Rada
Európskej únie

V Bruseli 10. decembra 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**

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Komu:	Delegácie
Predmet:	Komplementárne úsilie zamerané na zvyšovanie odolnosti a boj proti hybridným hrozbám – závery Rady (10. decembra 2019)

Delegáciám v prílohe zasielame závery Rady o komplementárnom úsilí zameranom na zvyšovanie odolnosti a boj proti hybridným hrozbám, ktoré Rada prijala na svojom 3 739. zasadnutí 10. decembra 2019.

PRÍLOHA

Závery Rady o komplementárnom úsilí zameranom na zvyšovanie odolnosti a boj proti hybridným hrozbám

1. Rada pripomína príslušné závery Európskej rady[1] a Rady[2] a vyjadruje svoje trvalé odhodlanie posilňovať odolnosť Únie a jej členských štátov proti mnohostranným a neustále sa vyvíjajúcim hybridným hrozbám a skvalitňovať spoluprácu s cieľom odhaľovať ich, predchádzať im a bojovať proti nim.

2. Rada uznáva pokrok, ktorý sa dosiahol pri vykonávaní spoločného rámca pre boj proti hybridným hrozbám (2016) a spoločného oznámenia s názvom Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby (2018), ako aj akčného plánu proti dezinformáciám (2018), v súlade s príslušnými závermi Rady.

3. Hlavnú zodpovednosť za boj proti hybridným hrozbám nesú členské štáty. Úsilie na úrovni EÚ má doplnkový charakter a nie je ním dotknutá výlučná zodpovednosť členských štátov v otázkach národnej bezpečnosti. Na riešenie hybridných hrozieb je potrebný komplexný prístup k bezpečnosti, ktorý je nadrezortný a celospoločenský, ako aj strategickejšie, koordinovanejšie a súdržnejšie úsilie vo všetkých príslušných sektoroch politík. Je dôležité, aby sa nadrezortný prístup zaujal a uplatňoval aj na úrovni EÚ.

4. V týchto záveroch Rada stanovuje priority týkajúce sa ochrany našich spoločností, občanov a slobôd a bezpečnosti našej Únie pred hybridnými hrozbami v kontexte vykonávania nového strategického programu na roky 2019 – 2024 prostredníctvom podpory komplexného prístupu k bezpečnosti s lepšou koordináciou, zdrojmi a technickými kapacitami, pričom vychádza z dôležitej práce, ktorá sa už vykonala v rôznych oblastiach politiky, a to aj v rámci bezpečnostnej a obrannej spolupráce EÚ.

---

[1] Najmä závery Európskej rady z júna 2019, marca 2019, decembra 2018, októbra 2018, júna 2018, marca 2018, júna 2015 a marca 2015.

[2] Konkrétne dokumenty ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19 a ST 7928/16.

5. Pri úsilí o ochranu našich demokratických inštitúcií pred hybridnými hrozbami sa musia vždy rešpektovať základné práva vrátane ochrany osobných údajov, slobody prejavu a práva na informácie a slobody združovania, ako sú zakotvené v Charte základných práv.

6. EÚ a jej členské štáty by mali pokračovať v rozvoji spôsobilostí na odhaľovanie hybridných činností, analýzu ich zdrojov a reagovanie na ne vrátane súvisiaceho odborného vzdelávania a cvičení a podporovať posilňovanie odolnosti členských štátov a inštitúcií, orgánov a agentúr EÚ proti hybridným hrozbám v dlhodobom horizonte, pričom by sa mali v plnej miere využívať existujúce nástroje vhodné na tento účel. Rada zdôrazňuje potrebu aktualizovať operačný protokol EÚ na boj proti hybridným hrozbám na základe získaných poznatkov a skúseností z predchádzajúcich cvičení.

7. Rada zdôrazňuje, že je naďalej potrebné spolupracovať s medzinárodnými organizáciami, ako sú OSN, OBSE a Rada Európy, a vo formátoch ako G7, s cieľom chrániť globálny poriadok založený na pravidlách, okrem iného aj v kontexte boja proti hybridným hrozbám, a aj prostredníctvom budovania dôvery a iných relevantných opatrení.

8. Rada zdôrazňuje záväzok EÚ pokračovať v úzkej a vzájomne sa posilňujúcej spolupráci v oblasti posilňovania odolnosti a boja proti hybridným hrozbám so všetkými príslušnými partnerskými krajinami, najmä v susedstve EÚ, a podporovať tieto krajiny v danej oblasti.

9. Rada vyzýva na nepretržité úsilie o ďalší pokrok pri vykonávaní všetkých opatrení súvisiacich s bojom proti hybridným hrozbám v rámci spoločného súboru návrhov na vykonávanie spoločných vyhlásení o spolupráci medzi EÚ a NATO, a to aj v oblasti situačného povedomia, strategickej komunikácie, predchádzania krízam a reakcie na ne a posilňovania odolnosti. V tejto súvislosti opätovne zdôrazňuje, že je potrebné ďalej posilňovať politický dialóg o boji proti hybridným hrozbám, ako aj organizovať pravidelné paralelné a koordinované cvičenia (PACE) za účasti všetkých členských štátov EÚ a spojencov z NATO, a vyzýva na včasnú finalizáciu nového plánu týchto cvičení. Rada zdôrazňuje potrebu zohľadniť identifikované poznatky a význam nerušenej, inkluzívnej a nediskriminačnej výmeny informácií.

Rada okrem toho zdôrazňuje cenné príspevky Európskeho centra excelentnosti pre boj proti hybridným hrozbám v Helsinkách a podporuje jeho spoluprácu s príslušnými centrami excelentnosti NATO. Víta aj pravidelné a štruktúrované výmeny zamestnancov vrátane spolupráce medzi strediskom pre hybridné hrozby Spravodajského a situačného centra EÚ (INTCEN) a útvarom NATO pre analýzu hybridných hrozieb.

10. Rada uznáva úsilie členských štátov, ktoré vyvíjajú v spolupráci s Komisiou a Európskou službou pre vonkajšiu činnosť (ESVČ) pri vykonávaní prieskumu hybridných rizík uvedeného v opatrení č. 1 spoločného rámca pre boj proti hybridným hrozbám (2016), a vyzýva na pokračovanie v práci a prípadnú revíziu prieskumu hybridných rizík s cieľom lepšie riešiť zraniteľné miesta.

Koherentné úsilie zamerané na posilnenie odolnosti a boj proti hybridným hrozbám

11. Pri vývoji a používaní nových a vznikajúcich technológií vrátane umelej inteligencie a techník zberu údajov by sa mali náležite zohľadňovať nové príležitosti na zvyšovanie odolnosti, ako aj možné zraniteľné miesta a kaskádové účinky v kontexte boja proti hybridným hrozbám, aby sa znížili celkové riziká, a to aj v procese strategického plánovania rámcového programu pre výskum a inováciu.

12. Rada konštatuje, že súčasťou hybridných hrozieb môžu byť škodlivé kybernetické činnosti, a v tejto súvislosti zdôrazňuje význam súboru nástrojov EÚ pre kybernetickú diplomaciu.

13. Vzťah medzi hybridnými hrozbami a hospodárskou bezpečnosťou je relevantným prvkom, ktorý by sa mal zohľadňovať a ktorý zostáva v prvom rade zodpovednosťou členských štátov.

14. Nové nástroje, ako je mechanizmus ustanovený v nariadení EÚ o preverovaní priamych zahraničných investícií, by sa mali účinne využívať na zvýšenie odolnosti a boj proti hybridným hrozbám ako prostriedky na identifikáciu priamych zahraničných investícií, ktoré môžu mať vplyv na bezpečnosť alebo verejný poriadok, a zaoberanie sa nimi.

15. Rada vyzýva Komisiu, aby zahrnula odolnosť proti hybridným hrozbám do procesu posudzovania vplyvu pre príslušné budúce legislatívne návrhy vrátane budúcich rámcových programov pre výskum a inováciu.

16. Rada zdôrazňuje význam pravidelných cvičení a diskusií, ktoré sú založené na scenároch, týkajúcich sa boja proti hybridným hrozbám na ministerskej a inej úrovni, ako aj začleňovania hybridných prvkov do ďalších príslušných činností EÚ v oblasti odbornej prípravy a cvičení na všetkých rôznych úrovniach s podporou členských štátov EÚ a prípadne príslušných orgánov, najmä Európskeho centra excelentnosti pre boj proti hybridným hrozbám.

17. S cieľom zabezpečiť súlad ďalších krokov v rámci spolupráce EÚ v oblasti posilňovania odolnosti a boja proti hybridným hrozbám Rada vyzýva Komisiu a vysokého predstaviteľa, aby komplexne zmapovali situáciu a zohľadnili doterajšie opatrenia a relevantné prijaté dokumenty so zreteľom na možné nové iniciatívy.

Prepojenie vnútornej a vonkajšej bezpečnosti

18. Orgány presadzovania práva, civilnej ochrany a iné príslušné orgány by mali naďalej rozvíjať svoju pripravenosť predchádzať hybridným hrozbám a bojovať proti nim. Spolupráca medzi príslušnými vnútroštátnymi orgánmi, ako aj inštitúciami, orgánmi a agentúrami EÚ v rámci prepojenia medzi vnútornou a vonkajšou bezpečnosťou založená na ich príslušných mandátoch sa musí neustále zlepšovať a zohľadňovať v ich činnosti, pričom sa zároveň musia zvyšovať synergie a musí sa predchádzať zdvojovaniu úsilia, a to aj prostredníctvom horizontálnych pracovných metód, dobrovoľnej výmeny informácií a medziodvetvovej odbornej prípravy a cvičení. Na tento účel by sa mali ďalej posudzovať podporné úlohy a príspevky príslušných mechanizmov EÚ a agentúr EÚ v medziach ich príslušných mandátov a pri rešpektovaní existujúcich rozpočtových obmedzení.

19. Inštitúcie a orgány EÚ by mali spolu s členskými štátmi podrobnejšie rozpracovať využívanie príslušných mechanizmov a nástrojov EÚ na podporu reakcií členských štátov na medziodvetvové a cezhraničné hrozby vrátane integrovaných dojednaní o politickej reakcii na krízu (IPCR), mechanizmu Únie v oblasti civilnej ochrany a jej Koordinačného centra pre reakcie na núdzové situácie (ERCC).

20. Rada uznáva, že členské štáty majú pri riešení vážnej krízy vyplývajúcej z hybridnej činnosti možnosť uplatniť doložku o solidarite (článok 222 ZFEÚ).

Situačné povedomie a analýza spravodajských informácií

21. Spolupráca EÚ v oblasti posilňovania odolnosti a boja proti hybridným hrozbám sa musí riadiť pravidelne aktualizovaným posudzovaním hrozieb a komplexným situačným povedomím. Toto posudzovanie aj povedomie musí rozvíjať EU INTCEN a jeho stredisko pre hybridné hrozby s cieľom zlepšiť schopnosti EÚ a jej členských štátov odhaľovať hybridné činnosti, predchádzať im, narúšať ich a reagovať na ne, a to pri súčasnom rešpektovaní právomocí členských štátov. Rada sa domnieva, že činnosť strediska EÚ pre hybridné hrozby by sa mala ďalej posilniť s prihliadnutím na primeranú úroveň zdrojov vrátane odborných znalostí.

22. Rada pripomína svoje závery o boji proti hybridným hrozbám z 19. apríla 2016, v ktorých vyzýva na mobilizáciu nástrojov EÚ na prevenciu hybridných hrozieb pre Úniu a jej členské štáty, ako aj pre partnerov, a taktiež na boj proti takýmto hrozbám. Rada zdôrazňuje, že je potrebné ďalej rozvíjať existujúce funkcie členských štátov a EÚ v oblasti situačného povedomia s prihliadnutím na zdroje hrozieb a lepšie využívať analýzy spravodajských informácií z EU INTCEN a jeho strediska pre hybridné hrozby, najmä v procese tvorby politiky EÚ a v procese krízového riadenia v oblasti boja proti hybridným hrozbám.

23. Rada uznáva relevantný príspevok, ktorý by mohli v relevantných prípadoch a podľa potreby poskytnúť misie a operácie SBOP, pokiaľ ide o určenie a analýzu ukazovateľov možných hybridných činností tretích strán vrátane dezinformácií zameraných na diskreditáciu činnosti EÚ a jej členských štátov a bránenie v tejto činnosti, a uznáva význam hlbšieho preskúmania možnosti rozvoja takéhoto príspevku.

Ochrana kritickej infraštruktúry

24. Ochrana vnútroštátnych a európskych kritických infraštruktúr, ako aj funkcií a služieb, ktoré sú kritické pre riadne fungovanie štátu, hospodárstva a spoločnosti, je kľúčovou prioritou, a to aj v kontexte posilňovania odolnosti proti hybridným hrozbám, a vyžaduje si nadrezortný a celospoločenský prístup. Pri tomto úsilí sa musí zohľadniť silná vzájomná závislosť rôznych kritických funkcií a služieb vrátane finančných služieb, kľúčová úloha súkromného sektora, meniace sa bezpečnostné prostredie a vznikajúce riziká, a to vo fyzickej, ako aj v kybernetickej sfére.

25. Okrem právnych, regulačných a dozorných požiadaviek na úrovni EÚ a členských štátov, ktorými sa upravuje operačná odolnosť a kontinuita činností, by sa mali podporovať dohody so súkromnými vlastníkmi a prevádzkovateľmi infraštruktúr a služieb s cieľom zaručiť kontinuitu kritických služieb a prístup k nim, aj nad rámec zásahu vyššej moci, a to zabezpečením prijateľnej úrovne pripravenosti reagovať na všetky relevantné hrozby, ako aj flexibility pri riešení a zmierňovaní následkov málo pravdepodobných udalostí s rozsiahlymi dôsledkami a pri obnove po nich.

26. Rada zdôrazňuje, že hoci zodpovednosť za ochranu kritickej infraštruktúry patrí v prvom rade do právomoci členských štátov, vysoký stupeň cezhraničnej a medziodvetvovej prepojenosti si vyžaduje koordinované alebo v prípade potreby harmonizované úsilie na úrovni EÚ, a to aj s cieľom zabezpečiť neprerušované fungovanie vnútorného trhu.

27. V nadväznosti na hodnotenie vykonávania smernice (2008/114/ES), ktoré sa uskutočnilo v júli 2019 a týkalo identifikácie a označenia európskych kritických infraštruktúr, Rada vyzýva Komisiu, aby sa poradila s členskými štátmi o prípadnom návrhu na revíziu smernice na začiatku nového legislatívneho cyklu vrátane prípadných dodatočných opatrení na posilnenie ochrany a odolnosti kritickej infraštruktúry v EÚ, pričom sa zohľadní silná vzájomná závislosť medzi kritickými funkciami a službami.

28. Rada vyzýva Komisiu, aby sa aj naďalej angažovala vo vzťahu s členskými štátmi a v relevantných prípadoch vypracovala nezáväzné dohody o spolupráci medzi členskými štátmi, ktoré majú spoločné a prepojené kritické infraštruktúry.

29. Rada uznáva význam smernice o bezpečnosti sietí a informačných systémov (smernica NIS) pre rozvoj kultúry riadenia rizík a bezpečnostnej kultúry, pokiaľ ide o prevádzkovateľov v kritických odvetviach, ako aj pre vnútroštátne spôsobilosti a stratégie, ktoré zabezpečujú vysokú úroveň bezpečnosti sietí a informačných systémov na území členských štátov, a to aj v kontexte hybridných hrozieb. Rada vyzýva členské štáty, Komisiu a Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA), aby pokračovali v rozvíjaní svojej spolupráce na všetkých príslušných úrovniach na základe odporúčania Komisie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu („koncepcia“).

Boj proti dezinformáciám a zabezpečenie slobodných a spravodlivých volieb

30. Rada víta správu o vykonávaní akčného plánu proti dezinformáciám a uznáva, že nepretržité vykonávanie akčného plánu zostáva stredobodom úsilia EÚ. Rada zdôrazňuje potrebu pravidelného preskúmavania tohto akčného plánu a jeho prípadnej aktualizácie s cieľom zabezpečiť účinný dlhodobý prístup.

31. Rada zdôrazňuje, že práca útvaru ESVČ pre strategickú komunikáciu a najmä troch osobitných skupín (východ, západný Balkán, juh) sa musí podporovať dostatočnými zdrojmi, ktoré umožnia dlhodobé plánovanie, vykonávanie a hodnotenie. Všetky tri osobitné skupiny by v rámci svojich úloh mali byť schopné neustále odhaľovať a analyzovať dezinformačné činnosti zahraničných štátnych subjektov a vonkajších neštátnych subjektov a podnikať kroky proti takýmto činnostiam. Osobitné skupiny by mali tiež naďalej prispievať k účinnej a faktami podloženej pozitívnej komunikácii a podpore zásad, hodnôt a politík Únie vo východnom a južnom susedstve EÚ a na západnom Balkáne a k posilňovaniu celkového mediálneho prostredia a občianskej spoločnosti vo svojich príslušných regiónoch. Rada vyzýva ESVČ, aby posúdila potreby a možnosti posilnenia svojej činnosti v oblasti strategickej komunikácie v iných zemepisných oblastiach, napríklad v subsaharskej Afrike, a zároveň zachovala spôsobilosť potrebnú na vykonávanie súčasných úloh strategickej komunikácie.

32. Rada uznáva, že na riešenie výziev spojených s dezinformáciami vrátane zásahov zameraných na narušanie slobodných a spravodlivých európskych volieb je potrebný komplexný prístup na všetkých úrovniach a čo najlepšie využitie všetkých dostupných online a offline nástrojov. Musí to zahŕňať monitorovanie a analýzu dezinformácií a manipulatívnych zásahov, presadzovanie európskych pravidiel na ochranu údajov, uplatňovanie volebných záruk a úsilie o posilnenie pluralitných médií, profesionálnej žurnalistiky a mediálnej gramotnosti, ako aj povedomia o tejto problematike medzi občanmi. Rada odporúča ďalšiu konsolidáciu aktívnej a nezávislej celoeurópskej siete overovateľov faktov a výskumných pracovníkov bojujúcich proti dezinformáciám. Rada uznáva význam a úlohu občianskej spoločnosti, akademickej obce a súkromného sektora pri riešení problému dezinformácií a pri budovaní odolnosti.

33. Rada uznáva potenciál systému včasného varovania (RAS) v súvislosti s bojom proti dezinformáciám, najmä pokiaľ ide o zasahovanie do volieb. Naliehavo vyzýva Komisiu a ESVČ, aby spolu s členskými štátmi ďalej rozvíjali RAS, aby z neho vznikla komplexná platforma pre členské štáty a inštitúcie EÚ, ktorá im umožní posilniť spoluprácu, koordináciu a výmenu informácií, ako je napríklad výskum a analytické poznatky, najlepšie postupy a komunikačné produkty, s cieľom podporiť riešenie dezinformačných kampaní v rámci širšieho spektra európskeho a vnútroštátneho úsilia.

34. Rada uznáva užitočnosť opatrení a odporúčaní, ktoré Komisia predložila 12. septembra 2018 vo svojom volebnom balíku na zabezpečenie európskych volieb. Rada nabáda Komisiu a členské štáty, aby preskúmali možnosti, ako pokračovať v činnostiach európskych sietí spolupráce pri voľbách s cieľom podporiť výmenu informácií a najlepších postupov. Rada víta úsilie Komisie zapájať všetky príslušné zainteresované strany a podporovať širokú škálu opatrení, ako je napríklad cvičenie v oblasti kybernetickej bezpečnosti európskych volieb (EU ELEx19), pričom zohľadňuje vnútroštátne právomoci v tejto oblasti.

35. Rada uznáva potrebu pokračovať v práci s platformami sociálnych médií s cieľom dosiahnuť vyššie normy zodpovednosti, transparentnosti a vyvodzovania zodpovednosti pri riešení problému dezinformácií. Okrem toho by sa mal na účely akademického výskumu zabezpečiť neobmedzený prístup k anonymizovaným údajom od poskytovateľov platforiem sociálnych médií pre akademický výskum s cieľom uľahčiť tvorbu politík založenú na faktoch. Rada vyzýva Komisiu, aby predložila iniciatívy týkajúce sa ďalšieho postupu pri riešení problému dezinformácií na online platformách. Tieto iniciatívy by mali vychádzať z posúdenia vykonávania Kódexu postupov proti šíreniu dezinformácií, v ktorom by sa mala zohľadniť analytická práca a správy akademických inštitúcií a organizácií občianskej spoločnosti, z monitorovacej správy o kódexe, ktorú vypracovala skupina európskych regulačných orgánov pre audiovizuálne mediálne služby, ako aj z poznatkov získaných z volieb do Európskeho parlamentu v máji 2019. Rada v tejto súvislosti vyzýva Komisiu, aby zvážila možnosti ďalšieho posilnenia vykonávania uvedeného kódexu vrátane prípadného mechanizmu jeho presadzovania, najmä tým, že zavedie nezávislé posudzovanie, či signatári dodržiavajú svoje záväzky.

Bezpečnosť inštitúcií, orgánov a agentúr EÚ

36. Bezpečnosť personálu, inštitúcií, orgánov a agentúr EÚ pred hybridnými hrozbami a inými škodlivými činnosťami je spoločným záujmom EÚ a jej členských štátov. Rada vyzýva inštitúcie, orgány a agentúry EÚ, podporované členskými štátmi, aby na základe komplexného posúdenia hrozieb zabezpečili schopnosť Únie brániť svoju integritu a zvyšovať bezpečnosť svojich informačných a komunikačných sietí a rozhodovacích procesov pred škodlivými činnosťami všetkých druhov. Na tento účel by inštitúcie, orgány a agentúry, podporované členskými štátmi, mali vypracovať a zaviesť komplexný súbor opatrení na zaistenie svojej bezpečnosti v súlade s mandátom Európskej rady z júna 2019. Rada zdôrazňuje, že je dôležité zabezpečiť interoperabilitu IT infraštruktúry EÚ na účely výmeny utajovaných skutočností medzi inštitúciami, orgánmi a agentúrami EÚ a členskými štátmi.