BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2025
Nr 2 (LIX)

Copyright© 2025 by the Author
Opublikowano w wolnym dostępie (Open Access) na licencji CC BY-NC-ND 4.0

https://doi.org/10.48269/2451-0718-btip-2025-2-009
Data wpłynięcia: 19.05.2025
Data akceptacji: 16.07.2025

Przeciwdziałanie dezinformacji jako element budowania odporności państwa na zagrożenia hybrydowe

Jerzy Gut

gen. bryg. w st. spocz., dr, prof. UAFM, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
https://orcid.org/0000-0002-6682-864X

Zofia Mazur

dr, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
https://orcid.org/0000-0002-1899-4926

Wprowadzenie

Codziennie jesteśmy wręcz bombardowani ogromną ilością informacji: w radiu, telewizji, Internecie czy komunikatorach społecznościowych. Świat mediów, na który jesteśmy skazani, jest obecnie niebezpiecznie „zanieczyszczony" zmanipulowanymi treściami. W przekazach medialnych pojawiają się informacje, które maja charakter propagandy, plotki czy też tzw. twardej dezinformacji, ukierunkowanej na wrzucenie do obiegu konkretnej narracji, która ma celowo wprowadzić w błąd potencjalnych odbiorców i spowodować ich określone zachowania, które będą zgodne z oczekiwaniami autorów tego typu przekazu.

Dezinformacja coraz bardziej przenika wszystkie sfery naszego życia, wywierając istotny wpływ na percepcję i polaryzację społeczeństwa w wielu obszarach. Prowadzi

do podważenia zaufania do instytucji państwowych i polityki rządu, wywołuje chaos i zachęca określone grupy społeczne do określonych działań. Szczególnego znaczenia nabierają treści dezinformacyjne wprowadzane do obiegu w ramach działań hybrydowych[1] przez Federację Rosyjską. Zgodnie ze Strategią Bezpieczeństwa Narodowego to właśnie „[...] Federacja Rosyjska prowadzi działania poniżej progu wojny (o charakterze hybrydowym) [...], podejmuje wszechstronne i kompleksowe działania za pomocą środków pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych"[2].

Publikacja zmanipulowanych treści jest umiejętnie przeplatana z prawdziwymi informacjami, które mają zwiększyć wiarygodność całości przekazu i jednocześnie utrudnić identyfikację ukrytych intencji nadawcy. Wg raportu *Dezinformacja oczami Polaków*, 74% Polaków uważa, że dezinformacja służy do manipulowania opinią społeczną, 57% – że służy do wywołania paniki społecznej, natomiast 56% – że jest dedykowana realizacji interesów politycznych[3].

Identyfikacja dezinformacji nie jest prosta, tym bardziej że autorzy tego procederu potrafią umiejętnie preparować przekaz, zamieszczając w danej treści naprzemiennie informacje prawdziwe i zmanipulowane. Wydaje się, że najprostszą metodą unikania treści dezinformacyjnych jest wybieranie konkretnych źródeł informacji, co do których mamy pewność, że są wiarygodne, lub sprawdzanie tej samej informacji podawanej w innych źródłach. Jednak czynnikami znacznie ograniczającymi tego typu możliwości weryfikacji prawdziwości przekazu są najczęściej towarzyszący nam w życiu deficyt czasowy oraz niepełna świadomość i wiedza w tym obszarze. Dlatego też w proces identyfikacji i przeciwdziałania dezinformacji powinny być zaangażowane wyspecjalizowane instytucje państwowe, których obowiązkiem jest „aktywnie przeciwdziałać dezinformacji poprzez budowę zdolności i stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych"[4]. W tym kontekście, budowanie odporności społeczeństwa i całego państwa na dezinformację nabiera szczególnej wagi, stając się ważnym zadaniem dla rządzących i społeczeństwa.

---

1 Działania hybrydowe to połączenie działań militarnych i niemilitarnych, a także ukrytych i jawnych środków, w tym dezinformacji, ataków cybernetycznych, presji gospodarczej, rozmieszczenia nieregularnych grup zbrojnych i wojsk regularnych. Służy do zatarcia granicy między wojną a pokojem i manipulacji określonych populacji. Ma na celu destabilizację i osłabienie społeczeństw, *NATO's response to hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm [dostęp: 25.03.2025].

2 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, s. 6.

3 *Dezinformacja oczami Polaków. Edycja 2024*, red. P. Mieczkowski, M. Kilian-Grzegorczyk, P. Figurska, Fundacja Digital Poland, Warszawa 2024, s. 5–8.

4 *Strategia Bezpieczeństwa Narodowego...*, *op. cit.*, s. 21, pkt. 5.3.

Celem artykułu jest identyfikacja zagrożeń, jakie niesie za sobą dezinformacja, oraz określenie możliwych sposobów budowania odporności państwa na wrogie działania w tym obszarze. Główne pytanie badawcze sformułowano następująco: Jakie zagrożenia generują działania dezinformacyjne w polskiej przestrzeni medialnej oraz jakie działania należałoby podjąć, aby zwiększyć odporność polskiego państwa na jej destrukcyjne oddziaływanie? Autorzy w procesie badawczym skupili się głównie na gromadzeniu, selekcji, opisie oraz naukowej interpretacji raportów i publikacji poświęconych dezinformacji.

Istota i pojęcie dezinformacji

Czym zatem jest dezinformacja? Najprościej ujmując, to „[...] wprowadzenie kogoś w błąd przez podanie mylących lub fałszywych informacji"[5]. Ważna jest tu celowość działań – zmanipulowana informacja jest przekazywana po to, aby osiągnąć określony efekt, dając odbiorcy wiedzę pozorną, nieprawdziwą, która ma posłużyć do podejmowania błędnych decyzji, korzystnych z punktu widzenia podmiotu dezinformującego, ale niekorzystnych dla odbiorcy zmanipulowanej informacji[6].

Kompleksowe ujęcie pojęcia dezinformacji prezentuje w swoim opracowaniu Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego, która określa dezinformację jako rozpowszechniane informacji całkowicie albo częściowo fałszywej, zmanipulowanej lub wprowadzającej w błąd albo opierającej się na nieetycznych technikach perswazji i dotyczącej kwestii ważnej z punktu widzenia interesu publicznego. Ma ona wywołać niepewność lub wrogość, doprowadzić do polaryzacji albo do zakłócenia procesów demokratycznych. Jest rozpowszechniana lub wzmacniana za pomocą zautomatyzowanych i agresywnych technik, takich jak boty społeczne, sztuczna inteligencja (AI), mikrotargetowanie lub trollowanie przez opłacanych ludzi w celu zwiększenia oddziaływania na społeczeństwo[7]. Podkreślić należy, że dezinformacja charakteryzuje się systematycznością działań, profesjonalnym ich przygotowaniem i organizowaniem oraz konsekwentnym wykorzystaniem środków masowego przekazu[8].

Ponieważ dezinformacja jest pojęciem szerokim i złożonym, w celu pełnego zrozumienia jej istoty i charakteru powinniśmy spojrzeć na to zjawisko nieco szerzej,

---

5 *Dezinformacja*, [hasło w:] *Słownik Języka Polskiego PWN*, https://sjp.pwn.pl/sjp/dezinformacja;2554971.html [dostęp: 25.03.2025].

6 T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2(24), s. 51.

7 Parlament Europejski, Komisja LIBE, *Dezinformacja i propaganda – wpływ na funkcjonowanie państwa prawa w UE i jej państwach członkowskich*, 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864(SUM01)_PL.pdf [dostęp: 30.03.2025].

8 T. Kacała, *op. cit.*, s. 52.

z perspektywy tzw. nieładu (zaburzenia) informacyjnego (*information disorder*). Takie podejście wg Claire Wardle pozwala na postrzeganie tego zjawiska z trzech perspektyw i skategoryzowanie go pojęciowo jako: dezinformację (*disinformation*), misinformację (*misinformation*) i malinformację (*malinformation*). Pierwsza kategoria to dezinformacja związana z celowym ukrywaniem lub manipulacją faktami, mająca spowodować u odbiorcy fałszywe przekonania na dany temat. Wszystko, co zawiera chociaż szczyptę prawdy, jest o wiele skuteczniejsze pod względem przekonywania i angażowania ludzi[9]. Jako przykład może posłużyć wydarzenie z lat 80. XX w., kiedy to Komitet Bezpieczeństwa Państwowego (KGB) przy Radzie Ministrów ZSRR i wschodnioniemieckie Ministerstwo Bezpieczeństwa Państwowego (Stasi) przeprowadziły operację „INFEKTION", aby poprzez niemieckiego biologa Jakoba Segala przekonać społeczeństwo, że wirus HIV został specjalnie stworzony w amerykańskich laboratoriach[10].

Druga kategoria to misinformacja (mylna informacja) – w przeciwieństwie do dezinformacji ma charakter nieumyślny, chociaż przekazywane informacje są fałszywe i wprowadzają potencjalnego odbiorcę w błąd. Związana jest ona z rozpowszechnianiem informacji niedokładnej, będącej wynikiem niezamierzonego ludzkiego błędu lub niedbalstwa. Bezrefleksyjnie udostępniana dezinformacja (gdy osoba udostępniająca nie zdaje sobie sprawy, że jest ona fałszywa lub wprowadzająca w błąd) często staje się misinformacją[11]. Jako przykład może posłużyć wystąpienie na forum ONZ w 2003 r. sekretarza stanu USA Collina Powella, który aby usprawiedliwić atak na Irak, oskarżał Saddama Husajna o posiadanie broni chemicznej i demonstrował fiolkę, w której rzekomo znajdowały się bakterie wąglika. Jak się z czasem okazało, cała ta narracja była nieprawdą, a więc okłamywaniem ONZ i społeczności międzynarodowej. Powell później tłumaczył się tym, że nie wiedział, że dostarczone mu dokumenty zawierały nieprawdziwe informacje[12].

Trzecią kategorią jest malinformacja, która wyróżnia się tym, że informacje są częściowo zgodne z prawdą, a ich celem jest wyrządzenie szkody. Zatem w tym przypadku mówimy o celowym, mylącym przedstawianiu faktów. Przekaz ten jest ukierunkowany na wywołanie w odbiorcy określonych emocji, ponieważ takim przekazem łatwiej się zarządza. Adresat przekazu otrzymuje więc wiadomość prawdziwą – ale jego odczucia będą zgoła inne, niż gdyby otrzymał neutralną i spójną co

---

9 C. Wardle, *Understanding Information Disorder*, 2019, First Draft, https://www.firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701 [dostęp: 30.03.2025].

10 E. Simchayoff, *Operation Infektion*, Medium, 30.07.2020, https://medium.com/lessons-from-history/operation-infektion-a1485fe85443 [dostęp: 30.03.2025].

11 D. Fallis, *What is Disinformation?*, „Library Trends" 2015, t. 63, nr 3, s. 401–402.

12 *Dezinformacja: broń XXI wieku*, ARTE.tv Dokumenty, https://www.youtube.com/watch?v=Nh55Dk7bFbk [dostęp: 30.03.2025].

do treści informację[13]. Jako przykład może posłużyć wykorzystanie przez rosyjską propagandę wybranych żołnierzy pułku Azow – mających na rękach nazistowskie tatuaże – aby promować narrację, że cała Ukraina jest przesiąknięta ideami nazistowskimi. Faktem jest, że pułk Azow istnieje, ale przecież w żaden sposób nie odzwierciedla całej ukraińskiej armii, a tym bardziej poglądów całego społeczeństwa ukraińskiego w tej kwestii.

Te trzy wyszczególnione powyżej kategorie zaburzeń informacyjnych opisują złożoność ekosystemu zjawiska dezinformacji. Ich oddziaływanie będzie różne w zależności od intencji twórcy tego przekazu, obranej formy, a także od osób, które będą przekazywać pozyskaną informacje do innych odbiorców.

Bardzo popularne w języku potocznym stało się określenie *fake news* – używane wtedy, gdy mówimy o fałszywych lub zmanipulowanych wiadomościach. Ponieważ z reguły struktura fałszywej i prawdziwej wiadomości jest niemal identyczna, to przeciętnemu odbiorcy bardzo trudno jest rozróżnić, co jest prawdą, a co fałszem[14].

Szczególnym przykładem dezinformacji jest *deepfake*, coraz częściej pojawiający się w przestrzeni publicznej. Zjawisko to polega na wykorzystaniu możliwości sztucznej inteligencji do tworzenia zmanipulowanych materiałów audio i video. Uzyskane w ten sposób łudząco realistyczne zdjęcia i przekazy filmowe stwarzają możliwość głębokiej manipulacji. Głównym problemem przy identyfikacji *deepfake'ów* jest trudność w rozróżnieniu, czy to, co widzimy, jest prawdą, czy fałszem[15]. Jednym z bardziej spektakularnych przykładów *deepfake'u* jest incydent z marca 2022 r., kiedy w sieci pojawiło się zmanipulowane nagranie z prezydentem Ukrainy Wołodymyrem Zełeńskim, który rzekomo ogłaszał kapitulację kraju i nawoływał do zaprzestania walk. Nagranie okazało się produktem rosyjskiej propagandy – i tylko dzięki szybkiej reakcji ukraińskiego rządu i analizie widocznych na filmie „niedoskonałości" udało się udowodnić jego fałszywość[16].

Należy także zwrócić uwagę na szczególnie niebezpieczną formę dezinformacji w kontekście naszego bezpieczeństwa narodowego, która jest rozprzestrzeniana w postaci dobrze zorganizowanych, zaawansowanych i długofalowych kampanii wymierzonych w określone środowiska na obszarze Polski, Unii Europejskiej czy też NATO. Równie niebezpieczne są kampanie dezinformacyjne organizowane przez

---

13 K. Bąkowicz, *Dezinformacja. Instrukcja obsługi*, CeDeWu , Warszawa 2023, s. 44.

14 M. Palczewski, *Fake news. A continuation or rejection of the traditional news paradigm?*, „Acta Universitatis Lodziensis. Folia Litteraria Polonica" 2017, t. 43, nr 5, s. 23–34, http://dx.doi.org/10.18778/1505-9057.43.02.

15 O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis" 2019, nr 289, „Studia de Securitate" t. 9, nr 3, s. 19–30, https://rep.up.krakow.pl/xmlui/handle/11716/11890 [dostęp: 3.04.2025].

16 M. Chwistek, *Do sieci trafił deepfake z prezydentem Zełenskim. W fałszywym wideo „namawiał" do poddania Ukrainy*, Komputer Świat, 17.03.2022, https://www.komputerswiat.pl/aktualnosci/wydarzenia/do-sieci-trafil-deepfake-z-prezydentem-zelenskim-w-falszywym-wideo-namawial-do/n40qel7 [dostęp: 3.04.2025].

grupy przestępcze, tzw. obce bandery (*foreign flags*), które używają w tym procesie elementów dyplomacji i wysoko zaawansowanej technologii – atakując szeroko pojęty biznes poprzez wykradanie danych, doprowadzanie do upadków firm czy też wpływanie na kursy walut[17].

Dezinformacja – przykłady i zagrożenia

Dezinformacja nie zna granic branżowych i może dotyczyć każdej dziedziny życia, np. bezpieczeństwa publicznego, biznesu, opieki zdrowotnej, nauki czy ochrony środowiska. Działania dezinformacyjne mogą pojawić się wszędzie tam, gdzie autor tych manipulacji będzie widział realne możliwości wpłynięcia na istniejącą rzeczywistość. Poniżej przedstawiono kilka przykładów działań dezinformacyjnych, które pojawiły się w ostatnich kilku latach na obszarze naszego kraju.

Przykładem działania destrukcyjnie wpływającego na organy bezpieczeństwa państwa i dezorganizującego życie publiczne były wydarzenia z maja 2019 r., kiedy to 663 szkoły średnie w Polsce podczas trwania egzaminów maturalnych zostały poinformowane za pośrednictwem poczty elektronicznej o zagrożeniu związanym z podłożeniem bomby. Wszystkie alarmy okazały się fałszywe. W toku podjętych czynności śledczych ustalono, że konta mailowe, z których przekazano fałszywą informację o podłożonych bombach, miały swoje serwery w Sankt Petersburgu i zgodnie z treścią podaną w prasie autorzy tej dezinformacji mieli być powiązani z rosyjskimi służbami specjalnymi[18].

Początek pandemii COVID-19 przyniósł chaos informacyjny, niepewność i lęk. Na temat COVID-19 i szczepionek pojawiło się wiele dezinformacji, z których m.in. dowiadujemy się, że pandemia to kłamstwo, a szczepienia są częścią wielkiego przekrętu, którego celem jest generowanie zysków i manipulowanie ludźmi. Istniejący deficyt zaufania do instytucji publicznych, polaryzacja społeczna oraz brak spójnej polityki informacyjnej rządu został wykorzystany do szerzenia dezinformacji na temat COVID-19 w polskiej przestrzeni medialnej. Takie działania wywoływały dezorientację w społeczeństwie i podkopywały zaufanie do działań rządu. Z pewnością wpłynęły także destrukcyjnie na całokształt działań wymierzonych w zwalczanie tej groźnej pandemii[19].

---

17 *Dezinformacja. Jedno z największych zagrożeń XXI wieku?*, Polskie Radio RDC, https://www.youtube.com/watch?v=cLf4KqffB5g [dostęp: 31.03.2025].

18 *Alarmy bombowe podczas zeszłorocznych matur. Wiadomo, kto za tym stoi*, Polsatnews.pl, 11.05.2020, https://www.polsatnews.pl/wiadomosc/2020-05-11/matury-alarmy-bombowe/ [dostęp: 7.04.2025].

19 *COVID-19 „największym kłamstwem"? To powracająca dezinformacja*, Demagog, 20.08.2024, https://demagog.org.pl/fake_news/covid-19-najwiekszym-klamstwem-powracajaca-dezinformacja/ [dostęp: 7.04.2025].

Podczas największego w historii Polski kryzysu migracyjnego, z jakim mieliśmy do czynienia na granicy polsko-białoruskiej w 2021 r., w przestrzeni medialnej prowadzona była zakrojona na szeroką skalę akcja dezinformacyjna rosyjskich i białoruskich służb specjalnych, opatrzona kryptonimem „Śluza" i będąca elementem planowanej agresji na Ukrainę. Miała ona na celu wykazanie, iż Polska poprzez swoje działania skierowane na zatrzymanie niekontrolowanej masowej migracji na naszej wschodniej granicy państwowej narusza obowiązujące konwencje międzynarodowe i łamie podstawowe prawa człowieka poprzez stosowanie przemocy wobec cudzoziemców[20]. Reżim Aleksandra Łukaszenki sztucznie generował presję migracyjną, by destabilizować sytuację na granicy, szczególnie z Polską i Litwą. Białoruskie służby organizowały przewóz migrantów z Bliskiego Wschodu i Afryki Północnej (wcześniej uproszczono regulacje wizowe, dzięki czemu można było sprowadzić do Europy więcej osób), kolejnym krokiem było zorganizowane kierowanie, a czasami wręcz zmuszanie tych migrantów do nielegalnego przekraczania granicy z Unią Europejską. Dezinformacja wymierzona w nasze państwo była podsycana prowokacjami białoruskich służb, które oskarżały polskich funkcjonariuszy o używanie wobec migrantów środków pirotechnicznych, substancji toksycznych, a także stosowanie tortur i nieludzkiego traktowania. Niestety te działania dezinformacyjne okazały się w wielu obszarach bardzo skuteczne. W polskiej przestrzeni informacyjnej mogliśmy zauważyć wzrastający hejt i ataki na funkcjonariuszy i żołnierzy strzegących granicy. Z perspektywy czasu możemy ocenić, że była to dobrze zaplanowana i przeprowadzona operacja dezinformacyjna, która miała zdyskredytować Polskę na arenie międzynarodowej – oskarżyć ją o nieprzestrzeganie prawa międzynarodowego i brak humanitaryzmu oraz stosowanie „podwójnych standardów". Miało to także osłabić wpływ Polski na politykę wschodnią w ramach NATO i UE[21].

W lutym 2022 r., kiedy Rosja rozpoczęła inwazje na Ukrainę, w polskiej przestrzeni medialnej rozprzestrzeniane były fałszywe informacje, że na polskich stacjach benzynowych kończy się paliwo. W Internecie zaczęły krążyć plotki o braku dostaw paliwa, co spowodowało ogromne kolejki do dystrybutorów, a kierowcy kupowali paliwo na zapas. W obliczu takiego szturmu na stacje paliw, Orlen zdecydował się wprowadzić limity tankowania. Wkrótce potem Instytut Badań Internetu i Mediów Społecznościowych (IBIMS) poinformował, iż w mediach społecznościowych i polskiej sieci został przeprowadzony zmasowany atak dezinformacyjny

---

[20] *Raport Zespołu ds. Dezinformacji*, Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024, Warszawa, 10 stycznia 2025, https://www.gov.pl/web/sprawiedliwosc/raport-zespolu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich [dostęp: 7.04.2025].

[21] F. Bryjka, A. Legucka, *Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego*, „Biuletyn PISM" 2021, nr 212 (2410), https://www.pism.pl/publikacje/dezinformacja-i-propaganda-rosji-oraz-bialorusi-w-kontekscie-polsko-bialoruskiego-kryzysu-granicznego [dostęp: 7.04.2025].

na rzecz Rosji, obejmujący co najmniej trzy zorganizowane grupy – łącznie około 300 fikcyjnych kont. Jak przekazał IBIMS, akcja dezinformacyjna dotarła do około 2 milionów kontaktów. Celem tych działań dezinformacyjnych było wywołanie kryzysu na rynku paliw w Polsce oraz osłabienie polskich przedsiębiorstw działających w tej branży[22].

Również po koniec lutego 2022 r. zaczęły krążyć fałszywe informacje o tym, że banki mają zamiar wprowadzić limity wypłat gotówki w bankomatach w związku z wojną na Ukrainie. Takie działania spowodowały zwiększenie liczby wypłat środków finansowych z bankomatów, co poskutkowało ich późniejszym niedoborem i koniecznością uzupełnienia. Aby uspokoić opinię publiczną, Narodowy Bank Polski i Komisja Nadzoru Finansowego wydały oświadczenia, że w związku z napiętą sytuacją na Ukrainie można spodziewać się wzmożonych działań dezinformacyjnych na terenie Polski, dotyczących np. właśnie dostępności gotówki. Podkreślono również, aby nie rozprzestrzeniać tego typu fałszywych informacji[23].

Kolejnym przykładem szerzenia dezinformacji w polskiej i zagranicznej przestrzeni informacyjnej była publikacja fałszywej statystyki, która pokazywała, że na Ukrainie zginęło 1963 polskich najemników – najwięcej spośród zaprezentowanych dziewięciu nacji. Wykres stwarza pozory materiału pobranego ze Statisty, niemieckiego serwisu zajmującego się wizualizacją danych statystycznych. Po udostępnieniu na platformie X przez anglojęzyczne konto @peacemaket71, wiadomość dotarła do 158 tysięcy odbiorców. Celem tej mistyfikacji było budowanie wizerunku Polski jako aktywnego i agresywnego uczestnika działań zbrojnych na Ukrainie oraz utrwalanie wśród społeczeństwa rosyjskiego i białoruskiego przekonania, że Rosja prowadzi rzekomo „wojnę obronną" przeciwko agresji ze strony Zachodu. Niepokojący jest także fakt rozprzestrzenienia tej fałszywej informacji przez zwykłych użytkowników na komunikatorach takich jak WhatsApp czy Telegram[24].

Tylko na kilku powyższych przykładach możemy zaobserwować rosnący wpływ zjawiska dezinformacji na życie publiczne, niosący w wielu przypadkach poważne skutki dla naszego bezpieczeństwa i komfortu życia.

---

22 M. Szpot, M. Szwarc, *Dezinformacja jako element walki w sieci – prawne aspekty odpowiedzialności karnej w prawie polskim*, SecurityBezTabu.pl, 2.08.2023, https://securitybeztabu.pl/dezinformacja-w-sieci-prawne-aspekty/ [dostęp: 7.04.2025].

23 *Uwaga na dezinformację! Nie będzie limitów na wypłatę gotówki*, CyberDefence24, 25.02.2022, https://cyberdefence24.pl/biznes-i-finanse/uwaga-na-dezinformacje-nie-bedzie-limitow-gotowki-wyplacanej-z-bankow [dostęp: 7.04.2025].

24 T. Dytkowski, *Statystyki o śmierci 1963 polskich najemników w Kursku zostały sfałszowane*, 23.04.2025, FakeNews.pl, https://fakenews.pl/spoleczenstwo/falsz-smierc-1963-polskich-najemnikow-kursk/ [dostęp: 29.04.2025].

Budowanie odporności państwa na dezinformację

Dezinformacja stanowi element wojny hybrydowej i jest niebezpieczną, a zarazem skuteczną bronią, której celem jest polaryzacja i wzbudzanie poczucia zagrożenia w społeczeństwie oraz wpływanie na przebieg procesów demokratycznych. Dlatego też zwiększanie odporności naszego państwa na zjawisko dezinformacji jest zadaniem ważnym i wymagającym priorytetowego traktowania.

Walka z dezinformacją realizowana jest przez instytucje międzynarodowe, takie jak Unia Europejska (UE) i NATO, działania wyspecjalizowanych instytucji na poziomie krajowym oraz wdrażanie programów i kampanii skierowanych bezpośrednio do polskich obywateli. Zasadniczym celem podjętych zabiegów jest uzyskanie elementu synergii i zniwelowanie luk w obszarze dostępności i bezkarnej publikacji dezinformacji w krajowej i międzynarodowej przestrzeni informacyjnej.

Unia Europejska od wielu lat problem dezinformacji w przestrzeni medialnej traktuje jako jedno z istotnych zagrożeń dla bezpieczeństwa państw członkowskich. Rada Europejska po raz pierwszy uznała zagrożenia płynące z internetowych kampanii dezinformacyjnych w 2015 r. W tym samym roku powołano Komórkę UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych (EU Hybrid Fusion Cell), z głównym zadaniem analizy zagrożeń hybrydowych, w tym kampanii dezinformacyjnych. Powołano także Zespół zadaniowy ds. komunikacji strategicznej dla krajów Partnerstwa Wschodniego (East StratCom Task Force). Bardzo szybko powołane podmioty ustaliły, że największe zagrożenie dla Unii Europejskiej stanowi dezinformacja ze strony Federacji Rosyjskiej. Dlatego też 5 grudnia 2018 r. UE ogłosiła Plan działania przeciwko dezinformacji (*Action Plan Against Disinformation*), który zawierał określone przedsięwzięcia do realizacji przez państwa członkowskie[25].

Rewizja ww. Planu nastąpiła w czerwcu 2022 r., kiedy to UE opublikowała wzmocniony Kodeks postępowania w zakresie dezinformacji, podpisany przez 34 różne podmioty (platformy internetowe, wyspecjalizowane firmy z branży reklamowej, instytucje weryfikujące fakty, organizacje badawcze i społeczne). Nowy Kodeks ukierunkowany został na poszerzenie zakresu zobowiązań i środków w celu przeciwdziałania dezinformacji online.

W ramach przyjętego Kodeksu sygnatariusze zobowiązali się do podjęcia m.in. następujących działań[26]:

- podmioty (media) rozpowszechniające dezinformację będą pozbawione korzyści z przychodów z reklam,

---

[25] R. Babraj, *Plan działania przeciwko dezinformacji (Action Plan Against Disinformation)*, NASK Cyber Policy, 17.12.2018, https://cyberpolicy.nask.pl/plan-dzialania-przeciwko-dezinformacji [dostęp:15.04.2025].

[26] *Kodeks postępowania w zakresie zwalczania dezinformacji z 2022 r.*, Komisja Europejska, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation [dostęp: 15.04.2025].

- wdrożenie bardziej transparentnych środków, umożliwiających użytkownikom łatwe rozpoznawanie reklam politycznych poprzez zapewnienie bardziej wydajnego etykietowania, ujawnianie sponsora, wydatków na reklamę i okresu wyświetlania,
- ograniczenie niedozwolonych zachowań manipulacyjnych wykorzystywanych do rozprzestrzeniania dezinformacji (np. fałszywe konta, wzmacnianie oparte na botach, podszywanie się, *deepfake*),
- zobowiązanie platform internetowych do lepszego i szerszego dostępu do danych platform dla pracowników naukowych zajmujących się badaniami nad dezinformacją,
- zobowiązanie platform medialnych do bardziej konsekwentnego korzystania z weryfikacji faktów w swoich usługach.

Przeciwdziałanie dezinformacji także w naszym kraju stało się przedmiotem badań i analiz prowadzonych przez instytucje państwa i podmioty sektora prywatnego. Strategia Bezpieczeństwa Narodowego z 2020 r. wskazuje na dezinformację jako jedno z głównych zagrożeń generowanych przez Federacje Rosyjską, które może prowadzić do destabilizacji struktur państwa i społeczeństwa oraz wywoływania podziałów wśród państw sojuszniczych[27].

W lutym 2022 r. w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK), działającego jako Państwowy Instytut Badawczy, powstał Dział Przeciwdziałania Dezinformacji (DPD), jako pierwsza tego typu jednostka w Polsce. Jego głównym zadaniem jest zbieranie i analiza prób wpływania na nastroje społeczne w Polsce. Od marca 2024 r. przeszedł znaczącą transformację i jego uwaga ma być skierowana na obszar zewnętrznych zagrożeń dla wszystkich instytucji cywilnych w Polsce. Po agresji Federacji Rosyjskiej na Ukrainę w lutym 2022 r. instytucje odpowiedzialne w Polsce za bezpieczeństwo narodowe zwiększyły monitoring mediów społecznościowych w celu wykrywania i przeciwdziałania kampaniom dezinformacyjnym prowadzonym przez zagraniczne podmioty[28]. We wrześniu 2022 r. na poziomie rządowym został powołany Pełnomocnik Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP. Do jego głównych zadań należała identyfikacja i prowadzenie działań zmierzających do neutralizacji zagrożeń dla bezpieczeństwa przestrzeni informacyjnej RP. Jednak w lutym 2024 r. powyższe stanowisko zostało zlikwidowane przez nowy rząd. Jako uzasadnienie podano, że zadania pełnomocnika pełnią w dużej mierze Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT-y) na poziomie MON, GOV i NASK oraz instytucje podległe resortowi cyfryzacji[29].

---

[27] *Strategia Bezpieczeństwa Narodowego..., op. cit.*, s. 21, pkt. 5.3.

[28] *Kim jesteśmy*, NASK, https://archiwum.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html [dostęp: 29.04.2025].

[29] Rozporządzenie Rady Ministrów z dnia 1 lutego 2024 r. w sprawie zniesienia Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej, Dz.U. z 2024 r., poz. 215.

Jedną z kluczowych instytucji w obszarze przeciwdziałania zagrożeniom dezinformacyjnym jest także Rządowe Centrum Bezpieczeństwa (RCB), które opracowuje scenariusze reagowania na różne formy zagrożeń, w tym hybrydowe, które mogą obejmować działania dezinformacyjne.

Pomimo funkcjonujących w kraju wyspecjalizowanych instytucji do przeciwdziałania dezinformacji, raporty dotyczące tej kwestii budzą niepokój. *Raport Zespołu ds. Dezinformacji* Komisji ds. badania wpływów rosyjskich i białoruskich, opublikowany w styczniu 2025 r., stwierdza, że szczególnie w ostatnich kilku latach przeciwdziałanie zagrożeniom dezinformacyjnym przez wyspecjalizowane instytucje państwowe było niewystarczające, niespójne i nie miało charakteru długofalowego i systemowego, a także nie wykorzystywało w sposób wystarczający posiadanego potencjału analitycznego pracowników[30]. Także raport zespołu ekspertów powołanego w ramach Forum Bezpieczeństwa stwierdza, że w Polsce wciąż nie mamy rozwiązań systemowych, które przeciwdziałałyby dezinformacji i ograniczały jej wpływ na społeczeństwo[31].

Podsumowanie

Skuteczna walka z dezinformacją ma kluczowe znaczenie dla konstytucyjnie chronionych wartości: zapewnienia przestrzegania wolności wyrażania poglądów oraz właściwego pozyskiwania i rozpowszechniania informacji. Wyniki prowadzonych badań sytuują Polskę w gronie państw o dużej świadomości zagrożeń powodowanych oddziaływaniem dezinformacji i propagandy, niemniej wskazuje się, że świadomość ta istnieje przede wszystkim wśród wyspecjalizowanych instytucji państwowych i że poziom odporności społeczeństwa na dezinformację i propagandę ciągle wymaga dalszych wysiłków ukierunkowanych na wzmacnianie świadomości i odporności[32].

Na podstawie krytycznego przeglądu literatury przedmiotu, a w szczególności analizy raportów eksperckich, rekomenduje się następujące zasadnicze działania w zakresie poprawy skuteczności zwalczania dezinformacji i budowania odporności państwa w tym obszarze:

- pilne wypracowanie na poziomie rządowym strategii przeciwdziałania dezinformacji i bezpieczeństwa informacyjnego państwa,
- poprawa edukacji społeczeństwa, w tym młodzieży, na wszystkich poziomach nauczania w zakresie rozpoznawania manipulacji i dezinformacji oraz krytycznego

---

30 Raport Zespołu ds. Dezinformacji, *op. cit.*, s. 31–32.

31 *Przeciwdziałanie dezinformacji w Polsce. Rekomendacje systemowe. Raport*, Forum Przeciwdziałania Dezinformacji, Warszawa, 8 grudnia 2022, s. 3, https://ffb.org.pl/wp-content/uploads/2023/02/Raport_Przeciwdzialanie_dezinformacji.pdf [dostęp: 7.05.2025].

32 *Identyfikacja otoczenia i uwarunkowań systemowych administracji publicznej w Polsce w kontekście współpracy z organizacjami pozarządowymi w zakresie przeciw działania rosyjskiej dezinformacji i propagandzie: luki, potrzeby, rekomendacje*, Grupa Defence24, Warszawa 2022, s. 13.

myślenia (zjawisko dezinformacji powinno być traktowane przez nauczycieli przede wszystkim jako problem społeczny, a nie techniczny),

- większe wykorzystanie ośrodków badawczych, szczególnie Polskiego Instytutu Spraw Międzynarodowych, Ośrodka Studiów Wschodnich oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego w zakresie prowadzenia badań naukowych dotyczących zjawiska dezinformacji,
- w celu ułatwienia prawnego zwalczania dezinformacji powinno nastąpić pilne i pełne wdrożenie przez Polskę europejskiego aktu o usługach cyfrowych (*Digital Services Act*) oraz powołanie niezależnego krajowego Koordynatora ds. usług cyfrowych[33],
- podjęcie bardziej zdecydowanych działań w celu lepszego rozpoznawania i przeciwdziałania dezinformacji, w tym wprowadzenie możliwości blokowania i wycofywania treści dezinformacyjnych z przestrzeni medialnej oraz identyfikacji autorów dezinformacji i źródeł ich finansowania,
- wprowadzenie w podmiotach medialnych standardów dotyczących postępowania z informacją – zwłaszcza w zakresie weryfikowania treści informacyjnych,
- poprawa sposobu komunikacji ze społeczeństwem i budowanie jego świadomości dzięki jawnym raportom o działaniach dezinformacyjnych publikowanym przez państwowe instytucje zwalczające tego typu zagrożenia,
- niedopuszczanie przez państwo, szczególnie w sytuacjach kryzysowych, do powstawania luk informacyjnych, które mogą być wykorzystane przez wrogie podmioty.

Kluczem do pomyślnego przeciwdziałania dezinformacji i budowania odporności społeczeństwa w tym obszarze jest wszechstronna współpraca wyspecjalizowanych instytucji państwowych z mediami, platformami internetowymi, dostawcami nowych technologii i – przede wszystkim – edukacja społeczeństwa w tym zakresie na wszystkich poziomach nauczania. Niezbędna jest także efektywna koordynacja przedsięwzięć wszystkich podmiotów zaangażowanych w przeciwdziałanie dezinformacji. Realizacja tych zadań nie będzie łatwa, ponieważ Polska będzie musiała stawić czoła ewoluującym zagrożeniom informacyjnym, które obejmują cyberprzestrzeń i zaawansowane technologie, możliwe ingerencje w wybory oraz wyzwania związane z nielegalną migracją.

---

[33] Polska niestety nie wdrożyła Aktu o usługach cyfrowych ani nie powołała krajowego Koordynatora ds. usług cyfrowych. Zgodnie z unijnym Aktem państwa członkowskie miały czas do 17 lutego 2024 r. na spełnienie wymaganych przepisami zobowiązań, *Polska pozwana do TSUE. Nie wdrożyła unijnego aktu*, Polsatnews.pl, 7.05.2025, https://www.polsatnews.pl/wiadomosc/2025-05-07/polska-pozwana-do-tsue-nie-wdrozyla-unijnej-regulacji/ [dostęp: 10.05.2025].

Bibliografia

Alarmy bombowe podczas zeszłorocznych matur. Wiadomo, kto za tym stoi, Polsatnews.pl, 11.05.2020, https://www.polsatnews.pl/wiadomosc/2020-05-11/matury-alarmy-bombowe/ [dostęp: 7.04.2025].

Babraj R., *Plan działania przeciwko dezinformacji (Action Plan Against Disinformation)*, NASK Cyber Policy, 17.12.2018, https://cyberpolicy.nask.pl/plan-dzialania-przeciwko-dezinformacji [dostęp:15.04.2025].

Bąkowicz K., *Dezinformacja. Instrukcja obsługi*, CeDeWu, Warszawa 2023.

Bryjka F., Legucka A., *Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego*, „Biuletyn PISM" 2021, nr 212 (2410), https://www.pism.pl/publikacje/dezinformacja-i-propaganda-rosji-oraz-bialorusi-w-kontekscie-polsko-bialoruskiego-kryzysu-granicznego [dostęp: 7.04.2025].

Chwistek M., *Do sieci trafił deepfake z prezydentem Zełenskim. W fałszywym wideo „namawiał" do poddania Ukrainy*, Komputer Świat, 17.03.2022, https://www.komputerswiat.pl/aktualnosci/wydarzenia/do-sieci-trafil-deepfake-z-prezydentem-zelenskim-w-falszywym-wideo-namawial-do/n40qel7 [dostęp: 3.04.2025].

COVID-19 „największym kłamstwem"? To powracająca dezinformacja, Demagog, 20.08.2024, https://demagog.org.pl/fake_news/covid-19-najwiekszym-klamstwem-powracajaca-dezinformacja/ [dostęp: 7.04.2025].

Dezinformacja: broń XXI wieku, ARTE.tv Dokumenty, https://www.youtube.com/watch?v=Nh55Dk7bFbk [dostęp: 30.03.2025].

Dezinformacja i propaganda – wpływ na funkcjonowanie państwa prawa w UE i jej państwach członkowskich, Parlament Europejski, Komisja LIBE, 2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864(SUM01)_PL.pdf [dostęp: 30.03.2025].

Dezinformacja. Jedno z największych zagrożeń XXI wieku?, Polskie Radio RDC, https://www.youtube.com/watch?v=cLf4KqffB5g [dostęp: 31.03.2025].

Dezinformacja oczami Polaków. Edycja 2024, red. P. Mieczkowski, M. Kilian-Grzegorczyk, P. Figurska, Fundacja Digital Poland, Warszawa 2024.

Dytkowski T., *Statystyki o śmierci 1963 polskich najemników w Kursku zostały sfałszowane*, 23.04.2025, FakeNews.pl, https://fakenews.pl/spoleczenstwo/falsz-smierc-1963-polskich-najemnikow-kursk/ [dostęp: 29.04.2025].

Fallis D., *What is Disinformation?*, „Library Trends" 2015, t. 63, nr 3, s. 401–426.

Identyfikacja otoczenia i uwarunkowań systemowych administracji publicznej w Polsce w kontekście współpracy z organizacjami pozarządowymi w zakresie przeciw działania rosyjskiej dezinformacji i propagandzie: luki, potrzeby, rekomendacje, Grupa Defence24, Warszawa 2022.

Kacała T., *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2(24), s. 49–65.

Kim jesteśmy, NASK, https://archiwum.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html [dostęp: 29.04.2025].

Kodeks postępowania w zakresie zwalczania dezinformacji z 2022 r., Komisja Europejska, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation [dostęp: 15.04.2025].

NATO's response to hybrid threats, NATO, https://www.nato.int/cps/en/natohq/topics_156338.htm [dostęp: 25.03.2025].

Palczewski M., *Fake news. A continuation or rejection of the traditional news paradigm?*, „Acta Universitatis Lodziensis. Folia Litteraria Polonica" 2017, t. 43, nr 5, s. 23–34, http://dx.doi.org/10.18778/1505-9057.43.02.

Polska pozwana do TSUE. Nie wdrożyła unijnego aktu, Polsatnews.pl, 7.05.2025, https://www.polsatnews.pl/wiadomosc/2025-05-07/polska-pozwana-do-tsue-nie-wdrozyla-unijnej-regulacji/ [dostęp: 10.05.2025].

Przeciwdziałanie dezinformacji w Polsce. Rekomendacje systemowe. Raport, Forum Przeciwdziałania Dezinformacji, Warszawa, 8 grudnia 2022, https://ffb.org.pl/wp-content/uploads/2023/02/Raport_Przeciwdzialanie_dezinformacji.pdf [dostęp: 7.05.2025].

Raport Zespołu ds. Dezinformacji, Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024, Warszawa, 10 stycznia 2025, https://www.gov.pl/web/sprawiedliwosc/raport-zespolu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich [dostęp: 7.04.2025].

Simchayoff E., *Operation Infektion*, Medium, 30.07.2020, https://medium.com/lessons-from-history/operation-infektion-a1485fe85443 [dostęp: 30.03.2025].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Szpot M., Szwarc M., *Dezinformacja jako element walki w sieci – prawne aspekty odpowiedzialności karnej w prawie polskim*, SecurityBezTabu.pl, 2.08.2023, https://securitybeztabu.pl/dezinformacja-w-sieci-prawne-aspekty/ [dostęp: 7.04.2025].

Uwaga na dezinformację! Nie będzie limitów na wypłatę gotówki, CyberDefence24, 25.02.2022, https://cyberdefence24.pl/biznes-i-finanse/uwaga-na-dezinformacje-nie-bedzie-limitow-gotowki-wyplacanej-z-bankow [dostęp: 7.04.2025].

Wardle C., *Understanding information disorder*, 2019, First Draft, https://www.firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701 [dostęp: 30.03.2025].

Wasiuta O., Wasiuta S., *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis" 2019, nr 289, „Studia de Securitate" t. 9, nr 3, s. 19–30, https://rep.up.krakow.pl/xmlui/handle/11716/11890 [dostęp: 3.04.2025].

Akty prawne

Rozporządzenie Rady Ministrów z dnia 1 lutego 2024 r. w sprawie zniesienia Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej, Dz.U. z 2024 r., poz. 215.

Przeciwdziałanie dezinformacji jako element budowania odporności państwa na zagrożenia hybrydowe

Streszczenie

Większość ekspertów postrzega dezinformację jako część wojny hybrydowej, toczącej się na poziomie informacyjnym. Silna kampania dezinformacyjna może doprowadzić do radykalizacji poglądów oraz konfliktu miedzy grupami społecznymi lub mniejszościami narodowymi. Skutki dezinformacji mogą wywoływać polaryzację społeczeństwa, osłabiać wiarygodność instytucji publicznych i obniżać zaufanie społeczeństwa do państwa, a także w określonych okolicznościach wywoływać panikę. Dlatego istnieje konieczność wzmacniania odporności społeczeństwa na manipulacje informacyjne oraz zwiększania zdolności instytucji państwowych dedykowanych przeciwdziałaniu tym zagrożeniom we współpracy z organizacjami pozarządowymi. Celem artykułu jest identyfikacja zagrożeń,

jakie niesie za sobą dezinformacja, oraz określenie możliwych sposobów budowania odporności państwa na wrogie działania w tym obszarze.

Słowa kluczowe: dezinformacja, wojna hybrydowa, fałszywe informacje, budowanie odporności państwa

Countering disinformation as an element of building state resilience to hybrid threats

Abstract

Most experts perceive disinformation as part of hybrid warfare, taking place at the information level. A strong disinformation campaign can lead to radicalization of views and conflict between social groups or national minorities. The effects of disinformation can polarize society, weaken the credibility of public institutions and reduce public trust in the state, and in certain circumstances cause panic. Therefore, there is a need to strengthen society's resilience to information manipulation and increase the capabilities of state institutions dedicated to counteracting these threats in cooperation with non-governmental organizations. The aim of the article is to identify the threats posed by disinformation and to determine possible ways of building state resilience to hostile actions in this area.

Keywords: disinformation, hybrid warfare, fake news, building state resilience