Parlament Europejski
2019-2024

Dokument z posiedzenia

A9-0022/2022

8.2.2022

SPRAWOZDANIE

w sprawie obcych ingerencji we wszystkie procesy demokratyczne w Unii Europejskiej, w tym dezinformacji
(2020/2268(INI))

Komisja Specjalna ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w Unii Europejskiej, w tym Dezinformacji

Sprawozdawczyni: Sandra Kalniete

SPIS TREŚCI

Strona

PROJEKT REZOLUCJI PARLAMENTU EUROPEJSKIEGO

w sprawie obcych ingerencji we wszystkie procesy demokratyczne w Unii Europejskiej, w tym dezinformacji
(2020/2268(INI))

Parlament Europejski,

– uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7, 8, 11, 12, 39, 40, 47 i 52,

– uwzględniając Kartę Narodów Zjednoczonych, w szczególności jej art. 1 i 2,

– uwzględniając rezolucję Zgromadzenia Ogólnego Narodów Zjednoczonych nr 2131 z dnia 21 grudnia 1965 r. pt. „Deklaracja w sprawie niedopuszczalności ingerowania w wewnętrzne sprawy państw i ochrony ich niezależności i suwerenności”,

– uwzględniając Konwencję o ochronie praw człowieka i podstawowych wolności, w szczególności jej art. 8, 9, 10, 11, 12, 13, 14, 16 i 17, oraz Protokół do tej konwencji, w szczególności jego art. 3,

– uwzględniając swoją rezolucję z dnia 23 listopada 2016 r. w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania propagandzie stron trzecich przeciwko Unii[1] oraz zalecenie z dnia 13 marca 2019 r. dotyczące podsumowania działań podjętych przez ESDZ dwa lata po sprawozdaniu Parlamentu w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich[2],

– uwzględniając swoją rezolucję z dnia 13 czerwca 2018 r. w sprawie cyberobrony[3],

– uwzględniając wspólne komunikaty Komisji i wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa z dnia 5 grudnia 2018 pt. „Plan działania na rzecz zwalczania dezinformacji” (JOIN(2018)0036) i z dnia 14 czerwca 2019 r. pt. „Sprawozdanie z realizacji planu działania przeciwko dezinformacji” (JOIN(2019)0012),

– uwzględniając wspólny dokument roboczy służb z dnia 23 czerwca 2021 r. na temat piątego sprawozdania z postępu prac w sprawie wdrażania wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym z 2016 r. oraz wspólnego komunikatu z 2018 r. w sprawie zwiększenia odporności i wzmocnienia zdolności reagowania na zagrożenia hybrydowe (SWD(2021)0729),

– uwzględniając europejski plan działania na rzecz demokracji (COM(2020)0790),

– uwzględniając komunikat Komisji z 3 grudnia 2020 r. pt. „Europejskie media w

[1] Dz.U. C 224 z 27.6.2018, s. 58.
[2] Dz.U. C 23 z 21.1.2021, s. 152.
[3] Dz.U. C 28 z 27.1.2020, s. 57.

cyfrowej dekadzie – plan działania na rzecz wsparcia odbudowy i transformacji” (COM(2020) 784),

– uwzględniając pakiet aktu prawnego o usługach cyfrowych,

– uwzględniając swoją rezolucję z dnia 20 października 2021 r. w sprawie europejskich mediów w dekadzie cyfrowej – plan działania na rzecz wsparcia odbudowy i transformacji[4],

– uwzględniając kodeks postępowania w zakresie zwalczania dezinformacji z 2018 r. oraz wytyczne z 2021 r. w sprawie wzmocnienia kodeksu postępowania w zakresie zwalczania dezinformacji (COM(2021)0262), a także zalecenia dotyczące nowego kodeksu postępowania w zakresie zwalczania dezinformacji wydane przez Europejską Grupę Regulatorów ds. Audiowizualnych Usług Medialnych w październiku 2021 r.,

– uwzględniając sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego nr 9/2021 pt. „Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany”,

– uwzględniając wniosek Komisji z dnia 16 grudnia 2020 r. dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych (COM(2020)0829) oraz proponowany załącznik do dyrektywy,

– uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/452 z dnia 19 marca 2019 r. ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii[5] (rozporządzenie w sprawie monitorowania BIZ) oraz wydane w marcu 2020 r. wytyczne dotyczące rozporządzenia w sprawie monitorowania BIZ (C(2020)1981),

– uwzględniając wspólny komunikat Komisji oraz wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa z dnia 16 grudnia 2020 r. pt. „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę” (JOIN(2020)0018),

– uwzględniając artykuły Komisji Prawa Międzynarodowego dotyczące odpowiedzialności państw za czyny niezgodne z prawem międzynarodowym,

– uwzględniając wniosek Komisji z dnia 16 grudnia 2020 r. dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 (COM(2020)0823),

– uwzględniając opublikowany w marcu 2021 r. zestaw unijnych narzędzi służących ograniczeniu ryzyka w zakresie cyberbezpieczeństwa w sieciach 5G,

– uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds.

[4] Teksty przyjęte, P9_TA(2021)0428.
[5] Dz.U. L 79 I z 21.3.2019, s. 1.

Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013[6],

– uwzględniając badania, briefingi i dogłębne analizy zlecone przez Komisję Specjalną ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w Unii Europejskiej, w tym Dezinformacji (INGE),

– uwzględniając wysłuchanie Frances Haugen z 8 listopada 2021 r. zorganizowane przez Komisję Rynku Wewnętrznego i Ochrony Konsumentów we współpracy z innymi komisjami,

– uwzględniając swoją rezolucję z 7 października 2021 r. w sprawie stanu zdolności cyberobronnych UE[7],

– uwzględniając cele zrównoważonego rozwoju ONZ, w szczególności cel nr 16 zakładający promowanie pokojowych i inkluzywnych społeczeństw z myślą o zrównoważonym rozwoju,

– uwzględniając orędzie o stanie Unii i list intencyjny z 2021 r.,

– uwzględniając sprawozdanie sekretarza generalnego ONZ z dnia 10 września 2021r. pt. „Nasza wspólna agenda”,

– uwzględniając wspólny komunikat Komisji oraz wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa z dnia 10 czerwca 2020 r. pt. „Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom” (JOIN(2020)0008),

– uwzględniając decyzję Rady z dnia 15 listopada 2021 r. w sprawie zmiany systemu sankcji wobec Białorusi, poszerzenia kryteriów umieszczania konkretnych osób i firm na liście sankcyjnej, które organizują lub wspomagają ataki hybrydowe białoruskiego reżimu i instrumentalnie traktują ludzi,

– uwzględniając swoją decyzję z dnia 18 czerwca 2020 r. w sprawie powołania, kompetencji, składu liczbowego i długości kadencji Komisji Specjalnej ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w Unii Europejskiej, w tym Dezinformacji, określającą jej kompetencje, skład liczbowy i długość kadencji[8], przyjętą zgodnie z art. 207 Regulaminu,

– uwzględniając art. 54 Regulaminu,

– uwzględniając sprawozdanie Komisji Specjalnej ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w Unii Europejskiej, w tym Dezinformacji (A9-0022/2022),

A. mając na uwadze, że obce ingerencje stanowią poważne naruszenie powszechnych wartości i zasad, na których opiera się Unia, takich jak godność człowieka, wolność, równość, solidarność, poszanowanie praw człowieka i podstawowych wolności,

[6] Dz.U. L 151 z 7.6.2019, s. 15.
[7] Teksty przyjęte, P9_TA(2021)0412.
[8] Dz.U. C 362 z 8.9.2021, s. 186.

demokracja i praworządność;

B. mając na uwadze, że obce ingerencje, manipulacja informacjami i dezinformacja stanowią naruszenie podstawowych wolności wypowiedzi i informacji, zapisanych w art. 11 Karty praw podstawowych Unii Europejskiej i zagrażają tym wolnościom, a także procesom demokratycznym w UE i jej państwach członkowskich, np. organizacji wolnych i uczciwych wyborów; mając na uwadze, że celem obcych ingerencji jest zniekształcanie lub fałszywe przedstawianie faktów, sztuczne wyolbrzymianie jednostronnych argumentów, dyskredytowanie informacji w celu degradacji dyskursu politycznego i ostatecznie podważenie zaufania do systemu wyborczego, a zatem do samego procesu demokratycznego;

C. mając na uwadze, że wszelkie przeciwdziałanie obcym ingerencjom i manipulacji informacjami samo musi respektować podstawowe wolności wypowiedzi i informacji; mając na uwadze, że Agencja Praw Podstawowych Unii Europejskiej (FRA) odgrywa kluczową rolę w ocenie przestrzegania praw podstawowych, w tym art. 11 karty praw podstawowych, aby uniknąć nieproporcjonalnych działań; mając na uwadze, że podmioty przeprowadzające obcą ingerencję i dopuszczające się manipulowania informacjami wykorzystują te swobody z korzyścią dla siebie, w związku z czym konieczne jest zintensyfikowanie zapobiegawczej walki z zagraniczną ingerencją i manipulowaniem informacjami, ponieważ demokracja zależy od podejmowania przez ludzi świadomych decyzji;

D. mając na uwadze, że, jak wskazują dowody, działające w złych intencjach i autorytarne państwowe i niepaństwowe podmioty zagraniczne, takie jak Rosja, Chiny i in., wykorzystują manipulowanie informacjami i inne metody w celu ingerowania w procesy demokratyczne w UE; mając na uwadze, że ataki te, stanowiące część strategii wojny hybrydowej i będące pogwałceniem prawa międzynarodowego, wprowadzają w błąd i oszukują obywateli oraz wpływają na ich zachowania wyborcze, pogłębiają debaty prowadzące do podziałów, dzielą, polaryzują i wykorzystują podatność społeczeństw na zagrożenia, promują nawoływanie do nienawiści, pogarszają sytuację słabszych grup społecznych, które są bardziej narażone na dezinformację, zakłócają integralność demokratycznych wyborów i referendów, wzbudzają nieufność do rządów krajowych, władz publicznych i liberalnego porządku demokratycznego, a ich celem jest destabilizacja demokracji europejskiej, a zatem stanowią poważne zagrożenie dla bezpieczeństwa i suwerenności UE;

E. mając na uwadze, że obce ingerencje to sposób postępowania zagrażający wartościom, procedurom demokratycznym, procesom politycznym, bezpieczeństwu państw i obywateli oraz zdolności radzenia sobie w wyjątkowych sytuacjach lub mogący wywierać negatywny wpływ; mając na uwadze, że takie ingerencje mają charakter manipulacyjny oraz są prowadzone i finansowane w sposób celowy i skoordynowany; mając na uwadze, że podmiotami odpowiedzialnymi za taką ingerencję, w tym ich pełnomocnikami na ich własnym terytorium i poza nim, mogą być podmioty państwowe lub niepaństwowe, a w ich zagranicznej ingerencji często pomagają im współsprawcy polityczni w państwach członkowskich, którzy czerpią korzyści polityczne i gospodarcze z faworyzowania strategii zagranicznych; mając na uwadze, że ze względu na wykorzystanie krajowych popleczników przez podmioty zagraniczne oraz na ich współpracę z krajowymi sojusznikami zatarciu ulega granica między ingerencją obcą a

krajową;

F. mając na uwadze, że taktyka obcej ingerencji przyjmuje wiele postaci, w tym dezinformowania, zatajania informacji, manipulowania platformami mediów społecznościowych, ich algorytmami, regulaminami i systemami reklamowymi, cyberataków, operacji typu hack-and-leak w celu uzyskania informacji o wyborcach i wpłynięcia na legalność procesu wyborczego, gróźb wobec dziennikarzy, badaczy, polityków i członków organizacji społeczeństwa obywatelskiego oraz nękania takich osób, potajemnych darowizn i pożyczek na potrzeby politycznych partii, kampanii sprzyjających określonym kandydatom, organizacji i mediów, fałszywych lub popleczniczych mediów i organizacji, przejmowania i kooptacji elit, tzw. brudnych pieniędzy, fikcyjnych osób lub tożsamości, presji na autocenzurę, nadużywania narracji historycznych, religijnych i kulturowych, nacisków na instytucje edukacyjne i kulturalne, przejmowania kontroli nad infrastrukturą krytyczną, wywierania presji na cudzoziemców mieszkających w UE, wykorzystywania migrantów i szpiegostwa; mając na uwadze, że taktyki te są często ze sobą łączone, aby uzyskać lepszy efekt;

G. mając na uwadze, że manipulowanie informacjami i rozpowszechnianie dezinformacji może służyć interesom gospodarczym podmiotów państwowych i niepaństwowych oraz ich popleczników, a także prowadzić do zależności gospodarczej, która może być wykorzystywana do celów politycznych; mając na uwadze, że w świecie niekinetycznej konkurencji międzynarodowej obce ingerencje mogą być głównym narzędziem destabilizacji i osłabiania przeciwników lub zwiększania własnej przewagi konkurencyjnej poprzez tworzenie kanałów wpływu, zależności w łańcuchu dostaw, szantaż lub przymus; mając na uwadze, że dezinformacja powoduje bezpośrednie i pośrednie szkody gospodarcze, które nie są systematycznie oceniane;

H. mając na uwadze, że informacja wprowadzająca w błąd jest weryfikowalną nieprawdziwą informacją, która nie ma na celu wyrządzenia szkody, natomiast dezinformacja jest weryfikowalną nieprawdziwą informacją celowo tworzoną, prezentowaną lub rozpowszechnianą w celu wyrządzenia szkody lub wywołania potencjalnie destrukcyjnych skutków dla społeczeństwa poprzez oszukanie opinii publicznej, lub uzyskania zamierzonego zysku gospodarczego;

I. mając na uwadze, że konieczne jest ustalenie w UE wspólnych i szczegółowych definicji oraz metodologii, aby poprawić wspólne zrozumienie zagrożeń i opracować odpowiednie standardy UE w celu skuteczniejszego demaskowania i reagowania; mając na uwadze, że Europejska Służba Działań Zewnętrznych wykonała znaczną pracę w tej dziedzinie; mając na uwadze, że definicje te muszą gwarantować odporność na ingerencję zewnętrzną i poszanowanie praw człowieka; mając na uwadze, że niezwykle ważna jest współpraca z partnerami o podobnych poglądach, prowadzona w ramach odpowiednich forów międzynarodowych, nad wspólnymi definicjami obcej ingerencji, aby ustanowić międzynarodowe normy i standardy; mając na uwadze, że UE powinna przodować w ustanawianiu jasnych międzynarodowych zasad demaskowania obcej ingerencji;

Potrzeba skoordynowanej strategii przeciwko obcym ingerencjom

J. mając na uwadze, że próby ingerencji zagranicznej na całym świecie nasilają się i stają

się coraz bardziej systemowe i wyrafinowane, ponieważ opierają się na powszechnym wykorzystaniu sztucznej inteligencji i zmniejszają możliwość wskazania podmiotu inicjującego;

K. mając na uwadze, że obowiązkiem UE i jej państw członkowskich jest obrona wszystkich obywateli i całej infrastruktury, a także ich systemów demokratycznych przed próbami obcych ingerencji; mając na uwadze, że, jak się jednak wydaje, UE i jej państwom członkowskim brakuje odpowiednich i wystarczających środków umożliwiających im lepsze zapobieganie takim zagrożeniom, ich wykrywanie, demaskowanie i przeciwdziałanie im oraz karanie za ich tworzenie;

L. mając na uwadze, że wśród wielu decydentów oraz obywateli w ogóle panuje ogólny brak świadomości, jaka jest rzeczywista sytuacja pod tym względem, co może w sposób niezamierzony przyczyniać się do powstawania kolejnych podatności; mając na uwadze, że kwestia kampanii dezinformacyjnych nie znajduje się na pierwszym miejscu agendy europejskich decydentów; mając na uwadze, że wysłuchania i prace komisji specjalnej INGE przyczyniły się do publicznego uznania i kontekstualizacji tych kwestii oraz z powodzeniem ukształtowały europejską debatę na temat ingerencji zagranicznych; mając na uwadze, że długotrwałe obce działania dezinformacyjne już przyczyniły się do pojawienia się rodzimych źródeł dezinformacji;

M. mając na uwadze, że przejrzyste monitorowanie przez organy instytucjonalne i niezależnych analityków i weryfikatorów informacji stanu obcych ingerencji w czasie rzeczywistym, skuteczna koordynacja ich działań oraz wymiana informacji mają zasadnicze znaczenie dla możliwości podjęcia właściwych działań, nie tylko w celu podania informacji o trwających atakach, lecz także przeciwdziałania im; mając na uwadze, że podobne zainteresowanie należy okazać mapowaniu społeczeństwa i identyfikowaniu jego najbardziej narażonych i podatnych grup na obce manipulacje i dezinformację oraz eliminowaniu przyczyn tych podatności;

N. mając na uwadze, że najważniejszy priorytet obrony UE, tj. odporność i przygotowanie obywateli UE na obce ingerencje i manipulowanie informacjami, wymaga długoterminowego podejścia obejmującego całość społeczeństwa, począwszy od edukacji i podnoszenia świadomości problemów na wczesnym etapie;

O. mając na uwadze, że niezbędna jest współpraca i koordynacja na wszystkich szczeblach administracji i we wszystkich sektorach między państwami członkowskimi, na poziomie UE i z krajami o podobnych poglądach oraz ze społeczeństwem obywatelskim i sektorem prywatnym w celu identyfikowania podatności, wykrywania ataków i neutralizowania ich skutków; mając na uwadze, że istnieje pilna potrzeba zsynchronizowania postrzegania zagrożeń z bezpieczeństwem narodowym;

Budowanie odporności przez orientację sytuacyjną, umiejętność korzystania z mediów i informacji, pluralizm mediów, niezależne dziennikarstwo i edukację

P. mając na uwadze, że orientacja sytuacyjna, solidne systemy demokratyczne, stabilna praworządność, prężne społeczeństwo obywatelskie oraz wczesna ocena ostrzeżeń i zagrożeń to pierwsze kroki w kierunku przeciwdziałania manipulowaniu informacjami i ingerencjom; mając na uwadze, że mimo wszystkich postępów w poprawianiu świadomości obcych ingerencji wiele osób, w tym decydentów i urzędników aktywnych

w obszarach mogących być celem ingerencji, nadal nie ma świadomości potencjalnego ryzyka związanego z obcymi ingerencjami i sposobów reagowania na nie;

Q. mając na uwadze, że odznaczające się wysoką jakością, finansowane w zrównoważony i przejrzysty sposób i niezależne media informacyjne i profesjonalne dziennikarstwo mają zasadnicze znaczenie dla wolności i pluralizmu mediów oraz praworządności, a zatem stanowią podporę demokracji i najlepszy sposób przeciwdziałania dezinformacji; mając na uwadze, że niektóre podmioty zagraniczne wykorzystują wolność zachodnich mediów do rozpowszechniania dezinformacji; mając na uwadze, że w erze cyfrowej profesjonalne media i tradycyjne dziennikarstwo, jako wysokiej jakości źródła informacji, stają przed wyzwaniami; mając na uwadze, że wysokiej jakości kształcenie i szkolenia dziennikarzy w UE i poza jej terytorium są niezbędne w celu zapewniania cennych analiz dziennikarskich oraz wysokich standardów redakcyjnych; mając na uwadze, że UE musi nadal wspierać dziennikarstwo w środowisku cyfrowym; mając na uwadze, że komunikacja oparta na dowodach naukowych powinna odgrywać ważną rolę;

R. mając na uwadze, że media publiczne cieszące się niezależnością redakcyjną są niezbędne i niezastąpione w zapewnianiu ogółowi społeczeństwa bezstronnych usług informacyjnych wysokiej jakości i należy je chronić przed ich przejmowaniem w złych zamiarach oraz wzmacniać jako podstawowy filar walki z dezinformacją;

S. mając na uwadze, że do celów analizy obcych ingerencji poszczególne zainteresowane strony i instytucje stosują różne metody i definicje – wszystkie o różnych stopniach kompleksowości, a także mając na uwadze, że te różnice mogą mieć niekorzystny wpływ na prowadzenie porównywalnego monitorowania, analizy i oceny poziomu zagrożenia, przez co wspólne działanie jest utrudnione; mając na uwadze, że istnieje potrzeba opracowania unijnej definicji i metodyki, aby poprawić wspólną analizę zagrożeń;

T. mając na uwadze, że adekwatne podejście do problemu wymaga uzupełnienia terminologii skupiającej się na treści, takiej jak fałszywe lub wprowadzające w błąd informacje i dezinformacja, o terminologię odnoszącą się do zachowań; mając na uwadze, że terminologia ta powinna być zharmonizowana i z uwagą stosowana;

U. mając na uwadze, że szkolenie w zakresie umiejętności korzystania z mediów i umiejętności cyfrowych oraz podnoszenie świadomości zarówno dzieci, jak i dorosłych to ważne narzędzia zwiększania odporności obywateli na próby ingerencji w przestrzeni informacyjnej oraz unikania manipulacji i polaryzacji; mając na uwadze, że ogólnie społeczeństwa umiejące korzystać z mediów są bardziej odporne na obce ingerencje; mając na uwadze, że metody pracy dziennikarskiej, takie jak konstruktywne dziennikarstwo, mogłyby przyczynić się do zwiększenia zaufania obywateli do dziennikarstwa;

V. mając na uwadze, że manipulowanie informacjami może przyjmować wiele form, takich jak rozpowszechnianie dezinformacji i całkowicie fałszywych informacji, zniekształcanie faktów, narracji i opinii, zatajanie niektórych informacji lub opinii, prezentowanie informacji bez kontekstu, manipulowanie uczuciami ludzi, szerzenie mowy nienawiści, propagowanie pewnych opinii kosztem innych oraz nękanie w celu

uciszenia i represjonowania; mając na uwadze, że jednym z celów manipulacji informacjami jest stworzenie chaosu prowadzącego do utraty zaufania obywateli do starych i nowych „strażników dostępu” do informacji; mając na uwadze, że granica między wolnością wypowiedzi a propagowaniem mowy nienawiści i dezinformacji jest bardzo cienka i nie należy jej naruszać;

W. mając na uwadze, że między innymi Azerbejdżan, Chiny, Turcja i Rosja atakują dziennikarzy i przeciwników w Unii Europejskiej, jak w przypadku azerbejdżańskiego blogera i opozycjonisty Mahammada Mirzaliego w Nantes czy tureckiego dziennikarza Erka Acarera w Berlinie;

X. mając na uwadze, że istnieją konkretne dowody na to, że kampanie dezinformacyjne kwestionujące ideały demokratyczne i prawa podstawowe są ukierunkowane na procesy demokratyczne UE i ingerują w nie; mając na uwadze, że dezinformacja związana z tematami obejmującymi m.in. płeć, LGBTIQ+, zdrowie i prawa seksualne i reprodukcyjne oraz mniejszości jest formą dezinformacji, która zagraża prawom człowieka, narusza prawa cyfrowe i polityczne oraz bezpieczeństwo i ochronę osób korzystających z tych praw, a także jest źródłem rozłamów i braku jedności wśród państw członkowskich; mając na uwadze, że podczas kampanii wyborczych kobiety będące kandydatkami politycznymi są zwykle w nieproporcjonalnej skali celem seksistowskich narracji, co prowadzi do zniechęcenia kobiet do udziału w procesach demokratycznych; mając na uwadze, że autorzy takich kampanii dezinformacyjnych pod przykrywką promowania tradycyjnych lub konserwatywnych wartości zawierają strategiczne sojusze z lokalnymi partnerami w celu uzyskania dostępu do lokalnych danych wywiadowczych i według doniesień otrzymują miliony euro w postaci finansowania zagranicznego;

Y. mając na uwadze, że poza instytucjami państwowymi dziennikarze, liderzy opinii i sektor prywatny, a także każdy segment społeczeństwa i każda osoba mają do odegrania ważną rolę polegającą na identyfikowaniu i powstrzymywaniu rozpowszechniania dezinformacji, a także na ostrzeganiu zagrożonych osób w swoim otoczeniu; mając na uwadze, że społeczeństwo obywatelskie, środowisko akademickie i dziennikarze już w znacznym stopniu przyczyniają się do podnoszenia świadomości społecznej i zwiększania odporności społecznej, w tym również we współpracy z partnerami w krajach partnerskich;

Z. mając na uwadze, że organizacje społeczeństwa obywatelskiego reprezentujące głosy mniejszości i organizacje praw człowieka w całej Europie pozostają niedofinansowane, mimo że odgrywają kluczową rolę w podnoszeniu świadomości i zwalczaniu dezinformacji; mając na uwadze, że organizacje społeczeństwa obywatelskiego powinny dysponować odpowiednimi zasobami, aby odgrywać swoją rolę w ograniczaniu wpływu obcych ingerencji;

AA. mając na uwadze, że kiedy zaczyna być rozpowszechniana dezinformacja, ważne jest posiadanie w odpowiednim czasie łatwego dostępu do informacji opartych na faktach i pochodzących z wiarygodnych źródeł;

AB. mając na uwadze, że szybkie wykrywanie ataków w ramach obcej ingerencji i prób manipulowania infosferą jest niezbędne dla przeciwdziałania im; mając na uwadze, że

analiza danych wywiadowczych UE i orientacja sytuacyjna zależą od gotowości państw członkowskich do wymiany informacji; mając na uwadze, że przewodnicząca Komisji zaproponowała rozważenie utworzenia Wspólnego Centrum Orientacji Sytuacyjnej UE; mając na uwadze, że zapobieganie i proaktywne środki, w tym wczesne identyfikowanie treści i zdrowy ekosystem informacyjny, to znacznie skuteczniejsze środki niż późniejsze działania związane ze sprawdzaniem faktów i dementowaniem informacji, które to działania mają mniejszy zasięg niż pierwotna dezinformacja; mając na uwadze, że UE i jej państwa członkowskie nie mają obecnie wystarczających zdolności do podejmowania takich środków; mając na uwadze, że nowe narzędzia analityczne oparte na sztucznej inteligencji, takie jak litewski Debunk.eu, mogłyby pomóc w wykrywaniu ataków, wymianie wiedzy i informowaniu opinii publicznej;

AC. mając na uwadze, że dezinformacji sprzyja słaba lub fragmentaryczna narracja na szczeblu krajowym lub unijnym, spolaryzowane i emocjonalne debaty, wykorzystywanie słabych punktów i uprzedzeń w społeczeństwie i wśród pojedynczych osób, a także mając na uwadze, że dezinformacja zakłóca debatę publiczną dotyczącą wyborów i inne procesy demokratyczne oraz może utrudnić obywatelom podejmowanie właściwych decyzji;

Obce ingerencje z wykorzystaniem platform internetowych

AD. mając na uwadze, że platformy internetowe mogą być łatwo dostępnymi i przystępnymi cenowo narzędziami dla podmiotów angażujących się w manipulowanie informacjami i inne ingerencje, takie jak nawoływanie do nienawiści i nękanie, szkodzenie zdrowiu i bezpieczeństwu naszych społeczności online, uciszanie oponentów, szpiegostwo lub rozpowszechnianie dezinformacji; mając na uwadze, że jak dowiedziono, ich funkcjonowanie zachęca do spolaryzowanych i skrajnych opinii kosztem informacji opartych na faktach; mając na uwadze, że platformy również mają swoje interesy i przy przetwarzaniu informacji mogą nie zachowywać neutralności; mając na uwadze, że niektóre platformy internetowe w dużym stopniu korzystają z systemu, który wzmacnia podziały, ekstremizm i polaryzację; mając na uwadze, że przestrzeń internetowa stała się równie ważna dla naszej demokracji jak przestrzeń fizyczna i w związku z tym wymaga odpowiednich zasad;

AE. mając na uwadze, że platformy przyspieszyły i pogłębiły rozprzestrzenianie się błędnych informacji i dezinformacji w bezprecedensowy sposób stwarzający wyzwania; mając na uwadze, że platformy internetowe kontrolują przepływ informacji i reklam w internecie oraz projektują i stosują algorytmy w celu kontrolowania tych przepływów, a także mając na uwadze, że platformy nie działają w przejrzysty sposób, nie posiadają odpowiednich procedur weryfikowania tożsamości, używają niejasnej i nieprecyzyjnej terminologii oraz nie udzielają informacji lub udzielają bardzo niewiele informacji na temat kształtu, zastosowania i oddziaływania algorytmów; mając na uwadze, że uzależniający element algorytmów platform internetowych stworzył poważny problem zdrowia publicznego, na który należy zareagować; mając na uwadze, że platformy internetowe powinny być odpowiedzialne za szkodliwe skutki swoich usług, ponieważ niektóre platformy były świadome wad swoich algorytmów, w szczególności ich roli w rozpowszechnianiu treści dzielących, ale nie zajęły się nimi w celu maksymalizacji zysków, co ujawnili sygnaliści;

AF. mając na uwadze, że mają miejsce ingerencje i prowadzi się kampanie manipulowania

informacjami wymierzone we wszystkie środki mające zapobiegać rozprzestrzenianiu się COVID-19, w tym szczepienia w całej UE, a platformy internetowe nie zdołały skoordynować swoich wysiłków w walce z takimi działaniami i mogły nawet przyczynić się do ich upowszechnienia; mając na uwadze, że taka dezinformacja może zagrażać życiu, zniechęcając ludzi do szczepienia lub promując fałszywe leczenie; mając na uwadze, że pandemia zaostrzyła systemową walkę między demokracją a autorytaryzmem, skłaniając autorytarne podmioty państwowe i niepaństwowe, takie jak Chiny i Rosję, do stosowania szerokiej gamy jawnych i ukrytych instrumentów w celu destabilizacji ich demokratycznych odpowiedników; mając na uwadze, że w dokumentach dotyczących Facebooka (Facebook Papers) ujawniono, iż platforma nie radzi sobie z dezinformacją związaną ze szczepionkami, w tym w języku angielskim; mając na uwadze, że sytuacja jest jeszcze gorsza w przypadku dezinformacji związanej ze szczepionkami w językach innych niż angielski; mając na uwadze, że kwestia ta dotyczy wszystkich platform;

AG. mając na uwadze, że liczni dostawcy zarejestrowani w UE sprzedają nieprawdziwe polubienia, komentarze i udostępnienia oraz fałszywych obserwujących każdemu podmiotowi pragnącemu sztucznie zwiększyć swoją widoczność online; mając na uwadze, że prawie niemożliwe jest wskazanie uzasadnionego zastosowania takich usług, podczas gdy do ich szkodliwych zastosowań zalicza się manipulowanie wyborami i innymi procesami demokratycznymi, propagowanie oszustw, negatywne recenzje produktów konkurencji, oszukiwanie reklamodawców oraz tworzenie fałszywej publiczności wykorzystywanej do kształtowania konwersacji, do osobistych ataków i sztucznego wyolbrzymiania pewnych punktów widzenia, które w przeciwnym razie nie zwróciłyby uwagi; mając na uwadze, że obce reżimy, takie jak Rosja i Chiny, wykorzystują te narzędzia internetowe na masową skalę, aby wpłynąć na debatę publiczną w krajach europejskich; mając na uwadze, że dezinformacja może destabilizować demokrację europejską;

AH. mając na uwadze, że platformy społeczne oraz urządzenia i aplikacje cyfrowe gromadzą i przechowują ogromne ilości bardzo szczegółowych i często wrażliwych danych osobowych na temat każdego użytkownika; mając na uwadze, że takie dane można wykorzystać do przewidywania tendencji w zakresie zachowania, nasilenia błędu poznawczego i ukierunkowania procesu decyzyjnego; mając na uwadze, że takie dane są wykorzystywane do celów handlowych; mając na uwadze powtarzające się wycieki danych, które osłabiają bezpieczeństwo ofiar takich wycieków, i fakt, że dane można sprzedać na czarnym rynku; mając na uwadze, że takie bazy danych mogą być kopalniami złota dla działających w złych intencjach podmiotów, które chcą zaatakować określone grupy lub osoby;

AI. mając na uwadze, że ogólnie platformy internetowe są projektowane w sposób zapewniający, by wybór opcji nieudostępniania danych nie był intuicyjny oraz był bardziej kłopotliwy i czasochłonny niż wybór opcji ich udostępniania;

AJ. mając na uwadze, że platformy internetowe są zintegrowane z większością obszarów naszego życia, a rozpowszechnianie informacji na platformach może mieć ogromy wpływ na nasze myślenie i zachowanie, np. w zakresie naszych preferencji wyborczych, wyborów gospodarczych i społecznych oraz wyboru źródeł informacji, a także mając na uwadze, że dokonywane decydujące wybory o znaczeniu publicznym są obecnie

w rzeczywistości uwarunkowane interesami handlowymi przedsiębiorstw prywatnych;

AK. mając na uwadze, że algorytmiczne mechanizmy selekcjonowania i inne cechy platform mediów społecznościowych są zaprojektowane z myślą o maksymalizacji zaangażowania; mając na uwadze, że regularne są doniesienia o tym, iż cechy te sprzyjają promowaniu treści polaryzujących, radykalizujących i dyskryminacyjnych oraz utrzymaniu użytkowników w kręgach o podobnych poglądach; mając na uwadze, że prowadzi to do stopniowej radykalizacji użytkowników platform, a także do kondycjonowania i zanieczyszczania zbiorowych procesów dyskusyjnych, a nie do ochrony procesów demokratycznych i jednostek; mając na uwadze, że nieskoordynowana działalność platform doprowadziła do rozbieżności w ich działaniach i umożliwiła rozprzestrzenianie się dezinformacji między platformami; mając na uwadze, że model biznesowy polegający na zarabianiu pieniędzy poprzez rozpowszechnianie polaryzujących informacji i projektowanie algorytmów sprawia, że platformy są łatwym celem manipulacji przez wrogie podmioty zagraniczne; mając na uwadze, że platformy mediów społecznościowych można by zaprojektować w inny sposób, aby wspierać zdrowszą internetową sferę publiczną;

AL. mając na uwadze, że tworzenie materiałów audio i wideo typu deepfake staje się coraz łatwiejsze wraz z pojawieniem się niedrogich i łatwych w użyciu technologii, a upowszechnianie się takich materiałów bardzo szybko staje się coraz większym problemem; mając jednak na uwadze, że obecnie 90 % badań dotyczy opracowywania materiałów typu deepfake, a tylko 10 % ich wykrywania;

AM. mając na uwadze, że systemy samoregulacji, takie jak kodeks postępowania w zakresie zwalczania dezinformacji z 2018 r., poprawiły sytuację; mając jednak na uwadze, że poleganie na dobrej woli platform nie działa ani nie jest skuteczne, a także dostarczyło niewiele wiarygodnych danych na temat ich ogólnego wpływu; mając ponadto na uwadze, że platformy podjęły indywidualne działania o różnym stopniu i różnym skutkach, co doprowadziło do powstania „tylnych drzwi” umożliwiających dalsze rozpowszechnianie treści w innych miejscach pomimo ich usunięcia; mając na uwadze, że aby kodeks postępowania miał wystarczający wpływ na środowisko internetowe, musi istnieć jasny zestaw zasad i sankcji;

AN. mając na uwadze, że europejski plan działania na rzecz demokracji ma na celu wzmocnienie kodeksu postępowania z 2018 r. i wraz z aktem o usługach cyfrowych stanowi próbę odejścia od samoregulacji, a także ma na celu wprowadzenie większej liczby gwarancji i skuteczniejszej ochrony dla użytkowników, zwiększenie autonomii i przezwyciężenie bierności w odniesieniu do oferowanych usług, wprowadzenie środków wymagających większej przejrzystości i rozliczalności od przedsiębiorstw oraz wprowadzenie większej liczby obowiązków dla platform;

AO. mając na uwadze, że obecne działania przeciwko kampaniom dezinformacyjnym na platformach internetowych nie są skuteczne ani zniechęcające oraz w dalszym ciągu umożliwiają platformom propagowanie treści dyskryminacyjnych i zamieszczanych w złym zamiarze;

AP. mając na uwadze, że w porównaniu z treściami anglojęzycznymi platformy przeznaczają znacznie mniejsze zasoby na zarządzanie treściami w rzadziej używanych

językach, a nawet w szeroko używanych językach innych niż angielski;

AQ. mając na uwadze, że stosowane przez platformy procedury składania skarg i odwołań są ogólnie nieodpowiednie;

AR. mając na uwadze, że w ostatnich miesiącach kilka dużych podmiotów zastosowało się do zasad cenzury, np. podczas rosyjskich wyborów parlamentarnych we wrześniu 2021 r., kiedy Google i Apple usunęły ze swoich sklepów w Rosji aplikację Smart Voting;

AS. mając na uwadze, że ze względu na brak przejrzystości w odniesieniu do algorytmicznych wyborów dokonywanych przez platformy niemożliwa jest weryfikacja twierdzeń ze strony platform, dotyczących tego, co robią lub efektów działań podejmowanych przez nie, aby przeciwdziałać manipulowaniu informacjami i ingerencji; mając na uwadze, że istnieją rozbieżności między deklarowanymi efektami działań platform w rocznych samoocenach a ich rzeczywistą skutecznością, jak wykazano w ujawnionych niedawno dokumentach dotyczących Facebooka;

AT. mając na uwadze, że ze względu na nieprzejrzysty charakter reklamy ukierunkowanej internetowe reklamy renomowanych marek, niekiedy nawet instytucji publicznych, trafiają w dużych ilościach na strony internetowe zachęcające do terroryzmu i zawierające nawoływanie do nienawiści i dezinformację, a tym samym finansują rozwój takich stron internetowych bez wiedzy czy zgody reklamodawców;

AU. mając na uwadze, że rynek reklamy internetowej jest kontrolowany przez niewielką liczbę dużych przedsiębiorstw zajmujących się technologiami reklamowymi, które dzielą między siebie rynek, przy czym największymi graczami są Google i Facebook; mając na uwadze, że tak wysoka koncentracja rynku na niewielu przedsiębiorstwach wiąże się z poważnym brakiem równowagi sił; mając na uwadze, że stosowanie technik typu clickbait i zdolność tych nielicznych podmiotów do określenia, jakie treści przynoszą zyski, a jakie nie, mimo że stosowane algorytmy nie są w stanie odróżnić dezinformacji od zwykłych treści informacyjnych, stanowi zagrożenie dla zróżnicowanych mediów; mając na uwadze, że ukierunkowany rynek reklamy jest bardzo nieprzejrzysty; mając na uwadze, że przedsiębiorstwa zajmujące się technologiami reklamowymi zmuszają marki do przyjmowania konsekwencji za swoje zaniedbania w zakresie monitorowania miejsc umieszczania reklam;

Infrastruktura krytyczna i sektory strategiczne

AV. mając na uwadze, że zarządzanie zagrożeniami dla infrastruktury krytycznej, zwłaszcza stwarzanymi przez zsynchronizowaną, złośliwą strategię hybrydową, wymaga skoordynowanych, wspólnych wysiłków we wszystkich sektorach, na różnych szczeblach – UE, krajowym, regionalnym i lokalnym – i w różnych terminach;

AW. mając na uwadze, że Komisja przedstawiła wniosek w sprawie nowej dyrektywy mającej na celu zwiększenie odporności podmiotów krytycznych świadczących usługi kluczowe w UE, obejmujący proponowany wykaz nowych typów infrastruktury krytycznej; mając na uwadze, że wykaz usług zostanie przedstawiony w załączniku do dyrektywy;

AX. mając na uwadze, że postępująca globalizacja podziału pracy i łańcuchów produkcji

doprowadziła do niedoborów produkcji i kwalifikacji w głównych sektorach w całej Unii; mając na uwadze, że doprowadziło to do znacznego uzależnienia UE od przywozu zza granicy wielu podstawowych produktów i aktywów, które mogą mieć wbudowane luki w zabezpieczeniach; mając na uwadze, że odporność łańcucha dostaw powinna być jednym z priorytetów decydentów w UE;

AY. mając na uwadze, że bezpośrednie inwestycje zagraniczne, czyli inwestycje państw trzecich i przedsiębiorstw zagranicznych, w strategicznych sektorach w UE, ale również na obszarach sąsiadujących, takich jak Bałkany Zachodnie, w szczególności nabywanie przez Chiny struktur o znaczeniu krytycznym, są w ostatnich latach źródłem coraz większego zaniepokojenia, zwłaszcza jeśli wziąć pod uwagę rosnące znaczenie powiązania handlu z bezpieczeństwem; mając na uwadze, że inwestycje te stwarzają ryzyko powstania zależności gospodarczych i mogą prowadzić do utraty wiedzy w kluczowych sektorach produkcyjnych i przemysłowych;

AZ. mając na uwadze, że otwarta strategiczna autonomia UE wymaga kontroli nad europejską infrastrukturą strategiczną; mając na uwadze, że Komisja i państwa członkowskie wyrażają rosnące zaniepokojenie kwestią bezpieczeństwa i kontroli w odniesieniu do technologii i infrastruktury w Europie;

Obce ingerencje w procesy wyborcze

BA. mając na uwadze, że działające w złych zamiarach podmioty, które starają się ingerować w procesy wyborcze, wykorzystują otwartość i pluralizm naszych społeczeństw jako strategiczną podatność, aby atakować procesy demokratyczne i osłabiać odporność UE i jej państw członkowskich; mając na uwadze, że właśnie w kontekście procesów wyborczych obca ingerencja staje się bardziej niebezpieczna, gdy obywatele wykazują ponownie zainteresowanie i są bardziej zaangażowani w konwencjonalny udział w życiu politycznym;

BB. mając na uwadze, że szczególny charakter obcych ingerencji w procesy wyborcze oraz wykorzystywanie w tym celu nowych technologii, a także ich potencjalne skutki stanowią szczególnie niebezpieczne zagrożenie dla demokracji; mając na uwadze, że obca ingerencja w procesy wyborcze wykracza daleko poza tzw. wojnę informacyjną w mediach społecznościowych i obejmuje faworyzowanie konkretnych kandydatów, hakowanie i wykorzystywanie baz danych w celu uzyskania dostępu do informacji o zarejestrowanych wyborcach i bezpośredniej ingerencji w normalne funkcjonowanie, konkurencyjność i legalność procesu wyborczego; mając na uwadze, że obca ingerencja ma na celu wzbudzenie wątpliwości i niepewności oraz osłabienie zaufania, a nie tylko zmianę wyniku wyborów, czyli również delegitymizację całego procesu wyborczego;

Potajemne finansowanie działalności politycznej przez podmioty i darczyńców zza granicy

BC. mając na uwadze, że, jak pokazuje solidny zestaw dowodów, podmioty zagraniczne aktywnie ingerują w demokratyczne funkcjonowanie UE i jej państw członkowskich, w szczególności podczas wyborów i referendów, poprzez operacje potajemnego finansowania;

BD. mając na uwadze, że na przykład Rosja, Chiny i inne reżimy autorytarne przekazały ponad 300 mln USD do 33 krajów, aby ingerować w procesy demokratyczne, a inne

podmioty, takie jak Iran i Wenezuela, a także podmioty z Bliskiego Wschodu i związane ze skrajną prawicą w USA, również były zaangażowane w ukryte finansowanie; mając na uwadze, że tendencja ta wyraźnie nasila się; mając na uwadze, że połowa tych przypadków dotyczy ingerencji Rosji w Europie; mając na uwadze, że korupcja i pranie pieniędzy to źródła finansowania politycznego z autorytarnych państw trzecich;

BE. mając na uwadze, że narzędzia medialne stworzone przez zagranicznych darczyńców w nieprzejrzysty sposób stały się bardzo skuteczne w gromadzeniu dużej liczby obserwatorów i generowaniu zaangażowania;

BF. mając na uwadze, że takie operacje finansują ekstremistyczne, populistyczne i antyeuropejskie partie oraz pewne inne partie i jednostki lub ruchy dążące do pogłębienia rozdrobnienia społecznego oraz podważenia legitymacji europejskich i krajowych organów publicznych; mając na uwadze, że przyczyniło się to do zwiększenia zasięgu tych partii i ruchów;

BG. mając na uwadze, że Rosja dąży do nawiązania kontaktów z partiami, osobistościami i ruchami, aby wykorzystać podmioty w instytucjach UE do legitymizacji rosyjskich stanowisk i popleczniczych rządów, lobbowania na rzecz złagodzenia sankcji i łagodzenia skutków izolacji międzynarodowej; mając na uwadze, że podmioty takie jak Wolnościowa Partia Austrii (Freiheitliche Partei Österreichs), francuskie Zjednoczenie Narodowe (Rassemblement National) i włoska Liga Północna (Lega Nord) podpisały umowy o współpracy z Jedną Rosją, partią prezydenta Rosji Władimira Putina, i stoją teraz wobec zarzutów medialnych, że są skłonne zaakceptować finansowanie polityczne z Rosji; mając na uwadze, że inne partie europejskie, takie jak niemiecka Alternatywa dla Niemiec (Alternative für Deutschland – AfD), węgierski Fidesz i Jobbik oraz Brexit Party w Zjednoczonym Królestwie, mają rzekomo również bliskie kontakty z Kremlem, a AfD i Jobbik pracowały także jako tzw. obserwatorzy wyborów podczas wyborów kontrolowanych przez Kreml, na przykład w Doniecku i Ługańsku na wschodniej Ukrainie, w celu monitorowania i legitymizacji wyborów sponsorowanych przez Rosję; mając na uwadze, że ustalenia dotyczące bliskich i regularnych kontaktów między rosyjskimi urzędnikami a przedstawicielami grupy secesjonistów katalońskich w Hiszpanii, a także między rosyjskimi urzędnikami a największym prywatnym darczyńcą w ramach kampanii na rzecz brexitu (Vote Leave) wymagają dogłębnego dochodzenia i stanowią część szerszej strategii Rosji polegającej na wykorzystywaniu każdej okazji do manipulowania dyskursem w celu szerzenia destabilizacji;

BH. mając na uwadze, że Grupa Państw przeciwko Korupcji (GRECO) Rady Europy i Komisja Wenecka przedstawiły już szeroko zakrojone zalecenia mające na celu zmniejszenie możliwości ewentualnej ingerencji podmiotów zagranicznych poprzez finansowanie polityczne;

BI. mając na uwadze, że prawa wyborcze, w szczególności przepisy dotyczące finansowania działalności politycznej, nie są wystarczająco dobrze skoordynowane na szczeblu UE, a zatem umożliwiają podmiotom zagranicznym stosowanie nieprzejrzystych metod finansowania; mając na uwadze, że definicja prawna darowizn na cele polityczne jest zbyt wąska, co pozwala na przekazywanie zagranicznych wkładów rzeczowych w Unii Europejskiej;

BJ. mając na uwadze, że w niektórych państwach członkowskich internetowa reklama polityczna nie podlega przepisom dotyczącym reklamy politycznej poza internetem; mając na uwadze poważny brak przejrzystości internetowej reklamy politycznej uniemożliwiający organom regulacyjnym egzekwowanie limitów wydatków i zapobieganie nielegalnym źródłom finansowania, co może mieć katastrofalne skutki dla integralności naszych systemów wyborczych;

BK. mając na uwadze, że brak przejrzystości finansowania tworzy środowisko dla korupcji, która często towarzyszy zagranicznemu finansowaniu i zagranicznym inwestycjom;

BL. mając na uwadze, że rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 1141/2014 z dnia 22 października 2014 r. w sprawie statusu i finansowania europejskich partii politycznych i europejskich fundacji politycznych[9] podlega przeglądowi mającemu na celu osiągnięcie wyższego poziomu przejrzystości pod względem finansowania działalności politycznej;

BM. mając na uwadze, że w ostatnich latach wzrosła rola fundacji politycznych, które w większości przypadków odgrywają pozytywną rolę w polityce i umacnianiu demokracji, ale czasami mogą stać się bardziej nieprzewidywalnym narzędziem finansowania w złych zamiarach i pośredniej ingerencji;

BN. mając na uwadze, że nowoczesne technologie i zasoby cyfrowe, takie jak kryptowaluta, są wykorzystywane do ukrywania nielegalnych transakcji finansowych podmiotów politycznych i partii politycznych;

Cyberbezpieczeństwo i odporność na cyberataki

BO. mając na uwadze, że w ostatnich latach coraz częściej dochodzi do cyberataków i cyberincydentów kierowanych przez wrogie podmioty państwowe i niepaństwowe; mając na uwadze, że w przypadku niektórych cyberataków, takich jak globalne kampanie mailowe typu phishing ukierunkowany, wymierzone w strategiczne struktury przechowywania szczepionek, oraz cyberataków na Europejską Agencję Leków (EMA), Europejski Urząd Nadzoru Bankowego, parlament norweski i niezliczone inne podmioty ustalono, że przeprowadzone zostały przez wspierane przez państwo grupy hakerów, powiązane głównie z rządami Rosji i Chin;

BP. mając na uwadze, że Unia Europejska jest zaangażowana w stosowanie obowiązującego prawa międzynarodowego w cyberprzestrzeni, w szczególności Karty Narodów Zjednoczonych; mając na uwadze, że wrogie podmioty zagraniczne wykorzystują brak silnych międzynarodowych ram prawnych w dziedzinie cyberbezpieczeństwa;

BQ. mając na uwadze, że państwa członkowskie zacieśniły współpracę w dziedzinie cyberobrony w ramach stałej współpracy strukturalnej (PESCO), w tym poprzez utworzenie zespołów szybkiego reagowania na cyberincydenty; mając na uwadze, że w Europejskim programie rozwoju przemysłu obronnego włączono do programów prac wywiad, bezpieczną komunikację i cyberobronę; mając na uwadze, że obecna zdolność do przeciwdziałania zagrożeniom cybernetycznym jest ograniczona ze względu na

[9] Dz.U. L 317 z 4.11.2014, s. 1.

ubóstwo zasobów ludzkich i finansowych, np. w obrębie infrastruktury krytycznej takiej jak szpitale; mając na uwadze, że w ramach programu „Cyfrowa Europa”[10] UE zobowiązała się do zainwestowania 1,6 mld EUR w zdolności reagowania i wdrożenie narzędzi cyberbezpieczeństwa dla administracji publicznej, przedsiębiorstw i osób fizycznych, a także we współpracę między sektorem publicznym a prywatnym;

BR. mając na uwadze, że luki w zdolnościach i strategiach UE w dziedzinie cyberprzestrzeni oraz ich fragmentacja stają się coraz większym problemem, jak zauważył Europejski Trybunał Obrachunkowy[11]; mając na uwadze, że unijny zestaw narzędzi dla dyplomacji cyfrowej, ustanowiony w maju 2019 r., pokazał wartość dodaną wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni; mając na uwadze, że 30 lipca 2020 r. Rada po raz pierwszy podjęła decyzję o nałożeniu środków ograniczających na osoby, podmioty i organy odpowiedzialne za różne cyberataki lub w nie zaangażowane;

BS. mając na uwadze, że zagraniczne podmioty państwowe wykorzystują na dużą skalę i nielegalnie programy inwigilacji, takie jak Pegasus, przeciwko dziennikarzom, działaczom na rzecz praw człowieka, naukowcom, urzędnikom rządowym i politykom, w tym głowom państw europejskich; mając na uwadze, że państwa członkowskie również korzystały z oprogramowania szpiegowskiego do celów inwigilacji;

Ochrona państw członkowskich UE oraz unijnych instytucji, agencji, delegatur i misji

BT. mając na uwadze, że ze względu na swój wielonarodowy i zdecentralizowany charakter instytucje UE, w tym jej misje i operacje, stają się coraz częściej celem dla działających w złych intencjach podmiotów zagranicznych i są przez nie wykorzystywane do powodowania podziałów w UE; mając na uwadze ogólny brak kultury bezpieczeństwa w instytucjach UE, mimo iż stanowią one wyraźny cel; mając na uwadze, że Parlament, jako demokratycznie wybrana instytucja UE, stoi w obliczu szczególnych wyzwań; mając na uwadze, że kilka przypadków pokazało, iż instytucje UE wydają się podatne na infiltrację z zagranicy; mając na uwadze, że należy zapewnić bezpieczeństwo pracowników UE;

BU. mając na uwadze, że priorytetem jest zapewnienie solidnych i spójnych procedur zarządzania kryzysowego; mając na uwadze, że należy zaoferować dodatkowe szkolenia w celu zwiększenia gotowości personelu;

BV. mając na uwadze, że kilka instytucji stało się ostatnio celem cyberataków, co uwypukla potrzebę silnej współpracy międzyinstytucjonalnej w zakresie wykrywania, monitorowania i dzielenia się informacjami podczas cyberataków lub w celu zapobiegania im, również podczas misji i operacji w ramach wspólnej polityki bezpieczeństwa i obrony UE (WPBiO); mając na uwadze, że UE i jej państwa członkowskie powinny organizować regularne wspólne ćwiczenia w celu identyfikowania słabych punktów i podejmowania niezbędnych środków;

[10] https://www.consilium.europa.eu/pl/policies/cybersecurity/

[11] https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PL.pdf

Ingerencja podmiotów globalnych za pośrednictwem przejmowania elit, narodowych diaspor, uniwersytetów i wydarzeń kulturalnych

BW. mając na uwadze, że szereg polityków, w tym byłych europejskich polityków i urzędników wysokiego szczebla jest zatrudnianych lub nakłanianych do współpracy przez zagraniczne przedsiębiorstwa państwowe lub prywatne kontrolowane przez autorytarne państwa, z uwagi na wiedzę posiadaną przez takie osoby i kosztem interesów obywateli UE i jej państw członkowskich;

BX. mając na uwadze, że niektóre państwa, zwłaszcza Rosja i Chiny, ale również Arabia Saudyjska i inne kraje Zatoki Perskiej, są szczególnie aktywne w zakresie przejmowania i pozyskiwania elit; można tu odnotować, że np. były kanclerz Niemiec Gerhard Schröder i były premier Finlandii Paavo Lipponen podjęli współpracę z Gazpromem, aby przyspieszyć proces składania wniosków w związku z projektami Nord Stream 1 i 2, była austriacka minister spraw zagranicznych Karin Kneissl została członkiem zarządu przedsiębiorstwa Rosneft, były premier Francji François Fillon został członkiem zarządu firmy Zaroubejneft, były premier Francji Jean-Pierre Raffarin aktywnie angażuje się w promowanie chińskich interesów we Francji, były czeski komisarz Štefan Füle pracował dla CEFC China Energy, były premier Finlandii Esko Aho obecnie zasiada w zarządzie kontrolowanego przez Kremlin banku Sberbank, były francuski minister do spraw stosunków z Parlamentem Jean-Marie Le Guen jest członkiem zarządu Huawei France, były premier Belgii Yves Leterme jest współprzewodniczącym chińskiego funduszu inwestycyjnego ToJoy; wielu innych polityków i urzędników wysokiego szczebla przyjmuje podobne funkcje;

BY. mając na uwadze, że strategie lobbingu ekonomicznego mogą łączyć się z celami obcych ingerencji; mając na uwadze, że zgodnie ze sprawozdaniem OECD na temat lobbingu w XXI wieku[12] jedynie USA, Australia i Kanada wdrożyły przepisy uwzględniające obce wpływy; mając na uwadze poważny brak prawnie wiążących przepisów w sprawie unijnego rejestru działalności lobbingowej oraz egzekwowania go, co praktycznie uniemożliwia śledzenie lobbingu spoza UE; mając na uwadze, że nie ma obecnie możliwości monitorowania w państwach członkowskich działań lobbystów, którzy wpływają na prawodawstwo i politykę zagraniczną za pośrednictwem Rady Europejskiej; mając na uwadze, że przepisy dotyczące lobbingu w UE koncentrują się głównie na kontaktach bezpośrednich i nie uwzględniają całego ekosystemu różnych rodzajów lobbingu istniejącego w Brukseli; mając na uwadze, że kraje takie jak Chiny i Rosja, ale również Katar, Zjednoczone Emiraty Arabskie i Turcja, dokonały znaczących inwestycji w działalność lobbingową w Brukseli;

BZ. mając na uwadze, że próby instrumentalizacji słabszych grup, w tym narodowych mniejszości i diaspory mieszkających na terytorium UE, stanowią ważny element strategii obcych ingerencji;

CA. mając na uwadze, że różne podmioty państwowe, takie jak rządy rosyjski, chiński i, w mniejszym stopniu, turecki, usiłują zwiększać swoje wpływy przez tworzenie i

[12] Organizacja Współpracy Gospodarczej i Rozwoju, „Lobbying in the 21st Century: Transparency, Integrity and Access" [Działalność lobbingowa w XXI w.: Przejrzystość, uczciwość i dostęp], 2021 r., OECD Publishing, Paryż, dostępne tu: https://doi.org/10.1787/c6d8eff8-en

wykorzystywanie instytucji kulturalnych, edukacyjnych (np. przez dotacje i stypendia) i religijnych w państwach członkowskich UE, mając na celu zdestabilizowanie europejskiej demokracji i rozszerzenie kontroli nad Europą Wschodnią i Środkową; mając na uwadze, że rzekoma trudna sytuacja mniejszości narodowej była w przeszłości wykorzystywana przez Rosję jako pretekst do bezpośredniej interwencji w państwach trzecich;

CB. mając na uwadze, że istnieją dowody rosyjskiej ingerencji i manipulowania informacjami w internecie w wielu liberalnych demokracjach na całym świecie, w tym m.in. w związku z referendum w sprawie brexitu w Zjednoczonym Królestwie oraz wyborami prezydenckimi we Francji i USA, a także dowody praktycznego wsparcia na rzecz ekstremistycznych, populistycznych i antyeuropejskich partii oraz pewnych innych partii i osób w całej Europie, w tym m.in. we Francji, Włoszech, w Niemczech i Austrii; mając na uwadze, że trzeba w większym stopniu wspierać badania naukowe i edukację, aby móc zrozumieć dokładny wpływ obcych ingerencji na konkretne wydarzenia, takie jak brexit i wybór prezydenta Trumpa w 2016 r.;

CC. mając na uwadze, że kontrolowane przez państwo i nadające na Zachodzie rosyjskie sieci Sputnik i RT oraz zachodnie media będące w pełni lub częściowo własnością rosyjskich lub chińskich podmiotów prawnych i osób fizycznych biorą czynny udział w działalności dezinformacyjnej wymierzonej w demokracje liberalne; mając na uwadze, że Rosja ucieka się do rewizjonizmu historycznego, próbuje na nowo napisać historię sowieckich zbrodni i promuje sowiecką nostalgię wśród podatnej na nią ludności w Europie Środkowej i Wschodniej; mając na uwadze, że krajowym nadawcom w Europie Środkowej i Wschodniej trudno jest konkurować z treściami telewizyjnymi nadawanymi w języku rosyjskim, które są finansowane przez rząd rosyjski; mając na uwadze, że istnieje ryzyko braku równowagi we współpracy między chińskimi i zagranicznymi mediami, biorąc pod uwagę, że chińskie media są głosem Komunistycznej Partii Chin na szczeblu krajowym i zagranicznym;

CD. mając na uwadze, że na całym świecie otwarto ponad 500 centrów Konfucjusza, w tym ok. 200 w Europie, oraz że Instytuty Konfucjusza i Klasy Konfucjańskie wykorzystywane są przez Chiny jako narzędzie ingerencji w UE; mając na uwadze znaczne ograniczanie wolności nauki w Instytutach Konfucjusza; mając na uwadze, że uniwersytety i programy kształcenia są celem masowego finansowania ze strony podmiotów zagranicznych, w szczególności z Chin lub Kataru, jak w przypadku Uniwersytetu Fudan w Budapeszcie;

CE. mając na uwadze, że UE nie posiada obecnie niezbędnego zestawu narzędzi, aby zaradzić przejmowaniu elit i przeciwdziałać tworzeniu kanałów oddziaływania, w tym w instytucjach UE; mając na uwadze wciąż nikłe zdolności w zakresie orientacji sytuacyjnej i ograniczone narzędzia kontrwywiadu na szczeblu UE oraz znaczną zależność od gotowości podmiotów krajowych do udostępniania informacji;

Odstraszanie, demaskowanie i zbiorowe środki zaradcze, w tym sankcje

CF. mając na uwadze, że UE i jej państwa członkowskie nie posiadają obecnie specjalnego systemu sankcji w związku z obcymi ingerencjami i kampaniami dezinformacji organizowanymi przez zagraniczne podmioty państwowe, a zatem podmioty takie mogą

bezpiecznie zakładać, że mogą prowadzić kampanie destabilizacji wymierzone w UE bez żadnych konsekwencji;

CG. mając na uwadze, że zapewnienie jednoznacznej identyfikacji źródła dezinformacji i ataków propagandowych, w tym publiczne wskazywanie sprawców, ich sponsorów i zamierzonych celów, a także ocena wpływu tych ataków na zamierzonych odbiorców stanowią pierwsze kroki w kierunku skutecznej obrony przed takimi działaniami;

CH. mając na uwadze, że UE powinna wzmocnić swoje narzędzia odstraszania, a także narzędzia umożliwiające demaskowanie tych ataków i ich klasyfikowanie jako zgodnych lub niezgodnych z prawem międzynarodowym w celu ustanowienia skutecznego systemu sankcji, aby działające w złej intencji podmioty zagraniczne musiały ponosić koszty i konsekwencje swoich decyzji; mając na uwadze, że skupienie uwagi na osobach fizycznych może nie być wystarczające; mając na uwadze możliwość stosowania innych narzędzi, takich jak środki dotyczące handlu, w celu ochrony europejskich procesów demokratycznych przed atakami hybrydowymi wspieranymi przez państwo; mając na uwadze, że środki odstraszające muszą być stosowane w sposób przejrzysty, z wszelkimi należnymi gwarancjami; mając na uwadze, że ataki hybrydowe są skalibrowane tak, aby celowo nie przekraczały progu określonego w art. 42 ust. 7 Traktatu o Unii Europejskiej i art. 5 Traktatu Północnoatlantyckiego;

Globalna współpraca i multilateralizm

CI. mając na uwadze, że działania organizowane w złej intencji przez zagraniczne podmioty państwowe i niepaństwowe dotykają wielu różnych partnerów demokratycznych na całym świecie; mając na uwadze, że demokratyczni sojusznicy polegają na swojej zdolności do połączenia sił w zbiorowej reakcji;

CJ. mając na uwadze, że kraje przystępujące do UE na Bałkanach Zachodnich szczególnie mocno odczuwają ataki w formie obcych ingerencji i kampanii dezinformacyjnych ze strony Rosji, Chin i Turcji, takich jak rosyjskie kampanie ingerencyjne podczas procesu ratyfikacji porozumienia znad Prespy w Macedonii Północnej; mając na uwadze, że Chiny i Rosja wykorzystały pandemię COVID-19 na Bałkanach Zachodnich do destabilizacji tych krajów i zdyskredytowania UE; mając na uwadze, że oczekuje się, iż kraje kandydujące i potencjalne kraje kandydujące przyłączą się do inicjatyw UE mających na celu zwalczanie obcych ingerencji;

CK. mając na uwadze, że partnerzy i sojusznicy o podobnych poglądach wciąż nie wypracowali wspólnego rozumienia i wspólnych definicji w odniesieniu do charakteru występujących zagrożeń; mając na uwadze, że sekretarz generalny ONZ wzywa do opracowania globalnego kodeksu postępowania w celu promowania integralności informacji publicznej; mając na uwadze, że Konferencja w sprawie przyszłości Europy jest ważną platformą dyskusji na ten temat;

CL. mając na uwadze, że potrzebne są: globalna, wielostronna współpraca i wsparcie między partnerami o podobnych poglądach na rzecz przeciwdziałania obcym ingerencjom podejmowanym w złych intencjach; mając na uwadze, że inne demokracje, takie jak Australia czy Tajwan, wypracowały zaawansowane umiejętności i strategie; mając na uwadze, że Tajwan odgrywa wiodącą rolę w walce z manipulowaniem informacjami, głównie ze strony Chin; mając na uwadze, że sukces tajwańskiego

systemu opiera się na współpracy między wszystkimi instytucjami rządowymi, a także na współpracy z niezależnymi organizacjami pozarządowymi specjalizującymi się w weryfikacji informacji i w umiejętnościach korzystania z mediów, a także z platformami mediów społecznościowych, takimi jak Facebook, oraz na promowaniu umiejętności korzystania z mediów przez wszystkie pokolenia, obalaniu dezinformacji i ograniczaniu rozprzestrzeniania się zmanipulowanych wiadomości; mając na uwadze, że komisja specjalna INGE odbyła trzydniową oficjalną misję na Tajwanie w celu omówienia dezinformacji i obcej ingerencji w wybory;

Potrzeba skoordynowanej strategii UE przeciwko obcym ingerencjom

1. wyraża głębokie zaniepokojenie coraz większą skalą i coraz lepszym przygotowaniem obcych ingerencji i prób manipulowania informacjami, w przeważającym stopniu realizowanych przez Rosję i Chiny i wymierzonych we wszystkie elementy demokratycznego funkcjonowania Unii Europejskiej i jej państw członkowskich;

2. apeluje, by Komisja zaproponowała, a współustawodawcy i państwa członkowskie poparli, wielopoziomową, skoordynowaną i międzysektorową strategię, a także odpowiednie zasoby finansowe, z myślą o zapewnieniu UE i jej państwom członkowskim odpowiednich strategii politycznych na rzecz prognozowania i odporności oraz narzędzi odstraszania, umożliwiających im przeciwdziałanie wszelkim zagrożeniom hybrydowym i atakom organizowanym przez obce podmioty państwowe i niepaństwowe; uważa, że strategia ta powinna opierać się na:

   a) wspólnych terminologiach i definicjach, jednolitej metodologii, ocenach i ocenach skutków ex post przyjętych dotychczas przepisów, na wspólnym systemie wywiadowczym oraz zrozumieniu, monitorowaniu, w tym wczesnym ostrzeganiu, oraz orientacji sytuacyjnej w zakresie przedmiotowych kwestii,

   b) konkretnych strategiach politycznych umożliwiających budowanie odporności obywateli UE zgodnie z wartościami demokratycznymi, w tym poprzez wspieranie społeczeństwa obywatelskiego,

   c) odpowiednich zdolnościach zakłócania i obrony,

   d) reakcjach dyplomatycznych i odstraszających, w tym na unijnym zestawie narzędzi służących przeciwdziałaniu obcym ingerencjom i działaniom w zakresie wywierania wpływu, w tym operacjom hybrydowym, poprzez odpowiednie środki, np. identyfikowanie i wskazywanie sprawców, sankcje i środki zaradcze, a także na globalnych partnerstwach na rzecz wymiany praktyk i promowania międzynarodowych norm odpowiedzialnego zachowania państwa;

3. podkreśla, że wszystkie środki służące zapobieganiu i przeciwdziałaniu obcej ingerencji, a także jej wykrywaniu, demaskowaniu i sankcjonowaniu muszą być projektowane w sposób respektujący i propagujący prawa podstawowe, w tym zdolność obywateli UE do komunikowania się w sposób bezpieczny, anonimowy i nieobjęty cenzurą, wolny od nadmiernej ingerencji wszelkich podmiotów zagranicznych;

4. uważa, że strategia ta powinna bazować na opartym na ocenie ryzyka, obejmującym całość społeczeństwa i administracji rządowej podejściu, uwzględniającym w

szczególności następujące obszary:

a) budowanie odporności UE przez orientację sytuacyjną, umiejętność korzystania z mediów i informacji, pluralizm mediów, niezależne dziennikarstwo i edukację,

b) obce ingerencje z wykorzystaniem platform internetowych,

c) infrastruktura krytyczna i sektory strategiczne,

d) obce ingerencje podczas procesów wyborczych,

e) potajemne finansowanie działalności politycznej przez podmioty i darczyńców z zagranicy,

f) cyberbezpieczeństwo i odporność na cyberataki,

g) ochrona państw członkowskich UE oraz unijnych instytucji, agencji, delegatur i misji,

h) ingerencja podmiotów globalnych za pośrednictwem przejmowania elit, narodowych diaspor, uniwersytetów i wydarzeń kulturalnych,

i) odstraszanie, demaskowanie ataków i zbiorowe środki zaradcze, w tym sankcje,

j) globalna współpraca i multilateralizm;

5. wzywa w szczególności UE i jej państwa członkowskie do zwiększenia zasobów i środków przeznaczonych dla organów i organizacji w całej Europie i na całym świecie (takich jak ośrodki analityczne i weryfikatorzy informacji), których zadaniem jest monitorowanie sytuacji i podnoszenie świadomości na temat powagi zagrożeń, w tym dezinformacji; podkreśla kluczową rolę UE w szerszym znaczeniu strategicznym; wzywa UE i jej państwa członkowskie do wzmocnienia zdolności prognozowania i interoperacyjności, aby były dobrze przygotowane do przewidywania zagranicznych manipulacji informacjami i ingerencji w informacje, zapobiegania im i ograniczania ich, a także by wzmocniły ochronę swoich strategicznych interesów i infrastruktury oraz zaangażowały się w wielostronną współpracę i koordynację w celu osiągnięcia wspólnego rozumienia tej kwestii na odpowiednich forach międzynarodowych; wzywa Radę do Spraw Zagranicznych do regularnego omawiania kwestii obcej ingerencji;

6. wyraża zaniepokojenie przytłaczającym brakiem świadomości, w tym wśród obywateli i urzędników rządowych, tego, jak poważne są zagrożenia stwarzane obecnie przez obce reżimy autorytarne i inne podmioty działające w złym zamiarze, które obierają za cel wszystkie szczeble i segmenty społeczeństwa europejskiego, zmierzają do podważenia praw podstawowych i legitymacji władz publicznych oraz pogłębienia podziałów politycznych i społecznych, a w niektórych przypadkach nawet do wyrządzenia obywatelom UE szkód zagrażających życiu;

7. wyraża zaniepokojenie brakiem norm oraz właściwych i wystarczających środków umożliwiających wskazywanie sprawców aktów obcej ingerencji i reagowanie na nie, co zapewnia działającym w złej intencji podmiotom atrakcyjne warunki, czyli

niewielkie koszty, małe ryzyko i duże korzyści, gdyż ryzyko poniesienia kary za działania jest obecnie bardzo niskie;

8. apeluje do Komisji, aby w ocenie skutków ex ante przeprowadzanej przed przedstawieniem nowych wniosków uwzględniała w stosownych przypadkach kwestie obcych ingerencji i manipulacji informacjami, w dążeniu do włączenia przeciwdziałania obcym ingerencjom i manipulacji informacjami w główny nurt kształtowania polityki UE; proponuje, aby ESDZ i Komisja przeprowadzały regularne przeglądy odporności i ocenę rozwoju zagrożeń oraz ich wpływu na obowiązujące przepisy i strategie polityczne;

9. apeluje do Komisji, aby przeanalizowała ustanowione niedawno instytucje krajowe, takie jak stanowisko krajowego koordynatora walki z obcymi ingerencjami w Australii, komitet bezpieczeństwa wspierający rząd i ministerstwa w Finlandii, agencja ds. ochrony ludności, nowa agencja obrony psychologicznej oraz krajowe centrum ds. chińskich w Szwecji, nowa państwowa agencja Viginum we Francji, krajowe centrum cyberbezpieczeństwa na Litwie oraz międzyagencyjna grupa zadaniowa ds. koordynacji w zakresie dezinformacji na Tajwanie, w celu ustalenia, czego możemy się nauczyć z tych najlepszych praktyk i czy podobne struktury można utworzyć na szczeblu UE; zachęca Komisję do wspierania wymiany informacji i najlepszych praktyk w tym zakresie między państwami członkowskimi; podkreśla, jak ważne są proaktywne podejście i proaktywne instrumenty, w tym komunikacja strategiczna, ponieważ umożliwiają realizację polityki UE i polityki krajowej w wypowiedziach i działaniach; apeluje do Komisji, aby zapewniła odpowiednie szkolenia w zakresie nauki o danych oraz aby utworzyła w swoich strukturach jeden organ monitorujący kwestie manipulacji informacjami;

10. wyraża zaniepokojenie licznymi brakami i lukami prawnymi w obowiązujących przepisach i strategiach politycznych na szczeblu UE i krajowym, mających na celu wykrywanie obcych ingerencji oraz zapobieganie i przeciwdziałanie im;

11. zauważa, że UE finansuje szereg długoterminowych projektów i programów ukierunkowanych na przeciwdziałanie dezinformacji na szczeblu technologicznym, prawnym, psychologicznym i informacyjnym; wzywa Komisję, aby przeprowadziła ocenę skutków tych projektów i programów oraz ich stosowania;

12. apeluje do Komisji o ustanowienie grupy zadaniowej podlegającej V. Jourovej, wiceprzewodniczącej Komisji ds. Wartości i Przejrzystości, i zlecenie jej kontrolowania obowiązujących przepisów i strategii politycznych z myślą o identyfikacji luk, które mogą zostać wykorzystane przez podmioty działające w złej intencji, a także wzywa Komisję do zaradzenia tym lukom; podkreśla, że struktura ta powinna współpracować z innymi instytucjami UE i państwami członkowskimi na szczeblu krajowym, regionalnym i lokalnym oraz ułatwiać wymianę najlepszych praktyk; wzywa Komisję i ESDZ, by rozważyły utworzenie niezależnego europejskiego centrum ds. zagrożeń ingerencjami i integralności informacyjnej dysponującego odpowiednimi zasobami, które powinno identyfikować, analizować i dokumentować operacje manipulacji informacjami i zagrożenia ingerencjami wobec UE jako całości, zwiększać orientację sytuacyjną, rozwijać wyspecjalizowane centrum wiedzy poprzez służenie jako platforma koordynacji działań ze społeczeństwem obywatelskim, sektorem

przedsiębiorstw oraz instytucjami unijnymi i krajowymi, a także podnosić świadomość społeczną, m.in. poprzez regularne sprawozdania na temat zagrożeń systemowych; podkreśla, że utworzenie takiego nowego niezależnego i dysponującego odpowiednimi zasobami europejskiego centrum ds. zagrożeń ingerencjami i integralności informacyjnej umożliwiłoby sprecyzowanie i zwiększenie roli zespołu StratCom ESDZ i jego grup zadaniowych jako strategicznego organu służb dyplomatycznych UE, a także zapobiegłoby powielaniu działań; podkreśla, że mandat StratCom ESDZ powinien koncentrować się na strategicznym opracowywaniu kierunków polityki zagranicznej z myślą o przeciwdziałaniu istniejącym i pojawiającym się wspólnym zagrożeniom oraz wzmacnianiu współpracy z partnerami międzynarodowymi w tej dziedzinie; zwraca uwagę, że StratCom ESDZ mógłby realizować te działania w ścisłej współpracy z nowo utworzonym europejskim centrum ds. zagrożeń ingerencjami i integralności informacyjnej i nową grupą zadaniową Komisji;

13. wzywa instytucje UE i państwa członkowskie do umożliwienia społeczeństwu obywatelskiemu odgrywania aktywnej roli w przeciwdziałaniu obcym ingerencjom; apeluje, aby na wszystkich szczeblach i we wszystkich segmentach społeczeństwa europejskiego ustanowiono systemy wzmacniające odporność organizacji i obywateli na obce ingerencje, aby umożliwić im wykrywanie ataków w porę i jak najskuteczniejsze przeciwdziałanie im, również dzięki edukacji i podnoszeniu świadomości, z uwzględnieniem unijnych ram praw podstawowych oraz w sposób przejrzysty i demokratyczny; wskazuje w tym kontekście na najlepsze praktyki i podejście obejmujące całe społeczeństwo, stosowane na Tajwanie; wzywa decydentów, by zapewnili społeczeństwu obywatelskiemu odpowiednie narzędzia i specjalne fundusze do badania, ujawniania i zwalczania obcych wpływów;

Budowanie odporności UE przez orientację sytuacyjną, umiejętność korzystania z mediów i edukację

14. podkreśla, że instytucje UE i państwa członkowskie potrzebują rzetelnych, solidnych i wzajemnie powiązanych systemów wykrywania, analizowania, śledzenia i mapowania przypadków podejmowania przez zagraniczne podmioty państwowe i niepaństwowe prób ingerencji w procesy demokratyczne, w celu rozwijania orientacji sytuacyjnej i jasnego zrozumienia, jak muszą zachowywać się UE i jej państwa członkowskie, aby odstraszać od takich aktów i przeciwdziałać im; apeluje o regularne badania socjologiczne i sondaże w celu monitorowania odporności i umiejętności korzystania z mediów, a także zrozumienia poparcia społecznego dla najpowszechniejszych narracji dezinformacyjnych i postrzegania tych narracji;

15. podkreśla, że równie ważne jest, aby wnioski płynące z takiej analizy nie były znane wyłącznie grupom specjalistów ds. obcych ingerencji, lecz aby były w miarę możliwości otwarcie udostępniane szerszym segmentom społeczeństwa, zwłaszcza osobom sprawującym wrażliwe funkcje, dzięki czemu wszyscy będą mieć świadomość rodzaju zagrożeń i będą w stanie unikać ryzyka;

16. podkreśla, że konieczne jest rozwijanie wspólnej metodologii wzmacniania orientacji sytuacyjnej, wczesnego ostrzegania i oceny zagrożeń, systematycznego gromadzenia dowodów i wykrywania na czas manipulacji środowiskiem informacyjnym, a także opracowanie standardów technicznej identyfikacji źródła ataku, na przykład w

odniesieniu do autentyczności treści, aby zapewnić skuteczną reakcję;

17. podkreśla, że konieczne jest, aby UE, we współpracy z państwami członkowskimi i w drodze wielostronnych działań na odnośnych forach międzynarodowych, opracowała konceptualną definicję zagrożenia ingerencją, przed jakim stoi UE; podkreśla, że ta definicja musi odzwierciedlać taktykę, techniki, procedury i narzędzia stosowane do opisania wzorców zachowań państwowych i niepaństwowych podmiotów stwarzających zagrożenia, które dziś obserwujemy; wzywa Komisję do zaangażowania w ten proces Agencji Praw Podstawowych Unii Europejskiej (FRA) w celu dopilnowania, by w tych konceptualnych definicjach nie było miejsca dla dyskryminacji, nierówności lub uprzedzeń;

18. podkreśla, że dyplomacja publiczna i komunikacja strategiczna stanowią niezbędne elementy stosunków zewnętrznych UE i ochrony demokratycznych wartości UE; apeluje do instytucji UE, aby nadal rozwijały i wzmacniały ważną działalność działu StratCom ESDZ i jego grup zadaniowych, Centrum Analiz Wywiadowczych UE (INTCEN), Komórki UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych, Dyrekcji ds. Wywiadu w Sztabie Wojskowym UE oraz systemu wczesnego ostrzegania, a także ugruntowaną współpracę na szczeblu administracyjnym między ESDZ, Komisją i Parlamentem, stworzoną przez Komisję sieć przeciw dezinformacji, administracyjną grupę zadaniową Parlamentu przeciwko dezinformacji, bieżącą współpracę z NATO, G-7, społeczeństwem obywatelskim i sektorem prywatnym w zakresie działań wywiadowczych, analiz, wymiany najlepszych praktyk oraz podnoszenia świadomości obcych ingerencji i manipulacji informacjami; z zadowoleniem przyjmuje sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego nr 9/2021 pt. „Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany”; wzywa ESDZ i Komisję do opublikowania szczegółowego harmonogramu realizacji zaleceń Trybunału;

19. podkreśla, że trzeba wzmocnić wysiłki na rzecz stałego monitorowania, szczególnie na długo przed wyborami, referendami lub innymi ważnymi procesami politycznymi w całej Europie;

20. apeluje do państw członkowskich o pełne wykorzystanie tych zasobów przez wymianę odpowiednich danych wywiadowczych z INTCEN i aktywniejszy udział w systemie wczesnego ostrzegania; jest zdania, że współpraca w zakresie analiz i wywiadu w UE i z NATO wymaga jeszcze większego pogłębienia oraz że należy zwiększyć jej przejrzystość i demokratyczną rozliczalność, w tym poprzez dzielenie się informacjami z Parlamentem;

21. z zadowoleniem odnotowuje przedstawiony przez przewodniczącą Komisji Ursulę von der Leyen pomysł ustanowienia wspólnego centrum orientacji sytuacyjnej, z myślą o wzmocnieniu prognozy strategicznej i otwartej strategicznej autonomii UE, i oczekuje dodatkowych wyjaśnień dotyczących jego struktury i misji; podkreśla, że takie centrum wymagałoby aktywnej współpracy z odpowiednimi służbami Komisji, ESDZ, Radą i Parlamentem oraz władzami krajowymi; przypomina jednak, jak ważne jest unikanie powielania prac i dublowania już istniejących struktur UE;

22. przypomina o potrzebie zapewnienia ESDZ rozszerzonego i wyraźnie zdefiniowanego

mandatu i niezbędnych zasobów dla działu ds. komunikacji strategicznej, grup zadaniowych i analizy informacji, aby mógł on monitorować sytuację i przeciwdziałać manipulacji informacjami i ingerencjom poza zagranicznymi źródłami obecnie objętymi działalnością trzech grup zadaniowych, a także dążyć do szerszego zasięgu geograficznego przez zastosowanie podejścia opartego na ocenie ryzyka; pilnie apeluje o wdrożenie przez ESDZ odpowiednich zdolności w celu przeciwdziałania manipulacji informacjami i ingerencjom ze strony Chin, w szczególności przez powołanie specjalnego zespołu ds. Dalekiego Wschodu; podkreśla ponadto, że należy znacznie wzmocnić wiedzę specjalistyczną i zdolności językowe w odniesieniu do Chin i innych regionów ważnych ze względów strategicznych, zarówno w ESDZ i państwach członkowskich, jak i w instytucjach UE w ogóle, oraz wykorzystywać informacje ze źródeł otwartych, które obecnie są niedostatecznie używane;

23. podkreśla znaczenie docierających w wiele miejsc, konkurencyjnych i pluralistycznych mediów, niezależnych dziennikarzy, weryfikatorów informacji i badaczy, a także silnych mediów publicznych dla ożywionej i swobodnej debaty demokratycznej; z zadowoleniem przyjmuje inicjatywy gromadzenia, szkolenia i wspierania na inne sposoby organizacji niezależnych dziennikarzy, weryfikatorów informacji i badaczy, takich jak Europejskie Obserwatorium Mediów Cyfrowych oraz Europejski Funduszu na rzecz Demokracji, w całej Europie, a w szczególności w regionach najbardziej zagrożonych; głęboko ubolewa, że Europejskie Obserwatorium Mediów Cyfrowych nie obejmuje państw bałtyckich; z zadowoleniem przyjmuje również inicjatywy mające na celu ustanowienie łatwo rozpoznawalnych wskaźników wiarygodności dziennikarstwa i weryfikacji informacji, takich jak inicjatywy zapoczątkowane przez Reporterów bez Granic; wzywa Komisję do przeciwdziałania monopolistycznej własności środków masowego przekazu;

24. pochwala niezbędne badania oraz liczne kreatywne i udane inicjatywy na rzecz umiejętności korzystania z mediów, umiejętności cyfrowych i podnoszenia świadomości, realizowane przez osoby fizyczne, szkoły, uniwersytety, organizacje medialne, instytucje publiczne i organizacje społeczeństwa obywatelskiego;

25. wzywa UE i państwa członkowskie do przeznaczenia źródeł unijnego finansowania publicznego na rzecz niezależnych weryfikatorów informacji, badaczy, wysokiej jakości mediów i dziennikarzy śledczych oraz organizacji pozarządowych prowadzących badania i dochodzenia w sprawie manipulacji informacjami i ingerencji, propagujących umiejętność korzystania z mediów i informacji, umiejętności cyfrowe, a także inne środki wzmacniania pozycji obywateli, a także prowadzących badania nad sposobami znaczącego pomiaru skuteczności szkolenia w zakresie umiejętności korzystania z mediów i informacji oraz umiejętności cyfrowych, podnoszenia świadomości, demaskowania fałszywych informacji i komunikacji strategicznej;

26. wzywa do wzmocnienia profesjonalnych i pluralistycznych mediów i zapewnienia wydawcom godziwego wynagrodzenia za wykorzystywanie ich treści w internecie; podkreśla, że szereg krajów na całym świecie podejmuje kroki w celu dopilnowania, aby media dysponowały odpowiednimi zasobami finansowymi; ponawia swój apel o utworzenie stałego unijnego funduszu mediów informacyjnych i w związku z tym z zadowoleniem przyjmuje inicjatywę „News”, w tym nowe możliwości finansowania sektora mediów oraz umiejętności korzystania z mediów i informacji w ramach

programu „Kreatywna Europa” na lata 2021–2027; zauważa jednak, że źródła finansowania mogą stwarzać zależności lub wywierać wpływ na niezależność mediów; podkreśla w związku z tym, jak ważna jest przejrzystość finansowania mediów; uważa, że aby chronić pluralizm mediów, trzeba publiczne ujawniać informacje na temat podmiotów posiadających lub kontrolujących media, przekazujących im środki finansowe i treści oraz płacących za treści dziennikarskie;

27. podkreśla, że trzeba skonsolidować analizy, sprawozdania dotyczące incydentów oraz oceny zagrożeń publicznych w oparciu o wiedzę wywiadowczą w zakresie manipulacji informacją i ingerencji, a także udostępniać te informacje społeczeństwu; w związku z tym proponuje utworzenie ogólnounijnej bazy danych na temat przypadków obcych ingerencji zgłaszanych przez organy UE i państw członkowskich; podkreśla, że informacje na temat tych incydentów mogłyby być udostępniane, w stosownych przypadkach, organizacjom społeczeństwa obywatelskiego i opinii publicznej we wszystkich językach UE;

28. apeluje do wszystkich państw członkowskich, aby włączały do swoich programów nauczania, od wczesnych lat po edukację dorosłych, włącznie ze szkoleniem nauczycieli i badaczy, umiejętność korzystania z mediów i umiejętności cyfrowe, a także edukację na temat demokracji, praw podstawowych, historii najnowszej i polityki światowej oraz myślenie krytyczne i zaangażowanie obywatelskie; wzywa Komisję i państwa członkowskie do zwiększenia wsparcia dla edukacji historycznej i badań nad tym, w jaki sposób obce ingerencje i dawny totalitaryzm wpłynęły ogólnie na społeczeństwo, a w szczególności na wydarzenia demokratyczne na dużą skalę;

29. apeluje do instytucji UE i państw członkowskich, na wszystkich szczeblach administracji, o identyfikację sektorów zagrożonych próbami ingerencji oraz o zapewnienie pracownikom tych sektorów regularnych szkoleń i ćwiczeń dotyczących sposobów wykrywania i unikania prób ingerencji oraz podkreśla, że dla takich wysiłków korzystny byłby ustandaryzowany format ustanowiony przez UE; zaleca oferowanie kompleksowych modułów szkoleń wszystkim urzędnikom; w związku z tym z zadowoleniem odnotowuje szkolenie oferowane posłom i posłankom oraz personelowi przez administrację Parlamentu; zaleca dalsze rozwijanie tego szkolenia;

30. podkreśla potrzebę podnoszenia świadomości na temat obcych ingerencji we wszystkie warstwach społeczeństwa; z zadowoleniem przyjmuje inicjatywy podejmowane przez ESDZ, Komisję i administrację Parlamentu, takie jak szkolenia i wydarzenia podnoszące świadomość dla dziennikarzy, nauczycieli, influencerów, studentów, starszych obywateli i gości, zarówno offline, jak i online, w Brukseli i we wszystkich państwach członkowskich UE, oraz zaleca ich dalsze rozwijanie;

31. apeluje do państw członkowskich, administracji UE i organizacji społeczeństwa obywatelskiego o dzielenie się najlepszymi praktykami dotyczącymi szkoleń i podnoszenia świadomości w zakresie umiejętności korzystania z mediów i informacji, zgodnie z tym, co przewidziano w dyrektywie o audiowizualnych usługach medialnych[13]; wzywa Komisję, aby organizowała te wymiany najlepszych praktyk we

[13] Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących

współpracy z grupą ekspertów ds. umiejętności korzystania z mediów; podkreśla, że państwa członkowskie powinny szybko i odpowiednio wdrożyć zmienioną dyrektywę;

32. wzywa instytucje UE do opracowania kodeksu etyki zawierającego wytyczne dla władz publicznych i przedstawicieli politycznych na temat korzystania z platform i sieci mediów społecznościowych; uważa, że niezbędne jest zachęcanie do odpowiedzialnego korzystania z takich platform i sieci w celu zwalczania manipulacji i informacji wprowadzających w błąd pochodzących ze sfery publicznej;

33. apeluje do UE i jej państw członkowskich o wdrażanie dostosowanych programów na rzecz podnoszenia świadomości oraz umiejętności korzystania z mediów i informacji, w tym dla diaspor i mniejszości, oraz apeluje do Komisji o ustanowienie systemu łatwego udostępniania materiałów w językach mniejszości, w celu ograniczenia kosztów tłumaczeń i trafiania do możliwie największej liczby osób; wzywa regiony i gminy do przejęcia wiodącej roli, ponieważ ważne jest dotarcie do obszarów wiejskich i do różnych grup demograficznych;

34. podkreśla, że zasadniczą reakcją na próby obcych ingerencji jest obrona najważniejszych grup docelowych, w które próby te są wymierzone; podkreśla, że potrzebne są ukierunkowane działania, dzięki zharmonizowanym ramom prawnym UE, przeciwko szerzeniu dezinformacji i mowy nienawiści w kwestiach związanych z płcią, osobami LGBTIQ+, mniejszościami i uchodźcami; wzywa Komisję do opracowania i wdrożenia strategii mających na celu powstrzymanie finansowania osób i grup, które aktywnie rozpowszechniają zmanipulowane informacje lub uczestniczą w manipulacji informacjami, często na temat wspomnianych grup lub tematów, i które robią to, aby podzielić społeczeństwo; wzywa do prowadzenia pozytywnych kampanii informacyjnych dotyczących tych kwestii i podkreśla, że potrzebne są szkolenia uwzględniające aspekt płci;

35. dostrzega, że ataki i kampanie dezinformacyjne wykorzystujące aspekt płci są często stosowane jako część szerszej strategii politycznej w celu podważenia równego uczestnictwa w procesach demokratycznych, w szczególności w odniesieniu do kobiet i osób LGBTIQ+; podkreśla, że dezinformacja na temat osób LGBTIQ+ podsyca nienawiść, zarówno w internecie, jak i poza nim, i powoduje zagrożenie życia; domaga się przeprowadzenia badań dotyczących dezinformacji w internecie z perspektywy intersekcjonalnej oraz nadzorowania zmian wprowadzanych przez platformy w celu reagowania na kampanie dezinformacyjne wykorzystujące aspekt płci w internecie; domaga się zwrócenia większej uwagi na dezinformację opartą na płci przez opracowanie systemów wczesnego ostrzegania, za pomocą których można zgłaszać i identyfikować kampanie dezinformacyjne wykorzystujące aspekt płci;

36. apeluje do Komisji, aby przedstawiła nadrzędną strategię na rzecz umiejętności korzystania z mediów i informacji, ze szczególnym naciskiem na zwalczanie manipulacji informacjami;

37. z zadowoleniem przyjmuje powołanie grupy ekspertów do spraw zwalczania dezinformacji i promowania umiejętności cyfrowych w drodze edukacji i szkoleń, która

---

świadczenia audiowizualnych usług medialnych, Dz.U. L 95 z 15.4.2010, s. 1.

skoncentruje się między innymi na myśleniu krytycznym, szkoleniu nauczycieli i zapobieganiu manipulacjom informacjami, demaskowaniu zmanipulowanych informacji i weryfikowaniu faktów oraz angażowaniu uczniów; wzywa Komisję do przedstawienia rezultatów prac tej grupy ekspertów oraz do wdrożenia jej konkluzji;

38. podkreśla znacznie komunikacji strategicznej dla walki z najbardziej rozpowszechnionymi narracjami antydemokratycznymi; apeluje o poprawę komunikacji strategicznej UE w celu zwiększenia jej zasięgu zarówno wśród obywateli, jak i za granicą; podkreśla, że wszystkie organizacje demokratyczne muszą bronić demokracji, przestrzegać praworządności oraz ponosić wspólną odpowiedzialność za zaangażowanie obywateli, przy wykorzystaniu ich preferowanych języków i platform;

39. wzywa państwa członkowskie do zapewnienia skutecznych publicznych kampanii komunikacyjnych dotyczących pandemii COVID-19, aby rozpowszechniać dokładne i terminowe informacje w celu zwalczania informacji wprowadzających w błąd, w szczególności na temat szczepionek;

40. wyraża głębokie zaniepokojenie rozpowszechnianiem się zagranicznej propagandy, pochodzącej głównie z Moskwy i Pekinu oraz Ankary i tłumaczonej na języki lokalne, np. mylnie prezentowanych jako dziennikarstwo treści medialnych sponsorowanych przez RT, Sputnik, Anadolu, CCTV, Global Times, Xinhua, TRT World i Komunistyczną Partię Chin, które to treści powielane są przez prasę; utrzymuje, że takich kanałów nie można uznawać za prawdziwe media, a w związku z tym nie powinny one korzystać z praw i ochrony przysługujących mediom demokratycznym; jest równie zaniepokojony tym, jak takie narracje przeniknęły do prawdziwego dziennikarstwa; podkreśla, że trzeba podnosić świadomość na temat rosyjskich i chińskich kampanii dezinformacyjnych, które uderzają w demokratyczne wartości i dzielą UE, ponieważ stanowią one główne źródło dezinformacji w Europie; wzywa Komisję do rozpoczęcia badania dotyczącego minimalnych standardów mediów jako podstawy do ewentualnego wycofywania licencji w przypadku naruszeń przepisów; apeluje do Komisji o włączenie ustaleń z badania do przyszłego prawodawstwa, takiego jak ewentualny akt prawny dotyczący wolności mediów; zauważa, że zagraniczne podmioty ingerujące mogą fałszywie przedstawiać się jako dziennikarze; uważa, że w takich przypadkach powinna istnieć możliwość nakładania sankcji na taką osobę lub organizację, na przykład poprzez jej wskazywanie i zawstydzanie, umieszczanie na czarnej liście wydarzeń prasowych lub cofnięcie akredytacji medialnej;

41. jest głęboko zaniepokojony atakami, nękaniem, przemocą i groźbami wobec dziennikarzy, obrońców praw człowieka i innych osób ujawniających obcą ingerencję i zaznacza, że może to również zagrozić ich niezależności; wzywa Komisję do szybkiego zaproponowania konkretnych i ambitnych wniosków dotyczących bezpieczeństwa wszystkich tych osób, w tym instrumentu przeciwko strategicznemu powództwu zmierzającemu do stłumienia debaty publicznej (SLAPP) oraz wsparcia gospodarczego, prawnego i dyplomatycznego, zgodnie z zapowiedzią zawartą w europejskim planie działania na rzecz demokracji; w tym kontekście z zadowoleniem przyjmuje zalecenie Komisji (UE) 2021/1534 z dnia 16 września 2021 r. w sprawie zapewnienia ochrony i bezpieczeństwa dziennikarzom i innym pracownikom sektora mediów oraz

wzmocnienia ich pozycji w Unii Europejskiej[14]; wzywa państwa członkowskie do skutecznej ochrony dziennikarzy i innych pracowników mediów za pomocą narzędzi ustawodawczych i nieustawodawczych;

42. podkreśla potrzebę angażowania decydentów lokalnych i regionalnych odpowiedzialnych za strategiczne decyzje w obszarach wchodzących w zakres ich kompetencji, takich jak infrastruktura, cyberbezpieczeństwo, kultura i edukacja; podkreśla, że lokalni i regionalni politycy oraz lokalne i regionalne organy często są w stanie identyfikować niepokojące procesy na wczesnym etapie, i zwraca uwagę, że ustalenie i wdrożenie odpowiednich przeciwśrodków często wymaga wiedzy lokalnej;

43. apeluje do Komisji i państw członkowskich o ustanowienie kanałów komunikacji i stworzenie platform, które umożliwią przedsiębiorstwom, organizacjom pozarządowym i osobom fizycznym, w tym członkom diaspory, padającym ofiarą manipulacji informacjami lub ingerencji zgłaszanie takich przypadków; apeluje do państw członkowskich o wspieranie osób, które są ofiarami ataków oraz osób, które wiedzą o takich atakach lub są poddawane presji;

Obce ingerencje z wykorzystaniem platform internetowych

44. z zadowoleniem przyjmuje proponowany przegląd kodeksu postępowania w zakresie zwalczania dezinformacji, a także wnioski dotyczące aktu o usługach cyfrowych, aktu o rynkach cyfrowych i innych środków związanych z europejskim planem działania na rzecz demokracji, ponieważ mogą to być skuteczne narzędzia zwalczania obcej ingerencji; zaleca, aby podczas ostatecznego czytania tych tekstów uwzględniono aspekty omawiane w pozostałej części niniejszej sekcji;

45. podkreśla, że wolność wypowiedzi nie może być błędnie interpretowana jako wolność angażowania się online w działalność, która jest nielegalna offline, jak nękanie, mowa nienawiści, dyskryminacja rasowa, terroryzm, przemoc, szpiegostwo i groźby; podkreśla, że platformy muszą nie tylko przestrzegać prawa kraju, w którym prowadzą działalność, lecz także działać zgodnie z własnymi warunkami, zwłaszcza jeśli chodzi o szkodliwe treści w internecie; wzywa platformy do wzmożenia wysiłków na rzecz zapobiegania ponownemu pojawianiu się nielegalnych treści identycznych z tymi, które zostały zidentyfikowane jako nielegalne i usunięte;

46. podkreśla, że trzeba przede wszystkim kontynuować badania nad intensyfikacją dezinformacji i obcej ingerencji w internecie oraz wprowadzić ogólnounijne przepisy zapewniające znacznie większe i istotne poziomy przejrzystości, monitorowania i rozliczalności w odniesieniu do operacji prowadzonych przez platformy internetowe i do dostępu do danych przysługującego osobom do niego uprawnionym, w szczególności w kontekście algorytmów i reklam internetowych; wzywa przedsiębiorstwa mediów społecznościowych do prowadzenia bibliotek reklamowych;

47. wzywa do wprowadzenia regulacji i podjęcia działań w celu zobowiązania platform, zwłaszcza tych, które stwarzają ryzyko systemowe dla społeczeństwa, do dołożenia starań w celu ograniczenia manipulacji informacjami i ingerencji, na przykład poprzez

[14] Dz.U. L 331 z 20.9.2021, s. 8.

stosowanie oznaczeń wskazujących prawdziwych autorów prowadzących dane konta, ograniczanie zasięgu kont regularnie wykorzystywanych do rozpowszechniania dezinformacji lub regularne naruszających warunki platformy, zawieszanie i, w razie potrzeby i w oparciu o jasne przepisy, usuwanie nieautentycznych kont wykorzystywanych do skoordynowanych kampanii ingerencyjnych lub demonetyzację stron rozpowszechniających dezinformację, ustanawianie środków ograniczających ryzyko ingerencji wynikające ze skutków ich algorytmów, modeli reklam, systemów rekomendacji i technologii sztucznej inteligencji, a także sygnalizowanie treści dezinformacyjnych w publikacjach i komentarzach; przypomina, że środki te należy wdrożyć w sposób przejrzysty i rozliczalny;

48. wzywa Komisję do pełnego uwzględnienia przyjętych w czerwcu 2021 r. wytycznych Rady Europy w sprawie najlepszych praktyk opracowywania skutecznych ram prawnych i proceduralnych dla mechanizmów samoregulacji i współregulacji moderacji treści;

49. apeluje o pełne i skuteczne wdrożenie ogólnego rozporządzenia o ochronie danych[15], które ogranicza ilość danych użytkowników, które mogą przechowywać platformy, a także czas, przez jaki takie dane mogą być wykorzystywane, zwłaszcza w przypadku platform i aplikacji wykorzystujących bardzo prywatne lub wrażliwe dane, np. komunikatorów oraz aplikacji zdrowotnych, finansowych i randkowych oraz małych grup dyskusyjnych; wzywa platformy pełniące rolę strażnika dostępu do powstrzymania się od łączenia danych osobowych z danymi osobowymi pochodzącymi z innych usług oferowanych przez strażnika dostępu lub z danymi osobowymi pochodzącymi z usług świadczonych przez osoby trzecie, aby równie łatwo jak zgadzać się można było nie zgadzać się na przechowywanie i udostępnianie danych oraz aby umożliwić użytkownikom wybranie, czy chcą otrzymywać spersonalizowane reklamy internetowe; z zadowoleniem przyjmuje wszelkie wysiłki na rzecz zakazu stosowania technik mikrotargetowania w reklamach politycznych, w szczególności, ale nie wyłącznie, technik opartych na wrażliwych danych osobowych, takich jak pochodzenie etniczne, przekonania religijne lub orientacja seksualna, i zwraca się do Komisji o rozważenie rozszerzenia zakazu mikrotargetowania na reklamę tematyczną;

50. apeluje o wiążące zasady UE zobowiązujące platformy do współpracy z właściwymi organami, aby regularnie testować systemy oraz określać, oceniać i łagodzić ryzyko manipulacji informacjami i ingerencji w informacje oraz podatności, z jakim wiąże się korzystanie z usług platform, co obejmuje sposób, w jaki projekt ich usług i zarządzanie nimi przyczyniają się do tego ryzyka; apeluje o wiążące zasady UE zobowiązujące platformy do ustanowienia systemów monitorowania sposobu korzystania z ich usług, np. monitorowania w czasie rzeczywistym najmodniejszych i najpopularniejszych postów w podziale na kraje, aby wykrywać manipulacje informacjami i ingerencje w informacje oraz zgłaszać właściwym organom podejrzenia dotyczące ingerencji, a także o zasady zwiększające koszty ponoszone przez podmioty, które umożliwiają przymykanie oka na wszelkie takie działania ułatwiane przez ich systemy;

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz.U. L 119 z 4.5.2016, s. 1.

51. wzywa platformy internetowe, aby przeznaczyły odpowiednie zasoby na zapobieganie szkodliwym obcym ingerencjom, a także na zapewnienie lepszych warunków pracy, opieki psychologicznej i sprawiedliwych wynagrodzeń dla moderatorów treści; wzywa duże platformy mediów społecznościowych, aby przedstawiały szczegółowe sprawozdania w podziale na kraje na temat zasobów przeznaczonych na weryfikację informacji w poszczególnych krajach, działalność badawczą, moderowanie treści, w tym zdolności zasobów ludzkich i AI w poszczególnych językach, oraz współpracę z lokalnym społeczeństwem obywatelskim; podkreśla, że platformy te muszą podjąć skuteczniejsze kroki, by przeciwdziałać dezinformacji na mniejszych i mniej rentowych rynkach w UE;

52. wzywa platformy mediów społecznościowych, aby w pełni respektowały równość wszystkich obywateli UE niezależnie od języka używanego przy projektowaniu ich usług, narzędzi i mechanizmów monitorowania, a także w środkach służących większej przejrzystości i bezpieczniejszemu środowisku internetowemu; podkreśla, że odnosi się to nie tylko do wszystkich urzędowych języków narodowych i języków regionalnych, ale również do języków dużych diaspor w UE; podkreśla, że usługi te powinny być również dostępne dla osób z ubytkiem słuchu;

53. postuluje wyraźne i czytelne oznaczanie materiałów typu deepfake zarówno dla użytkowników platform, jak i w metadanych treści, aby badacze i weryfikatorzy informacji byli w stanie lepiej identyfikować takie materiały; w związku z tym z zadowoleniem przyjmuje inicjatywy mające zwiększyć autentyczność i identyfikowalność treści, takie jak opracowanie znaków wodnych i norm autentyczności oraz wprowadzenie norm globalnych;

54. postuluje uregulowanie serwisów oferujących narzędzia i usługi manipulacji mediami społecznościowymi, takie jak zwiększanie zasięgu kont lub treści za pomocą sztucznego uczestnictwa lub nieautentycznych profili; podkreśla, że takie uregulowanie musi opierać się na dogłębnej ocenie obecnych praktyk i związanych z nimi zagrożeń oraz powinno zapobiegać wykorzystywaniu tych usług do ingerencji politycznej przez podmioty działające w złej wierze;

55. zwraca uwagę na potrzebę przejrzystości w odniesieniu do rzeczywistych osób fizycznych lub prawnych stojących za treściami lub kontami internetowymi, pragnących publikować reklamy; apeluje do platform, aby wprowadziły mechanizmy pozwalające wykrywać i zawieszać, w szczególności, nieautentyczne konta powiązane ze skoordynowanymi operacjami wywierania wpływu; podkreśla, że praktyki te nie powinny naruszać zdolności do zachowania anonimowości w internecie, która ma kluczowe znaczenie dla ochrony dziennikarzy, aktywistów, społeczności zmarginalizowanych i osób znajdujących się w trudnej sytuacji (np. sygnalistów, dysydentów i politycznych oponentów reżimów autokratycznych), a ponadto powinny dopuszczać istnienie kont o charakterze satyrycznym i humorystycznym;

56. podkreśla, że większa odpowiedzialność za usuwanie treści nie może prowadzić do arbitralnego usuwania treści legalnych; apeluje o ostrożność, jeśli chodzi o całkowite zawieszanie kont rzeczywistych osób fizycznych lub masowe stosowanie zautomatyzowanych filtrów; odnotowuje z zaniepokojeniem arbitralne decyzje platform dotyczące kasowania kont urzędników wybieranych; podkreśla, że konta te powinny

być likwidowane wyłącznie na podstawie jasnych przepisów opartych na wartościach demokratycznych, przekładających się na politykę biznesową i egzekwowanych przez niezależny nadzór demokratyczny, oraz że musi istnieć w pełni przejrzysty proces obejmujący prawo do odwołania;

57. apeluje o wiążące zasady zobowiązujące platformy do tworzenia łatwo dostępnych i skutecznych kanałów komunikacji dla osób lub organizacji pragnących zgłosić nielegalne treści, naruszenie warunków korzystania z usług, dezinformacje lub obce ingerencje lub manipulacje, w stosownych przypadkach umożliwiające oskarżonym osobom udzielenie odpowiedzi, zanim podjęte zostaną jakiekolwiek działania ograniczające, a także o ustanowienie bezstronnych, przejrzystych, szybkich i dostępnych procedur wyjaśniających i odwoławczych dla ofiar treści zamieszczanych w internecie, osób zgłaszających treści oraz osób fizycznych lub organizacji dotkniętych decyzją o zamieszczeniu etykiety, ograniczeniu widoczności, wyłączeniu dostępu do konta lub jego zawieszeniu bądź o ograniczeniu dostępu do dochodów z reklam; zaleca, aby platformy mediów społecznościowych wyznaczyły specjalny punkt kontaktowy dla każdego państwa członkowskiego i tworzyły grupy zadaniowe w związku z każdymi ważnymi wyborami odbywającymi się we wszystkich państwach członkowskich;

58. postuluje, aby zasady prawne zapewniały przejrzystość wobec użytkowników i ogółu społeczeństwa, np. zobowiązywały platformy do stworzenia publicznych i łatwych do przeszukiwania archiwów reklam internetowych, zawierających m.in. informacje do kogo są kierowane reklamy i kto za nie zapłacił, oraz treści moderowanych i usuniętych, do ustanowienia środków samoregulacji oraz do zapewnienia właściwym organom krajowym, zweryfikowanym badaczom powiązanym z instytucjami akademickimi, mediom, organizacjom społeczeństwa obywatelskiego oraz międzynarodowym organizacjom reprezentującym interes publiczny wszechstronnego i znaczącego dostępu do informacji o projekcie oraz o wykorzystaniu i wpływie algorytmów; uważa, że należy zharmonizować wskaźniki stosowane w tych bibliotekach, aby umożliwić analizy przekrojowe platform i ograniczyć obciążenia administracyjne dla platform;

59. apeluje, aby położyć kres modelom biznesowym, które polegają na zachęcaniu ludzi do dłuższego pozostawania na platformach poprzez dostarczanie im wciągających treści; wzywa organy decydujące o prawodawstwie i platformy, aby pilnowały – korzystając z ludzkich moderatorów i audytora będącego osobą trzecią – żeby algorytmy nie promowały nielegalnych, ekstremistycznych, dyskryminacyjnych lub radykalizujących treści, lecz raczej oferowały użytkownikom różnorodne perspektywy oraz priorytetowo traktowały i promowały treści oparte na faktach i nauce, w szczególności gdy dotyczą ważnych kwestii społecznych, takich jak zdrowie publiczne i zmiana klimatu; uważa, że systemy rankingowe oparte na zaangażowaniu i uzależnieniu stwarzają systemowe zagrożenie dla naszego społeczeństwa; wzywa Komisję, aby zajęła się aktualną kwestią zachęt cenowych, które często przewidują o wiele niższe ceny za taką samą liczbę wyświetleń silnie targetowanych reklam o stwarzających podziały treściach niż w przypadku mniej targetowanych reklam o treściach sprzyjających integracji społecznej;

60. apeluje o modyfikowanie algorytmów, aby wstrzymywać propagowanie treści pochodzących z nieautentycznych kont i kanałów, które sztucznie stymulują rozpowszechnianie szkodliwych zagranicznych manipulacji informacjami; apeluje o

modyfikowanie algorytmów tak, by nie promowały treści stwarzających podziały i wywołujących gniew; podkreśla, że UE musi wprowadzić środki, które prawnie zobowiążą przedsiębiorstwa z branży mediów społecznościowych, aby w możliwie największym stopniu zapobiegały rozprzestrzenianiu się dezinformacji po jej wykryciu, oraz że w przypadku gdy platformy nie stosują się do wymogu usunięcia dezinformacji, muszą ponosić konsekwencje;

61. podkreśla, że potrzebna jest udoskonalona faza testowa oraz systematyczny przegląd konsekwencji stosowania algorytmów, w tym sposobu, w jaki kształtują one debatę publiczną i wpływają na wyniki polityczne, oraz jak nadaje się treściom priorytet; podkreśla, że podczas takiego przeglądu należy również badać, czy platformy są w stanie dotrzymać gwarancji zawartych w odpowiednich warunkach korzystania z usług i czy wprowadziły wystarczające zabezpieczenia, aby zapobiegać skoordynowanym nieautentycznym zachowaniom na dużą skalę będących wynikiem manipulowania treściami zamieszczanymi na platformach;

62. wyraża zaniepokojenie średnią kwotą dochodów z reklam w wysokości 65 mln EUR, która przepływa każdego roku do około 1400 stron internetowych zawierających dezinformacje, skierowanych do obywateli UE[16]; podkreśla, że reklamy internetowe – czasami nawet instytucji publicznych – trafiają na szkodliwe strony internetowe propagujące mowę nienawiści i dezinformację, a zatem finansują takie strony, bez zgody czy nawet wiedzy odnośnych reklamodawców; zauważa, że pięć przedsiębiorstw, w tym Google Ads, płaci 97 % tych dochodów z reklam i odpowiada za wybór stron internetowych wydawców wyszczególnionych w ich katalogach, a zatem może decydować, które treści podlegają monetyzacji; uważa za niedopuszczalne, że algorytmy, które rozdzielają fundusze reklamowe, stanowią dla ogółu społeczeństwa kompletną czarną skrzynkę; wzywa Komisję, aby wykorzystała narzędzia polityki konkurencji i przepisy antymonopolowe do zapewnienia funkcjonalnego rynku i zlikwidowania tego monopolu; wzywa te podmioty, aby zapobiegły finansowaniu stron internetowych zawierających dezinformacje przez ich usługi reklamowe; wyraża uznanie dla organizacji zajmujących się podnoszeniem wiedzy o tej niepokojącej kwestii; podkreśla, że reklamodawcy powinni mieć prawo wiedzieć, gdzie zamieszczane są ich reklamy i który pośrednik przetwarzał ich dane, i decydować o tym; postuluje ustanowienie procesu mediacji, który umożliwi reklamodawcom uzyskanie refundacji, gdy ich reklamy zostaną umieszczone na stronach internetowych propagujących dezinformacje;

63. podkreśla, że zaktualizowany kodeks postępowania w zakresie zwalczania dezinformacji, akt o usługach cyfrowych, akt o rynkach cyfrowych i inne środki związane z europejskim planem działania na rzecz demokracji będą wymagać po ich przyjęciu skutecznego mechanizmu przeglądu, oceny i sankcji, aby możliwa była regularna ocena ich wdrożenia na szczeblu krajowym i unijnym, identyfikacja i bezzwłoczna eliminacja luk prawnych oraz nakładanie sankcji za niewłaściwe stosowanie i niewywiązywanie się z zobowiązań; domaga się w związku z tym silnych i dysponujących odpowiednimi zasobami koordynatorów ds. usług cyfrowych w każdym państwie członkowskim, a także wystarczających zasobów, aby umożliwić służbom

[16] https://disinformationindex.org/wp-content/uploads/2020/03/GDI_Adtech_EU.pdf

egzekwowania w Komisji realizację zadań przydzielonych im na mocy aktu o usługach cyfrowych; podkreśla ponadto, że należy dopilnować, aby platformy internetowe były poddawane niezależnym audytom certyfikowanym przez Komisję; zauważa, że audytorzy, aby zachować niezależność, nie mogą być finansowani przez poszczególne platformy;

64. apeluje w związku z tym o zdefiniowanie w drodze współregulacji obiektywnych kluczowych wskaźników efektywności, aby zapewnić weryfikowalność działań podejmowanych przez platformy i ich skutków; podkreśla, że te kluczowe wskaźniki efektywności powinny obejmować wskaźniki właściwe dla danego kraju, takie jak odbiorcy, do których skierowana jest dezinformacja, zaangażowanie (wskaźnik klikalności itp.), finansowanie weryfikacji informacji i badań w poszczególnych krajach, a także występowanie i siła krajowych związków ze społeczeństwem obywatelskim;

65. wyraża głębokie zaniepokojenie brakiem przejrzystości przeglądu kodeksu postępowania w zakresie zwalczania dezinformacji, gdyż dyskusja została w dużej mierze zastrzeżona dla sektora prywatnego i Komisji; ubolewa, że podczas opracowywania przeglądu kodeksu postępowania nie skonsultowano się w odpowiedni sposób z Parlamentem Europejskim, w szczególności z komisją specjalną INGE, i z niektórymi innymi zainteresowanymi stronami;

66. ubolewa nad utrzymującym się samoregulacyjnym charakterem kodeksu postępowania, ponieważ samoregulacja jest niewystarczająca, jeśli chodzi o ochronę społeczeństwa przed próbami ingerencji i manipulacji; jest zaniepokojony, że zaktualizowany kodeks postępowania w zakresie zwalczania dezinformacji może nie zapewnić odpowiedzi na przyszłe wyzwania; wyraża zaniepokojenie z powodu silnego oparcia wytycznych w sprawie wzmocnienia kodeksu postępowania na wniosku Komisji dotyczącym aktu o usługach cyfrowych; apeluje o podjęcie szybkich działań mających zapewnić, by kodeks postępowania zawierał wiążące zobowiązania dla platform, żeby zagwarantować gotowość UE przed następnymi wyborami lokalnymi, regionalnymi, krajowymi i europejskimi;

67. wzywa UE do ochrony i pobudzania dialogu w społeczności technologicznej oraz wymiany informacji na temat zachowań i strategii platform społecznościowych; uważa, że jedynie otwarta społeczność technologiczna może uodpornić opinię publiczną na ataki, manipulacje i ingerencje; apeluje o zbadanie możliwości ustanowienia publiczno-prywatnego ośrodka wymiany i analizy (ISAC) ds. dezinformacji, którego członkowie identyfikowaliby, oznaczali i udostępniali informacje o zagrożeniach treściami dezinformacyjnymi oraz ich dostawcach zgodnie z klasyfikacją zagrożenia; uważa, że mogłoby to zapewnić wkład w unijny system wczesnego ostrzegania i mechanizm G-7 oraz byłoby korzystne dla mniejszych podmiotów dysponujących ograniczonymi zasobami; apeluje również o ogólnosektorowy standard dotyczący dezinformacji dla usług reklamowych i internetowych usług monetyzacji, aby demonetyzować szkodliwe treści, oraz postuluje, aby standard ten był także stosowany przez internetowe systemy płatnicze i platformy handlu elektronicznego oraz podlegał audytowi przez stronę trzecią;

68. podkreśla, że kodeks musi funkcjonować jako skuteczne narzędzie do czasu wejścia w

życie aktu o usługach cyfrowych; uważa, że już w kodeksie należy wprowadzić niektóre obowiązki przewidziane w akcie o usługach cyfrowych oraz zobowiązać sygnatariuszy do wdrożenia szeregu przepisów tego aktu dotyczących dostępu badaczy i regulatorów do danych oraz przejrzystości reklam, w tym przejrzystości systemu algorytmicznego i systemu rekomendacji; wzywa sygnatariuszy, aby poddali zgodność z tymi obowiązkami kontroli przez niezależnego audytora, oraz domaga się opublikowania tych sprawozdań z audytu;

69. ubolewa z powodu braku przejrzystości procesu monitorowania zgodności z kodeksem, a także z powodu terminu przeglądu kodeksu, który zakończy się przed ukończeniem prac przez komisję specjalną INGE; zauważa, że do wiadomości publicznej należy przekazywać co najmniej porządki obrad, uwagi końcowe i listy obecności; wzywa sygnatariuszy, aby złożyli w Parlamencie oświadczenia na temat ich zobowiązań związanych z kodeksem oraz sposobu wywiązywania się z tych zobowiązań w przeszłości i przyszłości;

70. uważa, że niezależne organy regulacyjne ds. mediów, takie jak Europejska Grupa Regulatorów ds. Audiowizualnych Usług Medialnych, mogłyby odegrać kluczową rolę w monitorowaniu i egzekwowaniu kodeksu;

71. z zadowoleniem przyjmuje wniosek dotyczący ustanowienia grupy zadaniowej określonej w wytycznych Komisji w sprawie wzmocnienia kodeksu; nalega, by Komisja zaprosiła do udziału w tej grupie zadaniowej przedstawicieli Parlamentu, krajowych regulatorów i inne zainteresowane strony, w tym społeczeństwo obywatelskie i społeczność naukową;

Infrastruktura krytyczna i sektory strategiczne

72. uważa, że infrastruktura krytyczna, z uwagi na jej wzajemnie powiązany i transgraniczny charakter, jest w coraz większym stopniu podatna na ingerencje zewnętrzne, i sądzi, że obecnie obowiązujące ramy wymagają przeglądu; z zadowoleniem przyjmuje zatem wniosek Komisji w sprawie nowej dyrektywy mającej zwiększyć odporność podmiotów krytycznych świadczących usługi kluczowe w Unii Europejskiej;

73. zaleca, aby państwa członkowskie zachowały uprawnienia do identyfikowania podmiotów krytycznych, ale koordynacja na szczeblu UE jest konieczna po to, żeby:

    a) wzmocnić kanały połączeń i komunikacji wykorzystywane przez wiele podmiotów, w tym w celu zapewnienia ogólnego bezpieczeństwa misji i operacji UE,

    b) wspierać właściwe organy w państwach członkowskich za pośrednictwem Grupy ds. Odporności Podmiotów Krytycznych i zapewniać zróżnicowany udział zainteresowanych stron, a zwłaszcza skuteczne zaangażowanie małych i średnich przedsiębiorstw (MŚP), organizacji społeczeństwa obywatelskiego i związków zawodowych,

    c) propagować wymianę najlepszych praktyk nie tylko między państwami członkowskimi, ale również na szczeblu regionalnym i lokalnym, w tym z

Bałkanami Zachodnimi, oraz między właścicielami i operatorami infrastruktury krytycznej, m.in. poprzez komunikację międzyagencyjną, w celu wykrywania niepokojących sytuacji na wczesnym etapie i opracowywania odpowiednich środków zaradczych,

d) wdrożyć wspólną strategię reagowania na cyberataki na infrastrukturę krytyczną;

74. zaleca, aby rozszerzyć wykaz podmiotów krytycznych o cyfrową infrastrukturę wyborczą i systemy kształcenia, z uwagi na ich zasadnicze znaczenie, jeśli chodzi o zagwarantowanie długoterminowego funkcjonowania i stabilności UE i jej państw członkowskich, a także aby dopuścić elastyczność podczas podejmowania decyzji o dodaniu do wykazu nowych sektorów strategicznych, które należy objąć ochroną;

75. apeluje o przyjęcie nadrzędnego unijnego podejścia, aby poradzić sobie z problemem zagrożeń hybrydowych dla procesów wyborczych, oraz o poprawę koordynacji i współpracy między państwami członkowskimi; apeluje do Komisji o krytyczną ocenę zależności od platform i infrastruktury danych w kontekście wyborów; uważa, że brakuje nadzoru demokratycznego nad sektorem prywatnym; apeluje o bardziej demokratyczny nadzór nad platformami, w tym o odpowiedni dostęp właściwych organów do danych i algorytmów;

76. zaleca, aby obowiązki wynikające z proponowanej dyrektywy, w tym oceny zagrożeń, ryzyka i podatności w skali UE i poszczególnych krajów, odzwierciedlały najnowszy rozwój sytuacji i były realizowane przez Wspólne Centrum Badawcze we współpracy z centrum INTCEN ESDZ; podkreśla, że należy zapewnić tym instytucjom wystarczające zasoby, aby mogły one przedstawić najnowocześniejszą analizę, z silnym nadzorem demokratycznym, co nie powinno wykluczać uprzedniej oceny przez FRA w celu zadbania o poszanowanie praw podstawowych;

77. uważa, że aby zapobiec przejęciu dużych części infrastruktury krytycznej UE i krajów kandydujących przez państwa i przedsiębiorstwa spoza UE, jak w przypadku greckiego portu w Pireusie oraz, obecnie, chińskich inwestycji w kable podmorskie w Morzu Bałtyckim, Śródziemnym i Arktycznym, UE i jej państwa członkowskie muszą zapewnić alternatywne sposoby finansowania krajom kandydującym do UE z Bałkanów Zachodnich i innym potencjalnym krajom kandydującym, w których państwa trzecie wykorzystują BIZ jako narzędzie geopolityczne do zwiększania efektu dźwigni tych krajów; przyjmuje w związku z tym z zadowoleniem rozporządzenie w sprawie monitorowania BIZ jako ważne narzędzie koordynacji działań państw członkowskich dotyczących inwestycji zagranicznych oraz apeluje o silniejsze ramy regulacyjne i bardziej zdecydowane egzekwowanie tych ram, aby zagwarantować, że BIZ wpływające negatywnie na bezpieczeństwo UE, zgodnie z rozporządzeniem, będą blokowane, oraz że instytucje UE otrzymają więcej kompetencji w zakresie monitorowania BIZ; postuluje rezygnację z zasady najniższej oferty w rządowych decyzjach inwestycyjnych; wzywa wszystkie państwa członkowskie, które nie mają mechanizmów monitorowania inwestycji, do ustanowienia takich środków; uważa, że ramy prawne powinny być lepiej powiązane z niezależnymi analizami prowadzonymi przez krajowe i unijne instytuty lub inne odpowiednie zainteresowane strony, takie jak ośrodki analityczne, aby określić i ocenić przepływy BIZ; uważa, że właściwe mogłoby też być uwzględnienie w tych ramach innych sektorów strategicznych, takich jak 5G i

inne technologie informacyjno-komunikacyjne (ICT), aby ograniczyć zależność UE i jej państw członkowskich od dostawców wysokiego ryzyka; podkreśla, że podejście to powinno mieć zastosowanie w równej mierze do krajów kandydujących i potencjalnych krajów kandydujących;

78. uważa, że UE stoi przed większymi wyzwaniami ze względu na brak inwestycji w przeszłości, co przyczyniło się do jej zależności od zagranicznych dostawców technologii; zaleca zabezpieczenie łańcuchów produkcji i dostaw infrastruktury krytycznej i materiałów krytycznych w UE; uważa, że dążenie UE do otwartej autonomii strategicznej i suwerenności cyfrowej jest ważne i stanowi właściwy kierunek działania; podkreśla, że zgodnie z oczekiwaniami UE ma wdrożyć nowe narzędzia, aby wzmocnić swoją pozycję geopolityczną, w tym instrument chroniący przed wymuszaniem; uważa, że europejski akt prawny o mikroczipach zapowiedziany przez Komisję zagwarantuje, że części o zasadniczym znaczeniu dla produkcji mikroczipów wytwarzane będą w UE, co jest ważnym krokiem na drodze do ograniczenia zależności od państw trzecich, takich jak Chiny i USA; uważa, że inwestycje w produkcję mikroczipów muszą być skoordynowane w całej Unii i realizowane na podstawie analizy strony popytu, co pozwoli uniknąć wyścigu po krajowe dotacje publiczne i rozdrobnienia jednolitego rynku; apeluje zatem do Komisji, aby ustanowiła specjalny europejski fundusz na rzecz półprzewodników, który mógłby wspierać tworzenie bardzo potrzebnej wykwalifikowanej siły roboczej oraz rekompensować wyższe koszty zakładania obiektów produkcyjnych i projektowych w UE; uznaje Tajwan za ważnego partnera w zwiększaniu produkcji półprzewodników w UE;

79. apeluje o dalszy rozwój europejskich sieci infrastruktury danych i dostawców usług odpowiadających europejskim normom bezpieczeństwa, takich jak GAIA-X, jako ważny krok w kierunku stworzenia realnych alternatyw dla obecnych dostawców usług i w kierunku otwartej, przejrzystej i bezpiecznej gospodarki cyfrowej; podkreśla, że należy wzmocnić MŚP i zapobiec kartelizacji rynku usług w chmurze; przypomina, że ośrodki przetwarzania danych stanowią infrastrukturę krytyczną; wyraża zaniepokojenie wpływem państw trzecich i ich przedsiębiorstw na rozwój GAIA-X;

80. podkreśla, że integralność, dostępność i poufność publicznych sieci łączności elektronicznej, takich jak internetowa sieć szkieletowa i podmorskie kable komunikacyjne, mają zasadnicze znaczenie dla bezpieczeństwa; wzywa Komisję i państwa członkowskie, aby zapobiegały sabotażowi i szpiegostwu w tych sieciach komunikacyjnych oraz promowały stosowanie interoperacyjnych, bezpiecznych standardów routingu, żeby zapewnić integralność i solidność sieci i usług łączności elektronicznej, również za pośrednictwem niedawnej strategii Global Gateway;

81. wzywa Komisję, aby zaproponowała działania pozwalające zbudować sieć bezpiecznych, zrównoważonych i sprawiedliwych dostaw surowców wykorzystywanych do produkcji kluczowych komponentów i technologii, w tym baterii i sprzętu, 5G i późniejszych technologii oraz produktów chemicznych i farmaceutycznych, i jednocześnie podkreśla znaczenie światowego handlu, współpracy międzynarodowej z pełnym poszanowaniem praw pracowniczych i środowiska naturalnego oraz egzekwowania międzynarodowych norm społecznych i norm zrównoważonego rozwoju w odniesieniu do wykorzystania zasobów; przypomina, że

trzeba przyznać konieczne środki finansowe na badania i rozwój w celu znalezienia odpowiednich substytutów w przypadku zakłóceń w łańcuchach dostaw;

Obce ingerencje w procesy wyborcze

82. domaga się uznania ochrony całego procesu wyborczego za jedną z najważniejszych kwestii bezpieczeństwa unijnego i narodowego, gdyż wolne i uczciwe wybory są głównym elementem procesu demokratycznego; wzywa Komisję, aby opracowała lepsze ramy reagowania w celu przeciwdziałania obcej ingerencji w procesy wyborcze, które to ramy powinny obejmować między innymi bezpośrednie kanały komunikacji z obywatelami;

83. podkreśla, że trzeba wspierać odporność społeczną na dezinformację w trakcie procesów wyborczych, w tym w sektorze prywatnym i akademickim, oraz przyjąć całościowe podejście, w którym należy stale zajmować się tą ingerencją, począwszy od programów edukacji szkolnej po techniczną integralność i niezawodność głosowania, także za pomocą środków strukturalnych pozwalających zaradzić hybrydowemu charakterowi ingerencji; apeluje w szczególności o opracowanie planu, aby przygotować się do wyborów europejskich w 2024 r., obejmującego strategię, szkolenia i zwiększanie świadomości europejskich partii politycznych i ich personelu, a także wzmocnione środki bezpieczeństwa, aby zapobiegać obcym ingerencjom;

84. uważa, że wprowadzanie w błąd i dezinformacja za pośrednictwem mediów społecznościowych stają się coraz większym problemem dla uczciwości wyborów; uważa, że platformy mediów społecznościowych powinny dopilnować wdrażania i właściwego funkcjonowania strategii, aby chronić uczciwość wyborów; wyraża zaniepokojenie niedawnymi ustaleniami, że podmioty działające w złych zamiarach zatrudniają przedsiębiorstwa prywatne do zakłócania wyborów, rozpowszechniania fałszywych narracji i propagowania wirusowych teorii spiskowych, głównie za pośrednictwem mediów społecznościowych; apeluje o szczegółowe zbadanie, jak przeciwdziałać zjawisku dezinformacji na wynajem, gdyż staje się ono coraz bardziej wyszukane i powszechne w każdej części świata;

85. podkreśla ogromne znaczenie misji obserwacji wyborów, które dostarczają istotnych informacji i wydają konkretne zalecenia, aby zwiększyć odporność systemu wyborczego i pomóc w przeciwdziałaniu obcej ingerencji w procesy wyborcze; apeluje o usprawnienie i wzmocnienie procesów wyborczych, przy czym misje obserwacji wyborów są kluczowym instrumentem w walce z coraz częstszym wykorzystywaniem nieuczciwych i sfałszowanych procesów wyborczych przez nieliberalne reżimy, które chcą zachować pozory demokracji; podkreśla w związku z tym, że trzeba ponownie ocenić i zaktualizować narzędzia i metody stosowane podczas międzynarodowej obserwacji wyborów, aby stawić czoła nowym trendom i zagrożeniom, co obejmuje walkę z fałszywymi obserwatorami wyborów, wymianę najlepszych praktyk z partnerami o podobnych poglądach oraz ściślejszą współpracę z odpowiednimi organizacjami międzynarodowymi, takimi jak Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE) i Rada Europy, oraz wszystkimi właściwymi podmiotami w ramach Deklaracji zasad międzynarodowej obserwacji wyborów i Kodeksu postępowania międzynarodowych obserwatorów wyborów; podkreśla, że udział posłów do PE w niezatwierdzonych misjach obserwacji wyborów podważa

wiarygodność i reputację Parlamentu Europejskiego; przyjmuje z zadowoleniem i zaleca pełne wdrożenie procedury Zespołu ds. Wspierania Demokracji i Koordynacji Wyborów stosowanej w „przypadkach indywidualnej nieoficjalnej obserwacji wyborów przez posłów do Parlamentu Europejskiego” (przyjętej 13 grudnia 2018 r.), przewidującej wykluczenie posłów do PE z oficjalnych delegacji Parlamentu zajmujących się obserwacją wyborów na czas trwania mandatu;

Potajemne finansowanie działalności politycznej przez darczyńców zagranicznych

86. podkreśla, że choć nadal istnieje potrzeba lepszego zrozumienia wpływu potajemnego finansowania działalności politycznej na, przykładowo, tendencje antydemokratyczne w Europie, niemniej zagraniczne finansowanie działalności politycznej w drodze potajemnych operacji stanowi poważne naruszenie rzetelności demokratycznego funkcjonowania UE i jej państw członkowskich, w szczególności w okresach wyborczych, a tym samym jest sprzeczne z zasadą wolnych i uczciwych wyborów; podkreśla zatem, że angażowanie się we wszelkie potajemne działania finansowane przez zagraniczne podmioty, mające wywierać wpływ na europejskie lub krajowe procesy polityczne, należy uznać za nielegalne we wszystkich państwach członkowskich; zauważa w związku z tym, że kraje takie jak Australia wprowadziły przepisy zakazujące obcych ingerencji w politykę;

87. potępia to, że ekstremistyczne, populistyczne, antyeuropejskie partie i niektóre inne partie i osoby są powiązane z próbami ingerencji w procesy demokratyczne Unii i są wyraźnie współwinne takich prób, a także wyraża zaniepokojenie, że partie te są wykorzystywane jako głos podmiotów dokonujących obcych ingerencji, aby legitymizować ich autorytarne rządy; domaga się pełnego wyjaśnienia stosunków politycznych i ekonomicznych między tymi partiami i osobami a Rosją; uważa stosunki te za bardzo niewłaściwe oraz potępia współudział, który, motywowany osiągnięciem celów politycznych, może narazić UE i jej państwa członkowskie na ataki obcych mocarstw;

88. wzywa państwa członkowskie, aby podczas kolejnej harmonizacji przepisów krajowych wyeliminowały następujące luki i wprowadziły zakaz darowizn zagranicznych:

    a) wkłady niepieniężne ze strony podmiotów zagranicznych na rzecz partii politycznych, fundacji, osób piastujących stanowiska publiczne lub wybranych urzędników, w tym pożyczki finansowe od wszelkich osób prawnych lub fizycznych spoza UE i Europejskiego Obszaru Gospodarczego (EOG) (z wyjątkiem wyborców europejskich), anonimowe darowizny powyżej określonego progu oraz brak limitów wydatków na kampanie polityczne, co umożliwia wywieranie wpływu poprzez duże darowizny; politycy, podmioty polityczne lub partie polityczne, którym zaoferowano lub którzy przyjęli wsparcie finansowe lub wkład niepieniężny od podmiotu zagranicznego, muszą być zobowiązani zgłosić to właściwym organom i informację tę należy z kolei podać na szczeblu UE, aby umożliwić monitoring w skali UE;

    b) podstawionych darczyńców posiadających obywatelstwo danego kraju[17]:

[17] Osoba, która przekazuje pod swoim nazwiskiem w charakterze darowizny na rzecz partii politycznej lub

przejrzystość w odniesieniu do darczyńców będących osobami fizycznymi lub prawnymi musi być egzekwowana za pomocą deklaracji zgodności poświadczających status darczyńcy, a także przyznania komisjom wyborczym większych uprawnień w zakresie egzekwowania; darowizny pochodzące z terytorium UE, które przekraczają określony minimalny próg, powinny być rejestrowane w urzędowym rejestrze publicznym oraz powiązane z osobą fizyczną, oraz należy ustalić pułap darowizn od osób prywatnych i prawnych (oraz dotacji) na rzecz partii politycznych;

c) firmy przykrywki i krajowe spółki zależne zagranicznych spółek dominujących[18]: należy zakazać firm przykrywek oraz ustanowić bardziej efektywne wymogi dotyczące ujawniania pochodzenia środków finansowych otrzymywanych od spółek dominujących; finansowanie i darowizny na rzecz partii politycznych, które wykraczają poza określony próg, muszą zostać zarejestrowane w centralnym rejestrze publicznym wraz z oficjalną nazwą i adresem, które można powiązać z istniejącą osobą, i państwa członkowskie powinny gromadzić te informacje; wzywa Komisję, aby zapewniła organom w państwach członkowskich prawo do badania źródeł finansowania w celu weryfikacji informacji pochodzących od krajowych spółek zależnych, oraz rozwiązała problem braku wystarczających danych w rejestrach krajowych, zwłaszcza w sytuacjach, gdy wykorzystywana jest sieć firm przykrywek;

d) organizacje non-profit i strony trzecie[19], koordynowane przez podmioty zagraniczne i tworzone z myślą o wywieraniu wpływu na procesy wyborcze: należy rozważyć wprowadzenie w całej UE bardziej jednolitych zasad i przejrzystości w odniesieniu do organizacji zamierzających finansować działalność polityczną z myślą o wywieraniu bezpośredniego wpływu na procesy wyborcze, takie jak kampanie wyborcze i referendalne; takie zasady nie powinny uniemożliwiać organizacjom non-profit i stronom trzecim otrzymywania finansowania na kampanie tematyczne; zasady zapewniające przejrzystość finansowania lub darowizn muszą mieć zastosowanie również do fundacji politycznych;

e) internetowe reklamy polityczne nie podlegają zasadom dotyczącym reklamy telewizyjnej, radiowej i drukowanej i zwykle są nieuregulowane na poziomie UE: istnieje zatem potrzeba zakazania reklam kupowanych przez podmioty pochodzące spoza UE i EOG oraz zagwarantowania pełnej przejrzystości w odniesieniu do zakupu internetowej reklamy politycznej przez podmioty z obszaru UE; podkreśla, że trzeba zapewnić znacznie większą przejrzystość i demokratyczną rozliczalność, jeśli chodzi o korzystanie z algorytmów; z zadowoleniem przyjmuje zapowiedź nowego wniosku ustawodawczego Komisji w sprawie przejrzystości sponsorowanych treści politycznych, zgodnie z

---

kandydata pieniądze innej osoby.

[18] Omawiana luka prawna obejmuje dwa różne zjawiska: firmy przykrywki, które nie prowadzą rzeczywistej działalności gospodarczej i służą wyłącznie ukrywaniu źródeł finansowania; oraz krajowe spółki zależne zagranicznych spółek dominujących, wykorzystywane do zasilania pieniędzmi środowisk politycznych.

[19] Organizacje non-profit i strony trzecie nie mają obowiązku ujawniania tożsamości darczyńców, ale w wielu państwach członkowskich UE zezwala im się na finansowanie partii politycznych i kandydatów.

propozycją zawartą w europejskim planie działania na rzecz demokracji, który to wniosek powinien zapobiec fragmentacji powodowanej przez 27 różnych zbiorów przepisów krajowych dotyczących internetowych reklam politycznych oraz zagwarantuje, że partie UE będą mogły prowadzić kampanie internetowe przed wyborami europejskimi, a zarazem ograniczy ryzyko obcej interwencji i pozwoli przeanalizować, które zasady przyjęte dobrowolnie przez partie polityczne w poszczególnych państwach członkowskich i główne platformy mediów społecznościowych mogłyby stać się zasadami dla wszystkich w UE; wzywa UE i państwa członkowskie, aby zaktualizowały krajowe przepisy dotyczące reklam politycznych, nienadążające za konsekwentnym przechodzeniem na środki cyfrowe jako główne środki komunikacji politycznej; wzywa Komisję, aby zaproponowała, jak demokratycznie zdefiniować społeczne reklamy polityczne, aby położyć kres sytuacji, w której prywatne platformy nastawione na zysk decydują, co ma tematykę społeczną, a co nie;

f) należy wdrożyć monitorowanie wydatków wyborczych za pośrednictwem niezależnych audytorów oraz terminowo udostępniać im informacje na temat wydatków i darowizn, dzięki czemu zmniejszy się ryzyko wystąpienia np. konfliktów interesów i lobbingu związanego z finansami politycznymi; przy ustanawianiu proaktywnego ujawniania informacji należy przyznać instytucjom odpowiedzialnym za regulacje finansowe jasny mandat oraz zdolność, zasoby i uprawnienia do prowadzenia dochodzeń i kierowania spraw do ścigania;

89. apeluje zatem do Komisji, aby przeprowadziła analizę potajemnego finansowania w UE i przedstawiła konkretne wnioski, które pozwoliłyby wyeliminować wszystkie luki prawne umożliwiające nieprzejrzyste finansowanie partii i fundacji politycznych lub osób zajmujących wybieralne stanowiska ze źródeł znajdujących się w państwach trzecich, oraz zaproponowała wspólne unijne normy, które miałyby zastosowanie do krajowych ordynacji wyborczych we wszystkich państwach członkowskich; uważa, że państwa członkowskie powinny dążyć do wprowadzenia jasnych wymogów w zakresie przejrzystości finansowania partii politycznych oraz zakazu darowizn pochodzących spoza UE i EOG na rzecz partii politycznych i poszczególnych polityków, z wyjątkiem wyborców europejskich mieszkających poza UE i EOG, oraz określić jasną strategię dotyczącą systemu sankcji; wzywa Komisję i państwa członkowskie, aby ustanowiły organ UE ds. kontroli finansowej w celu zwalczania nielegalnych praktyk finansowych oraz ingerencji ze strony Rosji i innych reżimów autorytarnych; podkreśla, że trzeba wprowadzić zakaz przekazywania darowizn lub finansowania z wykorzystaniem nowych technologii, gdyż wyjątkowo trudno jest je prześledzić; zwraca się do państw członkowskich i Komisji, aby przyznały agencjom ds. nadzoru większe zasoby i silniejszy mandat z myślą o uzyskaniu danych lepszej jakości;

90. zobowiązuje się do dopilnowania, by wszystkie organizacje non-profit, ośrodki analityczne, instytuty i organizacje pozarządowe, które w trakcie prac parlamentarnych wnoszą wkład w opracowywanie polityki UE lub odgrywają rolę doradczą w procesie stanowienia prawa, były w pełni przejrzyste, niezależne i wolne od konfliktów interesów pod względem ich finansowania i własności;

91. z zadowoleniem odnotowuje trwający przegląd rozporządzenia (UE, Euratom) nr 1141/2014 w sprawie statusu i finansowania europejskich partii politycznych i

europejskich fundacji politycznych; popiera wszystkie działania zmierzające do osiągnięcia wyższego poziomu przejrzystości w zakresie finansowania europejskich partii i fundacji politycznych, w szczególności przed wyborami europejskimi w 2024 r., w tym zakaz wszelkich darowizn pochodzących spoza UE i z anonimowych źródeł, z wyjątkiem diaspory z państw członkowskich UE, oraz darowizn pochodzących spoza UE, których nie można udokumentować kontraktem, umowami o świadczenie usług lub opłatami związanymi z przynależnością do europejskiej partii politycznej, przy czym należy dopuścić składki członkowskie od krajowych partii członkowskich spoza UE i OEG na rzecz europejskich partii politycznych; wzywa europejskie i krajowe partie polityczne, aby zobowiązały się do zwalczania obcych ingerencji i rozpowszechniania dezinformacji, podpisując kartę zawierającą konkretne zobowiązania w tym względzie;

92. podkreśla, że wdrożenie wielu zaleceń GRECO i Komisji Weneckiej Rady Europy wzmocniłoby odporność systemu politycznego państw członkowskich i Unii jako całości na zagraniczne wpływy finansowe;

Cyberbezpieczeństwo i odporność na cyberataki

93. apeluje do instytucji UE i państw członkowskich o bezzwłoczne zwiększenie inwestycji w strategiczne zdolności i możliwości UE w zakresie wykrywania i ujawniania obcych ingerencji oraz przeciwdziałania im, takie jak AI, bezpieczna komunikacja oraz infrastruktura danych i chmury, aby poprawić cyberbezpieczeństwo UE, przy zapewnieniu poszanowania praw podstawowych; wzywa Komisję, aby również inwestowała więcej w wiedzę cyfrową i techniczną wiedzę specjalistyczną w UE, w celu lepszego zrozumienia systemów cyfrowych używanych w całej UE; wzywa Komisję, aby przeznaczyła dodatkowe zasoby ludzkie, materialne i finansowe na zdolności w zakresie analizy cyberzagrożeń, tj. INTCEN ESDZ, oraz cyberbezpieczeństwo instytucji, organów i agencji UE, tj. ENISA i zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE), oraz cyberbezpieczeństwo państw członkowskich; ubolewa z powodu braku współpracy i harmonizacji między państwami członkowskimi w kwestiach cyberbezpieczeństwa;

94. z zadowoleniem przyjmuje wnioski Komisji dotyczące nowej strategii w zakresie cyberbezpieczeństwa oraz nowej dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej, uchylającej dyrektywę (UE) 2016/1148[20] (NIS 2); zaleca, aby wynik końcowy trwających prac nad wnioskiem uwzględniał niedociągnięcia dyrektywy NIS z 2016 r., zwłaszcza przez wzmocnienie wymogów dotyczących bezpieczeństwa, rozszerzenie zakresu, utworzenie ram europejskiej współpracy i wymiany informacji, wzmocnienie zdolności państw członkowskich w obszarze cyberbezpieczeństwa, rozwój współpracy publiczno-prywatnej, wprowadzenie bardziej rygorystycznych wymogów w zakresie egzekwowania oraz przekazanie odpowiedzialności za cyberbezpieczeństwo kadrze kierowniczej najwyższego szczebla w europejskich podmiotach o kluczowym znaczeniu dla naszego społeczeństwa; podkreśla, że aby zmniejszyć liczbę słabych punktów we wspólnym cyberbezpieczeństwie UE, należy osiągnąć powszechny wysoki poziom

[20] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148, (COM(2020)0823).

cyberbezpieczeństwa we wszystkich państwach członkowskich UE; podkreśla, że najważniejszą potrzebą jest zapewnienie odporności systemów informacyjnych, i w związku z tym z zadowoleniem przyjmuje sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (CyCLONe); opowiada się za dalszym promowaniem działań OBWE służących budowaniu zaufania w cyberprzestrzeni;

95. z zadowoleniem przyjmuje wniosek Komisji zawarty w dyrektywie NIS 2 dotyczący przeprowadzania skoordynowanych ocen ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw – w duchu unijnego zestawu narzędzi 5G – z myślą o lepszym uwzględnieniu ryzyka związanego na przykład z wykorzystaniem oprogramowania i sprzętu produkowanego przez przedsiębiorstwa znajdujące się pod kontrolą obcych państw; wzywa Komisję do opracowywania globalnych standardów 6G i reguł konkurencji, zgodnie z europejskimi wartościami demokratycznymi; apeluje do Komisji, aby propagowała wymianę informacji między instytucjami UE a organami krajowymi na temat wyzwań, najlepszych praktyk i rozwiązań związanych ze środkami należącymi do unijnego zestawu narzędzi; uważa, że UE powinna inwestować więcej w swoje zdolności w zakresie technologii 5G i post-5G, aby ograniczyć zależność od zagranicznych dostawców;

96. podkreśla, że cyberprzestępczość nie ma granic, oraz wzywa UE, aby zintensyfikowała działania w skali międzynarodowej mające skutecznie jej przeciwdziałać; wskazuje, że UE powinna odegrać rolę lidera w opracowywaniu międzynarodowego traktatu o cyberbezpieczeństwie, ustanawiającego międzynarodowe normy w zakresie cyberbezpieczeństwa w celu zwalczania cyberprzestępczości;

97. z zadowoleniem przyjmuje zapowiedź przygotowania aktu dotyczącego cyberodporności, który uzupełniałby europejską politykę cyberobrony, gdyż cyberprzestrzeń i obronność są wzajemnie powiązane; apeluje o zwiększenie inwestycji w europejskie zdolności i koordynację w zakresie cyberobrony; zaleca wspieranie budowy cyberzdolności u naszych partnerów za pośrednictwem unijnych misji szkoleniowych lub cybermisji cywilnych; podkreśla potrzebę harmonizacji i standaryzacji szkoleń związanych z cyberprzestrzenią i apeluje o strukturalne finansowanie UE w tej dziedzinie;

98. potępia masowe i nielegalne wykorzystywanie oprogramowania szpiegowskiego Pegasus stworzonego przez NSO Group przez podmioty publiczne w państwach takich jak: Maroko, Arabia Saudyjska, Węgry, Polska, Bahrajn, Zjednoczone Emiraty Arabskie i Azerbejdżan, przeciwko dziennikarzom, obrońcom praw człowieka i politykom; przypomina, że Pegasus to tylko jeden z wielu przykładów programów niewłaściwie wykorzystywanych przez podmioty państwowe do nielegalnej inwigilacji niewinnych obywateli; potępia również inne państwowe operacje szpiegowskie wymierzone w europejskich polityków; nakłania Komisję, aby sporządziła wykaz oprogramowania do nielegalnej inwigilacji oraz stale aktualizowała ten wykaz; wzywa UE i państwa członkowskie, aby korzystały z tego wykazu do zapewnienia w pełni należytej staranności w zakresie praw człowieka oraz właściwej weryfikacji eksportu europejskiej technologii inwigilacji i pomocy technicznej oraz weryfikacji importu do państw członkowskich stwarzającego wyraźne zagrożenie dla praworządności; postuluje ponadto utworzenie unijnego Citizens' Lab, podobnego do laboratorium, które powstało w Kanadzie, składającego się z dziennikarzy, ekspertów ds. praw człowieka i

ekspertów w dziedzinie deasemblacji złośliwego oprogramowania i zajmującego się wykrywaniem i ujawnianiem bezprawnego korzystania z oprogramowania do nielegalnej inwigilacji;

99. apeluje do UE o przyjęcie solidnych ram regulacyjnych w tej dziedzinie, zarówno w UE, jak i na szczeblu międzynarodowym; z zadowoleniem przyjmuje w związku z tym decyzję Biura Przemysłu i Bezpieczeństwa Departamentu Handlu USA o umieszczeniu NSO Group Technologies na czarnej liście, co powoduje, że firma ta nie może otrzymywać amerykańskich technologii;

100. wyraża zaniepokojenie, iż UE współpracuje w sprawach sądowych i związanych ze ściganiem przestępstw z państwami trzecimi, które miały kontakty z NSO Group i używały oprogramowania szpiegującego Pegasus do szpiegowania obywateli Unii; domaga się dodatkowych zabezpieczeń i zwiększonej kontroli demokratycznej takiej współpracy;

101. wzywa Komisję, aby przyjrzała się inwestycjom UE w NSO Group Technologies i przyjęła ukierunkowane środki wobec obcych państw wykorzystujących oprogramowanie do szpiegowania obywateli UE lub osób posiadających status uchodźcy w krajach UE;

102. wyraża zaniepokojenie, że dziennikarze i działacze demokratyczni mogą być nielegalnie inwigilowani oraz nękani przez reżimy autorytarne, przed którymi starali się uciec, nawet na terytorium UE, i uważa, że stanowi to poważne naruszenie podstawowych wartości Unii oraz praw podstawowych jednostki, zapisanych w Karcie praw podstawowych, europejskiej konwencji praw człowieka (EKPC) oraz Międzynarodowym pakcie praw obywatelskich i politycznych; ubolewa nad brakiem wsparcia prawnego dla ofiar tego oprogramowania szpiegowskiego;

103. wskazuje na pilną potrzebę wzmocnienia ram ustawodawczych w taki sposób, aby pociągnąć do odpowiedzialności tych, którzy dystrybuują takie oprogramowanie, używają go i niewłaściwie wykorzystują do nielegalnych i niedozwolonych celów; odnosi się w szczególności do sankcji nałożonych 21 czerwca 2021 r. na Aleksandra Szatrowa, dyrektora generalnego białoruskiego przedsiębiorstwa produkującego oprogramowanie do rozpoznawania twarzy wykorzystywane przez reżim autorytarny, na przykład do identyfikowania protestujących członków opozycji politycznej; wzywa Komisję, aby zapobiegała wykorzystywaniu lub finansowaniu w UE nielegalnych technologii inwigilacji; apeluje do UE i państw członkowskich o współpracę z rządami państw trzecich, by wyeliminować represyjne praktyki i przepisy w dziedzinie cyberbezpieczeństwa i walki z terroryzmem, z zachowaniem zwiększonej kontroli demokratycznej; domaga się przeprowadzenia przez właściwe organy UE dochodzenia w sprawie nielegalnego wykorzystywania oprogramowania szpiegującego w UE i eksportu takiego oprogramowania z UE, a także wyciągnięcia konsekwencji wobec państw członkowskich i krajów stowarzyszonych, w tym krajów uczestniczących w programach UE, które zakupiły i stosowały takie oprogramowanie szpiegujące oraz z których je wyeksportowano, aby w nielegalny sposób wykorzystywać je przeciwko dziennikarzom, obrońcom praw człowieka, prawnikom i politykom;

104. apeluje o ambitny przegląd dyrektywy o e-prywatności[21] w celu wzmocnienia poufności komunikacji i danych osobowych podczas korzystania z urządzeń elektronicznych, bez obniżania poziomu ochrony zapewnianego przez tę dyrektywę, a także bez uszczerbku dla odpowiedzialności państw członkowskich za zapewnianie bezpieczeństwa narodowego; podkreśla, że organy publiczne powinny być zobowiązane do ujawniania zagrożeń wykrytych w urządzeniach informatycznych; apeluje do UE i państw członkowskich o dalszą koordynację działań na podstawie dyrektywy dotyczącej ataków na systemy informatyczne[22], tak aby nielegalny dostęp do systemów informatycznych i nielegalne przechwytywanie zdefiniowano jako przestępstwa karane odpowiednimi sankcjami; przypomina, że każde naruszenie poufności ze względów bezpieczeństwa narodowego musi odbywać się w sposób zgodny z prawem oraz w wyraźnych i prawnie uzasadnionych celach w społeczeństwie demokratycznym, z zastrzeżeniem absolutnej konieczności i proporcjonalności, jak tego wymagają EKPC i Trybunał Sprawiedliwości Unii Europejskiej;

Ochrona państw członkowskich UE oraz unijnych instytucji, agencji, delegatur i misji

105. podkreśla, że unijne instytucje, organy, agencje, delegatury, misje oraz sieci operacyjne, budynki i personel stanowią cel dla wszystkich typów zagrożeń i ataków hybrydowych ze strony zagranicznych podmiotów państwowych, a zatem wymagają należytej ochrony, przy czym szczególną uwagę należy zwrócić na zasoby, obiekty i działania ESDZ za granicą oraz na bezpieczeństwo personelu UE oddelegowanego do państw niedemokratycznych o represyjnych reżimach; apeluje o ustrukturyzowaną reakcję misji WPBiO na te zagrożenia, a także o bardziej konkretne wsparcie dla tych misji za pośrednictwem komunikacji strategicznej; dostrzega stałe nasilanie się inicjowanych przez państwa ataków wymierzonych w instytucje, organy i agencje UE, w tym w EMA, a także w instytucje i organy publiczne państw członkowskich;

106. wzywa do gruntownego i okresowego przeglądu wszystkich służb, sieci, wyposażenia i sprzętu instytucji, organów, agencji, delegatur, misji i operacji UE w celu wzmocnienia ich odporności na zagrożenia dla cyberbezpieczeństwa i wykluczenia potencjalnie niebezpiecznych programów i urządzeń, takich jak te opracowane przez Kaspersky Lab; wzywa instytucje UE i państwa członkowskie do zapewnienia należytych wytycznych i bezpiecznych narzędzi dla personelu; kładzie nacisk na potrzebę podnoszenia świadomości w zakresie korzystania z bezpiecznych usług i sieci w instytucjach i organach administracji, w tym podczas misji; dostrzega korzyści w wymiarze zaufania i bezpieczeństwa wynikające z sieciowych systemów operacyjnych opartych na otwartym oprogramowaniu, które są powszechnie stosowane przez sojusznicze agencje wojskowe i rządowe;

107. podkreśla, jak ważna jest skuteczna, terminowa i ścisła koordynacja między poszczególnymi instytucjami, organami i agencjami UE specjalizującymi się w cyberbezpieczeństwie, takimi jak CERT-UE, wraz z pełnym rozwojem jego zdolności operacyjnych, a także ENISA i mająca powstać wspólna jednostka ds. cyberprzestrzeni,

[21] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz.U. L 201 z 31.7.2002, s. 37.
[22] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz.U. L 218 z 14.8.2013, s. 8.

która zapewni skoordynowaną reakcję na wielkoskalowe zagrożenia dla cyberbezpieczeństwa w UE; z zadowoleniem przyjmuje trwającą zorganizowaną współpracę między CERT-UE a ENISA; z zadowoleniem przyjmuje również utworzenie w ramach INTCEN unijnej grupy roboczej ds. cyberwywiadu w celu zacieśnienia strategicznej współpracy wywiadowczej; docenia niedawne inicjatywy podejmowane przez sekretariaty generalne instytucji UE w celu rozwijania wspólnych zasad dotyczących informacji i cyberbezpieczeństwa;

108. oczekuje na dwa wnioski Komisji dotyczące rozporządzeń ustanawiających normatywne ramy bezpieczeństwa i cyberbezpieczeństwa we wszystkich instytucjach, organach i agencjach UE oraz jest zdania, że rozporządzenia te powinny obejmować budowanie zdolności i odporności; apeluje do Komisji i państw członkowskich o przydzielenie dodatkowych funduszy i zasobów na cyberbezpieczeństwo instytucji UE, aby sprostać wyzwaniom stale zmieniającego się krajobrazu zagrożeń;

109. oczekuje na sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego z audytu cyberbezpieczeństwa, spodziewane na początku 2022 r.;

110. wzywa do przeprowadzenia szczegółowego dochodzenia w sprawie zgłoszonych przypadków infiltracji pracowników instytucji UE z zagranicy; wzywa do dokonania przeglądu i ewentualnej rewizji procedur dotyczących zasobów ludzkich, w tym kontroli przed rekrutacją, w celu wyeliminowania luk prawnych umożliwiających infiltrację zagraniczną; wzywa organy zarządzające Parlamentu do usprawnienia procedur poświadczania bezpieczeństwa dla pracowników oraz do zaostrzenia zasad i kontroli dostępu do jego pomieszczeń, aby uniemożliwić osobom ściśle powiązanym z zagranicznymi interesami dostęp do poufnych spotkań i informacji; wzywa władze belgijskie, aby dokonały przeglądu i aktualizacji krajowych ram przeciwdziałania szpiegostwu, aby umożliwić skuteczne wykrywanie, ściganie i karanie przestępców; apeluje o podjęcie podobnych działań w innych państwach członkowskich, aby chronić instytucje i agencje UE na ich terytorium;

111. apeluje do wszystkich instytucji UE o podnoszenie świadomości wśród ich personelu przez należyte szkolenie i wytyczne w celu ograniczania cybernetycznych i niecybernetycznych zagrożeń dla bezpieczeństwa oraz zapobiegania i przeciwdziałania im; apeluje o obowiązkowe i regularne szkolenia w obszarze bezpieczeństwa i ICT dla całego personelu (w tym stażystów) oraz posłów do PE; apeluje o regularne i specjalne mapowanie i przeprowadzanie ocen ryzyka zagranicznych wpływów w instytucjach;

112. podkreśla, że w przypadkach manipulacji informacjami potrzebne są odpowiednie procedury zarządzania kryzysowego, w tym systemy ostrzegania funkcjonujące między szczeblami administracji i sektorami, aby zagwarantować wzajemną wymianę informacji oraz zapobiegać rozpowszechnianiu się zmanipulowanych informacji; z zadowoleniem przyjmuje w związku z tym system wczesnego ostrzegania i procedurę wczesnego ostrzegania ustanowioną przed wyborami europejskimi w 2019 r., a także procedury stosowane przez administracje Komisji i Parlamentu w celu ostrzegania o ewentualnych przypadkach wpływających na instytucje lub procesy demokratyczne UE; apeluje do administracji UE o nasilenie monitorowania, między innymi przez ustanowienie centralnego repozytorium i narzędzia do śledzenia incydentów, oraz o opracowanie wspólnego zestawu narzędzi, aktywowanego w razie ostrzeżenia

przekazanego przez system wczesnego ostrzegania;

113. domaga się wprowadzenia obowiązkowych zasad dotyczących przejrzystości w przypadku podróży oferowanych przez obce państwa i podmioty urzędnikom instytucji UE, w tym posłom do PE, asystentom parlamentarnym i doradcom grup, a także urzędnikom krajowym, przy czym zasady te powinny obejmować ujawnianie co najmniej następujących informacji; nazwy sponsorujących podmiotów, kosztów podróży i podanych powodów; przypomina, że takich zorganizowanych podróży nie można uznawać za oficjalne delegacje Parlamentu, oraz domaga się rygorystycznych sankcji w przypadku nieprzestrzegania tej zasady; podkreśla, że nieformalne grupy przyjaźni mogą podważać pracę oficjalnych organów Parlamentu, a także osłabiać jego reputację i spójność jego działań; wzywa organy decyzyjne Parlamentu do zwiększenia przejrzystości i rozliczalności tych grup oraz do egzekwowania obecnych zasad i podjęcia koniecznych środków w przypadku niewłaściwego wykorzystywania tych grup przyjaźni przez państwa trzecie; zwraca się do kwestorów o opracowanie i prowadzenie dostępnego i aktualnego rejestru grup przyjaźni i oświadczeń;

Ingerencja podmiotów globalnych za pośrednictwem przejmowania elit, narodowych diaspor, uniwersytetów i wydarzeń kulturalnych

114. potępia wszelkie rodzaje przejmowania elit oraz technikę kooptacji urzędników najwyższego szczebla oraz byłych polityków UE, stosowaną przez przedsiębiorstwa zagraniczne powiązane z rządami czynnie zaangażowanymi w ingerencje wymierzone w UE, a także ubolewa nad brakiem narzędzi i rozwiązań z zakresu egzekwowania, które są potrzebne, aby zapobiegać takim praktykom; uważa, że ujawnianie informacji poufnych uzyskanych w okresie sprawowania funkcji publicznych lub urzędniczych, kosztem strategicznych interesów UE i jej państw członkowskich, powinno mieć konsekwencje prawne i pociągać za sobą surowe sankcje, w tym natychmiastowe zwolnienie z pracy i/lub wykluczenie z rekrutacji przez instytucje w przyszłości; uważa, że oświadczenia o dochodach i majątku takich osób powinny być publicznie dostępne;

115. apeluje do Komisji, aby wspierała i koordynowała działania zapobiegające przejmowaniu elit, np. uzupełniając i wdrażając bezwyjątkowe egzekwowanie okresu karencji po zakończeniu sprawowania urzędu dla komisarzy UE i innych wysokich rangą urzędników służby cywilnej UE wraz z uwzględnieniem obowiązku sprawozdawczości po upływie takiego okresu, tak aby położyć kres praktyce „drzwi obrotowych”, oraz ustrukturyzowanych zasad walki z przejmowaniem elit na szczeblu UE; wzywa Komisję, by oceniła, czy istniejące wymogi dotyczące karencji nadal spełniają swoją rolę; podkreśla, że byli unijni politycy i urzędnicy służby cywilnej powinni zgłaszać próby nawiązania kontaktu przez obce państwo specjalnemu organowi nadzorczemu i powinni otrzymywać ochronę przysługującą sygnalistom; wzywa wszystkie państwa członkowskie do stosowania i harmonizacji okresów karencji dla ich przywódców politycznych oraz do zapewnienia, że dysponują one środkami i systemami zobowiązującymi urzędników publicznych do deklarowania ich działalności zewnętrznej, zatrudnienia, inwestycji, aktywów oraz prezentów lub korzyści o znacznej wartości, które mogą prowadzić do konfliktu interesów;

116. wyraża zaniepokojenie zintegrowanymi strategiami lobbingu, łączącymi interesy przemysłowe z obcymi celami politycznymi, w szczególności gdy sprzyjają one

interesom państwa autorytarnego; apeluje zatem, aby instytucje UE zreformowały rejestr służący przejrzystości, w tym przez wprowadzenie bardziej rygorystycznych zasad dotyczących przejrzystości, mapowanie zagranicznego finansowania na rzecz lobbingu związanego z UE, a także wprowadzenie pozycji umożliwiającej identyfikację finansowania pochodzącego od obcych rządów; apeluje o skuteczną współpracę w tej sprawie między wszystkimi instytucjami UE; uważa australijski system na rzecz przejrzystości wpływów zagranicznych za dobrą praktykę wartą naśladowania;

117. wzywa państwa członkowskie, aby rozważyły ustanowienie systemu rejestracji wpływów zagranicznych oraz utworzenie zarządzanego przez rządy rejestru działań podejmowanych na rzecz lub w imieniu obcego państwa, zgodnie z dobrą praktyką stosowaną przez demokracje o podobnych poglądach;

118. jest zaniepokojony próbami kontrolowania diaspor mieszkających na terytorium UE przez obce państwa autorytarne; zwraca uwagę na zasadniczą rolę, jaką odgrywa chiński Zjednoczony Front, będący departamentem odpowiedzialnym bezpośrednio przed Komitetem Centralnym Komunistycznej Partii Chin i mającym za zadanie koordynację strategii zewnętrznej ingerencji Chin przez ścisłą kontrolę nad Chińczykami i chińskimi przedsiębiorstwami za granicą; zwraca uwagę na doświadczenia Australii i Nowej Zelandii w radzeniu sobie ze Zjednoczonym Frontem;

119. zdecydowanie potępia wysiłki Kremla mające na celu instrumentalne wykorzystywanie mniejszości w państwach członkowskich UE poprzez wdrażanie tzw. programów wsparcia rodaków, w szczególności w państwach bałtyckich i w krajach wschodniego sąsiedztwa, w ramach geopolitycznej strategii reżimu Putina, której celem jest dzielenie społeczeństw w UE, a także realizacja koncepcji „rosyjskiego świata”, służącej uzasadnieniu ekspansjonistycznych działań reżimu; zauważa, że wiele rosyjskich „prywatnych fundacji”, „prywatnych przedsiębiorstw”, „organizacji medialnych” i „organizacji pozarządowych” jest albo własnością państwa, albo ma ukryte powiązania z państwem rosyjskim; podkreśla, że przy nawiązywaniu dialogu z rosyjskim społeczeństwem obywatelskim niezwykle ważne jest rozróżnienie między organizacjami, które nie ulegają wpływom rosyjskich władz, a tymi, które mają powiązania z Kremlem; przypomina, że istnieją również dowody na rosyjskie ingerencje i manipulacje w wielu innych zachodnich liberalnych demokracjach, a także na aktywne wsparcie dla sił ekstremistycznych i podmiotów o radykalnych poglądach w celu promowania destabilizacji Unii; zauważa, że Kreml na szeroką skalę wykorzystuje kulturę, w tym muzykę popularną, treści audiowizualne i literaturę, jako część swojego ekosystemu dezinformacji; ubolewa nad podejmowanymi przez Rosję próbami nieuznania w pełni historii sowieckich zbrodni i wprowadzenia w zamian nowej rosyjskiej narracji;

120. jest zaniepokojony podejmowanymi przez rząd turecki próbami wywierania wpływu na osoby o tureckich korzeniach w celu wykorzystania diaspory jako przekaźnika dla stanowisk Ankary i dzielenia społeczeństw europejskich, w szczególności za pośrednictwem Prezydencji dla Turków za Granicą oraz Pokrewnych Społeczności (YTB); potępia jawne próby wykorzystania przez Turcję tureckiej diaspory w Europie do zmiany przebiegu wyborów;

121. potępia wysiłki Rosji zmierzające do wykorzystania napięć etnicznych na Bałkanach

Zachodnich, aby zaognić konflikty i dzielić społeczności, co może doprowadzić do destabilizacji całego regionu; wyraża zaniepokojenie podejmowanymi przez Kościół prawosławny w krajach takich jak Serbia, Czarnogóra oraz Bośnia i Hercegowina, zwłaszcza jej część składowa Republika Serbska, próbami promowania Rosji jako obrońcy tradycyjnych wartości rodzinnych i umacniania stosunków między państwem a kościołem; jest zaniepokojony, że Węgry i Serbia pomagają Chinom i Rosji w realizacji ich celów geopolitycznych; zaleca organizowanie dialogu ze społeczeństwem obywatelskim Bałkanów Zachodnich i sektorem prywatnym, aby koordynować działania antydezinformacyjne w regionie, z naciskiem na badania i analizy oraz włączenie wiedzy fachowej na szczeblu regionalnym; apeluje do Komisji, aby rozbudowała infrastrukturę potrzebną do wypracowania opartych na dowodach reakcji na krótko- i długoterminowe zagrożenia dezinformacyjne na Bałkanach Zachodnich; wzywa ESDZ, aby zmieniła swoje stanowisko na bardziej proaktywne, koncentrując się na budowaniu wiarygodności UE w regionie, a nie na jej obronie, na rozszerzaniu monitorowania prowadzonego przez grupę zadaniową StratCom, aby skupić się na transgranicznych zagrożeniach dezinformacyjnych pochodzących z krajów położonych na Bałkanach Zachodnich i sąsiadujących z nimi;

122. podkreśla potrzebę zwiększenia wsparcia dla krajów Partnerstwa Wschodniego przez UE i jej państwa członkowskie, w szczególności prowadząc współpracę w dziedzinie budowania odporności państw i społeczeństw na dezinformację i rosyjską propagandę państwową, aby przeciwdziałać strategicznemu osłabianiu i fragmentacji ich społeczeństw i instytucji;

123. jest zaniepokojony eksterytorialnym stosowaniem środków przymusu wynikających z nowej ustawy o bezpieczeństwie narodowym Hongkongu i chińskiej ustawy o przeciwdziałaniu zagranicznym sankcjom, w połączeniu z umowami o ekstradycji zawartymi przez Chiny z innymi krajami, co umożliwia Chinom prowadzenie działań odstraszających na dużą skalę wobec krytycznie nastawionych osób niebędących obywatelami Chin, czego przykładem jest niedawna sprawa przeciwko dwóm duńskim parlamentarzystom, a także chińskie kontrsankcje przeciwko pięciu posłom do PE, Podkomisji Praw Człowieka Parlamentu Europejskiego, trzem posłom z państw członkowskich UE, Komitetowi Politycznemu i Bezpieczeństwa Rady UE, dwóm europejskim naukowcom i dwóm europejskim ośrodkom analitycznym w Niemczech i Danii; wzywa wszystkie państwa członkowskie, by sprzeciwiły się ekstradycji i odmówiły jej przeprowadzenia, a w stosownych przypadkach zapewniły zainteresowanym osobom odpowiednią ochronę, aby zapobiec potencjalnym naruszeniom praw człowieka;

124. wyraża zaniepokojenie liczbą europejskich uniwersytetów, szkół i ośrodków kulturalnych zaangażowanych w partnerstwa z podmiotami chińskimi, w tym z Instytutami Konfucjusza, co umożliwia kradzież wiedzy naukowej i sprawowanie ścisłej kontroli nad wszystkimi tematami związanymi z Chinami w dziedzinie badań naukowych i nauczania, co narusza konstytucyjną zasadę ochrony wolności i autonomii akademickiej, a także nad wyborem działań kulturalnych mających związek z Chinami; obawia się, że takie działania mogą doprowadzić do utraty wiedzy na temat kwestii związanych z Chinami, pozbawiając UE niezbędnych kompetencji; wyraża zaniepokojenie np. sponsorowaniem w 2014 r. Biblioteki Chińskiej Kolegium

Europejskiego przez Biuro Informacyjne Rady Państwa chińskiego rządu[23]; jest głęboko zaniepokojony chińskimi próbami nacisku np. na muzeum w Nantes i ocenzurowania jego działalności w związku z wystawą poświęconą Czyngis-Chanowi, zaplanowaną pierwotnie na 2020 r.[24]; zwraca się do Komisji, by ułatwiała wymianę dobrych praktyk między państwami członkowskimi, aby przeciwdziałać obcym ingerencjom w sektor kultury i edukacji;

125. wyraża zaniepokojenie przypadkami ukrytego finansowania badań naukowych prowadzonych w Europie, w tym chińskimi próbami podkradania talentów za pomocą planu „Tysiąc talentów" i stypendiów Instytutu Konfucjusza, a także celowym łączeniem wojskowych i cywilnych projektów naukowych za pomocą chińskiej strategii fuzji cywilno-wojskowej; zwraca uwagę na próby podpisania przez chińskie instytucje szkolnictwa wyższego protokołów ustaleń z instytucjami partnerskimi w Europie zawierających klauzule utrwalające chińską propagandę lub wspierające stanowisko Komunistycznej Partii Chin lub inicjatywy polityczne, takie jak inicjatywa „Jeden pas i jeden szlak", omijając w ten sposób i podważając oficjalne stanowiska rządów poszczególnych krajów; zwraca się do instytucji kulturalnych, akademickich i pozarządowych o poprawę przejrzystości w odniesieniu do wpływu Chin i wzywa je do upublicznienia wszelkich kontaktów i współpracy z rządem chińskim i związanymi z nim organizacjami;

126. potępia podjętą przez rząd węgierski decyzję o otwarciu filii Uniwersytetu Fudan, przy jednoczesnym zamknięciu Uniwersytetu Środkowoeuropejskiego w Budapeszcie; wyraża zaniepokojenie coraz większą zależnością finansową europejskich uniwersytetów od Chin i innych obcych państw, biorąc pod uwagę ryzyko przepływu wrażliwych danych, technologii i wyników badań do obcych państw oraz konsekwencje, jakie zależność ta może to mieć dla wolności akademickiej; podkreśla, jak ważna jest wolność akademicka w walce z dezinformacją i działaniami związanymi z wywieraniem wpływu; zachęca te instytucje, aby przed zawarciem nowych umów partnerskich z zagranicznymi podmiotami przeprowadzały szczegółowe oceny podatności na zagrożenia; podkreśla, że kadra akademicka powinna być przeszkolona w zakresie informowania o ukrytym finansowaniu lub wpływie za pośrednictwem specjalnej linii interwencyjnej oraz że osoby zgłaszające powinny zawsze otrzymywać ochronę przysługującą sygnalistom; apeluje do Komisji i państw członkowskich o zapewnienie, by środki na badania o znaczeniu geopolitycznym prowadzone na uniwersytetach europejskich pochodziły ze źródeł europejskich; apeluje do Komisji, aby zaproponowała przepisy mające na celu zwiększenie przejrzystości zagranicznego finansowania uniwersytetów oraz organizacji pozarządowych i ośrodków analitycznych, np. przez obowiązkowe deklaracje darowizn, analizy due diligence w odniesieniu do ich strumieni finansowania oraz ujawnianie finansowania, wkładów niepieniężnych i dotacji od podmiotów zagranicznych; wzywa organy państw członkowskich, by przyjęły skuteczne przepisy dotyczące zagranicznego finansowania instytucji szkolnictwa wyższego, w tym rygorystyczne pułapy i wymogi sprawozdawcze;

127. podkreśla, że podobne zagrożenia dla bezpieczeństwa i związane z kradzieżą własności

[23] https://www.coleurope.eu/events/official-inauguration-china-library
[24] https://www.chateaunantes.fr/en/expositions/mongole-son-of-the-sky-ans-steps-genghis-khan-and-the-birth-of-an-empire/

intelektualnej istnieją w sektorze prywatnym, gdzie pracownicy mogą mieć dostęp do kluczowych technologii i do tajemnic przedsiębiorstwa; wzywa Komisję i państwa członkowskie, by zachęcały zarówno instytucje akademickie, jak i sektor prywatny do tworzenia kompleksowych programów bezpieczeństwa i zgodności z przepisami, w tym do przeprowadzania specjalnych przeglądów bezpieczeństwa w przypadku nowych umów; zauważa, że w przypadku niektórych profesorów lub pracowników prowadzących badania i prace nad produktami o kluczowym znaczeniu uzasadnione mogą być zwiększone ograniczenia w dostępie do systemów i sieci, a także poświadczenia bezpieczeństwa;

128. zauważa, że zmieniona dyrektywa w sprawie niebieskiej karty[25], która ułatwia wykwalifikowanym migrantom spoza UE przyjazd do Unii, umożliwia na przykład chińskim i rosyjskim przedsiębiorstwom mającym siedzibę w Europie sprowadzanie wykwalifikowanych migrantów z ich krajów; zwraca uwagę, że może to utrudnić państwom członkowskim sprawowanie kontroli nad napływem tych obywateli, co może prowadzić do ryzyka obcych ingerencji;

129. odnotowuje coraz większą liczbą Instytutów Konfucjusza zakładanych na całym świecie, w szczególności w Europie; zauważa, że Centrum Edukacji Językowej i Współpracy, znane wcześniej jako siedziba Instytutu Konfucjusza lub Hanban (Biuro Międzynarodowej Rady Języka Chińskiego), odpowiedzialne za program Instytutów Konfucjusza na całym świecie, jest częścią chińskiego partyjno-państwowego systemu propagandy; apeluje do państw członkowskich i Komisji o wsparcie niezależnych kursów języka chińskiego bez zaangażowania państwa chińskiego lub powiązanych organizacji; uważa, że niedawno ustanowione Krajowe Centrum Chińskie w Szwecji może służyć jako ważny przykład zwiększenia niezależnych kompetencji na temat Chin w Europie;

130. uważa ponadto, że Instytuty Konfucjusza stanowią platformę lobbingową dla chińskich interesów gospodarczych oraz pole działania dla chińskich służb wywiadowczych i rekrutacji agentów i szpiegów; przypomina, że wiele uniwersytetów postanowiło zaprzestać współpracy z Instytutami Konfucjusza ze względu na ryzyko szpiegostwa i ingerencji, jak np. uniwersytety w Düsseldorfie w 2016 r., Brukseli (VUB i ULB) w 2019 r. oraz w Hamburgu w 2020 r., a także wszystkie uniwersytety w Szwecji; apeluje, by więcej uniwersytetów zastanowiło się nad swoją obecną współpracą, aby upewnić się, że nie narusza ona wolności akademickiej; wzywa państwa członkowskie, by ściśle monitorowały nauczanie, badania i inne działania prowadzone w Instytutach Konfucjusza, a w przypadku gdy domniemane szpiegostwo lub ingerencja są poparte jasnymi dowodami, aby podjęły działania egzekwujące, by chronić europejską suwerenność gospodarczą i polityczną, w tym poprzez odmowę finansowania lub cofnięcie licencji stowarzyszonym instytutom;

131. zauważa, że obcą ingerencję mogą również stanowić wpływy w instytucjach religijnych i ich instrumentalizacja, czego przykładem są rosyjskie wpływy w kościołach prawosławnych, szczególnie w Serbii, Czarnogórze, Bośni i Hercegowinie, zwłaszcza w

[25] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2021/1883 z dnia 20 października 2021 r. w sprawie warunków wjazdu i pobytu obywateli państw trzecich w celu zatrudnienia w zawodzie wymagającym wysokich kwalifikacji oraz uchylenia dyrektywy Rady 2009/50/WE, Dz.U. L 382 z 28.10.2021, s. 1.

jej części składowej Republice Serbskiej, Gruzji i do pewnego stopnia w Ukrainie, w tym przez wywoływanie podziałów wśród miejscowej ludności, rozwijanie tendencyjnego pisarstwa historycznego oraz promowanie agendy antyunijnej, a także wpływy tureckiego rządu wywierane za pośrednictwem meczetów we Francji i w Niemczech oraz wpływy saudyjskie wywierane za pośrednictwem meczetów salafickich w całej Europie, które promują radykalny islam; apeluje do Komisji i państw członkowskich o zapewnienie lepszej koordynacji w zakresie ochrony instytucji religijnych przed obcymi ingerencjami oraz do ustalenia limitu finansowania i zwiększenia jego przejrzystości; apeluje do państw członkowskich, by ściśle monitorowały działania prowadzone w instytucjach religijnych, a w stosownych przypadkach, popartych dowodami, podjęły działania, w tym poprzez odmowę finansowania lub cofnięcie licencji stowarzyszonym instytucjom;

132. wzywa ESDZ do opracowania badania na temat rozprzestrzenienia i wpływu podmiotów państwowych działających w złej wierze w europejskich ośrodkach analitycznych, na uniwersytetach, w organizacjach religijnych i instytucjach medialnych; wzywa wszystkie instytucje UE i państwa członkowskie, aby współpracowały z zainteresowanymi stronami i ekspertami oraz prowadziły z nimi systematyczny dialog, by dokładnie określić i monitorować obce wpływy w sferze kultury, szkolnictwa wyższego i religii; apeluje o szersze dzielenie się treściami przez europejskich nadawców krajowych, w tym nadawców z krajów sąsiadujących;

133. jest zaniepokojony doniesieniami o obcej ingerencji w europejskie systemy sądownicze; zwraca szczególną uwagę na wykonywanie przez europejskie sądy rosyjskich wyroków wobec przeciwników Kremla; wzywa państwa członkowskie, aby podnosiły świadomość pracowników wymiaru sprawiedliwości i współpracowały ze społeczeństwem obywatelskim, by zapobiegać nadużywaniu przez obce rządy międzynarodowej współpracy sądowej oraz europejskich trybunałów i sądów; apeluje do ESDZ, by zleciła przeprowadzenie badania na temat powszechności i wpływu obcych ingerencji w europejskie postępowania sądowe; zauważa, że w oparciu o to badanie konieczne może być zaproponowanie zmian w wymogach dotyczących przejrzystości i finansowania postępowań sądowych;

Odstraszanie, demaskowanie i zbiorowe środki zaradcze, w tym sankcje

134. uważa, że systemy sankcji ustanowione niedawno przez UE, takie jak środki ograniczające podejmowane w związku z cyberatakami zagrażającymi Unii i jej państwom członkowskim[26] oraz globalny system sankcji UE za naruszenia praw człowieka[27] (europejska ustawa Magnickiego), przyjęte odpowiednio 17 maja 2019 r. oraz 7 grudnia 2020 r., wykazały swoją wartość dodaną, zapewniając UE cenne narzędzia odstraszania; wzywa Komisję do przedstawienia wniosku ustawodawczego w sprawie przyjęcia nowego systemu sankcji tematycznych w celu przeciwdziałania poważnym aktom korupcji; przypomina, że systemy sankcji za cyberataki i za naruszenia praw człowieka zastosowano dwukrotnie, odpowiednio w 2020 i 2021 r.; wzywa do nadania trwałego charakteru systemowi sankcji w odpowiedzi na cyberataki oraz apeluje do państw członkowskich o udostępnianie wszelkich dowodów i informacji

[26] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ%3AL%3A2019%3A129I%3ATOC
[27] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L:2020:410I:TOC

wywiadowczych zgromadzonych na potrzeby utworzenia wykazu sankcji za cyberataki;

135. apeluje do UE i jej państw członkowskich o dalsze przeciwdziałanie obcym ingerencjom, w tym zakrojonym na szeroką skalę kampaniom dezinformacyjnym, zagrożeniom hybrydowym i wojnie hybrydowej, przy pełnym poszanowaniu wolności wyrazu i informacji, w tym przez ustanowienie systemu sankcji; uważa, że powinno to obejmować wprowadzenie międzysektorowych i asymetrycznych ram sankcji, a także sankcji dyplomatycznych, zakazów podróży, zamrożenia aktywów i odebrania obcokrajowcom i członkom ich rodzin pozwoleń na pobyt w UE w związku z próbami obcych ingerencji, które to sankcje powinny być jak najprecyzyjniej wymierzone w decydentów i organy odpowiedzialne za agresywne działania, nie prowadząc do powstania sytuacji „wet za wet”, zgodnie z art. 29 TUE i art. 215 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) (środki ograniczające) oraz w ścisłej integracji z filarami wspólnej polityki zagranicznej i bezpieczeństwa Unii (WPZiB) i WPBiO; apeluje do państw członkowskich, by uczyniły obce i krajowe ingerencje oraz dezinformację stałym punktem porządku obrad Rady do Spraw Zagranicznych; apeluje do UE, aby zdefiniowała, czym jest niezgodne z prawem międzynarodowym działanie oraz by w następstwie tej nowej definicji przyjęła minimalne progi dla uruchomienia środków przeciwdziałania, czemu towarzyszyć powinna ocena skutków w celu zagwarantowania pewności prawnej; zauważa, że Rada powinna mieć możliwość decydowania o sankcjach związanych z obcymi ingerencjami większością głosów, a nie jednomyślnie; jest zdania, że kraje zaangażowane w obce ingerencję i manipulację informacjami w celu zdestabilizowania sytuacji w UE powinny ponieść koszty swoich decyzji oraz konsekwencje gospodarcze, wizerunkowe lub dyplomatyczne; apeluje do Komisji i wiceprzewodniczącego Komisji / wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa o przedstawienie konkretnych propozycji w tym zakresie;

136. nalega, aby, dążąc zarazem do ochrony procesów demokratycznych, praw człowieka i wolności zdefiniowanych w traktatach, w systemie sankcji zwrócono szczególną uwagę na wpływ wszelkich nakładanych sankcji na prawa i wolności podstawowe, aby zapewnić poszanowanie Karty praw podstawowych, a także by zachowano przejrzystość co do powodów podjęcia decyzji o nałożeniu sankcji; podkreśla potrzebę zwiększenia przejrzystości na szczeblu UE w odniesieniu do zakresu i wpływu sankcji na osoby powiązane, takie jak obywatele UE i przedsiębiorstwa;

137. uważa, że podczas gdy charakter ataków hybrydowych zmienia się, groźba, jaką stanowią one dla wartości UE i jej państw członkowskich, ich fundamentalnych interesów, bezpieczeństwa, niezależności i integralności, a także dla wzmocnienia i poparcia demokracji, praworządności, praw człowieka, zasad prawa międzynarodowego i podstawowych wolności, może być znaczna pod względem skali ataków, ich rodzaju lub skumulowanego efektu; z zadowoleniem przyjmuje fakt, że europejski plan działania na rzecz demokracji przewiduje, iż Komisja i ESDZ wspólnie opracują zestaw narzędzi służących przeciwdziałaniu obcym ingerencjom i operacjom związanym z wywieraniem wpływu, w tym operacjom hybrydowym, oraz jednoznacznemu demaskowaniu złośliwych ataków stron trzecich i państw trzecich przeciwko UE;

138. zauważa, że coraz szersze jest międzynarodowe zrozumienie poważnego oddziaływania niektórych obcych ingerencji na procesy demokratyczne oraz ich wpływu na

korzystanie z praw i wywiązywanie się z obowiązków; odnotowuje w związku z tym zmiany wprowadzone w 2018 r. australijską ustawą o zmianie ustawodawstwa w zakresie bezpieczeństwa narodowego (szpiegostwo i obce ingerencje), mające na celu kryminalizację potajemnych i wprowadzających w błąd działań podmiotów zagranicznych zamierzających ingerować w procesy polityczne lub rządowe, wpływać na prawa lub obowiązki bądź wspierać działalność wywiadowczą obcego rządu, przez ustanowienie nowych przestępstw, takich jak „celowa obca ingerencja”;

139. ma świadomość, że zgodnie z art. 21 ust. 3 TUE Unia musi zapewnić spójność między poszczególnymi dziedzinami swoich działań zewnętrznych oraz ich spójność z innymi strategiami politycznymi, zdefiniowanymi w traktatach; zauważa w związku z tym, że obcych ingerencji, w tym zagrożenia, jakie stanowią zagraniczni terroryści i grupy terrorystyczne mające wpływ na osoby pozostające w UE, dotyczyła także dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu[28];

140. podkreśla, że w celu wzmocnienia ich oddziaływania sankcje należy nakładać zbiorowo, w miarę możliwości w koordynacji z partnerami o podobnych poglądach, ewentualnie z udziałem organizacji międzynarodowych i w sposób sformalizowany w umowie międzynarodowej, rozważając także inne rodzaje reakcji na ataki; zwraca uwagę, że kraje kandydujące i potencjalne kraje kandydujące powinny również przyłączyć się do tych sankcji, aby dostosować się do unijnej WPZiB; odnotowuje ważną pracę wykonaną przez NATO w dziedzinie zagrożeń hybrydowych i przypomina w związku z tym komunikat ze spotkania NATO z 14 czerwca 2021 r., w którym potwierdzono, że decyzja o tym, kiedy cyberatak powoduje uruchomienie art. 5 Traktatu północnoatlantyckiego, będzie podejmowana w trybie indywidualnym przez Radę Północnoatlantycką oraz że wpływ istotnych skumulowanych działań cybernetycznych prowadzonych w złej intencji może być w pewnych okolicznościach uznany za równoważny atakowi zbrojnemu[29]; podkreśla, że UE i NATO powinny przyjąć bardziej dalekowzroczne i strategiczne podejście do zagrożeń hybrydowych, skupiające się na motywach i celach przeciwników, a także powinny wyjaśnić, w jakich przypadkach UE jest lepiej przygotowana do radzenia sobie z zagrożeniem oraz jaka jest komparatywna przewaga jej zdolności; przypomina, że kilka państw członkowskich UE nie należy do NATO, ale mimo to współpracuje z NATO, na przykład za pośrednictwem programu Partnerstwa dla Pokoju (PfP) i inicjatywy partnerstwa na rzecz interoperacyjności (PII), w związku z czym podkreśla, że wszelka współpraca UE-NATO musi pozostawać bez uszczerbku dla polityki bezpieczeństwa i obrony państw członkowskich UE nienależących do NATO, w tym tych, które prowadzą politykę neutralności; podkreśla znaczenie wzajemnej pomocy i solidarności zgodnie z art. 42 ust. 7 TUE i art. 222 TFUE oraz wzywa UE, by opracowała konkretne scenariusze uruchomienia tych artykułów w przypadku hipotetycznego cyberataku; wzywa UE i wszystkie państwa członkowskie do powiązania tej kwestii z innymi aspektami stosunków utrzymywanych z państwami odpowiedzialnymi za ingerencje i kampanie dezinformacyjne, w szczególności Rosją i Chinami;

[28] Dz.U. L 88 z 31.3.2017, s. 6.
[29] https://www.nato.int/cps/en/natohq/news_185000.htm

Globalna współpraca i multilateralizm

141. dostrzega, że wiele krajów demokratycznych na całym świecie stoi w obliczu podobnych operacji destabilizacyjnych prowadzonych przez obce podmioty państwowe i niepaństwowe;

142. zwraca uwagę na potrzebę globalnej i wielostronnej współpracy na odpowiednich forach międzynarodowych między krajami o podobnych poglądach na te kwestie o zasadniczym znaczeniu, w formie partnerstwa opartego na wspólnym zrozumieniu i wspólnych definicjach, w celu ustanowienia międzynarodowych norm i zasad; podkreśla znaczenie ścisłej współpracy ze Stanami Zjednoczonymi i innymi państwami o podobnych poglądach dla modernizacji organizacji wielostronnych; w związku z tym z zadowoleniem przyjmuje szczyt na rzecz demokracji i oczekuje, że jego wynikiem będą konkretne propozycje i działania mające na celu wspólne stawienie czoła największym zagrożeniom, przed którymi stoją obecnie demokracje;

143. uważa, że, opierając się na wspólnej orientacji sytuacyjnej, partnerzy o podobnych poglądach powinni wymieniać się najlepszymi praktykami oraz ustalać wspólne reakcje na globalne, ale także wspólne, krajowe wyzwania, takie jak sankcje zbiorowe, ochrona praw człowieka i standardów demokratycznych; wzywa UE, by przewodniczyła debacie na temat prawnych skutków obcych ingerencji, promowała wspólne międzynarodowe definicje i zasady demaskowania oraz opracowała międzynarodowe ramy reakcji na ingerencję w wybory w celu ustanowienia Globalnego kodeksu postępowania w zakresie wolnych i odpornych procesów demokratycznych;

144. apeluje do UE i jej państw członkowskich o rozważenie odpowiednich formatów międzynarodowych, które umożliwiłyby partnerstwo i współpracę między partnerami o podobnych poglądach; wzywa UE i jej państwa członkowskie, aby zainicjowały na szczeblu ONZ proces przyjęcia globalnej konwencji w celu promowania i obrony demokracji, ustanawiającej wspólną definicję obcych ingerencji; wzywa UE, by zaproponowała globalny zestaw narzędzi obrony demokracji, który miałby zostać włączony do konwencji i obejmowałby wspólne działania i sankcje w celu przeciwdziałania obcym ingerencjom;

145. z zadowoleniem przyjmuje deklarację NATO z 14 czerwca 2021 r., w której dostrzega się coraz poważniejsze wyzwanie, jakie stanowią zagrożenia cybernetyczne i hybrydowe oraz inne zagrożenia niesymetryczne, w tym kampanie dezinformacyjne, a także wykorzystanie w złej intencji coraz bardziej zaawansowanych powstających i przełomowych technologii; z zadowoleniem przyjmuje postępy we współpracy między UE a NATO w dziedzinie cyberobrony; z zadowoleniem przyjmuje utworzenie przez Litwę regionalnego centrum obrony cybernetycznej z udziałem Stanów Zjednoczonych i krajów Partnerstwa Wschodniego; popiera ściślejszą współpracę z krajami partnerskimi w dziedzinie cyberobrony zarówno w zakresie wymiany informacji, jak i pracy operacyjnej; z zadowoleniem przyjmuje rozmowy między Stanami Zjednoczonymi a UE na temat wielostronnych kontroli wywozu produktów służących do cyberinwigilacji na forum Rady ds. Handlu i Technologii;

146. z zadowoleniem odnotowuje podjęte już inicjatywy, w szczególności na szczeblu administracyjnym, na rzecz dzielenia się wiedzą na temat ataków hybrydowych, w tym

kampanii dezinformacyjnych, w czasie rzeczywistym, takie jak ustanowiony przez ESDZ system wczesnego ostrzegania, częściowo otwarty dla krajów o podobnych poglądach, ustanowiony przez grupę G-7 mechanizm szybkiego reagowania oraz Połączony Pion Wywiadu i Bezpieczeństwa NATO;

147. podkreśla, że globalna współpraca powinna opierać się na wspólnych wartościach znajdujących odzwierciedlenie we wspólnych projektach, angażujących organizacje międzynarodowe, takie jak OBWE i UNESCO, i budujących zdolności demokratyczne oraz trwały pokój i bezpieczeństwo w krajach stojących w obliczu podobnych zagrożeń obcymi ingerencjami; apeluje do UE o ustanowienie europejskiego funduszu na rzecz demokratycznych mediów, wspierającego niezależne dziennikarstwo w krajach objętych procesem (potencjalnego) rozszerzenia i europejskiego sąsiedztwa oraz w krajach kandydujących i potencjalnych krajach kandydujących; zwraca uwagę na praktyczne potrzeby, takie jak zdobycie technicznego sprzętu roboczego, które regularnie zgłaszają niezależni dziennikarze z krajów sąsiadujących;

148. podkreśla pilną potrzebę zwalczania informacji wprowadzających w błąd i dezinformacji na temat klimatu; z zadowoleniem przyjmuje wysiłki podczas COP26 na rzecz przyjęcia powszechnej definicji informacji wprowadzających w błąd i dezinformacji dotyczących klimatu oraz określenia działań w celu ich zwalczania; apeluje o wykorzystanie modeli takich jak Międzyrządowy Zespół ds. Zmian Klimatu w celu stworzenia globalnego kodeksu postępowania w zakresie dezinformacji, procesu, który stanowiłby podstawę porozumienia paryskiego w sprawie dezinformacji;

149. podkreśla, jak ważne jest zapewnienie jasnej perspektywy krajom kandydującym i potencjalnym krajom kandydującym oraz wspieranie krajów partnerskich i sąsiadujących, takich jak kraje Bałkanów Zachodnich oraz kraje należące do wschodniego i południowego sąsiedztwa UE, ponieważ takie kraje, jak Rosja, Turcja i Chiny usiłują wykorzystywać je jako laboratorium manipulacji informacjami i wojny hybrydowej w celu osłabienia UE; uważa, że Stany Zjednoczone są ważnym partnerem w walce z obcymi ingerencjami, kampaniami dezinformacyjnymi i zagrożeniami hybrydowymi w tych regionach; jest szczególnie zaniepokojony rolą odgrywaną przez Serbię i Węgry w szerokim rozpowszechnianiu dezinformacji w sąsiednich krajach; podkreśla, że UE powinna wspierać te kraje i współpracować z nimi, jak przewidziano w rozporządzeniu w sprawie ISWMR[30]; uważa, że jej działania mogą przybrać formę promowania wartości dodanej UE i pozytywnego wpływu UE w regionie, finansowania projektów mających na celu zapewnienie wolności mediów, wzmocnienie społeczeństwa obywatelskiego i praworządności oraz zacieśnianie współpracy w zakresie umiejętności korzystania z mediów, technologii cyfrowych i informacji, przy jednoczesnym poszanowaniu suwerenności tych krajów; wzywa do zwiększenia zdolności ESDZ w tym zakresie;

150. zachęca UE i jej państwa członkowskie do pogłębienia współpracy z Tajwanem w

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/947 z dnia 9 czerwca 2021 r. ustanawiające Instrument Sąsiedztwa oraz Współpracy Międzynarodowej i Rozwojowej – Globalny wymiar Europy, zmieniające i uchylające decyzję Parlamentu Europejskiego i Rady nr 466/2014/UE oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1601 i rozporządzenie Rady (WE, Euratom) nr 480/2009, Dz.U. L 209 z 14.6.2021, s. 1.

przeciwdziałaniu operacjom zakłócającym i kampaniom dezinformacyjnym prowadzonym przez nieprzychylnie nastawione państwa trzecie, w tym do dzielenia się najlepszymi praktykami oraz wspólnymi podejściami do wspierania wolności mediów i dziennikarstwa, do pogłębiania współpracy w zakresie cyberbezpieczeństwa i cyberzagrożeń, uświadamiania obywateli i podnoszenia ogólnego poziomu umiejętności cyfrowych wśród ludności w celu wzmacniania odporności naszych systemów demokratycznych; popiera pogłębioną współpracę między właściwymi europejskimi i tajwańskimi agencjami rządowymi, organizacjami pozarządowymi i ośrodkami analitycznymi w tej dziedzinie;

151. apeluje do Parlamentu, aby aktywnie promował narrację UE oraz by odgrywał wiodącą rolę w promowaniu wymiany informacji i omawiał najlepsze praktyki z parlamentami partnerskimi na całym świecie, wykorzystując swoją rozległą sieć delegacji międzyparlamentarnych, a także inicjatywy demokratyczne i wsparcie koordynowane przez jego Zespół ds. Wspierania Demokracji i Koordynacji Wyborów; podkreśla, jak ważna jest ścisła współpraca z parlamentarzystami z krajów trzecich za pomocą dostosowanych do potrzeb projektów wspierających europejską perspektywę krajów kandydujących i potencjalnych krajów kandydujących;

152. apeluje do ESDZ o wzmocnienie roli delegatur UE i misji UE w dziedzinie WPBiO w państwach trzecich, aby zwiększyć ich zdolność do wykrywania i demaskowania kampanii dezinformacyjnych organizowanych przez zagraniczne podmioty państwowe oraz finansowania projektów edukacyjnych wzmacniających wartości demokratyczne i prawa podstawowe; zdecydowanie zaleca utworzenie z inicjatywy ESDZ Centrum Komunikacji Strategicznej w celu nawiązania współpracy strukturalnej w zakresie zwalczania dezinformacji i obcych ingerencji, które powinno mieć siedzibę w Tajpej; wzywa ponadto delegatury UE, aby wniosły wkład do walki UE z dezinformacją przez przetłumaczenie odpowiednich decyzji UE, takich jak rezolucje Parlamentu w trybie pilnym, na język ich delegowanego kraju;

153. apeluje, aby kwestię obcych ingerencji prowadzonych w złej intencji uwzględniono w przygotowywanym kolejnym Kompasie strategicznym UE;

154. apeluje o utworzenie w Parlamencie Europejskim trwałego rozwiązania instytucjonalnego w celu monitorowania realizacji tych zaleceń, tak aby przeciwdziałać obcym ingerencjom i dezinformacji w UE w usystematyzowany sposób, poza obecnym mandatem komisji specjalnej INGE; apeluje o lepszą zinstytucjonalizowaną wymianę informacji między Komisją, ESDZ i Parlamentem za pośrednictwem tego organu;

°

° °

155. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, wiceprzewodniczącemu Komisji / wysokiemu przedstawicielowi Unii do spraw zagranicznych i polityki bezpieczeństwa oraz rządom i parlamentom państw członkowskich.

UZASADNIENIE

Kontekst

Kiedy 18 czerwca 2020 r. Parlament Europejski postanowił powołać Komisję Specjalną ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w Unii Europejskiej, w tym Dezinformacji, powierzył jej zadanie zapewnienia długoterminowego podejścia do dowodów na obce ingerencje w demokratyczne instytucje i procesy w UE i jej państwach członkowskich.

Rok po posiedzeniu inauguracyjnym Komisji, które miało miejsce 23 września 2020 r., opierając się na dużej liczbie wypowiedzi różnych ekspertów i praktyków, sprawozdawczyni jest już w stanie przedstawić stan rzeczywisty, zakres i wysoki poziom zaawansowania licznych form przyjmowanych przez agresywne operacje podejmowane i finansowane przez podmioty zagraniczne w celu ingerowania w UE. Sprawozdawczyni jest także w stanie stwierdzić, z zaniepokojeniem, szybkość adaptacji, ulotność i coraz wyższe tempo tego zjawiska – w którym w okresie zaledwie roku wprowadza się nowe podmioty, nowe narracje, nowe narzędzia.

Od prowadzonych na nieznaną wcześniej skalę kampanii dezinformacyjnych dotyczących pandemii COVID-19 po cyberataki przeciwko organom publicznym, w tym infrastrukturze zdrowia publicznego, od strategii ingerencji łączących przejmowanie elit i lobbing przemysłowy do potajemnego finansowania działalności politycznej, od kontroli nad ośrodkami akademickimi i kulturalnymi po instrumentalizację diaspor międzynarodowych, nasza komisja analizowała wieloaspektowy i dynamiczny wymiar tego nowego rodzaju wojny, którego celem jest podważenie spójności społecznej i wzajemnego zaufania w naszych europejskich demokratycznych społeczeństwach z myślą o ich osłabieniu.

Komisja na szczęście była także świadkiem wzrostu świadomości w odniesieniu do tych zasadniczych kwestii, w tym powszechnego zrozumienia, że UE i jej państwa członkowskie powinny zostać bezzwłocznie wyposażone we w pełni rozwinięte strategie polityczne na rzecz odporności i narzędzia odstraszania, oparte na podejściu obejmującym całość społeczeństwa, umożliwiające im przeciwdziałanie wszelkim rodzajom zagrożeń hybrydowych i ataków i w związku z tym zabezpieczających zrównoważone funkcjonowanie demokracji.

Budowanie odporności przez orientację sytuacyjną, umiejętność korzystania z mediów i informacji, pluralizm mediów, niezależne dziennikarstwo i edukację

Jest jasne, że pierwszy filar skutecznej obrony przed obcymi ingerencjami to posiadanie orientacji sytuacyjnej. W tym celu musimy wykonać dwa ważne kroki: po pierwsze musimy monitorować, mapować i analizować poszczególne ingerencje i ataki, aby w pełni zrozumieć zagrożenie; po drugie, musimy dopilnować, aby każdy, kto potrzebuje takiej wiedzy, znał tę analizę.

Wielu badaczy, organizacji społeczeństwa obywatelskiego, dziennikarzy i pracowników instytucji europejskich wykonuje ważne zadanie, jakim jest analizowanie zagrożenia. Wielu z

nich należy do komisji INGE. Na szczeblu europejskim sprawozdawczyni docenia w szczególności pracę grup zadaniowych StratCom ESDZ. Musimy jednak nadal rozwijać tę działalność. Nie możemy godzić się z tym, że nadal nie istnieje grupa zadaniowa monitorująca ingerencje ze strony Chin.

Musimy także upewnić się, że te ustalenia trafią do szerszych grup społeczeństwa. Ważne są zarówno ukierunkowane szkolenia dla osób sprawujących funkcje podatne na obce ingerencje, jak i ogólne kampanie podnoszenia świadomości. W tym kontekście edukacja w zakresie umiejętności korzystania z mediów i umiejętności cyfrowych ma zasadnicze znaczenie dla umożliwienia obywatelom lepszej interpretacji i oceny napotykanych informacji.

Dziennikarze odgrywają kluczową rolę, zapewniając zdrowy klimat debaty. Niestety ucierpieli oni finansowo w wyniku cyfryzacji, zwłaszcza że systemy reklamowe, jak się wydaje, preferują raczej treści nacechowane emocjonalnie, w tym opinie i dezinformację, niż wysokiej jakości dziennikarstwo. Poszczególni dziennikarze zajmujący się wrażliwymi tematami często padają ofiarami nękania i zorganizowanych gróźb. Ze względu na to, jak istotna jest obrona niezależności wysokiej jakości mediów, ważne jest również przeanalizowanie sposobów wsparcia nowych mediów i dziennikarzy, zarówno finansowo, jak i zapewniając ochronę przed nękaniem.

Obce ingerencje z wykorzystaniem platform internetowych

Jest jasne, że obecny system rozpowszechniania informacji za pośrednictwem platform prowadzi do wypaczenia klimatu w internecie, w którym kwitnie dezinformacja i inne rodzaje manipulowania informacjami. Doniesienia o wyciekach i sprzedaży wrażliwych danych, algorytmach promujących treści radykalizujące i platformach przymykających oko na naruszenia ich własnych warunków są tak powszechne, że niemal przywykliśmy do nich i przestały nas one niepokoić. Musimy położyć temu kres.

Liczne dyskusje z ekspertami przekonały mnie, że obecna metoda samoregulacji nie działa i należy ją zastąpić wiążącymi przepisami. Nie możemy godzić się na to, że zagraniczne podmioty swobodnie manipulują treściami, które otrzymujemy w internecie za pośrednictwem platform lub nadużywają systemów reklamowych, przez co reklamodawcy nieświadomie przyczyniają się do ich finansowania. Nie możemy także godzić się na to, że platformom pozwala się na bezczynność bez żadnych konsekwencji.

Wprowadzono wprawdzie wiele usprawnień, zarówno z inicjatywy samych platform, jak i wynikających ze środków publicznych, takich jak kodeks postępowania. Bez znaczącej przejrzystości nie jest jednak możliwe wyrobienie sobie opinii na temat skutków tych działań. Istotne jest także, aby kodeksowi postępowania, z zasady dobrowolnemu, towarzyszył skuteczny mechanizm egzekwowania i aby uzupełniały go efektywne przepisy. Ponadto uderzające jest, jak wiele strategii politycznych na rzecz przeciwdziałania ingerencji stosuje się tylko w odniesieniu do treści w języku angielskim lub w bardzo ograniczonej liczbie języków. Nie możemy akceptować sytuacji, w której użytkownicy języka łotewskiego, bułgarskiego, greckiego, czy nawet francuskiego lub niemieckiego są chronieni przed manipulacjami w internecie znacznie słabiej niż rodzimi użytkownicy języka angielskiego tylko dlatego, że platformy priorytetowo traktują treści w tym języku.

Infrastruktura krytyczna i sektory strategiczne

Infrastruktura krytyczna ma zasadnicze znaczenie dla funkcjonowania gospodarki i społeczeństwa. Lepsza ochrona sektorów krytycznych wymaga skoordynowanych i wspólnych działań obejmujących wszystkie sektory oraz szczeble – unijny, krajowy, regionalny i lokalny. Nowa dyrektywa Komisji mająca na celu zwiększenie odporności podmiotów krytycznych to ważny punkt wyjścia. Sprawozdawczyni jest jednak zdania, że wykaz infrastruktury krytycznej należy poszerzyć o media, a także o infrastrukturę wyborczą, biorąc pod uwagę ich zasadnicze znaczenie dla zagwarantowania funkcjonowania UE i jej państw członkowskich, jak również że należy dopuścić elastyczność przy dodawaniu w przyszłości nowych sektorów strategicznych do wykazu. Jest niezwykle ważne, aby w dyrektywie utrzymano podejście odznaczające się dużymi możliwościami adaptacji, umożliwiające szybkie aktualizacje i modyfikacje.

Ponadto zależność w zakresie infrastruktury krytycznej zarówno od inwestycji zagranicznych, jak i od zagranicznych dostawców technologii stwarza wiele zagrożeń dla autonomicznego funkcjonowania takiej infrastruktury. Dlatego też dążenie UE do autonomii strategicznej i suwerenności cyfrowej ma kluczowe znaczenie dla przeciwdziałania tym zagrożeniom.

Potajemne finansowanie działalności politycznej przez podmioty i darczyńców z zagranicy

Jak pokazują wiarygodne dowody, podmioty zagraniczne aktywnie ingerują w demokratyczne wybory i referenda w krajach europejskich przez potajemne operacje finansowania podczas kampanii.

Takie prowadzone w złej intencji operacje zagrażają rzetelności wyborów organizowanych w UE, skutkując nieuczciwą konkurencją między partiami i kandydatami, gdyż zapewniają dodatkowe zasoby niektórym partiom – zwykle przeciwnym UE – nieuwzględniane w oficjalnych rozliczeniach wydatków na kampanię.

Według sprawozdania przedstawionego w 2020 r. przez Sojusz w Obronie Demokracji (Alliance for Securing Democracy) dotyczącego potajemnego finansowania z zagranicy[1], w ciągu minionej dekady Rosja, Chiny i inne reżimy autorytarne przekazały już ponad 300 mln USD do 33 krajów, aby ingerować w procesy demokratyczne ponad 100 razy, z czego połowa przypadków dotyczy działań Rosji w Europie.

Niektóre z tych operacji nie są nawet nielegalne: wykorzystują one liczne luki prawne wynikające z tego, że przepisy krajowego prawa wyborczego państw członkowskich dotyczące finansowania działalności politycznej nie są zharmonizowane na szczeblu UE.

Cyberbezpieczeństwo i odporność na cyberataki

Postępująca cyfryzacja usług doprowadziła do coraz większego uzależnienia infrastruktury krytycznej od systemów internetowych, zwiększając tym samym ich podatność na cyberataki i narażenie danych. Liczba cyberataków wzrosła w ostatnich latach, przy czym wymierzone są one w podmioty o znaczeniu strategicznym, takie jak Europejska Agencja Leków (EMA) i parlament norweski.

Rozdrobnienie zdolności i możliwości oraz ograniczona dostępność zasobów ludzkich i

[1] https://securingdemocracy.gmfus.org/covert-foreign-money/

finansowych wskazują na podatność UE na cyberataki. Takich agresywnych działań nie powstrzymują granice. Jest zatem bardzo ważne, aby UE bezzwłocznie zaczęła inwestować w swoje strategiczne cyfrowe zdolności i możliwości – przez przydzielanie dodatkowych zasobów, zarówno ludzkich, jak i finansowych, na cyberbezpieczeństwo – zarazem zapewniając, aby we wszystkich państwach członkowskich osiągnięto wspólny wysoki stopień cyberbezpieczeństwa. Unijna strategia cyberbezpieczeństwa z 2020 r. i dyrektywa NIS 2 to ważne propozycje dotyczące poprawy cyberbezpieczeństwa w UE, które w przyszłości zostanie wzmocnione przez akt w sprawie odporności cybernetycznej i politykę cyberobrony.

Ponadto bezzwłocznie należy zająć się kwestią oprogramowania szpiegowskiego, takiego jak Pegasus, wzmacniając ramy ustawodawcze, aby rozliczać podmioty dystrybuujące takie oprogramowanie oraz używające i nadużywające go.

Ochrona państw członkowskich UE oraz unijnych instytucji, agencji, delegatur i misji

Cyberbezpieczeństwo powinno zostać poprawione nie tylko w państwach członkowskich, lecz także w instytucjach UE. Niedawne ataki wymierzone w te instytucje uwypukliły potrzebę silnej współpracy międzyinstytucjonalnej w zakresie wykrywania, monitorowania i udostępniania informacji podczas cyberataków lub w celu zapobiegania im. Instytucje europejskie podjęły już środki na rzecz wzmocnienia swojego cyberbezpieczeństwa i dysponują narzędziami koordynacji swoich działań, a także wykrywania cyberataków, takimi jak CERT-UE i ENISA, do których dołączy wspólna jednostka ds. cyberprzestrzeni.

Niezbędne są jednak dalsze działania. Po pierwsze, należy zwiększyć zasoby zarówno ludzkie, jak i finansowe, aby sprostać wyzwaniom stale zmieniającego się krajobrazu zagrożeń. Po drugie, instytucje UE powinny przeprowadzić gruntowny przegląd usług i sieci, z których korzystają, aby ograniczyć ryzyko i zagwarantować, że ich bezpieczeństwo nie będzie zależne od zagranicznych technologii. I wreszcie wszystkim pracownikom należy zapewnić podnoszenie świadomości oraz odpowiednie szkolenia i wytyczne, aby ograniczać cybernetyczne i niecybernetyczne zagrożenia dla bezpieczeństwa i przeciwdziałać im.

Ingerencja podmiotów globalnych za pośrednictwem przejmowania elit, narodowych diaspor, uniwersytetów i wydarzeń kulturalnych

Kolejny zestaw narzędzi, jakim dysponują obce kraje pragnące ingerować w funkcjonowanie UE opiera się na ingerencji wykorzystującej ludzi.

„Przejmowanie elit”, czyli kooptacja, to niestety szeroko rozpowszechnione zjawisko, a jego najbardziej znana forma to zatrudnianie byłych europejskich polityków i urzędników wysokiego szczebla przez przedsiębiorstwa kontrolowane przez obce państwa, w zamian za ich wiedzę nabytą podczas sprawowania urzędów lub funkcji publicznych. Ich wiedza, często oparta na poufnych informacjach i kontaktach, jest następnie wykorzystywana kosztem interesów strategicznych UE i jej państw członkowskich. Operacje takie często wiążą się ze strategiami lobbingu przemysłowego, a wówczas połączone zostają cele gospodarcze i polityczne.

Inną formą ingerencji wykorzystującej ludzi jest zwiększanie przez agentów obcych państw wpływów na uniwersytetach, w szkołach, a także w instytucjach kulturalnych i religijnych, a w końcu przejmowanie kontroli nad nimi w kwestiach istotnych dla danego kraju obcego.

Sposób, w jaki Instytuty Konfucjusza – niedawno nazwane „Centrami Edukacji Językowej i Współpracy” – dążą do kontrolowania wszystkich typów badań, nauczania, a nawet wystaw związanych z Chinami na wielu europejskich uniwersytetach i w muzeach to wyrazisty przykład takich praktyk. Także inne kraje są bardzo aktywne w tej dziedzinie, np. Rosja działająca przez kościoły prawosławne.

Ta forma ingerencji w dużej mierze korzysta z wysiłków zmierzających do kontrolowania diaspor narodowych mieszkających w UE, które potencjalnie stanowią potężny czynnik nacisku obejmujący wszystkie segmenty społeczeństw europejskich. Wysiłki te mają również na celu uciszanie oponentów politycznych mieszkających za granicą.

Odstraszanie, demaskowanie i zbiorowe środki zaradcze, w tym sankcje

UE i jej państwa członkowskie muszą wypracować wiarygodne narzędzia odstraszania. W istocie UE i państwa członkowskie nie posiadają obecnie żadnego specjalnego systemu sankcji związanych z obcymi ingerencjami i kampaniami dezinformacyjnymi organizowanymi przez zagraniczne podmioty państwowe.

Sprawozdawczyni jest świadoma wyzwań prawnych, jakie mogą towarzyszyć tworzeniu takiego systemu sankcji i do których zalicza się m.in. potrzeba precyzyjnego zdefiniowania elementów przestępstw i ich potencjalnych skumulowanych efektów zgodnie z prawem unijnym i międzynarodowym.

Sprawozdawczyni uważa jednak, że przydatnym źródłem inspiracji dla UE mogą być działania podjęte przez innych partnerów, takich jak np. Australia, która opracowała definicję „celowej obcej ingerencji” oraz doprowadziła do kryminalizacji potajemnych i wprowadzających w błąd działań podmiotów zagranicznych.

Sprawozdawczyni uważa również, że możemy bazować na tym, co już wypracowano na szczeblu UE, zwłaszcza na środkach ograniczających mających przeciwdziałać cyberatakom zagrażającym Unii i jej państwom członkowskim, których w zeszłym roku użyto dwukrotnie.

I wreszcie podkreślamy potrzebę ścisłej współpracy w zakresie każdego systemu sankcji z międzynarodowymi partnerami o podobnych poglądach w celu wspólnego nakładania sankcji, co wzmocni ich skuteczność i efekt odstraszający.

Podmioty zagraniczne odpowiedzialne za agresywne ingerencje wymierzone w nasze demokracje nie mogą zakładać, że ich kampanie destabilizacji pozostaną bez konsekwencji.

Globalna współpraca i multilateralizm

UE nie jest jedynym obszarem demokratycznym na świecie stojącym w obliczu nasilających się agresywnych obcych ingerencji. Wiele innych krajów – czy to rozwiniętych, czy to rozwijających się – także jest celem takich operacji ze strony Chin czy Rosji i innych reżimów autorytarnych, które zawsze służą tym samym celom: podważeniu demokratycznego funkcjonowania z myślą o uzyskaniu wpływów.

Musimy zebrać partnerów o podobnych poglądach, aby stawić czoła tym problemom w skoordynowany sposób, na bazie partnerstwa demokracji.

Po pierwsze, musimy uzgodnić wspólne definicje i osiągnąć wspólne zrozumienie wchodzących w grę kwestii, aby ustalić międzynarodowe normy i standardy.

Precyzyjnego i zbiorowego rozważenia i odpowiedzi wymagają następujące pytania: Czym jest agresywna obca ingerencja? Jak zakwalifikować prawnie dezinformację i manipulacje sterowane z obcego kraju? W jaki sposób możemy zdefiniować te zagrożenia i ataki jako przestępstwa? Jaki system zbiorowych sankcji należy wprowadzić?

Światowa współpraca powinna następnie opierać się na wymianie najlepszych praktyk i zarządzaniu konkretnymi projektami. Parlament Europejski, przez swoją rozległą sieć forów międzyparlamentarnych, będzie miał tutaj wiodącą rolę do odegrania, tak samo jak delegatury UE w państwach trzecich.

Metody pracy

Niezależnie od naszych poglądów politycznych na poszczególne przepisy i od naszych barw w spektrum politycznym, jako członkowie komisji INGE jednomyślnie wyrażamy pogląd, że nasza demokracja musi zdecydowanie opierać się próbom obcych ingerencji. Z tego względu prace naszej komisji oparliśmy na pogłębionej kooperacji między grupami politycznymi. Koordynatorzy wspólnie z przewodniczącym podejmowali decyzje o tym, których ekspertów zaprosić i jakie analizy zlecić. Jako sprawozdawczyni, podczas prac nad sprawozdaniem regularnie konsultowałam się z kontrsprawozdawcami.

Pod względem tematycznym możemy wyróżnić fazę diagnozy i fazę ukierunkowaną na rozwiązania. W pierwszej fazie zaprosiliśmy ekspertów, którzy pomogli nam zrozumieć zagrożenia i metody w całym ich zróżnicowaniu. Kierując się naszym mandatem, zorganizowaliśmy szereg wysłuchań dotyczący ingerencji w sferze publicznej i prywatnej, podczas których analizowaliśmy metody poszczególnych podmiotów zagranicznych. W fazie ukierunkowanej na rozwiązania, komisja INGE skupiła się na identyfikacji potencjalnych narzędzi i strategii na rzecz zapobiegania i przeciwdziałania stwierdzonym problemom.

Komisja INGE zleciła także sześć analiz i zaprosiła autorów do przedstawienia ich ustaleń. Sytuacja sanitarna związana z pandemią COVID-19 uniemożliwiła nam zorganizowanie jakichkolwiek misji podczas dwóch pierwszych semestrów istnienia komisji INGE. W czasie przygotowania niniejszego dokumentu jednakże przedstawiciele komisji INGE powrócili z pierwszej udanej misji w Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w Atenach, Grecja. Zaplanowano trzy kolejne misje: do Tajpej, Paryża i Waszyngtonu.

Aby dodatkowo opracować zalecenia, przygotowaliśmy dwa pytania wymagające odpowiedzi ustnej. W lipcu 2021 r. zapytaliśmy wysokiego przedstawiciela i wiceprzewodniczącego Josepa Borrella, jak zamierza poprawić sytuację braku zasobów i mandatu dla grup zadaniowych Stratcom ESDZ, a także braku należytych sankcji wobec podmiotów zagranicznych dopuszczających się ingerencji. W październiku 2021 r. zapytaliśmy wiceprzewodniczącą Komisję Věrę Jourovą, w jaki sposób planuje zapewnić, aby brak koordynacji między sektorami i szczeblami polityki nie zwiększył narażenia na obce ingerencje, a także jak poprawić przejrzystość algorytmów i wesprzeć umiejętność korzystania z mediów.

Jedna z naszych konkluzji dotyczy tego, jak ważna jest współpraca i wymiana informacji, zarówno globalnie jak i pomiędzy szczeblami zarządzania i poszczególnymi sektorami w UE.

Od początku zatem zapraszaliśmy na nasze posiedzenia inne komisje i delegacje dysponujące kompetencjami odnoszącymi się do obcych ingerencji. Wiedza specjalistyczna pozyskana od tych siostrzanych podmiotów wzbogaciła debaty, które prowadziliśmy z zaproszonymi gośćmi i zagwarantowała, że spostrzeżenia z naszych wysłuchań trafiły do zwykłych komisji pracujących nad odpowiednimi wnioskami ustawodawczymi.

Jednym z głównych wydarzeń będzie posiedzenie międzyparlamentarne, którego gospodarzem będziemy w listopadzie 2021 r. To spotkanie między parlamentarzystami z krajów UE a grupą wybranych partnerów światowych o podobnych poglądach będzie doskonałą okazją, aby uczyć się od siebie nawzajem oraz przedyskutować wspólne wyzwania i rozwiązania.

Aby przygotować niniejsze sprawozdanie, sprawozdawczyni sporządziła cztery dokumenty robocze: o sytuacji w zakresie obcych ingerencji w Unii Europejskiej, w tym dezinformacji, o potajemnym finansowaniu działalności politycznej przez zagranicznych darczyńców, o obcych ingerencjach z wykorzystaniem platform internetowych oraz o budowaniu odporności UE na zagrożenia hybrydowe.

Oprócz wszystkich wspomnianych formalnych posiedzeń, sprawozdawczyni pozyskała wiedzę w drodze spotkań, udziału w konferencjach oraz lektury licznych analiz i artykułów prasowych.

Współpraca z innymi organami Paramentu Europejskiego i UE

Ze względu na międzysektorowy charakter naszego mandatu, komisja INGE zaprosiła w celu omówienia poszczególnych aspektów obcych ingerencji pięciu komisarzy:

- Věrę Jourovą, wiceprzewodniczącą do spraw wartości i przejrzystości,
- Margaritisa Schinasa, wiceprzewodniczącego ds. promowania naszego europejskiego stylu życia,
- Josepa Borrella, wiceprzewodniczącego Komisji Europejskiej / wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa,
- Thierry'ego Bretona, komisarza do spraw rynku wewnętrznego, oraz
- Margrethe Vestager, wiceprzewodniczącą wykonawczą do spraw Europy na miarę ery cyfrowej.

Odbyliśmy również szereg dyskusji z pracownikami Komisji i Europejskiej Służby Działań Zewnętrznych oraz specjalne spotkanie, wraz z komisją CONT, z Europejskim Trybunałem Obrachunkowym, poświęcone jego sprawozdaniu specjalnemu nr 09/2021 pt. „Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany".

Komisja specjalna INGE opracowała także plan współpracy z szeregiem komisji PE o kompetencjach częściowo pokrywających się z jej własnymi. Komisja INGE ma jak dotąd 11 komitetów i 11 delegacji.

Wiedza ekspertów zewnętrznych

Komisja Specjalna ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w Unii Europejskiej, w tym Dezinformacji, zwróciła się o udostępnienie zewnętrznej wiedzy eksperckiej w następujących obszarach istotnych dla bieżących prac komisji:

- dezinformacja – mapowanie i rozwiązania, w tym regulacja platform;
- finansowanie – mapowanie i rozwiązania;
- infrastruktura;
- najlepsze praktyki w obejmującym całość społeczeństwa podejściu do przeciwdziałania zagrożeniom hybrydowym;
- wpływ kampanii dezinformacyjnych na migrantów, osoby LGBTI i grupy mniejszościowe;
- wnioski płynące z nadużyć, których dopuszczają się reżimy autorytarne.

Przegląd wysłuchań ekspertów zewnętrznych

Wysłuchania tematyczne

- **Zagrożenia hybrydowe, dezinformacja i polaryzacja – przegląd instytucjonalny**, 24 września 2020 r.
- **Ingerencje w wybory, finansowanie partii politycznych i platformy społecznościowe – przegląd**, 2 października 2020 r.
- **Jak ingerencje zagraniczne podważają suwerenność: przykład naszych wschodnich sąsiadów**, 21 października 2020 r.
- **Obce ingerencje w sferze publicznej: weryfikacja faktów, platformy społecznościowe oraz ich wykorzystanie do celów dezinformacji i obcych ingerencji oraz budowanie odporności**, 26 października 2020 r. i 9 listopada 2020 r.
- **Obce ingerencje w sferze publicznej: zewnętrzna ingerencja w procesy wyborcze, w tym cyberataki, wycieki danych i rozpowszechnianie szkodliwych informacji**, 12 listopada 2020 r.
- **Obce ingerencje w sferze publicznej: finansowanie do celów politycznych za pośrednictwem legalnych lub nielegalnych kanałów i pozornych darczyńców ze źródeł w państwach trzecich**, 2 grudnia 2020 r.
- **Dziennikarstwo przeciwko propagandzie**, 11 grudnia 2020 r.
- **Możliwe groźby ingerencji ze strony państw trzecich w kontekście geopolitycznym**, 25 stycznia 2021 r. i 1 lutego 2021 r.
- **Komunikacja strategiczna w celu przeciwdziałania ingerencjom zagranicznym**, 22 lutego 2021 r.

- **Jak zwiększyć przejrzystość finansowania partii i kampanii politycznych: jakich przepisów potrzebujemy w UE?**, 23 lutego 2021 r.,

- **Demokracja w internecie: jakie są zagrożenia? Jak możemy się przed nimi chronić?**, 17 marca 2021 r.

- **Obce ingerencje w finansowanie organizacji przeciwnych prawu do aborcji w UE**, 25 marca 2021 r.

- **Rozwój technologiczny i podejścia regulacyjne do dezinformacji – ingerencja za pośrednictwem reklamy**, 13 kwietnia 2021 r.

- **Rozwój technologiczny i podejścia regulacyjne do dezinformacji**, 15 kwietnia 2021 r.

- **Wymiana poglądów z Michaiłem Chodorkowskim, założycielem Dossier Center**, 10 maja 2021 r.

- **Wysłuchanie z udziałem serwisów Facebook, Twitter i YouTube w sprawie roli platform społecznościowych w zakresie rozpowszechniania i rozwijania dezinformacji oraz wykrywania i przeciwdziałania jej**, 10 maja 2021 r.

- **Wkład historii, kultury i edukacji w przeciwdziałanie dezinformacji**, 15 czerwca 2021 r.

- **Dezinformacja i dyskryminacja**, 12 lipca 2021 r.

- **Europejski plan działania na rzecz demokracji i akt o usługach cyfrowych oraz inne instrumenty UE: w jaki sposób propozycje te mogłyby chronić procesy demokratyczne w UE przed obcymi ingerencjami oraz dalsze działania**, 2 września 2021 r.

- **Sankcje i zbiorowe środki zaradcze**, 2 września 2021 r.

Wymiana poglądów z

- **Rola edukacji, mediów i kultury w przeciwdziałaniu dezinformacji i obcym ingerencjom**, 9 września 2021 r.

- **Obce ingerencje oraz szpiegowanie europejskich polityków i instytucji**, 9 września 2021 r.

- **Bezpieczeństwo instytucji UE reagowanie na eskalację cyberataków**, 9 września 2021 r.

- **Szkody gospodarcze wynikające z obcych ingerencji i dezinformacji, w tym rynek danych**, 14 października 2021 r.

STANOWISKO MNIEJSZOŚCI WYRAŻONE PRZEZ CLARE DALY W IMIENIU LEWICY

Obca ingerencja wywołuje poważne szkody społeczne i wymaga szczególnej uwagi, ale ani nie jest niczym nowym, ani nie dotyczy wyłącznie Europy. Jednym z najbardziej znaczących i systemowych przykładów ingerencji w procesy demokratyczne w Unii Europejskiej jest znaczna koncentracja kapitału – zarówno zagranicznego, jak i europejskiego – umożliwiająca wywieranie wpływu na stanowienie prawa i kształtowanie polityki.

Nie zostało to w pełni dostrzeżone przez większość w komisji specjalnej INGE, która zamiast tego prowadziła pozornie słuszną narrację na temat Europy padającej ofiarą złośliwych przeciwników geopolitycznych. Dochodzenie wykorzystano do wyolbrzymienia gróźb rosyjskiej i chińskiej ingerencji, zignorowania istotnych przyczyn kryzysu legitymacji politycznej w Europie, napiętnowania sprzeciwu wobec oficjalnej polityki zagranicznej UE oraz uzasadnienia ograniczenia wolności wypowiedzi i innych praw podstawowych bezpieczeństwem.

W sprawozdaniu będącym wynikiem tego podejścia brakuje równowagi i obiektywizmu, a samo w sobie szerzy ono dezinformację. Liczne odniesienia do „wiedzy eksperckiej” pozyskanej z atlantycystycznych i natowskich ośrodków analitycznych, lobbujących na rzecz interesów czerpiących korzyści z konfliktu, należy postrzegać same w sobie jako formę obcej ingerencji. Kierunek polityczny, do którego obrania niniejsze sprawozdanie zobowiązuje Unię, oznacza poważne i długotrwałe szkody dla demokratycznego charakteru społeczeństw europejskich. Potomność będzie żałowała przyjęcia tego dokumentu.

INFORMACJE O PRZYJĘCIU PRZEZ KOMISJĘ PRZEDMIOTOWO WŁAŚCIWĄ

Data przyjęcia	25.1.2022
Wynik głosowania końcowego	+: 25 –: 8 0: 1
Posłowie obecni podczas głosowania końcowego	Vladimír Bilčík, Andrea Bocskor, Ioan-Rareş Bogdan, Jorge Buxadé Villalba, Włodzimierz Cimoszewicz, Gwendoline Delbos-Corfield, Anna Júlia Donáth, Marco Dreosto, Nicolaus Fest, Sunčana Glavak, Raphaël Glucksmann, Markéta Gregorová, Bart Groothuis, Balázs Hidvéghi, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Nathalie Loiseau, Juan Fernando López Aguilar, Morten Løkkegaard, Pierfrancesco Majorino, Lukas Mandl, Thierry Mariani, Dace Melbārde, Maite Pagazaurtundúa, Tonino Picula, Manu Pineda, Robert Roos, Andreas Schieder, Sabine Verheyen, Viola Von Cramon-Taubadel, Javier Zarzalejos
Zastępcy obecni podczas głosowania końcowego	Clare Daly, Petra Kammerevert

GŁOSOWANIE IMIENNE

Głosowanie końcowe – projekt po poprawkach (głosowanie imienne)	+ 25/8/1

WYNIKI GŁOSOWANIA IMIENNEGO

Głosowanie imienne: Głosowanie końcowe

25	**+**
ECR	Dace Melbārde
PPE	Vladimír Bilčík, Ioan-Rareş Bogdan, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Lukas Mandl, Sabine Verheyen, Javier Zarzalejos
Renew	Anna Júlia Donáth, Bart Groothuis, Nathalie Loiseau, Morten Løkkegaard, Maite Pagazaurtundúa
S&D	Włodzimierz Cimoszewicz, Raphaël Glucksmann, Petra Kammerevert, Juan Fernando López Aguilar, Pierfrancesco Majorino, Tonino Picula, Andreas Schieder
Verts/ALE	Gwendoline Delbos-Corfield, Markéta Gregorová, Viola Von Cramon-Taubadel

8	**-**
ECR	Jorge Buxadé Villalba, Robert Roos
ID	Nicolaus Fest, Thierry Mariani
NI	Andrea Bocskor, Balázs Hidvéghi
The Left	Clare Daly, Manu Pineda

1	**0**
ID	Marco Dreosto