



Bruksela, 10 grudnia 2019 r.
(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

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Dotyczy:	Dodatkowe wysiłki na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych – Konkluzje Rady (10 grudnia 2019 r.)

Delegacje otrzymują w załączeniu konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych przyjęte na 3739. posiedzeniu Rady w dniu 10 grudnia 2019 r.

Konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych

1. Rada przywołuje odnośne konkluzje Rady Europejskiej¹ i Rady² i stwierdza, że jest niezmiennie zdecydowana zwiększać odporność Unii i jej państw członkowskich na wieloaspektowe i stale zmieniające się zagrożenia hybrydowe oraz wzmacniać współpracę na rzecz ich wykrywania, zapobiegania im i ich zwalczania.

2. Rada dostrzega postępy poczynione w realizacji wspólnych ram z 2016 r. dotyczących zwalczania zagrożeń hybrydowych i wspólnego komunikatu z 2018 r. pt. „Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe”, a także Planu działania z 2018 r. na rzecz zwalczania dezinformacji, zgodnie z odpowiednimi konkluzjami Rady.

3. Główna odpowiedzialność za zwalczanie zagrożeń hybrydowych spoczywa na państwach członkowskich. Wysiłki na szczeblu UE mają charakter uzupełniający i nie wpływają na spoczywającą wyłącznie na państwach członkowskich odpowiedzialność za bezpieczeństwo narodowe. Aby przeciwdziałać zagrożeniom hybrydowym, konieczne jest kompleksowe podejście do bezpieczeństwa przewidujące zaangażowanie całej administracji rządowej i całego społeczeństwa, wymagające prowadzenia prac we wszystkich odnośnych sektorach polityki w bardziej strategiczny, skoordynowany i spójny sposób. Ważne jest, by takie podejście przewidujące zaangażowanie całej administracji rządowej było przestrzegane i stosowane także na szczeblu UE.

4. W niniejszych konkluzjach Rada określa priorytety dotyczące ochrony naszych społeczeństw, obywateli i swobód oraz bezpieczeństwa naszej Unii przed zagrożeniami hybrydowymi – w kontekście realizacji Nowego programu strategicznego na lata 2019–2024 – poprzez propagowanie kompleksowego podejścia do bezpieczeństwa polegającego na sprawniejszej koordynacji, lepszych zasobach i zdolnościach technologicznych, z wykorzystaniem istotnych prac, które już przeprowadzono w różnych sektorach polityki, w tym jako element unijnej współpracy w dziedzinie bezpieczeństwa i obrony.

¹ W szczególności konkluzje Rady Europejskiej z czerwca 2019 r., marca 2019 r., grudnia 2018 r., października 2018 r., czerwca 2018 r., marca 2018 r., czerwca 2015 r. i marca 2015 r.

² W szczególności zawarte w dokumentach: ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16.

5. Wysiłki, by chronić nasze instytucje demokratyczne przed zagrożeniami hybrydowymi zawsze muszą być podejmowane z poszanowaniem praw podstawowych, w tym ochrony danych osobowych, wolności wypowiedzi, wolnego dostępu do informacji i wolności zrzeszania się, zapisanych w karcie praw podstawowych.

6. UE i jej państwa członkowskie powinny nadal rozwijać, szkolić i ćwiczyć zdolności w zakresie wykrywania działań hybrydowych, analizowania ich źródeł i reagowania na nie oraz wspierać zwiększanie długoterminowej odporności państw członkowskich i instytucji, organów i jednostek organizacyjnych UE na zagrożenia hybrydowe, przy pełnym wykorzystaniu przydatnych w tym celu istniejących instrumentów. Rada podkreśla, że należy zaktualizować unijny protokół operacyjny do celów zwalczania zagrożeń hybrydowych na podstawie zebranych, zgłoszonych i wdrożonych doświadczeń i wniosków wyciągniętych z poprzednich ćwiczeń.

7. Rada podkreśla ciągłą potrzebę współpracy z organizacjami międzynarodowymi, takimi jak ONZ, OBWE i Rada Europy, oraz w takim składzie jak np. grupa G7, po to by bronić opartego na określonych zasadach ładu światowego, także w kontekście zwalczania zagrożeń hybrydowych, w tym poprzez budowanie zaufania i inne odpowiednie środki.

8. Rada podkreśla, że UE jest zdecydowana kontynuować ściśle i wzajemnie się wzmacniającą współpracę z wszystkimi odpowiednimi krajami partnerskimi, w szczególności w sąsiedztwie UE, w zakresie zwiększania odporności i zwalczania zagrożeń hybrydowych oraz nadal je wspierać w tym obszarze.

9. Rada apeluje o stałe i konsekwentne wysiłki na rzecz dalszych postępów w realizacji wszystkich działań związanych ze zwalczaniem zagrożeń hybrydowych na mocy wspólnego zestawu propozycji służących wdrożeniu wspólnych deklaracji dotyczących współpracy UE–NATO, w tym w dziedzinach orientacji sytuacyjnej, komunikacji strategicznej, zapobiegania kryzysom i reagowania na nie oraz wzmacniania odporności. W tym kontekście ponownie podkreśla potrzebę dalszego pogłębiania dialogu politycznego w sprawie zwalczania zagrożeń hybrydowych, a także regularnego przeprowadzania równoległych i skoordynowanych ćwiczeń (PACE), z udziałem wszystkich państw członkowskich UE i sojuszników z NATO, a także wzywa do terminowego sfinalizowania nowego planu PACE. Rada podkreśla potrzebę uwzględniania zebranych i zgłoszonych doświadczeń i wniosków oraz znaczenie niezakłóconej wymiany informacji prowadzonej w inkluzywny i niedyskryminacyjny sposób.

Ponadto Rada podkreśla cenne uwagi Europejskiego Centrum ds. Zwalczania Zagrożeń Hybrydowych w Helsinkach i zachęca je do współpracy z odpowiednimi centrami doskonałości NATO. Z zadowoleniem przyjmuje również regularną i zorganizowaną wymianę personelu, w tym współpracę między Komórką UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych w Centrum Analiz Wywiadowczych UE (INTCEN) a komórką ds. analizy zagrożeń hybrydowych NATO.

10. Rada docenia wysiłki państw członkowskich podejmowane we współpracy z Komisją i Europejską Służbą Działań Zewnętrznych (ESDZ), które odnoszą się do prowadzenia badania na temat zagrożeń hybrydowych przewidzianego w działaniu 1 wspólnych ram z 2016 r. dotyczących zwalczania zagrożeń hybrydowych; apeluje też o kontynuowanie tych prac i ewentualny przegląd wspomnianego badania, tak by lepiej zająć się słabymi stronami.

Spójne działanie na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych

11. Opracowując i wykorzystując nowe i powstające technologie, w tym sztuczną inteligencję i techniki gromadzenia danych, aby ograniczyć ogólne zagrożenia, należy odpowiednio uwzględnić nowe możliwości zwiększania odporności oraz potencjalne słabe strony i efekty kaskadowe w kontekście zwalczania zagrożeń hybrydowych, również w ramach strategicznego planowania programu ramowego w zakresie badań naukowych i innowacji.

12. Rada zauważa, że szkodliwe działania w cyberprzestrzeni mogą być elementem zagrożeń hybrydowych, i w związku z tym podkreśla znaczenie unijnego zestawu narzędzi dla dyplomacji cyfrowej.

13. Związek między zagrożeniami hybrydowymi a bezpieczeństwem gospodarczym to istotny element, który należy brać pod uwagę i który pozostaje przede wszystkim w sferze odpowiedzialności państw członkowskich.

14. Nowe instrumenty, np. mechanizm przewidziany w rozporządzeniu o monitorowaniu bezpośrednich inwestycji zagranicznych w UE, należy skutecznie wykorzystywać do zwiększania odporności i zwalczania zagrożeń hybrydowych poprzez zapewnienie środków pozwalających wskazywać bezpośrednio inwestycje zagraniczne, które mogłyby niekorzystnie wpłynąć na bezpieczeństwo lub porządek publiczny, i zająć się problemem takich inwestycji.

15. Rada zachęca Komisję do uwzględniania odporności na zagrożenia hybrydowe w ocenach skutków opracowywanych w odniesieniu do odnośnych przyszłych wniosków ustawodawczych, w tym przyszłych programów ramowych w zakresie badań naukowych i innowacji.

16. Rada podkreśla, jak ważne są regularne ćwiczenia i dyskusje oparte na scenariuszach dotyczące zwalczania zagrożeń hybrydowych przeprowadzane na szczeblu ministerialnym i innych szczeblach, a także włączanie elementów związanych z tymi zagrożeniami do innych stosownych szkoleń i ćwiczeń UE na poszczególnych szczeblach, przy wsparciu ze strony państw członkowskich i odpowiednich organów, w szczególności, w stosownych przypadkach, Europejskiego Centrum ds. Zwalczania Zagrożeń Hybrydowych.

17. Aby zapewnić spójność kolejnych etapów unijnej współpracy w zakresie zwiększania odporności i zwalczania zagrożeń hybrydowych, Rada zachęca Komisję i Wysokiego Przedstawiciela do sporządzenia kompleksowego zestawienia, w którym uwzględnione zostaną już podjęte działania i stosowne przyjęte dokumenty, z myślą o ewentualnych nowych inicjatywach.

Powiązanie między bezpieczeństwem wewnętrznym i zewnętrznym

18. Organy odpowiedzialne za ściganie przestępstw, ochronę ludności i inne odpowiednie organy powinny nadal zwiększać swoją gotowość do zapobiegania zagrożeniom hybrydowym i ich zwalczania. Współpraca między odpowiednimi organami krajowymi, a także instytucjami, organami i jednostkami organizacyjnymi UE w ramach powiązania między bezpieczeństwem wewnętrznym i zewnętrznym, prowadzona na podstawie ich odnośnych mandatów, musi być stale usprawniana i włączana w główny nurt; jednocześnie należy zwiększać synergie i unikać powielania działań, także poprzez horyzontalne metody pracy, dobrowolną wymianę informacji oraz przekrojowe szkolenia i ćwiczenia. W tym celu należy dokładniej ocenić rolę i wkłady odpowiednich unijnych mechanizmów i jednostek organizacyjnych – w ramach ich odnośnych mandatów i z poszanowaniem istniejących ograniczeń budżetowych.

19. Instytucje i organy UE wraz z państwami członkowskimi, także w ramach zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), Unijnego Mechanizmu Ochrony Ludności i jego Centrum Koordynacji Reagowania Kryzysowego (ERCC), powinny dokładniej omówić stosowanie odnośnych mechanizmów i instrumentów UE, które mają wspierać działania podejmowane przez państwa członkowskie w reakcji na zagrożenia międzysektorowe i transgraniczne.

20. Rada przyznaje, że państwa członkowskie mogą powołać się na klauzulę solidarności (art. 222 TFUE), gdy muszą stawić czoła poważnemu kryzysowi wynikającemu z działań hybrydowych.

Orientacja sytuacyjna i analiza wywiadowcza

21. Podstawą unijnej współpracy w zakresie zwiększania odporności i zwalczania zagrożeń hybrydowych musi być regularnie aktualizowana ocena zagrożeń i kompleksowa orientacja sytuacyjna. Powinny być one rozwijane przez INTCEN i jego Komórkę ds. Syntezy Informacji o Zagrożeniach Hybrydowych, tak by zwiększać zdolności UE i jej państw członkowskich do wykrywania działań hybrydowych, zapobiegania im, przerywania ich i reagowania na nie, przy jednoczesnym poszanowaniu kompetencji państw członkowskich. Rada jest zdania, że prace Komórki ds. Syntezy Informacji o Zagrożeniach Hybrydowych należy jeszcze zintensyfikować, zapewniając przy tym odpowiedni poziom zasobów, w tym wiedzy fachowej.

22. Rada przywołuje swoje konkluzje z dnia 19 kwietnia 2016 r. o przeciwdziałaniu zagrożeniom hybrydowym, w których zaapelowała o zmobilizowanie instrumentów UE w celu zapobiegania zagrożeniom hybrydowym dla Unii i jej państw członkowskich i partnerów oraz przeciwdziałania takim zagrożeniom. Rada podkreśla, że należy dalej rozwijać istniejące instrumenty państw członkowskich i UE służące zapewnieniu orientacji sytuacji, uwzględniając źródła zagrożeń, i lepiej wykorzystywać analizę wywiadowczą zapewnianą przez INTCEN i jego Komórkę ds. Syntezy Informacji o Zagrożeniach Hybrydowych, w szczególności w ramach kształtowania unijnej polityki i unijnych działań zarządzania kryzysowego w zakresie przeciwdziałania zagrożeniom hybrydowym.

23. Rada docenia istotny wkład, który misje i operacje w dziedzinie WPBiO mogłyby wnieść, w stosownych przypadkach, w identyfikowanie i analizowanie wskaźników możliwych działań hybrydowych prowadzonych przez strony trzecie, w tym dezinformacji służącej zdyskredytowaniu i utrudnianiu działania UE i jej państw członkowskich; Rada uznaje też celowość dalszego badania możliwości zwiększania tego wkładu.

Ochrona infrastruktury krytycznej

24. Ochrona krajowej i europejskiej infrastruktury krytycznej, a także funkcji i usług o krytycznym znaczeniu dla prawidłowego funkcjonowania państwa, gospodarki i społeczeństwa jest jednym z kluczowych priorytetów, w tym w kontekście zwiększania odporności na zagrożenia hybrydowe, i wymaga podejścia przewidującego zaangażowanie całej administracji rządowej i całego społeczeństwa. W pracach tych należy uwzględnić silne współzależności między poszczególnymi funkcjami i usługami krytycznymi, w tym usługami finansowymi, kluczową rolę sektora prywatnego, zmienne środowisko bezpieczeństwa oraz pojawiające się zagrożenia, zarówno fizyczne, jak i w cyberprzestrzeni.

25. Ponadto – obok unijnych i krajowych prawnych, regulacyjnych i nadzorczych wymogów dotyczących odporności operacyjnej i ciągłości działania – należy propagować dokonywanie ustaleń z właścicielami i operatorami infrastruktury i usług z sektora prywatnego, po to by zagwarantować ciągłość i dostęp do usług krytycznych nie tylko w przypadku wystąpienia siły wyższej, poprzez zapewnienie zadowalającego poziomu gotowości do reagowania na wszystkie odnośne zagrożenia, a także zapewnienie elastyczności w zakresie stawiania czoła zdarzeniom o niskim prawdopodobieństwie wystąpienia, ale poważnych konsekwencjach, łagodzenia ich skutków i stabilizowania sytuacji.

26. Rada podkreśla, że choć odpowiedzialność za ochronę infrastruktury krytycznej jest przede wszystkim kwestią kompetencji krajowych, wysoki stopień wzajemnych zależności transgranicznych i międzysektorowych sprawia, że konieczne są skoordynowane, a w razie potrzeby – zharmonizowane wysiłki na szczeblu UE, w tym z myślą o niezakłóconym funkcjonowaniu rynku wewnętrznego.

27. W nawiązaniu do przeprowadzonej w lipcu 2019 r. oceny wdrażania dyrektywy 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej Rada zwraca się do Komisji, by już na początku nowego cyklu legislacyjnego zasięgnęła opinii państw członkowskich na temat ewentualnej propozycji zmian do tej dyrektywy, w tym na temat ewentualnych dodatkowych środków służących wzmocnieniu ochrony i odporności infrastruktury krytycznej w UE, z uwzględnieniem silnych współzależności między funkcjami i usługami krytycznymi.

28. Rada zachęca Komisję, by nadal współpracowała z państwami członkowskimi, a w stosownych przypadkach – by nawiązywała niewiążące porozumienia o współpracy między państwami członkowskimi współdzielącymi połączoną infrastrukturę krytyczną.

29. Rada dostrzega znaczenie dyrektywy dotyczącej bezpieczeństwa sieci i systemów informatycznych dla rozwijania kultury zarządzania ryzykiem i bezpieczeństwa przez operatorów w kluczowych sektorach, a także dla krajowych zdolności i strategii zapewniających wysoki poziom bezpieczeństwa sieci i systemów informatycznych na ich terytorium, w tym w kontekście zagrożeń hybrydowych. Rada zwraca się do państw członkowskich, Komisji i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), by nadal rozwijały swoją współpracę na wszystkich odpowiednich szczeblach w oparciu o zalecenie Komisji w sprawie planu skoordynowanego reagowania na wypadek wystąpienia transgranicznych incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych.

Przeciwdziałanie dezinformacji i zapewnienie wolnych i uczciwych wyborów

30. Rada z zadowoleniem przyjmuje sprawozdanie z realizacji Planu działania na rzecz zwalczania dezinformacji i przyznaje, że dalsze wdrażanie tego planu pozostaje w centrum działań UE. Rada podkreśla, że należy regularnie dokonywać przeglądu tego planu, a w razie potrzeby aktualizować go, tak by zapewnić skuteczne podejście długoterminowe.

31. Rada podkreśla, że prace zespołu ds. komunikacji strategicznej ESDZ, a zwłaszcza trzech grup zadaniowych (Wschód, Bałkany Zachodnie, Południe) należy wesprzeć dostatecznymi zasobami umożliwiającymi długoterminowe planowanie, wdrażanie i ocenę. Do zadań wszystkich trzech grup zadaniowych powinno należeć stałe wykrywanie, analizowanie i unieszkodliwianie działań dezinformacyjnych prowadzonych przez zagraniczne podmioty państwowe i zewnętrzne podmioty niepaństwowe. Grupy zadaniowe powinny także nadal przyczyniać się do skutecznego, merytorycznego pozytywnego przekazywania i promowania zasad, wartości i polityki Unii w krajach wschodniego i południowego sąsiedztwa UE i na Bałkanach Zachodnich oraz do polepszania ogólnych warunków działalności mediów i społeczeństwa obywatelskiego w regionach, którymi się zajmują. Rada zachęca ESDZ, by oceniła potrzeby i możliwości wzmocnienia prac w zakresie komunikacji strategicznej w innych obszarach geograficznych, takich jak Afryka Subsaharyjska, przy jednoczesnym utrzymaniu zdolności niezbędnych do prowadzenia istniejących zadań komunikacyjnych.

32. Rada przyznaje, że aby stawić czoła wyzwaniom związanym z dezinformacją, w tym działaniami mającymi przeszkodzić w przeprowadzaniu wolnych i uczciwych wyborów europejskich, konieczne jest kompleksowe podejście na wszystkich szczeblach, optymalnie wykorzystujące wszelkie dostępne narzędzia online i offline. Podejście to musi obejmować monitorowanie i analizę dezinformacji i manipulacji, wdrożenie europejskich przepisów o ochronie danych, stosowanie zabezpieczeń wyborczych, wysiłki na rzecz wzmocnienia pluralistycznych mediów, profesjonalnego dziennikarstwa i umiejętności korzystania z mediów, a także podnoszenia świadomości wśród obywateli. Rada zaleca dalsze umacnianie aktywnej niezależnej ogólnoeuropejskiej sieci weryfikatorów informacji i badaczy wobec dezinformacji. Rada docenia znaczenie i rolę społeczeństwa obywatelskiego, środowisk akademickich i sektora prywatnego w przeciwdziałaniu dezinformacji i budowaniu odporności.

33. Rada dostrzega potencjał systemu wczesnego ostrzegania w odniesieniu do zwalczania dezinformacji, w szczególności w odniesieniu do prób zakłócania przebiegu wyborów. Apeluje do Komisji i ESDZ, by wraz z państwami członkowskimi nadal rozwijały ten system, z myślą o przekształceniu go w kompleksową platformę pozwalającą państwom członkowskim i instytucjom UE wzmacniać współpracę, koordynację i wymianę informacji, np. wyników badań i analiz, najlepszych praktyk oraz produktów komunikacyjnych, tak by wspierać przeciwdziałanie kampaniom dezinformacyjnym w ramach szeregu wysiłków europejskich i krajowych.

34. Rada dostrzega użyteczność środków i zaleceń przedstawionych przez Komisję w dniu 12 września 2018 r. w pakiecie dotyczącym zapewnienia wolnych i uczciwych wyborów europejskich. Rada zachęca Komisję i państwa członkowskie do zbadania możliwości kontynuowania działalności przez europejskie sieci współpracy w zakresie wyborów, by wesprzeć wymianę informacji i najlepszych praktyk. Rada z zadowoleniem przyjmuje wysiłki Komisji na rzecz zaangażowania wszystkich odpowiednich zainteresowanych stron i wspierania szerokiego spektrum środków, takich jak ćwiczenie w dziedzinie cyberbezpieczeństwa dotyczące wyborów europejskich (EU ELEx19), z uwzględnieniem kompetencji krajowych w tym zakresie.

35. Rada uznaje potrzebę dalszej współpracy z platformami mediów społecznościowych w celu zapewnienia wyższych standardów odpowiedzialności, przejrzystości i rozliczalności w przeciwdziałaniu dezinformacji. Ponadto należy przyznać nieograniczony dostęp do zanonimizowanych danych przekazanych przez operatorów platform mediów społecznościowych do celów badań naukowych, tak by ułatwić kształtowanie polityki w oparciu o merytoryczne dane. Rada zwraca się do Komisji, by przedstawiła ona inicjatywy dotyczące dalszych działań na rzecz przeciwdziałania dezinformacji na platformach internetowych. Inicjatywy te powinny opierać się na ocenie wdrożenia kodeksu postępowania w zakresie zwalczania dezinformacji, w której należy uwzględnić prace analityczne i sprawozdania środowisk akademickich i organizacji społeczeństwa obywatelskiego, na sprawozdaniu monitorującym dotyczącym tego kodeksu przygotowanym przez europejską grupę regulatorów audiowizualnych usług medialnych, a także na wdrożonych doświadczeniach i wnioskach z wyborów do Parlamentu Europejskiego w maju 2019 r. W tym kontekście Rada zachęca Komisję, by rozważyła sposoby – także mające postać ewentualnych mechanizmów egzekwowania na potrzeby platform internetowych – dalszego usprawniania wdrażania wspomnianego kodeksu postępowania, zwłaszcza poprzez uwzględnienie niezależnej oceny przestrzegania przez jego sygnatariuszy podjętych przez nich zobowiązań.

Bezpieczeństwo instytucji, organów i jednostek organizacyjnych UE

36. We wspólnym interesie UE i jej państw członkowskich leży zapewnienie personelowi, instytucjom, organom i jednostkom organizacyjnym UE ochrony przed zagrożeniami hybrydowymi i innymi szkodliwymi działaniami. Rada apeluje do instytucji, organów i jednostek organizacyjnych UE, by przy wsparciu ze strony państw członkowskich zapewniły zdolność Unii do chronienia jej integralności i do zwiększania ochrony unijnych informacji, sieci komunikacyjnych i procesów decyzyjnych przed szkodliwymi działaniami wszelkiego rodzaju, na podstawie kompleksowej oceny zagrożenia. W tym celu instytucje, organy i jednostki organizacyjne UE powinny przy wsparciu ze strony państw członkowskich opracować i wdrożyć kompleksowy zestaw środków w celu zapewnienia sobie bezpieczeństwa, zgodnie z mandatem Rady Europejskiej z czerwca 2019 r. Rada podkreśla znaczenie zapewnienia interoperacyjności unijnej infrastruktury informatycznej do wymiany informacji niejawnych między instytucjami, organami i jednostkami organizacyjnymi UE i jej państwami członkowskimi.
