Consiliul
Uniunii Europene

Bruxelles, 10 decembrie 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**

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Subiect:	Eforturi complementare de sporire a rezilienței și de contracarare a amenințărilor hibride – Concluziile Consiliului (10 decembrie 2019)

În anexă, se pun la dispoziția delegațiilor Concluziile Consiliului privind eforturi complementare de sporire a rezilienței și de contracarare a amenințărilor hibride, adoptate în cadrul celei de a 3739-a reuniune a Consiliului din 10 decembrie 2019.

ANEXĂ

Concluziile Consiliului privind eforturi complementare de sporire a rezilienței și de contracarare a amenințărilor hibride

1. Consiliul reamintește concluziile relevante ale Consiliului European[1] și ale Consiliului[2] și își exprimă angajamentul continuu de a spori reziliența Uniunii și a statelor sale membre la amenințările hibride, un fenomen cu multiple fațete și aflat în continuă evoluție și de a consolida cooperarea pentru a detecta, a preveni și a contracara aceste amenințări.

2. Consiliul recunoaște progresele înregistrate în ceea ce privește punerea în aplicare a Cadrului comun privind contracararea amenințărilor hibride (2016), a Comunicării comune privind „Creșterea rezilienței și consolidarea capacităților necesare pentru a aborda amenințările hibride" (2018), precum și a celei privind Planul de acțiune împotriva dezinformării (2018), în conformitate cu concluziile relevante ale Consiliului.

3. Responsabilitatea principală în ceea ce privește contracararea amenințărilor hibride le revine statelor membre. Eforturile de la nivelul UE au un caracter complementar și nu aduc atingere responsabilității exclusive a statelor membre în materie de securitate națională. Pentru a gestiona amenințările hibride este necesară o abordare a securității cuprinzătoare, la nivelul întregii administrații și al întregii societăți, care să acționeze, în cadrul tuturor sectoarelor de politică relevante, într-un mod mai strategic, mai coordonat și mai coerent. Este important ca și la nivelul UE să fie urmărită și aplicată o abordare la nivelul întregii administrații.

4. Prin prezentele concluzii, Consiliul stabilește prioritățile pentru a ne proteja societățile, cetățenii și libertățile, precum și pentru securitatea Uniunii noastre împotriva amenințărilor hibride, în contextul punerii în aplicare a noii Agende strategice pentru perioada 2019-2024, prin promovarea unei abordări cuprinzătoare a securității, asigurând un nivel mai ridicat al coordonării, resurselor și capacităților tehnologice, pe baza lucrărilor importante desfășurate deja în diferite sectoare de politică, inclusiv ca parte a cooperării în materie de securitate și apărare a UE.

---

1 În special, concluziile Consiliului European din iunie 2019, martie 2019, decembrie 2018, octombrie 2018, iunie 2018, martie 2018, iunie 2015 și martie 2015.

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

5. Eforturile de protecție a instituțiilor noastre democratice împotriva amenințărilor hibride trebuie să respecte întotdeauna drepturile fundamentale, inclusiv protecția datelor cu caracter personal, libertatea de exprimare și de informare și libertatea de asociere, astfel cum sunt consacrate în Carta drepturilor fundamentale.

6. UE și statele sale membre ar trebui să continue să dezvolte și să formeze capabilități, precum și să desfășoare exerciții în materie de capabilități pentru a detecta activitățile hibride, a analiza sursele acestora și a răspunde la acestea și să sprijine consolidarea rezilienței statelor membre și a instituțiilor, organismelor și agențiilor UE la amenințările hibride pe termen lung, profitând pe deplin de instrumentele existente adecvate în acest scop. Consiliul subliniază necesitatea actualizării protocolului operațional al UE pentru contracararea amenințărilor hibride, pe baza învățămintelor identificate și a experienței acumulate în urma exercițiilor anterioare.

7. Consiliul subliniază necesitatea continuă de a coopera cu organizații internaționale precum ONU, OSCE și Consiliul Europei și cu alte structuri precum formula G7 în vederea apărării ordinii mondiale bazate pe norme, inclusiv în contextul combaterii amenințărilor hibride, printre altele, prin instaurarea unui climat de încredere și alte măsuri relevante.

8. Consiliul subliniază angajamentul UE de a continua să asigure o cooperare strânsă și care să genereze o consolidare reciprocă a forțelor cu toate țările partenere relevante, în special din vecinătatea UE, și să le ofere sprijin, în ceea ce privește sporirea rezilienței și combaterea amenințărilor hibride.

9. Consiliul solicită depunerea unor eforturi continue și susținute pentru a înainta în punerea în aplicare a tuturor acțiunilor legate de contracararea amenințărilor hibride în cadrul setului comun de propuneri pentru punerea în aplicare a declarațiilor comune privind cooperarea UE-NATO, inclusiv în domenii precum conștientizarea situației, comunicarea strategică, prevenirea crizelor și răspunsul la acestea, precum și sporirea rezilienței. În acest context, Consiliul reiterează necesitatea de a consolida în continuare dialogul politic privind contracararea amenințărilor hibride, precum și de a desfășura exerciții paralele și coordonate (PACE) periodice, cu participarea tuturor statelor membre ale UE și a aliaților NATO, și solicită finalizarea la timp a noului plan privind PACE. Consiliul subliniază că este necesar să se țină seama de lecțiile identificate și de importanța schimburilor libere de informații într-un mod incluziv și nediscriminatoriu.

În plus, Consiliul subliniază contribuțiile valoroase ale Centrului European de Excelență pentru Contracararea Amenințărilor Hibride din Helsinki și încurajează cooperarea sa cu centrele de excelență relevante ale NATO. Acesta salută, de asemenea, schimburile periodice și structurate la nivel de personal, inclusiv cooperarea dintre celula de fuziune a UE împotriva amenințărilor hibride a Centrului de situații și de analiză a informațiilor al UE (INTCEN) și departamentul de analiză a amenințărilor hibride din cadrul NATO.

10. Consiliul recunoaște eforturile depuse de statele membre, în cooperare cu Comisia și cu Serviciul European de Acțiune Externă (SEAE), pentru realizarea studiului privind riscurile hibride prevăzut la Acțiunea 1 a Cadrului comun privind contracararea amenințărilor hibride (2016) și solicită continuarea lucrărilor și o posibilă revizuire a studiului menționat, pentru a aborda mai bine vulnerabilitățile.

Asigurarea coerenței eforturilor de sporire a rezilienței și de contracarare a amenințărilor hibride

11. Atunci când se dezvoltă și se utilizează tehnologii noi și emergente, inclusiv în domeniul inteligenței artificiale și al tehnicilor de culegere de date, ar trebui să se țină seama în mod corespunzător de noile oportunități de sporire a rezilienței, precum și de potențialele vulnerabilități și efecte în cascadă în contextul contracarării amenințărilor hibride, pentru a reduce riscurile generale, inclusiv în procesul de planificare strategică a Programului-cadru pentru cercetare și inovare.

12. Consiliul ia act de faptul că activitățile cibernetice răuvoitoare pot face parte din amenințările hibride și, în acest context, subliniază relevanța setului de instrumente ale UE pentru diplomația cibernetică.

13. Relația dintre amenințările hibride și securitatea economică este un element relevant, care ar trebui luat în considerare și care rămâne în primul rând o responsabilitate a statelor membre.

14. Pentru a spori reziliența și a contracara amenințările hibride, ar trebui să fie utilizate în mod eficace noi instrumente, cum ar fi mecanismul prevăzut de Regulamentul UE privind examinarea investițiilor străine directe, astfel încât să se ofere mijloace de identificare și de abordare a investițiilor străine directe care pot afecta securitatea sau ordinea publică.

15. Consiliul invită Comisia să includă reziliența la amenințările hibride în procesul de evaluare a impactului pentru viitoarele propuneri legislative relevante, inclusiv pentru viitoarele programe-cadru pentru cercetare și inovare.

16. Consiliul subliniază importanța discuțiilor bazate pe scenarii și a exercițiilor periodice privind contracararea amenințărilor hibride la nivel ministerial și la alte niveluri, precum și includerea elementelor hibride în alte activități relevante de formare și de desfășurare de exerciții ale UE la toate nivelurile, cu sprijinul statelor membre și al organismelor relevante, în special al Centrului European de Excelență pentru Contracararea Amenințărilor Hibride, după caz.

17. Pentru a asigura coerența următoarelor etape ale cooperării UE în ceea ce privește sporirea rezilienței și contracararea amenințărilor hibride, Consiliul invită Comisia și Înaltul Reprezentant să realizeze o cartografiere care să țină seama de măsurile luate până în prezent și de documentele relevante adoptate în mod cuprinzător, în vederea unor posibile noi inițiative.

Conexiunea dintre securitatea internă și cea externă

18. Autoritățile de aplicare a legii, autoritățile responsabile cu protecția civilă și alte autorități relevante ar trebui să își îmbunătățească în continuare gradul de pregătire pentru prevenirea și contracararea amenințărilor hibride. Cooperarea dintre autoritățile naționale relevante, precum și între instituțiile, organismele și agențiile UE în ceea ce privește conexiunea dintre securitatea internă și cea externă, bazată pe mandatele lor respective, trebuie să fie în mod continuu îmbunătățită și integrată, amplificând totodată sinergiile și evitând dublarea eforturilor, inclusiv prin metode de lucru orizontale, schimbul voluntar de informații și prin formare și instrucție la nivel transsectorial. În acest scop, ar trebui să se evalueze suplimentar rolurile de sprijin și contribuțiile mecanismelor relevante ale UE și ale agențiilor UE, în cadrul mandatelor lor respective și cu respectarea restricțiilor bugetare existente.

19. Instituțiile și organismele UE, împreună cu statele membre, inclusiv mecanismul integrat pentru un răspuns politic la crize (IPCR), mecanismul de protecție civilă al Uniunii (UCPM) și Centrul de coordonare a răspunsului la situații de urgență (ERCC) din cadrul acestuia ar trebui să dezvolte în continuare utilizarea de mecanisme și instrumente relevante ale UE pentru a sprijini răspunsurile statelor membre la amenințările transsectoriale și transfrontaliere.

20. Consiliul recunoaște că statele membre au posibilitatea de a invoca clauza de solidaritate (articolul 222 din TFUE) în abordarea unei crize grave care rezultă din activitatea hibridă.

Conștientizarea situației și analiza informațiilor

21. Cooperarea UE în ceea ce privește sporirea rezilienței și combaterea amenințărilor hibride trebuie să se bazeze pe o evaluare a amenințărilor actualizată periodic și pe o conștientizare cuprinzătoare a situației. Acestea trebuie să fie elaborate de INTCEN al UE și de celula de fuziune a UE împotriva amenințărilor hibride, care face parte din acesta, pentru a consolida capacitățile UE și ale statelor sale membre de a depista, preveni și împiedica activitățile hibride, precum și de a răspunde la acestea, respectând în același timp competențele statelor membre. Consiliul consideră că activitatea celulei de fuziune a UE împotriva amenințărilor hibride ar trebui să fie consolidată în continuare, luându-se în calcul un nivel adecvat al resurselor, inclusiv expertiză profesională.

22. Consiliul reamintește concluziile sale privind contracararea amenințărilor hibride din 19 aprilie 2016 prin care se solicita mobilizarea de instrumente ale UE pentru prevenirea și contracararea amenințărilor hibride pentru Uniune și statele sale membre, precum și pentru parteneri. Consiliul subliniază necesitatea de a dezvolta în continuare funcțiile existente de conștientizare a situației ale statelor membre și ale UE, ținând seama de sursele amenințărilor și de a utiliza mai bine analiza informațiilor furnizată de INTCEN al UE și de celula sa de fuziune împotriva amenințărilor hibride, în special în procesul de elaborare a politicilor UE și cel de gestionare a crizelor în ceea ce privește contracararea amenințărilor hibride.

23. Consiliul recunoaște contribuția relevantă pe care ar putea-o avea misiunile și operațiile PSAC, dacă și după cum este cazul, în identificarea și analiza indicatorilor unor posibile acțiuni hibride ale terților, inclusiv a dezinformării care vizează discreditarea și împiedicarea acțiunilor UE și ale statelor sale membre; Consiliul recunoaște, de asemenea, valoarea explorării suplimentare a posibilității de a dezvolta această contribuție.

Protecția infrastructurilor critice

24. Protecția infrastructurilor critice naționale și europene, precum și a funcțiilor și serviciilor critice pentru buna funcționare a statului, a economiei și a societății reprezintă o prioritate-cheie, inclusiv în contextul sporirii rezilienței la amenințările hibride, care necesită o abordare la nivelul întregii administrații și al întregii societăți. Lucrările în acest sens trebuie să țină seama de interdependențele puternice dintre diferitele funcții și servicii critice, inclusiv serviciile financiare, rolul esențial al sectorului privat, mediul de securitate în schimbare și riscurile emergente, atât în domeniul fizic, cât și în cel cibernetic.

25. În plus, pe lângă cerințele juridice, de reglementare și de supraveghere de la nivelul UE și de la nivel național care reglementează reziliența operațională și continuitatea activității, ar trebui promovate acorduri cu proprietarii și operatorii de infrastructuri și servicii din sectorul privat, pentru a garanta continuitatea serviciilor critice și accesul la acestea, inclusiv dincolo de cazurile de forță majoră, prin asigurarea unui nivel acceptabil de pregătire pentru a răspunde tuturor amenințărilor relevante, precum și de flexibilitate pentru a aborda și atenua efectele evenimentelor cu probabilitate mică și impact ridicat, precum și în scopul recuperării în urma acestora.

26. Consiliul subliniază faptul că, deși responsabilitatea pentru protecția infrastructurii critice este în primul rând o chestiune de competență națională, gradul ridicat al interdependențelor transfrontaliere și transsectoriale necesită eforturi coordonate sau, după caz, armonizate la nivelul UE, inclusiv în vederea funcționării fără obstacole a pieței interne.

27. În urma evaluării din iulie 2019 privind punerea în aplicare a Directivei (2008/114/CE) privind identificarea și desemnarea infrastructurilor critice europene (ICE), Consiliul invită Comisia să se consulte cu statele membre cu privire la o posibilă propunere de revizuire a directivei la începutul noului ciclu legislativ, inclusiv cu privire la posibile măsuri suplimentare de consolidare a protecției și rezilienței infrastructurii critice din UE, ținând seama de interdependențele puternice dintre funcțiile și serviciile critice.

28. Consiliul invită Comisia să colaboreze în continuare cu statele membre și, după caz, să dezvolte acorduri de cooperare fără caracter obligatoriu între statele membre care dețin în comun infrastructuri critice conectate.

29. Consiliul recunoaște importanța Directivei privind securitatea rețelelor și a informațiilor (Directiva NIS) pentru dezvoltarea unei culturi a gestionării riscurilor și a securității de către operatorii din sectoarele critice, precum și pentru asigurarea de către capabilitățile și strategiile naționale a unui nivel ridicat de securitate a rețelelor și a sistemelor informatice pe teritoriul lor, inclusiv în contextul amenințărilor hibride. Consiliul invită statele membre, Comisia și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) să își dezvolte în continuare cooperarea pe baza Recomandării Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (*Blueprint*), la toate nivelurile relevante.

Combaterea dezinformării și asigurarea unor alegeri libere și corecte

30. Consiliul salută raportul privind punerea în aplicare a Planului de acțiune împotriva dezinformării și recunoaște că punerea în aplicare în continuare a planului de acțiune rămâne în centrul eforturilor UE. Consiliul subliniază necesitatea de a revizui periodic și, atunci când este necesar, de a actualiza planul de acțiune pentru a asigura o abordare eficientă pe termen lung.

31. Consiliul subliniază că activitatea Departamentului pentru comunicare strategică al SEAE și, în special, a celor trei grupuri operative (privind Europa de Est, Balcanii de Vest și Europa de Sud) trebuie să fie sprijinită cu resurse suficiente, care să permită planificarea, punerea în aplicare și evaluarea pe termen lung. Toate cele trei grupuri operative au, printre alte sarcini, obligația de a fi în măsură, în mod continuu, să depisteze, să analizeze și să conteste activitățile de dezinformare ale actorilor statali străini și ale actorilor nestatali externi. De asemenea, grupurile operative ar trebui să contribuie în continuare la o comunicare pozitivă eficace și bazată pe fapte, la promovarea principiilor, valorilor și politicilor Uniunii în vecinătatea estică și sudică a UE și în Balcanii de Vest, precum și la consolidarea, la nivel general, a cadrului mediatic și a societății civile din regiunile respective. Consiliul invită SEAE să evalueze nevoile și posibilitățile de consolidare a activității sale de comunicare strategică în alte zone geografice, cum ar fi Africa Subsahariană, menținând, în același timp, capacitatea necesară pentru a îndeplini sarcinile de comunicare strategică existente.

32. Consiliul recunoaște că este necesară o abordare cuprinzătoare la toate nivelurile pentru a aborda provocările legate de dezinformare, inclusiv ingerințele menite să submineze desfășurarea unor alegeri europene libere și corecte, utilizându-se în mod optim toate instrumentele disponibile online și offline. Aceasta trebuie să includă monitorizarea și analiza dezinformării și a ingerințelor manipulatoare, asigurarea aplicării normelor europene de protecție a datelor, aplicarea garanțiilor electorale, eforturi de consolidare a pluralismului mediatic, a jurnalismului profesionist și a educației în domeniul mass-mediei, precum și sensibilizarea cetățenilor. Consiliul recomandă consolidarea în continuare a unei rețele transeuropene active și independente de verificatori de fapte și de cercetători împotriva dezinformării. Consiliul recunoaște importanța și rolul jucat de societatea civilă, mediul academic și sectorul privat în abordarea dezinformării și în consolidarea rezilienței.

33. Consiliul recunoaște potențialul sistemului de alertă timpurie (RAS) în ceea ce privește lupta împotriva dezinformării, în special în ceea ce privește ingerințele electorale. Consiliul îndeamnă Comisia și SEAE, împreună cu statele membre, să dezvolte în continuare RAS pentru a deveni o platformă cuprinzătoare prin intermediul căreia statele membre și instituțiile UE să își poată intensifica cooperarea, coordonarea și schimbul de informații, de exemplu în domeniul cercetării și cunoștințelor analitice, al bunelor practici și al produselor de comunicare, astfel încât să sprijine abordarea campaniilor de dezinformare în cadrul unei serii de eforturi europene și naționale.

34. Consiliul recunoaște utilitatea măsurilor și a recomandărilor prezentate de Comisie la 12 septembrie 2018 în pachetul său electoral pentru garantarea unor alegeri europene libere și corecte. Consiliul încurajează Comisia și statele membre să examineze posibilitățile de continuare a activităților rețelelor europene de cooperare în materie de alegeri pentru a sprijini schimbul de informații și de bune practici. Consiliul salută eforturile Comisiei de a implica toate părțile interesate relevante și de a sprijini o gamă largă de măsuri, cum ar fi exercițiul privind securitatea cibernetică a alegerilor europene (UE ELEx19), ținând seama de competențele naționale în acest domeniu.

35. Consiliul recunoaște necesitatea de a continua colaborarea cu platformele de comunicare socială pentru a atinge standarde mai ridicate de responsabilitate, transparență și asumare a răspunderii în ceea ce privește combaterea dezinformării. În plus, ar trebui ca furnizorii de platforme să acorde acces neîngrădit la date anonimizate în vederea cercetării academice, pentru a facilita politicile bazate pe date concrete. Consiliul invită Comisia să prezinte inițiative privind calea de urmat pentru combaterea dezinformării de pe platformele online. Aceste inițiative ar trebui să se bazeze pe o evaluare a punerii în aplicare a Codului de bune practici privind dezinformarea, care ar trebui să țină seama de activitatea și rapoartele analitice elaborate de mediul academic și de organizațiile societății civile, de raportul de monitorizare privind codul, elaborat de către Grupul autorităților europene de reglementare pentru serviciile mass-media audiovizuale, precum și de lecțiile învățate în urma alegerilor pentru Parlamentul European din mai 2019. În acest context, Consiliul invită Comisia să analizeze modalitățile de consolidare în continuare a punerii în aplicare a codului de bune practici, inclusiv posibile mecanisme de asigurare a conformității în cazul platformelor online, în special prin includerea unei evaluări independente a respectării de către semnatari a angajamentelor asumate.

Securitatea instituțiilor, organelor și agențiilor UE

36. Securitatea personalului, a instituțiilor, a organismelor și a agențiilor UE împotriva amenințărilor hibride și a altor activități răuvoitoare reprezintă un punct de interes comun pentru UE și statele sale membre. Consiliul solicită instituțiilor, organelor și agențiilor UE, sprijinite de statele membre, să asigure capacitatea Uniunii de a-și proteja integritatea și de a spori securitatea rețelelor de informare și comunicare și a proceselor decizionale ale UE împotriva activităților răuvoitoare de toate tipurile, pe baza unei evaluări cuprinzătoare a amenințărilor. În acest scop, instituțiile, organismele și agențiile, sprijinite de statele membre, ar trebui să elaboreze și să pună în aplicare un set cuprinzător de măsuri care să asigure securitatea acestora, în conformitate cu mandatul Consiliului European din iunie 2019. Consiliul subliniază importanța asigurării interoperabilității infrastructurii informatice a UE pentru schimbul de informații clasificate între instituțiile, organismele, agențiile UE și statele membre.