s ciljem osiguravanja kontinuiteta ključnih usluga i pristup tim uslugama u slučaju više sile, osiguravanjem prihvatljive razine pripravnosti za odgovor na sve relevantne prijetnje te prilagodljivosti za suočavanje s događajima koji imaju snažan učinak, a mala je vjerojatnost da će se dogoditi, te u njihovu ublaživanju i oporavku od njih.

26. Vijeće naglašava da su za visoku razinu prekograničnih i međusektorskih međuovisnosti, unatoč tomu što je odgovornost za zaštitu kritične infrastrukture prvenstveno pitanje nacionalne nadležnosti, potrebni koordinirani ili, prema potrebi, usklađeni napori na razini EU-a, među ostalim u pogledu nesmetanog funkcioniranja unutarnjeg tržišta.

27. Nakon evaluacije provedbe Direktive (2008/114/EZ) o utvrđivanju i označivanju europske kritične infrastrukture (EGI) iz srpnja 2019. Vijeće poziva Komisiju da se u ranoj fazi novog zakonodavnog ciklusa savjetuje s državama članicama o mogućem prijedlogu revizije Direktive, uključujući moguće dodatne mjere za poboljšanje zaštite i otpornosti kritične infrastrukture u EU-u, uzimajući u obzir snažne međuovisnosti ključnih funkcija i usluga.

28. Vijeće poziva Komisiju da nastavi surađivati s državama članicama te da, prema potrebi, osmisli neobvezujuće sporazume o suradnji među državama članicama koje dijele ključne infrastrukture.

29. Vijeće prepoznaje važnost Direktive o sigurnosti mrežnih i informacijskih sustava za razvoj kulture upravljanja rizicima i kulture sigurnosti koju provode subjekti u ključnim sektorima te za nacionalne sposobnosti i strategije kojima se osigurava visoka razina sigurnosti mrežnih i informacijskih sustava na njihovu državnom području, među ostalim u kontekstu hibridnih prijetnji. Vijeće poziva države članice, Komisiju i Agenciju Europske unije za kibersigurnost (ENISA) da nastave razvijati međusobnu suradnju na temelju Preporuke Komisije o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (*Blueprint*) na svim relevantnim razinama.

Borba protiv dezinformiranja te osiguravanje slobodnih i poštenih izbora

30. Vijeće pozdravlja Izvješće o provedbi Akcijskog plana za borbu protiv dezinformiranja te potvrđuje da je nastavak provedbe akcijskog plana i dalje u središtu napora EU-a. Vijeće ističe potrebu za redovitim preispitivanjem i, prema potrebi, ažuriranjem akcijskog plana radi osiguravanja učinkovitog i dugoročnog pristupa.

31. Vijeće naglašava da je rad Odjela za stratešku komunikaciju ESVD-a, te osobito tri radne skupine (istok, zapadni Balkan, jug), potrebno podržati resursima dostatnim za dugoročno planiranje, provedbu i evaluaciju. U okviru svojih zadaća sve tri radne skupine trebale bi moći kontinuirano otkrivati, analizirati i osporavati aktivnosti dezinformiranja stranih državnih aktera i vanjskih nedržavnih aktera. Radne skupine također bi trebale nastaviti s doprinosom učinkovitoj i na činjenicama utemeljenoj pozitivnoj komunikaciji te promicanju načela, vrijednosti i politika Unije u istočnom i južnom susjedstvu EU-a te na zapadnom Balkanu, kao i s jačanjem općeg medijskog okružja i civilnog društva u njihovim regijama. Vijeće poziva ESVD da procijeni potrebe i mogućnosti jačanja svojeg strateškog komunikacijskog rada u drugim zemljopisnim područjima, kao što je supsaharska Afrika, te da istodobno zadrži potrebnu sposobnost za provedbu postojećih strateških komunikacijskih zadaća.

32. Vijeće uviđa da je potreban sveobuhvatan pristup na svim razinama kako bi se riješili izazovi dezinformiranja, uključujući upletanje s ciljem potkopavanja slobodnih i poštenih europskih izbora, uz optimalno iskorištavanje svih dostupnih alata na internetu i izvan njega. To mora uključivati praćenje i analizu dezinformacija i manipulativnog upletanja, provedbu europskih pravila o zaštiti podataka, primjenu izbornih zaštitnih mjera, napore za jačanje pluralističkih medija, profesionalnog novinarstva i medijske pismenosti, kao i osviještenosti građana. Vijeće preporučuje daljnju konsolidaciju aktivne i neovisne paneuropske mreže osoba za provjeru činjenica i istraživanje u borbi protiv dezinformiranja. Vijeće uviđa važnost civilnog društva, akademske zajednice i privatnog sektora te uloge koje imaju u borbi protiv dezinformiranja i jačanju otpornosti.

33. Vijeće uviđa potencijal sustava brzog uzbunjivanja (RAS) za borbu protiv dezinformiranja, posebno u pogledu upletanja u izbore. Poziva Komisiju i ESVD da zajedno s državama članicama nastave razvijati RAS u smjeru sveobuhvatne platforme za države članice i institucije EU-a kako bi se poboljšale suradnja, koordinacija i razmjena informacija, primjerice istraživanje i analitički uvidi, najbolje prakse i komunikacijski proizvodi, radi pružanja potpore borbi protiv kampanja dezinformiranja u okviru niza europskih i nacionalnih napora.

34. Vijeće prepoznaje korist od mjera i preporuka koje je Komisija 12. rujna 2018. predstavila u okviru svojeg paketa za osiguravanje europskih izbora. Vijeće potiče Komisiju i države članice da ispituju mogućnosti za nastavak aktivnosti europskih mreža suradnje na izborima, kako bi se podržala razmjena informacija i najboljih praksi. Vijeće pozdravlja napore Komisije na uključivanju svih relevantnih dionika i potpori širokom rasponu mjera, primjerice provođenju mjera kibersigurnosti na europskim izborima (EU ELEx19), uzimajući u obzir nacionalne nadležnosti u tom području.

35. Vijeće prepoznaje potrebu za nastavkom rada s platformama društvenih medija kako bi se postigli viši standardi odgovornosti, transparentnost i odgovornost u rješavanju problema dezinformiranja. Osim toga, trebalo bi omogućiti neometan pristup anonimiziranim podacima pružatelja platformi društvenih medija za akademsko istraživanje, kako bi se olakšalo donošenje politika utemeljenih na dokazima. Vijeće poziva Komisiju da predstavi inicijative s daljnjim koracima za rješavanje problema dezinformiranja na internetskim platformama. Te bi se inicijative trebale temeljiti na procjeni provedbe Kodeksa dobre prakse u suzbijanju dezinformacija, pri kojoj bi se u obzir trebao uzeti analitički rad i izvješća koja se provode u okviru akademske zajednice i organizacija civilnog društva, izvješće o praćenju Kodeksa koje provodi Europska skupina regulatora za audiovizualne medijske usluge te iskustva stečena na izborima za Europski parlament u svibnju 2019. U tom kontekstu Vijeće poziva Komisiju da razmotri na koje bi se načine, uključujući moguće mehanizme provedbe za internetske platforme, mogla dodatno poboljšati provedba Kodeksa dobre prakse, posebno uključivanjem neovisne procjene o tome u kojoj mjeri potpisnici ispunjavaju svoje obveze.

Sigurnost institucija, tijela i agencija EU-a

36. Sigurnost osoblja, institucija, tijela i agencija EU-a u pogledu hibridnih prijetnji te drugih zlonamjernih aktivnosti u interesu je i EU-a i njegovih država članica. Vijeće poziva institucije, tijela i agencije EU-a da, uz potporu država članica i na temelju sveobuhvatne procjene prijetnje, osiguraju sposobnost Unije da zaštiti svoj integritet i poboljša sigurnost informacijskih i komunikacijskih mreža EU-a te postupaka donošenja odluka od zlonamjernih aktivnosti svih vrsta. U tu bi svrhu institucije, tijela i agencije, uz potporu država članica, trebale razviti i provesti sveobuhvatni skup mjera za osiguravanje njihove sigurnosti, u skladu s mandatom Europskog vijeća iz lipnja 2019. Vijeće ističe važnost osiguravanja interoperabilnosti informatičke infrastrukture EU-a za razmjenu klasificiranih podataka između institucija, tijela, agencija i država članica EU-a.
