

Juliusz Sikorski*

UNIA EUROPEJSKA W OBLICZU AGRESJI KOGNITYWNEJ. BUDOWA SYSTEMU ODPORNOŚCI NA DEZINFORMACJĘ

Streszczenie

Artykuł analizuje działania Unii Europejskiej wobec narastającego zagrożenia dezinformacją i agresją kognitywną. Autor przedstawia ewolucję unijnych mechanizmów przeciwdziałania dezinformacji od powołania East StratCom Task Force, przez działania legislacyjne (DSA, AI Act), po budowanie odporności poznawczej społeczeństw. Wskazuje na znaczenie edukacji medialnej, transparentności platform cyfrowych oraz rolę współpracy z NATO. Artykuł identyfikuje także kluczowe wyzwania, jak fragmentaryczność wdrożeń, ograniczenia instytucjonalne i konieczność lepszej koordynacji. Zwięźleniem analizy jest postulat stworzenia zintegrowanego systemu odporności UE na zagrożenia informacyjne.

Słowa kluczowe: Unia Europejska, dezinformacja, walka kognitywna, odporność systemowa, odporność poznawcza społeczeństw

Wstęp

Od czasu rosyjskiej aneksji Krymu w 2014 roku problem zorganizowanych kampanii dezinformacyjnych i propagandowych stał się jednym z kluczowych wyzwań bezpieczeństwa dla Unii Europejskiej. Dezinformacja, definiowana jako zamierzone rozpowszechnianie fałszywych lub zmanipulowanych informacji w celu wywarcia wpływu na postawy, zachowania lub decyzje, przestała być jedynie zagrożeniem medialnym. Stała się komponentem szerszej strategii destabilizacyjnej, uderzającej w integralność debat publicznych, zaufanie społeczne i fundamenty demokracji.

W odpowiedzi na te wyzwania UE rozpoczęła dyskusję, a w konsekwencji budowę złożonego systemu odporności na zagrożenia informacyjne, obejmującego zarówno działania instytucjonalne, jak i legislacyjne. Kluczową cezurą był marzec 2015 roku, gdy Rada Europejska zainicjo-

* Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim, e-mail: jsikorski@ajp.edu.pl, ORCID: 0000-0002-0579-0158.

wała proces przeciwdziałania wrogim kampaniom manipulacyjnym inspirowanym przez państwa trzecie, w szczególności Federację Rosyjską. Wówczas po raz pierwszy instytucjonalnie uznano dezinformację za zagrożenie dla bezpieczeństwa wspólnoty¹.

Z czasem samą dezinformację zaczęto postrzegać (przede wszystkim w NATO) jako element szerszej strategii określanej mianem walki i wojny kognitywnej, których wyróżniki stanowią:

1. oddziaływanie na umysł jako pole bitwy,
2. wykorzystanie technologii i danych,
3. zacieranie granicy między informacją i dezinformacją,
4. trwałość i głębokość wpływu,
5. wielowymiarowość i skoordynowanie działań².

Ramy teoretyczne

Problem badawczy, który postawił przed sobą autor artykułu, należy sformułować następująco: W jakim stopniu i w jaki sposób instytucje UE budują systemową odporność na agresję kognitywną i prowadzoną w jej zakresie dezinformację oraz jakie są kluczowe bariery i luki w istniejących ramach prawnych i operacyjnych? Tak sformułowane pytanie narzuca niemalże analizę od jakościowej oceny dokumentów legislacyjnych i *case study* kluczowych mechanizmów po identyfikację momentów, w których narzędzia UE (np. East StratCom, DSA, AI Act) wymagają wzmocnienia, by skuteczniej chronić integralność procesu demokratycznego.

W artykule przyjęto paradygmat interpretatywnokrytyczny, w którym dezinformację i odpowiedź na nią traktuje się jako społecznie skonstruowane zjawisko, a jednocześnie poddaje krytycznej analizie asymetrii władzy i wpływu w „walce kognitywnej”. Perspektywa interpretatywna pozwala zrozumieć, w jaki sposób instytucje UE i NATO nadają sens i kształt prawnooperacyjnym narzędziom przeciwdziałania fałszywym narracjom, zaś wrażliwość krytyczna uwypukla potrzebę budowy systemowej odporności, jako mechanizmu niwelującego nierówności informacyjne i chroniącego fundamenty demokracji.

W badaniu zastosowano przede wszystkim metodę jakościowej analizy dokumentów (*desk research*), obejmującą szczegółowe studium aktów

¹ Rezolucja Parlamentu Europejskiego z dnia 21 maja 2013 r. w sprawie Karty praw podstawowych UE: standardy określające wolność mediów w UE (2011/2246(INI)) (2016/C 055/05) (Dz.U. UE C z 2016, nr 55).

² B. Claverie, F. Du Cluzel, *The Cognitive Warfare Concept* [w:] *Cognitive Warfare: The Future of Cognitive Dominance*, red. B. Claverie [i in.], Neuilly-sur-Seine 2022, s. 21–22.

prawnych UE (rezolucji, dyrektyw, rozporządzeń) oraz komunikatów instytucji UE. Uzupełnieniem tej analizy jest podejście studium przypadku, w ramach którego opisano wybrane mechanizmy i narzędzia przeciwdziałania dezinformacji. Dodatkowo wykorzystano analizę chronologiczną, ukazując ewolucję polityki UE od roku 2014 poprzez kolejno przyjmowane ramy prawne i operacyjne. Całość syntezuje podejście interdyscyplinarne, łączące perspektywę prawną, strategiczną i komunikacyjną, co pozwala na zbudowanie spójnego modelu systemowej odporności na agresję kognitywną.

Konsolidacja instytucjonalnych mechanizmów operacyjnych

Jednym z pierwszych i zarazem najważniejszych narzędzi operacyjnych w ramach rozwoju odporności kognitywnej UE było powołanie, jeszcze w 2015 roku, w strukturze Europejskiej Służby Działań Zewnętrznych (ESDZ) zespołu East StratCom Task Force (ESCTF). Zespół ten, m.in. poprzez portal EUvsDisinfo.eu, zajmuje się identyfikowaniem i demaskowaniem prorosyjskich narracji dezinformacyjnych oraz komunikacją strategiczną promującą wartości i działania UE. W krótkim czasie jego działalność została uzupełniona przez kolejne zespoły wyspecjalizowane regionalnie (Bałkany Zachodnie, Bliski Wschód, region Zatoki) oraz poziomo (nowe zagrożenia, analiza danych, polityka i współpraca międzynarodowa)³.

Równolegle rozwijano system analiz i wczesnego ostrzegania. W 2016 roku powołano Komórkę UE ds. Syntezy Informacji o Zagro-

³ W latach 2015–2017 ESCTF nie dysponował własnym budżetem. Dziewięćoosobowy zespół składał się wówczas głównie z wolontariuszy oraz pracowników oddelegowanych z państw członkowskich. Finansowanie pochodziło z ograniczonych środków ESDZ oraz dobrowolnych wkładów państw członkowskich. W roku 2018, dzięki inicjatywie Parlamentu Europejskiego *StratCom Plus*, ESCTF po raz pierwszy otrzymał dedykowane finansowanie z budżetu UE w wysokości 1,1 mln euro rocznie na lata 2018–2020. Dodatkowo ESDZ przyznano 800 tys. euro na komunikację strategiczną. W 2019 roku budżet ESCTF zwiększono do 3 mln euro, choć pierwotnie planowano 5 mln. Zespół liczył wtedy 16 pełnoetatowych pracowników. W 2022 roku budżet przeznaczony na komunikację strategiczną, w tym działania ESCTF, wyniósł już 11 mln euro. Zespół składał się wówczas z 40 ekspertów ds. polityki i języka. W 2024 roku ESCTF dysponował budżetem w wysokości 15 mln euro z tym samym stanem zatrudnienia. *EU action against disinformation*, Eubusiness, <https://www.eubusiness.com>, 5.12.2018 (13.05.2025); A. Legucka, *Countering Russian Disinformation in the European Union*, Polski Instytut Spraw Międzynarodowych, <https://pism.pl>, 6.08.2019 (1.04.2025); S. Lob, *Der schwierige Kampf um die Wahrheit im Ukraine-Krieg*, AFP Faktencheck, <https://faktencheck.afp.com>, 8.02.2023 (21.05.2025); *EU's Stratcom struggles to counter Russian election disinformation*, EUROACTIV, <https://www.euractiv.com>, 4.04.2024 (4.04.2025); J. Sikorski, *Polska w obliczu rosyjskiej ekspansji informacyjnej. Zarys problemów [w:] Rosja w procesie wyzwań – między demokracją a autorytaryzmem*, red. J. Tymanowski, A. Skwariski, N. Moch, Warszawa 2020, s. 169.

zeniach Hybrydowych działającą w ramach Centrum Analiz Wywiadowczych UE powołanej przy ESDZ, której zadaniem jest dostarczanie strategicznych informacji decyzyjnych opartych na danych pochodzących zarówno z otwartych źródeł, jak i wywiadu. Współpracuje ona z unijnym CERT-em, Dyрекcją Wywiadu Wojskowego oraz siecią krajowych punktów kontaktowych ds. zagrożeń hybrydowych. To podejście wieloźródłowe umożliwia formułowanie syntetycznych raportów przekazywanych do instytucji UE i państw członkowskich⁴.

Kolejnym krokiem było przyjęcie przez Parlament Europejski w listopadzie 2016 roku rezolucji dotyczącej komunikacji strategicznej i przeciwdziałania propagandzie stron trzecich. W dokumencie tym podkreślono, że Federacja Rosyjska wykorzystuje różnorodne instrumenty, od fundacji (np. Russkij Mir) i stacji telewizyjnych (RT, Sputnik), po trolle i boty, do tego, by siać dezinformację, podważać wartości demokratyczne i wprowadzać podziały w społeczeństwach europejskich⁵.

W 2017 roku w Helsinkach powołano z kolei Europejskie Centrum Doskonalenia w zakresie Zwalczania Zagrożeń Hybrydowych (Hybrid CoE), które stało się symbolem pogłębiającej się współpracy UE i NATO w zakresie walki z dezinformacją i zagrożeniami hybrydowymi⁶.

Ramy prawno-legislacyjne

W połowie 2017 roku Parlament Europejski (PE) uchwalił kolejną rezolucję, w której odnosił się do problemu dezinformacji, choć sam termin

⁴ Komisja Europejska (KE), Wysoki Przedstawiciel ds. Zagranicznych i Polityki Bezpieczeństwa, Wspólny komunikat do Parlamentu Europejskiego i Rady, Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej, Bruksela, 6.04.2016, JOIN(2016) 18 final, s. 2–6; Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018, Bruksela, 13.06.2018, Join (2018) 14 final, s. 1–2; Joint Staff Working Document „Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats”, Bruksela, 28.5.2019 SWD(2019) 200 final.

⁵ Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2016 roku w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich (2016/2030(INI)) (Dz. Urz. UE C z 2016, nr 224).

⁶ *Wspólny zestaw propozycji w sprawie realizacji wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego [w:] Konkluzje Rady w sprawie realizacji wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego, Bruksela 2016, s. 5.*

nie pada w niej ani razu⁷. Niemniej jednak w dokumencie poświęconym platformom internetowym i jednolitemu rynkowi cyfrowemu, w części zawierającej „wyjaśnienie odpowiedzialności pośredników” umieszczono kilka istotnych i brzemiennych w skutkach zapisów.

Europejskie podejście do dezinformacji cechuje wielopoziomowość i hybrydowość działań, łączy ono mechanizmy samoregulacyjne (np. Kodeks postępowania w zakresie zwalczania dezinformacji podpisany przez platformy cyfrowe), narzędzia legislacyjne (np. RODO w kontekście ochrony danych i profilowania wyborców), działania edukacyjne (promocja umiejętności cyfrowych i medialnych) oraz rozwój partnerstw transatlantyckich i regionalnych. Kluczowym elementem strategii stała się także tzw. odporność poznawcza społeczeństw, definiowana jako zdolność do krytycznego odbioru informacji, rozpoznawania manipulacji i reagowania na nią w sposób racjonalny i odporny na emocjonalne wzbudzenia⁸.

W kwietniu 2018 r. opublikowano komunikat Komisji Europejskiej (KE) do PE zatytułowany *Zwalczanie dezinformacji w Internecie: podejście europejskie*. Wskazano w nim na najważniejsze przyczyny rozprzestrzeniania dezinformacji, takie jak: szybkie zmiany kulturowe, społeczne i gospodarcze, które powodują spadek poczucia bezpieczeństwa i zaufania do instytucji publicznych; transformację sektora mediów oraz wzrost popularności platform internetowych; oraz fakt, że stała się ona skutecznym i tanim narzędziem wpływu na decyzje polityczne⁹.

Komunikat wymienił pięć istotnych obszarów działania w zakresie przeciwdziałania temu zjawisku:

1. bardziej przejrzysty, godny zaufania i odpowiedzialny ekosystem internetowy,
2. bezpieczne i odporne procesy wyborcze,
3. wspieranie edukacji i umiejętności korzystania z mediów,
4. wspieranie wysokiej jakości dziennikarstwa, oraz
5. zwalczanie przez komunikację strategiczną wewnętrznych i zewnętrznych zagrożeń wynikających z dezinformacji¹⁰.

⁷ Rezolucja Parlamentu Europejskiego z dnia 15 czerwca 2017 r. w sprawie platform internetowych i jednolitego rynku cyfrowego (2016/2276(INI)) (Dz. Urz. UE C z 2018, nr 331/19).

⁸ Pluralizm mediów i wolność mediów w Unii Europejskiej. Rezolucja Parlamentu Europejskiego z dnia 3 maja 2018 r. w sprawie pluralizmu mediów i wolności mediów w Unii Europejskiej (2017/2209(INI)) (Dz. Urz. UE C z 2018, nr 41).

⁹ KE, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Zwalczanie dezinformacji w internecie: podejście europejskie, Bruksela, 26 kwietnia 2018 r.

¹⁰ *Ibidem*, s. 8–18.

Następstwem komunikatu było powstanie *Kodeksu postępowania w zakresie zwalczania dezinformacji*, który został opublikowany we wrześniu 2018 roku. Dokument ten to samoregulacja sektora biznesowego. Podkreśla się w nim, że działania w zakresie zwalczania dezinformacji należy podjąć w takich obszarach, jak:

1. transparentność sponsorowanych treści,
2. identyfikacja fałszywych kont i botów,
3. przejrzystość i możliwość weryfikacji algorytmów,
4. dostęp do różnorodnych źródeł informacji, oraz
5. monitoring prowadzony przez instytucje badawcze i władze publiczne¹¹.

Kilka miesięcy później, w grudniu 2018 roku, KE przyjęła plan działania przeciwko dezinformacji. Wskazano w nim na konieczność zwiększenia zdolności instytucji UE do wykrywania, analizowania i ujawniania dezinformacji, zwłaszcza przez rozszerzenie wsparcia dla działających już w UE grup zadaniowych walczących z tym zagrożeniem. Za istotne uznano także wzmocnienie skoordynowanych reakcji na nie przez opracowanie systemu szybkiego ostrzegania przed dezinformacją (Rapid Alert System)¹², który utworzono w marcu 2019 roku¹³.

Pandemia COVID-19 znacząco zwiększyła zagrożenia związane z dezinformacją. Atmosfera strachu i niepewności, która wówczas zapanała, istotnie wpłynęła na podatność społeczeństwa na dezinformację. W internecie masowo rozprzestrzeniano zmanipulowane i nieprawdziwe informacje na temat wirusa, szczepionek, testów oraz innych aspektów związanych z pandemią¹⁴.

W odpowiedzi na to w czerwcu 2020 roku KE opublikowała komunikat zatytułowany *Walka z dezinformacją wokół COVID-19 – dajemy dość do głosu faktom*. Jako kluczowe działanie wskazano w nim wzmocnienie komunikacji strategicznej w UE. Zwrócono także uwagę na konieczność zwiększenia efektywności współpracy pomiędzy instytucjami UE i państwami członkowskimi oraz państwami trzecimi i partnerami międzynarodowymi. Wówczas także powołano Europejskie Obserwatorium Mediów

¹¹ *EU Code of Practice on Disinformation*, European Commission, s. 11–15, 17–19, <https://ec.europa.eu> (6.07.2021).

¹² KE, WPU ds. ZiPB, Wspólny komunikat do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Plan działania na rzecz zwalczania dezinformacji”, JOIN(2018) 36 final, Bruksela 5.12.2018.

¹³ *A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council*, European Council, <https://ec.europa.eu>, 14.06.2019 (5.11.2020).

¹⁴ J. Sikorski, *Social Implications of Infodemic Concurrent with COVID-19*. „Polish Political Science Yearbook”, 2023, vol. 52 (4), s. 79–89.

Cyfrowych (European Digital Media Observatory, EDMO), mające na celu zwiększanie odporności obywateli na dezinformację oraz wyposażanie ich w narzędzia służące edukacji medialnej¹⁵.

Po rozpoczęciu pełnoskalowej wojny Kreml znacząco nasilił kampanie dezinformacyjne wymierzone w Unię Europejską i jej państwa członkowskie, dążąc przede wszystkim do zniechęcenia ich do udzielania wsparcia broniącej się przed inwazją Ukrainy. W ramach tych działań próbowano ukrywać popełniane zbrodnie oraz budować negatywny obraz ofiary agresji w oczach zachodnich społeczeństw. Fałszywe narracje uderzały również w uchodźców, przedstawianych jako osoby niebezpieczne, agresywne i stanowiące zagrożenie dla bezpieczeństwa krajów przyjmujących. Działania te były prowadzone m.in. w mediach społecznościowych, także za pośrednictwem kont wspierających promoskiewską narrację¹⁶.

Kluczową decyzją UE w kontekście walki z tą informacyjną agresją było zakazanie unijnym operatorom nadawania rosyjskich stacji państwowych szerzących dezinformację, m.in. Sputnika, RT, Rossiya RTP, Rossiya 24 oraz TV Centre International. Zakaz został wprowadzony w ramach sankcji i dotyczył wszelkich środków transmisji na terytorium UE, w tym telewizji kablowej, satelitarnej oraz internetowej¹⁷. Niektóre państwa, w tym Polska, Litwa, Łotwa i Estonia, na mocy *Dyrektywy o audiowizualnych usługach medialnych* z 2010 roku, ograniczyły działalność także innych rosyjskich mediów¹⁸.

¹⁵ Europejskie Obserwatorium Mediów Cyfrowych, <https://digital-strategy.ec.europa.eu> (23.05.2025).

¹⁶ E. Kaca, *Zwalczanie w UE rosyjskiej dezinformacji na temat Ukrainy*, Polski Instytut Spraw Międzynarodowych, <https://www.pism.pl>, 5.09.2022; M. Rogalewicz, *Russian Disinformation about Ukrainian Refugees in Poland*, Warsaw Institute, <https://warsawinstitute.org>, 13.05.2022; J. Sikorski, *Świat wg Kremla, czyli mantry rosyjskiej propagandy i dezinformacji wojennej*, Stopfake, <https://www.stopfake.org>, 1.10.2023 (15.07.2025).

¹⁷ E. Kaca, *op.cit.*; *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*, European Council, <https://www.consilium.europa.eu>, 2022; *Zakaz nadawania programów Russia Today i Sputnik*, Urząd Komunikacji Elektronicznej, <https://www.uke.gov.pl>, 2022 (15.07.2025).

¹⁸ Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine; I. Andersone, L. Strauta, *Restrictions on harmful or illegal content and Russian propaganda channels*, European Audiovisual Observatory (Council of Europe), <https://merlin.obs.coe.int>, 2022; *Freedom on the Net 2024 – Estonia*, Freedom House, <https://freedomhouse.org>, 2024; *Freedom in the World 2024 – Lithuania*, Freedom House, <https://freedomhouse.org>, 2024 (15.07.2025).

Wzmocnienie technologiczne i edukacyjne

W marcu 2022 roku Rada UE zatwierdziła *Strategic Compass for Security and Defence* wyznaczający kierunki rozwoju wspólnej polityki bezpieczeństwa i obrony UE do roku 2030. Zadaniem tej strategii jest wzmocnienie koordynacji i zdolności Unii w zakresie przeciwdziałania zagrożeniom informacyjnym, w tym zwiększanie odporności na zagraniczne manipulacje informacyjne. Co szczególne ważne, w dokumencie jednoznacznie zaliczono dezinformację i manipulacje informacjami do głównych zagrożeń hybrydowych, obok cyberataków, sabotażu czy presji energetycznej. Zapowiedziano w nim również wzmacnianie odporności społecznej na tego typu kognitywne agresje, poprzez m.in. edukację medialną, ochronę procesów demokratycznych i wsparcie dla niezależnych mediów. Położono w nim również nacisk na lepszą koordynację działań antydezinformacyjnych w obrębie samej UE, ale również we współpracy z NATO¹⁹.

W dokumencie przewidziano ponadto rozwój dedykowanych mechanizmów szybkiego reagowania na manipulacje informacyjne, ale także zwiększenie wykrywalności i przeciwdziałania zagranicznym wpływom. Wprost zachęca się w nim do stosowania systemów wczesnego ostrzegania oraz kampanii informacyjnych przeciwdziałających fałszywym narracjom, w szczególności pochodzącym z Rosji i Chin. Mało tego, zapowiedziano opracowanie elastycznego zestawu narzędzi (środków i mechanizmów) służących przeciwdziałaniu dezinformacji, tzw. EU Hybrid Toolbox (zestaw narzędzi hybrydowych UE). Z jednej strony, mają one umożliwiać i ułatwiać identyfikację, przeciwdziałanie i reagowanie na zagrożenia hybrydowe, takie jak: dezinformacja, cyberataki, presja gospodarcza, sabotaż, wpływy polityczne wspierane przez państwa trzecie. Z drugiej zaś, muszą integrować działania cywilne i wojskowe, instytucji unijnych, państw członkowskich oraz służb specjalnych. To wszystko ma sprawić, iż nie będą sztywnym zestawem procedur, lecz zbiorem środków, które można będzie dostosowywać do konkretnych sytuacji kryzysowych. Owe narzędzia, mechanizmy i środki mają także być koordynowane z narzędziami i ocenami NATO. Wreszcie powinny wchodzić w skład szerszych ram reagowania kryzysowego UE, obejmujących także wspomniany *Kompas Strategiczny UE*, *Cyber Toolbox* i *Foreign Information Manipulation and Interference Toolbox* (FIMI Toolbox)²⁰.

¹⁹ *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security*, Brussels 2022, s. 7, 11, 21–22.

²⁰ *Ibidem*, s. 27–28, 40–44.

Kompas ów nie tylko identyfikuje dezinformację jako zagrożenie dla bezpieczeństwa, ale także oferuje strategiczne ramy działania, które integrują podejście wojskowe, dyplomatyczne, technologiczne i społeczne. Stanowi także podstawę wspólnej polityki antydezinformacyjnej w ramach szerszego systemu bezpieczeństwa UE, zaś zapowiadany wówczas EU Hybrid Toolbox ma stać się praktycznym narzędziem służącym koordynowaniu i usprawnianiu reakcji na zagrożenia hybrydowe, które trudno byłoby umiejscowić w tradycyjnych ramach wojny i pokoju.

W 2022 r. przyjęto również udoskonalony kodeks postępowania w zakresie dezinformacji, będący rozszerzeniem kodeksu z 2018 roku. Wprowadzono w nim pewne nowości w zakresie samoregulacji sektora biznesowego, ale nade wszystko, jego jakościowy ciężar przesunięto z ogólnych deklaracji na konkretne działania, policzalne zobowiązania i transparentność w walce z dezinformacją. Kluczowe zmiany objęły kilka kwestii:

1. wiążące i bardziej mierzalne zobowiązania,
2. zwiększenie liczby sygnatariuszy (obejmujących platformy cyfrowe, firmy technologiczne, organizacje *fact-checkerskie* oraz reklamodawców),
3. transparentność reklam politycznych w zakresie ich finansowania oraz profilowania,
4. ograniczenie monetyzacji dla kont i stron internetowych rozpowszechniających reklamy zawierające dezinformację,
5. wzmocnienie organizacji *fact-checkingowych* poprzez rozwój współpracy i dostęp do danych i narzędzi platform,
6. zapewnienie dostępu do danych i narzędzi platform dla zweryfikowanych badaczy,
7. rozwój współpracy między platformami poprzez dzielenie się wiedzą i narzędziami w celu efektywniejszej reakcji na zorganizowane kampanie dezinformacyjne, oraz
8. obowiązkową sprawozdawczość i weryfikację skuteczności działań²¹.

Istotną rolę w procesie przeciwdziałania kampaniom dezinformacyjno-propagandowym odgrywa także *Akt o usługach cyfrowych (Digital Services Act, DSA)*, który ostatecznie w całości zaczął obowiązywać od lutego 2024 roku. W tym miejscu należy wspomnieć, iż rok później Komisja i Europejska Rada Usług Cyfrowych w jego ramy włączyła wspomniany już rozszerzony „Kodeks postępowania w zakresie zwalczania dezinformacji”²².

²¹ *The Strengthened Code of Practice on Disinformation*, Brussels 2022. s. 4–6, 9, 26–31, 35–39.

²² *Commission endorses the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act*, European Commission, <https://digital-strategy.ec.europa.eu>, 13.02.2025 (17.07.2025).

Sam DSA zwiększył odpowiedzialność platform, które teraz muszą szybciej usuwać nielegalne treści i przeciwdziałać ich rozpowszechnianiu, skuteczniej chronić użytkowników, nie mogą stosować i tolerować manipulacyjnych interfejsów (*dark patterns*), muszą dbać przejrzystość reklam oraz łatwy dostęp do mechanizmów zgłaszania. Dokumentem powołano także organy nadzorcze oraz wprowadzono wysokie kary za nieprzestrzeganie przepisów (do 6% globalnych przychodów), rozszerzając w ten sposób zakres dotychczasowych przepisów o moderowaniu treści, a przy okazji zapewniając także organom państwowym szerszy dostęp do danych²³.

Przepisy te nie są przełomowe w kontekście walki z dezinformacją, ale mogą przyczynić się do ograniczania tego zjawiska. Platformy internetowe i wyszukiwarki są bowiem zobowiązane do dostosowania swojego systemu rekomendacyjnego tak, aby zapobiegać algorytmicznemu wzmacnianiu dezinformacji. Mają też obowiązek usuwania treści dezinformacyjnych, jeżeli te zostaną w danym państwie członkowskim UE uznane za nielegalne. Jednocześnie w DSA nie wprowadzono prawnej definicji dezinformacji. Mało tego, uznano, iż treści uznawane za nielegalne mogą się różnić w zależności od państwa, podkreślając, iż najważniejsze wyzwanie w tym zakresie związane jest z osiągnięciem równowagi pomiędzy walką z dezinformacją a wolnością słowa²⁴.

W przeciwdziałaniu dezinformacji kreowanej za pomocą sztucznej inteligencji istotną rolę odgrywa *Akt o sztucznej inteligencji (Artificial Intelligence Act, AIA)*²⁵. Wszedł on w życie 1 sierpnia 2024 roku i dotyczy rozwoju systemów AI, wprowadzania ich do obrotu, oddawania do użytku i wykorzystywania. Jego celem jest upowszechnianie sztucznej inteligencji godnej zaufania i ukierunkowanej na człowieka oraz zapewnienie wysokiego poziomu ochrony zdrowia, bezpieczeństwa i praw zapisanych w Karcie Praw Podstawowych UE. Akt ma również wspierać innowacje oraz zapewniać swobodny, transgraniczny przepływ towarów i usług opartych na AI. Dokument wyraźnie uwzględnia zagrożenie dezinformacją jako element ryzyka systemowego, wskazując, iż zaawansowane mo-

²³ Unia Europejska. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) oraz zmiany dyrektywy 2000/31/WE (Dz. Urz. UE L 277, 27.10.2022).

²⁴ *Ibidem*, s. 4, 17, 50–51, 67–68.

²⁵ Unia Europejska. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 roku w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (tekst mający znaczenie dla EOG) (Dz.U. L, 2024/1689, 12.07.2024).

dele AI mogą ułatwiać masowe rozpowszechnianie treści wprowadzających w błąd oraz podważać integralność ekosystemu informacyjnego. Akt nakłada na dostawców obowiązek znakowania generowanych przez AI wyników w formacie odczytywalnym maszynowo i obowiązek transparentności, który wyrażać się musi w informowaniu użytkowników o interakcji z maszyną²⁶.

Wyzwania przyszłości

Dezinformacja stanowi coraz większe zagrożenie dla UE. Rozwój internetu i sztucznej inteligencji sprawił, że docieranie z nieprawdziwymi informacjami do odbiorców jest możliwe na masową skalę. Wobec wzrostu zagrożeń związanych z dezinformacją UE podjęła w czasie ostatniej dekady wiele działań, które mają na celu walkę z tym zjawiskiem, a kolejnych bez wątpienia należy spodziewać się w przyszłości.

Pomimo rozbudowanych działań Unia wciąż boryka się z ograniczeniami instytucjonalnymi. Z wielu analiz wynika bowiem, iż mandat ESDZ ogranicza się wyłącznie do zewnętrznego wymiaru dezinformacji. Tymczasem znaczna część treści dezinformacyjnych, zwłaszcza o tematyce migracyjnej, zdrowotnej czy tożsamościowej, powstaje i krąży wewnątrz UE. Zresztą granica między źródłami „zewnętrznymi” i „wewnętrznymi” staje się coraz bardziej zatarta. Dezinformacja ma przecież już obecnie formę sieciową, transgraniczną, a jej aktorzy są zarówno państwowi, jak i niepaństwowi.

Odpowiedzią na to złożone zjawisko powinno być wypracowanie zintegrowanego systemu odporności poznawczej UE, który połączy monitorowanie treści i sieci, szybkie reagowanie strategiczne, ochronę procesów demokratycznych oraz rozwój edukacji cyfrowej i kultury debaty. Konieczne jest również ciągłe pogłębianie współpracy państw członkowskich oraz zwiększanie transparentności platform cyfrowych, które wzmacniają (na ile świadomie, na ile nie, pozostawiam poza nawiasem tych rozważań) zasięg dezinformacji dzięki mechanizmom wirusowego rozprzestrzeniania treści.

W obliczu dynamicznej ewolucji środowiska informacyjnego oraz coraz bardziej wyrafinowanych form manipulacji UE musi postawić na podejście systemowe i długofalowe, które nie tylko reaguje na zagrożenia, ale wzmacnia strukturalnie odporność demokratycznych społeczeństw na wrogie wpływy poznawcze.

²⁶ *Ibidem*, s. 28, 33.

Zakończenie

Jak się wydaje, przeprowadzona analiza wykazała, iż instytucje UE budują systemową odporność na agresję kognitywną i dezinformację poprzez skonstruowanie wielowarstwowego zestawu narzędzi prawnych i operacyjnych. Z jednej strony podejście oparte na ocenie ryzyka oraz obowiązki przejrzystości umożliwiają wczesne wykrywanie i oznaczanie treści generowanych lub manipulowanych przez AI, z drugiej jednak – dostrzegalne są także bariery ograniczające efektywność tego systemu ze względu na fragmentaryczność wdrożeń w poszczególnych państwach członkowskich, ograniczone zasoby ludzkie i techniczne, a także wyzwania w zakresie interoperacyjności narzędzi i egzekwowania norm w ekosystemie cyfrowym o wysokiej dynamice zmian. Te luki wskazują na potrzebę dalszego zacieśniania koordynacji, inwestycji w rozwój kompetencji cyfrowych oraz wzmocnienia mechanizmów egzekwowania przepisów, tak by UE mogła skuteczniej chronić procesy demokratyczne przed erozją spowodowaną agresją kognitywną państw trzecich.

Bibliografia

- A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council*, European Council, <https://ec.europa.eu>, 14.06.2019 (5.11.2020).
- Andersone I., Strauta L., *Restrictions on harmful or illegal content and Russian propaganda channels*, European Audiovisual Observatory (Council of Europe), 2022, <https://merlin.obs.coe.int>, 2022 (15.07.2025).
- Claverie B., Du Cluzel F., *The Cognitive Warfare Concept* [w:] *Cognitive Warfare: The Future of Cognitive Dominance*, red. B. Claverie [i in.], Neuilly-sur-Seine 2022.
- Commission endorses the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act*, European Commission, <https://digital-strategy.ec.europa.eu>, 13.2.2025 (17.07.2025).
- Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.
- EU action against disinformation*, Eubusiness, <https://www.eubusiness.com/internet>, 5.12.2018 (13.05.2025).
- EU Code of Practice on Disinformation*, European Commission, <https://ec.europa.eu> (6.07.2021).
- EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*, European Council, <https://www.consilium.europa.eu>, 2022 (15.07.2025).
- EU's Stratcom struggles to counter Russian election disinformation*, Euractiv, <https://www.euractiv.com>, 4.04.2024 (4.04.2025).
- Europejskie Obserwatorium Mediów Cyfrowych, <https://digital-strategy.ec.europa.eu> (23.05.2025).

- Freedom in the World 2024 – Lithuania*, Freedom House, <https://freedomhouse.org>, 2024 (15.07.2025).
- Freedom on the Net 2024 – Estonia*, Freedom House, 2024, <https://freedomhouse.org>, 2024 (15.07.2025).
- Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018, Brussels, 13.06.2018, JOIN (2018) 14 final.
- Joint Staff Working Document „Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats”, Brussels, 28.5.2019 SWD(2019) 200 final.
- Kaca E., *Zwalczanie w UE rosyjskiej dezinformacji na temat Ukrainy*, Polski Instytut Spraw Międzynarodowych, <https://www.pism.pl>, 5.09.2022 (15.07.2025).
- Komisja Europejska, Wysoki Przedstawiciel ds. Zagranicznych i Polityki Bezpieczeństwa, Wspólny komunikat do Parlamentu Europejskiego i Rady, Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej, Bruksela, 6.4.2016, JOIN(2016) 18 final.
- Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Zwalczanie dezinformacji w internecie: podejście europejskie, Bruksela 26 kwietnia 2018.
- Komisja Europejska, Wysoki Przedstawiciel Unii ds. Zagranicznych i Polityki Bezpieczeństwa, Wspólny komunikat do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Plan działania na rzecz zwalczania dezinformacji”, JOIN(2018) 36 final, Bruksela 5.12.2018.
- Komisja Europejska, Wysoki Przedstawiciel Unii ds. Zagranicznych i Polityki Bezpieczeństwa, Wspólny komunikat do Parlamentu Europejskiego i Rady: Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej, JOIN(2016) 18 final, Bruksela, 6 kwietnia 2016.
- Legucka A., *Countering Russian Disinformation in the European Union*, Polski Instytut Spraw Międzynarodowych, <https://pism.pl>, 6.08.2019 (1.04.2025).
- Lob S., *Der schwierige Kampf um die Wahrheit im Ukraine-Krieg*, AFP Faktencheck, <https://faktencheck.afp.com>, 8.02.2023 (21.05.2025).
- Parlament Europejski, Directorate-General for External Policies, Policy Department, EU strategic communications with a view to counteracting propaganda, May 2016.
- Rezolucja Parlamentu Europejskiego z dnia 21 maja 2013 r. w sprawie Karty praw podstawowych UE: standardy określające wolność mediów w UE (2011/2246(INI)) (2016/C 055/05) (Dz.U. UE C z 2016, nr 55).
- Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2016 r. w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich (2016/2030(INI)) (Dz. Urz. UE C z 2016, nr 224).
- Rezolucja Parlamentu Europejskiego z dnia 15 czerwca 2017 r. w sprawie platform internetowych i jednolitego rynku cyfrowego (2016/2276(INI)) (Dz. Urz. UE C z 2018, nr 331/19).
- Rezolucja Parlamentu Europejskiego z dnia 3 maja 2018 r. w sprawie pluralizmu mediów i wolności mediów w Unii Europejskiej (2017/2209(INI)) (Dz.U. UE C z 2018, nr 41).
- Rogalewicz M., *Russian Disinformation about Ukrainian Refugees in Poland*. Warsaw Institute, <https://warsawinstitute.org>, 13.5.2022 (15.07.2025).

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) oraz zmiany dyrektywy 2000/31/WE (Dz. Urz. UE L 277, 27.10.2022).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. UE L, 2024/1689, 12.07.2024).
- Sikorski J., *Polska w obliczu rosyjskiej ekspansji informacyjnej. Zarys problemów* [w:] *Rosja w procesie wyzwań – między demokracją a autorytaryzmem*, red. J. Tymanowski, A. Skwarski, N. Moch, Warszawa 2020.
- Sikorski J., *Social Implications of Infodemic Concurrent with COVID-19*. „Polish Political Science Yearbook”, 2023, vol. 52 (4).
- Sikorski J., *Świat wg Kremla, czyli mantry rosyjskiej propagandy i dezinformacji wojennej*, Stopfake, <https://www.stopfake.org>, 1.10.2023 (15.07.2025).
- Unia Europejska. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) oraz zmiany dyrektywy 2000/31/WE (Dz. Urz. UE L 277, 27.10.2022).
- Wspólny zestaw propozycji w sprawie realizacji wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego* [w:] *Konkluzje Rady w sprawie realizacji wspólnej deklaracji Przewodniczącego Rady Europejskiej, Przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego*, Bruksela 2016.
- Zakaz nadawania programów Russia Today i Sputnik*, Urząd Komunikacji Elektronicznej, 2022, <https://www.uke.gov.pl>, 2022 (15.07.2025).

The European Union Confronting Cognitive Aggression. Building Systemic Resilience to Disinformation

Abstract

The article analyzes the European Union's response to the growing threat of disinformation and cognitive aggression. The author outlines the evolution of the EU's counter-disinformation mechanisms – from the establishment of the East StratCom Task Force, through legislative initiatives (such as the DSA and AI Act), to the development of societies' cognitive resilience. The article highlights the importance of media literacy, the transparency of digital platforms, and cooperation with NATO. It also identifies key challenges, including fragmented implementation, institutional limitations, and the need for better coordination. The analysis concludes with a call for an integrated EU resilience system against information threats.

Keywords: European Union, disinformation, cognitive warfare, systemic resilience, cognitive resilience of societies