Kamil Jaszczuk[1]

Państwowa Akademia Nauk Stosowanych w Chełmie

https://doi.org/10.29316/9788368103359_10

MECHANIZMY DEZINFORMACJI W MEDIACH SPOŁECZNOŚCIOWYCH I ICH WPŁYW NA BEZPIECZEŃSTWO NARODOWE

MECHANISMS OF DISINFORMATION IN SOCIAL MEDIA AND THEIR IMPACT ON NATIONAL SECURITY

Streszczenie

Celem rozdziału jest analiza mechanizmów dezinformacji funkcjonujących w mediach społecznościowych oraz ocena ich wpływu na bezpieczeństwo narodowe, ze szczególnym uwzględnieniem uwarunkowań Polski i regionu Europy Środkowo-Wschodniej. Sformułowano problem badawczy: w jaki sposób dezinformacja, wykorzystująca narzędzia cyfrowe, algorytmy platform społecznościowych oraz zautomatyzowane i skoordynowane działania aktorów państwowych i niepaństwowych, oddziałuje na odporność informacyjną państwa, procesy demokratyczne

[1] https://orcid.org/0009-0005-5403-514X, kjaszczuk@panschelm.edu.pl

oraz stabilność społeczną. Przyjęto hipotezę badawczą zakładającą, że dezinformacja w mediach społecznościowych stanowi istotny komponent współczesnych działań hybrydowych i realnie zagraża bezpieczeństwu narodowemu poprzez erozję zaufania społecznego, polaryzację opinii publicznej oraz osłabianie zdolności państwa do skutecznego zarządzania kryzysowego. W rozdziale zastosowano metody badawcze, w szczególności analizę literatury przedmiotu, analizę raportów instytucji krajowych i międzynarodowych, studium przypadków wybranych kampanii dezinformacyjnych oraz metodę porównawczą. Główny wniosek z przeprowadzonych badań wskazuje, że skuteczne przeciwdziałanie dezinformacji wymaga zintegrowanego podejścia obejmującego działania edukacyjne, technologiczne, organizacyjne i prawne, a także współpracę państwa, sektora prywatnego i społeczeństwa obywatelskiego w celu wzmacniania odporności informacyjnej państwa.

Słowa kluczowe: dezinformacja, media społecznościowe, bezpieczeństwo narodowe, wojna informacyjna, odporność informacyjna

Abstract

The aim of the chapter is to analyze the mechanisms of disinformation functioning in social media and assess their impact on national security, with particular emphasis on the conditions of Polish and the region of Central and Eastern Europe. The research problem was formulated: how disinformation, using digital tools, algorithms of social platforms and automated and coordinated actions of state and non-state actors, affects the information resilience of the state, democratic processes and social stability. A research hypothesis was adopted assuming that disinformation in social media is an important component of contemporary hybrid activities and poses a real threat to national security by eroding social trust, polarizing public opinion and weakening the state's ability to effectively manage crises. The chapter uses research methods, in particular the analysis of the literature on the subject, the analysis of reports of national and international institutions, a case study of selected disinformation campaigns and a comparative method. The main conclusion of the conducted research indicates that effective counteracting disinformation requires an integrated approach including educational, technological, organizational and legal activities, as well as cooperation between the state, the private sector and civil society in order to strengthen the information resilience of the state.

Keywords: disinformation, social media, national security, information warfare, information resilience

Wstęp

Rozwój technologii informacyjnych i komunikacyjnych na początku XXI wieku doprowadził do zasadniczych przemian funkcjonowania społeczeństw, instytucji, a także państw. Zmienił sposób, w jaki podmioty te zdobywają i przetwarzają informacje. Media społecznościowe, które pierwotnie miały pełnić funkcję demokratyzującą, umożliwiając każdemu obywatelowi udział w debacie publicznej oraz wymianę informacji stały się jednocześnie narzędziem kształtowania opinii publicznej o ogromnym potencjale destabilizacyjnym oraz instrumentem w nowoczesnych strategiach wojny informacyjnej (Bencsik i in., 2023). W dobie globalizacji i powszechnego dostępu do internetu zjawisko dezinformacji urasta do rangi jednego z kluczowych wyzwań dla bezpieczeństwa narodowego i międzynarodowego (Fundacja DigitalPoland, 2024).

W Polsce i regionie Europy Środkowo-Wschodniej zagrożenie dezinformacją nabiera szczególnego znaczenia ze względu na geopolityczne położenie regionu oraz aktywność Federacji Rosyjskiej, która traktuje obok działań wojskowych i ekonomicznych przestrzeń informacyjną jako strategiczny obszar prowadzenia działań hybrydowych. Rosyjska dezinformacja, oparta na starannie zaplanowanych kampaniach propagandowych, ma na celu osłabienie zaufania do instytucji demokratycznych, pogłębianie podziałów społecznych oraz podważanie pozycji Polski w strukturach Unii Europejskiej i NATO.

Zjawisko dezinformacji, choć nie jest nowe, w epoce cyfrowej przybrało zupełnie nowy wymiar. Treści rozprzestrzeniają się znacznie szybciej i skuteczniej niż kiedykolwiek wcześniej. Dzieje się to dzięki algorytmem rekomendacyjnym platform społecznościowych oraz masowym kontom automatycznym. Zasięg i szybkość rozpowszechniania informacji powodują, że manipulacja informacyjna może osiągnąć skalę trudną do opanowania.

Celem niniejszego rozdziału jest analiza mechanizmów dezinformacji w mediach społecznościowych oraz ocena ich wpływu na bezpieczeństwo narodowe ze szczególnym uwzględnieniem doświadczeń Polski i regionu Europy Środkowo-Wschodniej.

Definicja dezinformacji

Pojęcie dezinformacji nie posiada jednoznacznej, powszechnie akceptowanej definicji. W literaturze naukowej często stosuje się je zamiennie z takimi określeniami jak „propaganda" czy „fałszywa informacja", choć w praktyce mogą one oznaczać nieco odmienne zjawiska. Dezinformacja odnosi się zazwyczaj do celowego rozpowszechniania nieprawdziwych lub wprowadzających w błąd treści, mających na celu wywołanie określonych reakcji społecznych lub politycznych.

Warto zauważyć, że samo pojęcie dezinformacji ma swoje korzenie w Rosji. Zarówno w języku, jak i w praktykach politycznych tego państwa. Już w czasach Związku Radzieckiego stosowano zorganizowane działania polegające na szerzeniu fałszywych informacji, mających na celu destabilizację przeciwnika lub manipulowanie opinią publiczną, zarówno wewnątrz kraju, jak i za granicą. Z biegiem lat termin ten zyskał międzynarodowy zasięg i jest dziś powszechnie używany do opisu różnorodnych strategii manipulacji informacją w przestrzeni publicznej, zwłaszcza w kontekście nowoczesnych technologii i mediów cyfrowych (Kaczmarek, 2024).

Dezinformacja jest rozumiana jako celowe, systematyczne wprowadzanie w błąd poprzez tworzenie, rozpowszechnianie lub wykorzystywanie fałszywych bądź zmanipulowanych informacji, mających za zadanie wywołanie określonych reakcji społecznych lub politycznych (Materska, 2007). W literaturze podkreśla się, że dezinformacja różni się od nieświadomego rozpowszechniania nieprawdziwych wiadomości tym, że jest intencjonalna i najczęściej służy interesom określonych podmiotów, państwowych lub pozapaństwowych. To świadome i nieetyczne dążenie do realizacji własnych zamierzeń przy użyciu wszelkich dostępnych środków, w tym także metod niezgodnych z prawem. Takie działania mogą dotyczyć różnych obszarów funkcjonowania państwa będącego celem dezinformacji – zwłaszcza kwestii związanych z bezpieczeństwem. Zarówno obronnością, jak i bezpieczeństwem wewnętrznym, gospodarką (na przykład bezpieczeństwem energetycznym czy dostępem do kluczowych surowców), pozycją międzynarodową (w tym wiarygodnością i możliwościami negocjacyjnymi), a także relacjami między państwem a obywatelami (np. podstawowymi wartościami demokratycznymi, jak przejrzystość życia publicznego czy uczciwość wyborów). Kluczową rolę w tym procesie odgrywa środowisko informacyjne, które

staje się narzędziem wywierania presji na instytucje zarządzające państwem (NASK Państwowy Instytut Badawczy, 2024).

Dezinformacja nastawiona jest na tworzenie zamieszania oraz promowanie wyniku końcowego. Może być ona skierowana do określonej wyimaginowanej grupy odbiorów może zawierać całościowe lub częściowo fałszywe stwierdzenia, a także sensacyjne nagłówki mające na celu przyciągnięcie uwagi (Hetmański, 2003).

Dezinformacja funkcjonuje według podobnych zasad jak reklama. Kluczowe znaczenie mają tutaj emocje, jakie pojawiają się u odbiorcy w momencie zetknięcia się z nową informacją. Uczucia takie jak gniew, smutek, radość czy zaskoczenie sprawiają, że wiele osób nie analizuje źródła ani wiarygodności przekazu, zwłaszcza w środowisku mediów społecznościowych. Charakterystycznym elementem czarnej propagandy w sieci jest nadawanie fałszywej wiarygodności przedstawianym informacjom. Zamiast odwoływać się do autorytetów branżowych lub instytucji państwowych, często stosuje się chwytliwe słowa kluczowe, które mają przekonać odbiorców do prawdziwości przekazu (Urban, 2009).

Internet a co za tym idzie media społecznościowe również ma ogromny wpływ na rozprzestrzenianie dezinformacji i wprowadzanie społeczeństwa w błąd, głównie dzięki swojej globalnej dostępności przez całą dobę oraz szerokiemu zasięgowi oddziaływania. Wystarczy dostęp do sieci, by dotrzeć do niemal każdego miejsca na świecie. Dodatkowo, brak skutecznej weryfikacji publikowanych treści sprawia, że łatwo jest rozpowszechniać nieprawdziwe informacje. Dopóki autorzy fałszywych wiadomości nie złamią wyraźnych zasad obowiązujących na portalach społecznościowych czy serwisach informacyjnych, takich jak zakaz szerzenia nienawiści, przypisywania publicznym osobom nieprawdziwych wypowiedzi, nawoływania do przestępstw czy obrażania uczuć religijnych ich treści rzadko podlegają blokadzie. Nawet jeśli pojawią się sprostowania lub wyjaśnienia, nie zmienia to faktu, że pierwotna dezinformacja nadal krąży po internecie, prowadząc do nieporozumień i sporów wśród użytkowników (Stelmaszczyk, 2023).

Typologia dezinformacji w mediach społecznościowych

Współczesne media społecznościowe stały się jednym z głównych kanałów dystrybucji dezinformacji, co wynika zarówno z ich powszechnej

dostępności, jak i specyfiki mechanizmów komunikacji online (Kmiecik, 2019).

Thomas Aichner oraz Frank. H. Jacob wyróżnili katalog mediów społecznościowych do którego zaliczają się:

1. Blogi – osobiste wpisy komentowane przez innych.
2. Sieci biznesowe – kontakty zawodowe i wymiana doświadczeń.
3. Wspólne projekty – współpraca nad treściami, np. Wikipedia.
4. Fora internetowe – dyskusje tematyczne, brak rozmów w czasie rzeczywistym.
5. Sieci społecznościowe firm – integracja pracowników wewnątrz firmy.
6. Mikroblogi – krótkie, ograniczone wpisy (np. Twitter).
7. Udostępnianie zdjęć – publikowanie i komentowanie fotografii.
8. Recenzje – opinie o produktach i usługach.
9. Social bookmarking – dzielenie się zakładkami (np. Pinterest).
10. Społeczności gier – interakcje graczy online.
11. Portale społecznościowe – tworzenie profili i grup (np. Facebook).
12. Udostępnianie wideo – publikacja i komentowanie filmów.
13. Wirtualne światy – interakcja przez awatary w cyfrowych środowiskach (Aichner, Jacob, 2025).

Warto zwrócić uwagę iż, katalog ten podlega ciągłej ewolucji, w miejsce mniej używanych mediów społecznościowych mogą pojawiać się nowe, cieszące się większą popularnością.

W literaturze przedmiotu oraz licznych raportach badawczych wyróżnia się kilka podstawowych form dezinformacji, które szczególnie często pojawiają się w przestrzeni mediów społecznościowych. Pierwszą i najbardziej rozpoznawalną kategorią są tzw. fake newsy, czyli fałszywe informacje podszywające się pod treści pochodzące z wiarygodnych źródeł (Gov.pl, 2023). Fake newsy mają na celu przede wszystkim wywołanie silnych emocji, takich jak gniew, lęk czy zaskoczenie, a także polaryzację opinii publicznej. Bardzo często są one konstruowane w taki sposób, by wydawały się autentyczne. Wykorzystuje się w tym celu szatę graficzną przypominającą portale informacyjne, powoływanie się na fikcyjnych ekspertów, czy manipulację zdjęciami i nagłówkami. Zjawisko fake newsów jest szczególnie niebezpieczne w okresach zwiększonego napięcia społecznego, na przykład podczas kampanii wyborczych, kryzysów politycznych czy konfliktów

międzynarodowych. Fałszywe wiadomości rozprzestrzeniają się w mediach społecznościowych znacznie szybciej niż rzetelne informacje, co wynika z mechanizmów wiralności oraz algorytmów promujących treści budzące emocje (Raport Cyberprofilaktyka, 2023).

Drugą istotną formą dezinformacji jest propaganda, rozumiana jako długofalowe, systematyczne działania komunikacyjne, których celem jest kształtowanie i zmiana postaw politycznych lub społecznych określonych grup odbiorców. Propaganda nie zawsze wiąże się z przekazywaniem nieprawdziwych informacji. Często polega na selektywnym doborze faktów, manipulacji kontekstem czy powtarzaniu określonych narracji. W mediach społecznościowych propaganda może przyjmować różne formy. Od regularnych publikacji i kampanii informacyjnych, poprzez wykorzystywanie tzw. botów internetowych, aż po współpracę z influencerami czy mikrocelebrytami, którzy świadomie lub nie wzmacniają przekaz propagandowy. Propaganda jest szczególnie skuteczna w środowisku cyfrowym, gdzie łatwo jest dotrzeć do szerokiego grona odbiorców i precyzyjnie targetować przekaz do wybranych grup społecznych (Kaczmarek, 2024).

Kolejną formą dezinformacji jest trolling i hejt, których to w mediach społecznościowych jest coraz więcej. Trolling w przestrzeni internetowej stanowi złożone zjawisko komunikacyjne, polegające na celowym zamieszczaniu prowokacyjnych, obraźliwych bądź wprowadzających w błąd treści, których głównym celem jest wywołanie silnych reakcji emocjonalnych u innych uczestników dyskusji lub zakłócenie jej przebiegu. Osoby dopuszczające się trollingu, określane mianem „trolli", często korzystają z anonimowości oferowanej przez środowisko cyfrowe, co sprzyja eskalacji konfliktów oraz generowaniu chaosu informacyjnego. Trolling może przybierać formy od subtelnych aluzji i ironii, po jawną agresję słowną czy dezinformację. W literaturze przedmiotu podkreśla się, że działania trolli nie zawsze motywowane są rzeczywistą wrogością wobec innych użytkowników, lecz często stanowią formę zabawy, eksperymentowania z tożsamością lub próbę uzyskania poczucia kontroli nad przebiegiem interakcji online. Instrumentalizacja mediów społecznościowych takich jak Twitter, Instagram czy Facebook, doprowadziła do sytuacji, gdzie dla potrzeb walki informacyjnej np. Rosja, korzysta z płatnych usług blogerów oraz tzw. fabryki trolli (Kuczma, 2016). Hejt natomiast, określany również jako mowa nienawiści, odnosi się do wszelkich przejawów agresji słownej, obrażania, poniżania lub wykluczania

osób bądź grup społecznych ze względu na ich cechy indywidualne, światopogląd, pochodzenie czy przynależność do określonej kategorii społecznej. Hejt charakteryzuje się intencjonalnością oraz ukierunkowaniem na konkretnych odbiorców, co często prowadzi do ich stygmatyzacji, wykluczenia społecznego, a w skrajnych przypadkach także do poważnych konsekwencji psychologicznych. Współczesne badania wskazują, że hejt w środowisku internetowym jest zjawiskiem powszechnym i trudnym do zwalczania, m.in. ze względu na szybkie tempo rozprzestrzeniania się treści oraz trudności w identyfikacji sprawców. Zarówno hejt jak i trolling są poważnym zagrożeniem dla bezpieczeństwa państwa, ponieważ mogą prowadzić do destabilizacji sytuacji wewnętrznej, osłabienia zaufania do instytucji publicznych oraz pogłębiania podziałów społecznych (Dziwak, 2019).

Ostatnią wyróżnianą kategorią jest astroturfing, czyli praktyka polegająca na tworzeniu pozornie spontanicznych ruchów społecznych lub inicjatyw oddolnych, które w rzeczywistości są sterowane przez konkretne grupy interesu. Nazwa astroturfing pochodzi od sztucznej trawy (ang. astroturf), co symbolizuje sztuczność tych działań. W praktyce polega to na zakładaniu fałszywych kont w mediach społecznościowych, fałszywych tożsamości, tworzeniu grup dyskusyjnych czy inicjowaniu działań, które mają sprawiać wrażenie autentycznych. Astroturfing jest wykorzystywany zarówno przez podmioty komercyjne, jak i polityczne, a jego celem jest wywarcie wpływu na opinię publiczną poprzez kreowanie iluzji masowego poparcia lub sprzeciwu wobec danej sprawy. Astroturfing jest szczególnie trudny do wykrycia, ponieważ często wykorzystuje zaawansowane techniki ukrywania tożsamości oraz automatyzacji działań (np. boty, farmy trolli) (Gałek, 2022).

Typologia dezinformacji w mediach społecznościowych obejmuje szereg zróżnicowanych zjawisk, które wraz z postępem technologicznym ewaluują i pojawiają się nowe wykorzystujące zawansowane narzędzia sztucznej inteligencji. Łączy je jednak wspólny cel – manipulowanie opinią publiczną i osiąganie określonych korzyści przez twórców tych działań. Różnorodność form i metod stosowanych w przestrzeni cyfrowej sprawia, że przeciwdziałanie dezinformacji jest niezwykle trudne i wymaga zarówno działań edukacyjnych, jak i rozwiązań technologicznych oraz prawnych.

Mechanizmy dezinformacji w mediach społecznościowych

Dezinformacja w mediach społecznościowych jest wspierana przez szereg mechanizmów technologicznych i społecznych, które zwiększają jej skuteczność i skalę oddziaływania. Do najważniejszych należą:

1. Boty to programy komputerowe, których zadaniem jest automatyczne wykonywanie określonych czynności w przestrzeni internetowej. W kontekście dezinformacji są to najczęściej fałszywe, zautomatyzowane konta, które imitują aktywność prawdziwych użytkowników. Ich głównym celem jest wzmacnianie wybranych treści poprzez masowe polubienia, udostępnienia oraz komentowanie postów i artykułów. Dzięki postępowi technologicznemu coraz trudniej odróżnić boty od autentycznych profili, co stanowi poważne wyzwanie dla użytkowników i administratorów portali. Boty działają zazwyczaj w dużych, zorganizowanych grupach – tzw. farmach botów – obejmujących nawet tysiące kont, umożliwiając tym samym szybkie i tanie manipulowanie przekazem na szeroką skalę.
2. Zorganizowane Sieci Trolli są wykorzystywane do masowego rozpowszechniania fałszywych informacji, kreowania sztucznego poparcia dla określonych narracji oraz wzmacniania wybranych przekazów. Troll to rzeczywisty użytkownik mediów społecznościowych, który poprzez swoją aktywność celowo wywołuje konflikty, podziały oraz wzmacnia chaos i zamieszanie, utrudniając prowadzenie merytorycznej dyskusji.
3. Algorytmy rekomendacyjne i bańki informacyjne stosowane przez platformy społecznościowe personalizują przekaz, dostosowując wyświetlane treści do preferencji użytkownika. Prowadzi to do powstawania tzw. baniek informacyjnych, w których odbiorca jest narażony na powtarzające się, często zmanipulowane lub fałszywe komunikaty, wzmacniające jego wcześniejsze przekonania.
4. Manipulacja materiałami wizualnymi – dezinformacja coraz częściej wykorzystuje zmanipulowane zdjęcia, filmy, memy i grafiki, które oddziałują na emocje odbiorców i zwiększają wiarygodność fałszywych informacji (NASK Państwowy Instytut Badawczy, 2024).

5. Astroturfing i sterowane kampanie społeczne. Tworzenie pozornie spontanicznych ruchów i akcji społecznych, które w rzeczywistości są sterowane przez wyspecjalizowane podmioty, pozwala na wywieranie presji na instytucje państwowe oraz kształtowanie opinii publicznej (Gałek, 2022).
6. Targetowanie przekazu. Zaawansowane narzędzia analityczne i reklamowe umożliwiają precyzyjne kierowanie treści do wybranych grup odbiorców, z uwzględnieniem ich przekonań politycznych, zainteresowań czy emocji. To zwiększa skuteczność kampanii dezinformacyjnych, szczególnie w okresach napięć społecznych i politycznych (Fundacja DigitalPoland, 2024).

Wpływ dezinformacji na bezpieczeństwo narodowe

Dezinformacja rozumiana jako intencjonalne wprowadzanie w błąd za pomocą treści cyfrowych stała się jednym z kluczowych wektorów zagrożeń informacyjnych i może prowadzić do szeregu negatywnych skutków dla bezpieczeństwa państwa. Wśród nich wymienia się: destabilizację procesów politycznych, w tym wybory i funkcjonowanie instytucji państwowych; podważanie zaufania społecznego do instytucji publicznych; wzrost polaryzacji społecznej i napięć; osłabienie morale obywateli oraz służb państwowych w sytuacjach kryzysowych; wpływ na decyzje ekonomiczne i polityczne poprzez manipulację opinią publiczną (Kaczmarek, 2024).

Według raportu Digital Poland, ponad 60% Polaków uznaje dezinformację za realne zagrożenie dla stabilności państwa, a 70% dostrzega jej wpływ na bezpieczeństwo narodowe (Fundacja DigitalPoland, 2024). W debacie eksperckiej i w analizach instytucji publicznych coraz częściej ujmuje się ją w szerszej kategorii FIMI (Foreign Information Manipulation and Interference), tj. obcych manipulacji i ingerencji informacyjnych, które oddziałują na procesy polityczne, bezpieczeństwo wewnętrzne oraz odporność społeczną (Bryjka, 2024). W Polsce zagrożenia te są systemowo rozpoznawane m.in. w publikacjach Biura Bezpieczeństwa Narodowego i Rządowego Centrum Bezpieczeństwa, które wiążą dezinformację z hybrydowym charakterem współczesnych konfliktów i koniecznością integracji reakcji

państwa. Zagrożenia te mogą przyjąć różne mechanizmy oddziaływania na bezpieczeństwo państwa:

1) Erozja zaufania i odporności społecznej.

Stała ekspozycja na zmanipulowane treści w mediach społecznościowych obniża zaufanie do instytucji i ekspertów, utrudnia akceptację działań władz w sytuacjach kryzysowych oraz sprzyja polaryzacji. Dane z polskiego badania *„Dezinformacja oczami Polaków 2024"* pokazują, że 79 % respondentów w 2024 roku zetknęła się z fałszywymi informacjami, a zdaniem 81 % z nich, zjawisko ich rozpowszechniania nasiliło się w ciągu minionej dekady. Znaczna część z nich uznała fałszywe informacje za prawdziwe, co ilustruje skalę podatności środowiska informacyjnego (Fundacja DigitalPoland, 2024).

2) Naruszanie integralności procesów demokratycznych.

Media społecznościowe ułatwiają mikrotargetowanie emocjonalnych przekazów i koordynację kampanii wpływu z wykorzystaniem botów, a także kradzionych oraz sfałszowanych kont, co zwiększa ryzyko zakłócania kampanii wyborczych i przebiegu samego głosowania. Polskie analizy wskazują na taktyki stosowane przed wyborami oraz ich nasilenie w ostatnich 72 godzinach poprzedzających wybory. Taka działalność ma charakter manipulacyjny, jest prowadzona w sposób celowy i skoordynowany i może negatywnie wpłynąć na procesy polityczne (Legucka, 2024). Operacje wpływu podważają legitymizację instytucji, osłabiają procesy wyborcze i deliberację publiczną. Rozwarstwienie informacyjne i polaryzacja utrudniają zarządzanie kryzysowe i komunikację ryzyka. (Bryjka, 2024).

3) Integracja z działaniami hybrydowymi.

W perspektywie obronnej dezinformacja stanowi jeden z kluczowych elementów współczesnej walki informacyjnej, ujmowanej jako zorganizowany i celowy proces oddziaływania na percepcję, postawy oraz decyzje odbiorców poprzez manipulowanie zasobami informacyjnymi. W literaturze przedmiotu podkreśla się, że działania dezinformacyjne są ściśle powiązane z realizacją celów militarnych, umożliwiają one m.in. maskowanie rzeczywistych intencji operacyjnych, wprowadzanie przeciwnika w błąd, a także osłabianie morale zarówno sił zbrojnych, jak i społeczeństwa państwa będącego celem ataku (Kaczmarek, 2024).

Analizy prowadzone na łamach „Kwartalnika Bezpieczeństwo Narodowe" oraz w raportach Rządowego Centrum Bezpieczeństwa wskazują, że doświadczenia wyniesione z konfliktu zbrojnego w Ukrainie uwidoczniły nowy wymiar walki informacyjnej, w której cyberprzestrzeń i media społecznościowe stają się areną intensywnych działań propagandowych oraz kampanii dezinformacyjnych. Zjawisko to określa się „szumem informacyjnym", polegającym na celowym zalewaniu przestrzeni publicznej nadmiarem sprzecznych, niezweryfikowanych lub zmanipulowanych przekazów, co utrudnia odbiorcom odróżnienie informacji prawdziwych od fałszywych (Włodyka, 2024).

Wojna w Ukrainie stanowi przykład synergicznego wykorzystania narzędzi cybernetycznych oraz kampanii narracyjnych w mediach społecznościowych, gdzie ataki hakerskie, sabotaż teleinformatyczny oraz szeroko zakrojone operacje dezinformacyjne były ze sobą ściśle skoordynowane. Celem tych działań było nie tylko uzyskanie przewagi operacyjnej na polu walki, ale również destabilizacja zaplecza społeczno-politycznego przeciwnika, wywołanie paniki, a także zdezorganizowanie systemów komunikacji i zarządzania kryzysowego. Połączenie cyberataków, operacji psychologicznych i kampanii narracyjnych w mediach społecznościowych tworzy efekt synergii (Pelc, 2024).

4) Bezpieczeństwo wewnętrzne i porządek publiczny.

Fale dezinformacji dotyczące zdrowia publicznego, migracji czy bezpieczeństwa mogą generować panikę, eskalować napięcia oraz obciążać administrację publiczną i służby. Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK) – w ramach programu *„Przeciwdziałamy dezinformacji"* – dokumentuje metody i taktyki wykorzystywane w Polsce oraz prowadzi działania ostrzegawcze i edukacyjne adresowane do instytucji i obywateli. Z przeprowadzonego badania wynika, że 87% badanych jest przekonanych, że zjawisko dezinformacji wywarło już duży wpływ na życie publiczne w ich kraju (NASK Państwowy Instytut Badawczy, 2024).

5) Nowa dynamika ryzyka: generatywna AI.

Najnowsze analizy z zakresu bezpieczeństwa informacyjnego podkreślają rosnące znaczenie treści syntetycznych – takich jak generowane komputerowo obrazy, nagrania audio oraz materiały wideo w kontekście podatności platform społecznościowych na manipulacje informacyjne. Zjawisko

to jest szczególnie widoczne w świetle dynamicznego rozwoju narzędzi sztucznej inteligencji, które umożliwiają nie tylko automatyzację, ale i znaczące przyspieszenie procesu tworzenia materiałów o wysokim stopniu wiarygodności percepcyjnej. Warto zwrócić szczególną uwagę, że współczesne algorytmy generatywne, które pozwalają na produkcję treści trudnych do odróżnienia od autentycznych, co znacząco utrudnia skuteczną weryfikację źródeł informacji przez użytkowników oraz moderatorów platform społecznościowych. Ponadto, mechanizmy rekomendacyjne tych platform sprzyjają szybkiej i szerokiej dystrybucji syntetycznych materiałów, zwiększając tym samym zasięg potencjalnych kampanii dezinformacyjnych. Niepokojącym aspektem, jest również zagrożenie związane z „uczeniem" modeli sztucznej inteligencji na danych już skażonych dezinformacją. Proces ten może prowadzić do powstawania błędnych lub zniekształconych wzorców decyzyjnych w systemach AI, co w konsekwencji wzmacnia efekt dezinformacyjny poprzez dalszą automatyczną produkcję i dystrybucję fałszywych treści. Oznacza to, że nie tylko użytkownicy, ale także same technologie cyfrowe stają się podatne na manipulacje, co stwarza nowe wyzwania dla systemów bezpieczeństwa informacyjnego państwa (Wójtowicz, 2025).

Przykłady kampanii dezinformacyjnych w Polsce

W ostatnich latach w Polsce wykryto szereg kampanii dezinformacyjnych. Dezinformacja w mediach społecznościowych najczęściej nasila się w okresach podwyższonego napięcia społecznego i politycznego. Szczególnie podatne na manipulację są tematy związane z bezpieczeństwem narodowym, kryzysami migracyjnymi, pandemią oraz konfliktami międzynarodowymi, z których najbardziej znaczące dotyczyły wojny w Ukrainie oraz pandemii COVID-19.

1. Dezinformacja wokół wojny w Ukrainie.

W ciągu dwóch dni poprzedzających rosyjską inwazję na Ukrainę (24 lutego 2022 roku) Instytut Badań Internetu i Mediów Społecznościowych (IBIMS) odnotował znaczący wzrost liczby publikacji w polskiej przestrzeni informacyjnej, których celem było wywołanie poczucia zagrożenia ze strony obywateli Ukrainy. Wśród najczęściej pojawiających się sformułowań

w odniesieniu do Ukrainy dominowały takie zwroty jak „banderowcy", „UPA", „rzeź Polaków" czy „ludobójstwo" (ibims.pl, 2024).

W raporcie Digital Poland opisano zorganizowane kampanie polegające na rozpowszechnianiu fałszywych informacji dotyczących działań wojennych, rzekomych zbrodni ukraińskich żołnierzy oraz zagrożeń związanych z napływem uchodźców. Przykładem były zmanipulowane zdjęcia i filmy publikowane na Facebooku i Twitterze, które miały wywołać strach i niechęć wobec uchodźców oraz podważyć zaufanie do polskich władz. Jednym z istotnych elementów działań dezinformacyjnych, wymierzonych w solidarność społeczeństw Unii Europejskiej z Ukrainą, jest również szerzenie fałszywych narracji dotyczących rzekomo dramatycznej sytuacji gospodarczej państw członkowskich. Przekazy te sugerują, że wsparcie udzielane Ukrainie generuje ogromne koszty, które mają prowadzić do poważnych problemów ekonomicznych całej wspólnoty. W ramach takich kampanii pojawiają się nieprawdziwe informacje o domniemanych planach władz UE, mających na celu na przykład przejmowanie kont bankowych obywateli czy wprowadzanie drastycznych ograniczeń finansowych, rzekomo w odpowiedzi na wydatki związane z pomocą dla uchodźców i wsparciem dla Ukrainy (Wolska, 2024). Tego typu przekazy mają wywoływać niepokój, wzbudzać poczucie zagrożenia oraz zniechęcać do dalszego okazywania wsparcia naszym wschodnim sąsiadom, jednocześnie podważając zaufanie do instytucji unijnych i polityki solidarnościowej.

2. Dezinformacja w okresie pandemii COVID-19.

Według analiz Cyberprofilaktyka.pl, okres pandemii COVID-19 charakteryzował się intensyfikacją działań dezinformacyjnych mających na celu szerzenie fałszywych informacji na temat szczepień, potencjalnych skutków ubocznych oraz różnego rodzaju teorii spiskowych związanych z pochodzeniem i przebiegiem pandemii. W procesie tym wykorzystywano zarówno zautomatyzowane konta, jak i osoby publiczne oraz influencerów, którzy często nieświadomie przyczyniali się do upowszechniania nieprawdziwych treści w mediach społecznościowych (Raport Cyberprofilaktyka, 2023).

Szczególnie aktywne były rosyjskie konta, które już wcześniej zajmowały się propagowaniem postaw antyszczepionkowych oraz negowaniem istnienia wirusa SARS-CoV-2. Profile te wykorzystywały różnorodne techniki manipulacji, by wzmacniać przekaz dezinformacyjny, docierać do szerokiego grona odbiorców i budować atmosferę nieufności wobec oficjalnych

zaleceń zdrowotnych oraz instytucji publicznych. W efekcie tego typu działania przyczyniały się do wzrostu sceptycyzmu wobec szczepień, utrudniały walkę z pandemią i osłabiały społeczną solidarność w obliczu kryzysu zdrowotnego.

3. Dezinformacja w kampaniach wyborczych.

Przypadki rozpowszechniania fałszywych informacji o kandydatach, manipulowania wynikami sondaży oraz szerzenia fake newsów mających na celu polaryzację społeczną i wpłynięcie na decyzje wyborców również pojawiały się w mediach społecznościowych. Przykładem była kampania przed wyborami parlamentarnymi w 2023 roku, podczas której zidentyfikowano zorganizowane sieci trolli publikujące zmanipulowane materiały (Legucka, 2024). Celem takiego ukierunkowanego oddziaływania jest selektywna mobilizacja. – chodzi o to, by zachęcić do udziału w głosowaniu osoby popierające daną partię lub potencjalnie skłonne ją poprzeć, a jednocześnie zniechęcić do udziału wyborców konkurencji. Ma to szczególne znaczenie, ponieważ współczesne kampanie wyborcze coraz rzadziej koncentrują się na przekonywaniu elektoratu do zmiany preferencji partyjnych, a zamiast tego skupiają się przede wszystkim na aktywizowaniu własnych zwolenników oraz demobilizowaniu sympatyków przeciwników (Cześnik, Miśta, Żerkowska-Balas, 2020).

Mikrotargetowanie reklam politycznych stało się głośnym tematem po kampanii prezydenckiej Donalda Trumpa w 2016 roku, kiedy to na Facebooku jednocześnie emitowano dziesiątki tysięcy różnych reklam. Brak przejrzystości sprzyjał nie tylko mobilizacji własnych wyborców, ale też prowadzeniu kampanii negatywnej zniechęcającej potencjalnych zwolenników przeciwnika do udziału w wyborach. Obecnie platformy takie jak Meta i Google umożliwiają bardzo precyzyjne docieranie do użytkowników według wielu kryteriów: demografii, lokalizacji, zainteresowań czy zachowań w sieci. Reklamodawcy mogą też tworzyć własne grupy odbiorców, np. na podstawie wizyt na stronie internetowej lub podobieństwa do wybranych użytkowników. W Polsce podobne praktyki pojawiły się np. podczas kampanii samorządowej w 2018 roku, kiedy na Facebooku powstały strony wyśmiewające kandydatów. Publikowały one reklamy skierowane do konkretnych grup, by zniechęcić je do udziału w głosowaniu. Takie działania, prowadzone poza oficjalnymi kampaniami wyborczymi, budzą wątpliwości związane z przejrzystością i finansowaniem kampanii. Negatywne kampanie

prowadzone przez podmioty niezwiązane oficjalnie z komitetami wyborczymi są problematyczne ze względu na brak kontroli, przejrzystości i możliwość obchodzenia przepisów dotyczących finansowania. W Polsce takie działania nie zdążyły się upowszechnić, ponieważ od 2019 roku Facebook wprowadził obowiązek rejestracji i oznaczania reklam politycznych oraz udostępnił tzw. bibliotekę reklam, co zwiększyło transparentność (Batorski, Izdebski, 2023). Dodatkowo, od wyborów do Parlamentu Europejskiego w 2024 roku, nowe unijne regulacje jeszcze bardziej poprawią przejrzystość reklamy politycznej w sieci (Rozporządzenie Parlamentu Europejskiego i Rady sprawie przejrzystości i targetowania reklamy politycznej, 2021). Ograniczona skala takich działań wynika z kilku czynników: rosnącej przejrzystości, niższych budżetów kampanijnych niż np. w USA oraz rygorystycznych przepisów dotyczących ochrony danych osobowych w Europie. Największym wyzwaniem pozostaje jednak weryfikacja finansowania reklam, ponieważ obecny system sprawozdawczości nie pozwala w pełni kontrolować, czy wszystkie wydatki są prawidłowo rozliczane w kampaniach wyborczych.

Warto zauważyć, że polityczna aktywność w internecie jest niemal nieprzerwana. Kampania wyborcza trwa przez cały czas. Politycy i partie systematycznie prowadzą działania informacyjne i dbają o stałe zwiększanie zasięgów. Liczba obserwujących i poziom zaangażowania użytkowników pozostają wysokie. Przykładowo, od stycznia 2021 do czerwca 2022 roku na Facebooku codziennie reagowało na treści PiS co najmniej 10 tysięcy osób, a Platformy Obywatelskiej – co najmniej 20 tysięcy. Średnio było to odpowiednio niemal 16 tysięcy i 35 tysięcy zaangażowanych użytkowników dziennie (Batorski, Izdebski, 2023).

Systematyczne raporty m.in. Fundacji Batorego czy Rządowego Zespołu ds. Dezinformacji (Gov.pl, 2023) pokazują, jak platformy społecznościowe stają się polem zarówno legalnej komunikacji politycznej, jak i dezinformacji o charakterze kampanijnym.

Narzędzia monitorowania i przeciwdziałania dezinformacji

Polskie instytucje państwowe oraz organizacje pozarządowe wdrażają szereg rozwiązań mających na celu ograniczenie skutków dezinformacji w mediach społecznościowych. NASK, Digital Poland oraz Demagog.org.pl prowadzą systematyczny monitoring mediów społecznościowych,

identyfikując fałszywe informacje, analizując źródła i skalę zjawiska. Użytkownicy, którzy natkną się na podejrzaną informację mają możliwość jej zgłaszania. W raporcie Digital Poland podkreślono znaczenie automatycznych narzędzi analitycznych, które pozwalają na szybkie wykrywanie kampanii dezinformacyjnych i informowanie opinii publicznej o zagrożeniach (Fundacja DigitalPoland, 2024).

Skuteczna walka z dezinformacją wymaga wielowymiarowych działań, wśród których kluczową rolę odgrywa edukacja. Podnoszenie świadomości społecznej na temat zagrożeń związanych z dezinformacją powinno koncentrować się na rozwijaniu krytycznego myślenia, umiejętności oceny wiarygodności źródeł oraz sprawdzania faktów. Istotne jest również wdrażanie programów nauczania, które uczą kompetencji medialnych i pomagają rozpoznawać techniki manipulacji oraz stronniczość przekazów. Ważną rolę w przeciwdziałaniu dezinformacji pełnią same platformy społecznościowe, które zobowiązane są do usuwania fałszywych treści, ograniczania zasięgu kont rozpowszechniających dezinformację oraz współpracy z niezależnymi organizacjami zajmującymi się weryfikacją faktów. Tradycyjne media także powinny wykazywać się odpowiedzialnością, rzetelnie weryfikując informacje przed publikacją. Odpowiedzialność za kształtowanie bezpiecznego środowiska informacyjnego spoczywa także na samych użytkownikach, którzy powinni krytycznie oceniać treści i dbać o wiarygodność przekazywanych informacji. Wreszcie, niezbędne są działania legislacyjne, które ograniczają zasięg dezinformacji, jednocześnie respektując fundamentalne zasady wolności słowa.

Polska aktywnie uczestniczy w międzynarodowych inicjatywach na rzecz przeciwdziałania dezinformacji, współpracując z UE, NATO oraz organizacjami pozarządowymi. W raporcie Biura Bezpieczeństwa Narodowego podkreślono znaczenie wymiany informacji i doświadczeń w zakresie identyfikacji oraz neutralizacji zagrożeń dezinformacyjnych Prawo polskie oraz regulacje unijne przewidują szereg mechanizmów umożliwiających walkę z dezinformacją. Kluczowa jest konieczność dostosowania przepisów do dynamicznie zmieniającego się środowiska cyfrowego oraz na wyzwania związane z egzekwowaniem prawa wobec międzynarodowych korporacji technologicznych.

Podsumowanie

Współczesna dezinformacja w polskich mediach społecznościowych to zjawisko, którego skala i złożoność rosną z każdym rokiem. Nie jest to już tylko problem kilku fałszywych postów czy pojedynczych kont trolli, a systemowy mechanizm wpływania na całe społeczeństwo, mogący podważać zaufanie obywateli do instytucji państwa, procesów wyborczych czy nawet codziennych relacji międzyludzkich. W dobie narzędzi generatywnych, takich jak sztuczna inteligencja zdolna do tworzenia realistycznych tekstów, obrazów czy filmów, granica między prawdą, a fałszem staje się coraz trudniejsza do uchwycenia. To sprawia, że odbiorcy mediów muszą być nie tylko czujni, ale także aktywnie poszukiwać rzetelnych informacji, weryfikować źródła i kwestionować to, co widzą w internecie.

Walka z dezinformacją nie może opierać się wyłącznie na reakcji na poszczególne przypadki. Potrzebne jest systemowe podejście, które zaczyna się od edukacji. Wzmacnianie kompetencji cyfrowych i medialnych powinno być priorytetem zarówno w szkołach, jak i w programach dla osób dorosłych, a szczególnie osób starszych. Społeczeństwo musi nauczyć się rozpoznawać techniki manipulacji, rozumieć mechanizmy działania algorytmów oraz świadomie korzystać z mediów społecznościowych. Tylko wtedy możliwe będzie budowanie odporności na fałszywe przekazy i manipulacje.

Równie ważne jest rozwijanie zaawansowanych narzędzi monitorowania treści w internecie oraz szybkiego reagowania na pojawiające się dezinformacje. Tu kluczowa staje się współpraca między państwem, organizacjami pozarządowymi, sektorem prywatnym i samymi użytkownikami. Instytucje publiczne muszą być otwarte na dialog ze społeczeństwem obywatelskim, wspierać działania fact-checkerów i aktywistów, a także inwestować w technologie wykrywania fałszywych treści.

Wyzwania technologiczne wymagają również nowoczesnych regulacji prawnych, które będą nadążać za zmianami w sposobach rozpowszechniania informacji. Prawo powinno chronić obywateli przed szkodliwymi treściami, nie ograniczając przy tym wolności słowa i dostępu do różnorodnych opinii. To trudna równowaga, ale niezbędna dla zachowania zdrowej debaty publicznej.

Nie można też zapominać o potrzebie prowadzenia systematycznych badań nad mechanizmami dezinformacji. Tylko dzięki pogłębionemu rozumieniu tego zjawiska, zarówno na poziomie technologicznym, jak

i społecznym będzie możliwe przewidywanie nowych zagrożeń i opracowywanie skutecznych strategii przeciwdziałania. Przyszłość walki z dezinformacją zależy od aktywnego zaangażowania wszystkich uczestników życia publicznego, gotowości do uczenia się i adaptacji oraz otwartości na współpracę ponad podziałami.

Literatura

1. Aichner, T., Jacob, F. H. (2015). Measuring the Degree of Corporate Social Media Use. *International Journal of Market Research, 57*(2), 257-276. https://doi.org/10.2501/IJMR-2015-018
2. Batorski, D., Izdebski, K. (2023). *Media społecznościowe i wybory*, Fundacja im. Stefana Batorego.
3. Bencsik, A., Karpiuk, M., Kelemen, M., Włodyka, E. (2023). *Cybersecurity in the Visegrad Group Countries, Institute for Local Self-Government*, Maribor.
4. Bryjka, F. (2024). *Ofensywa dezinformacyjna Rosji przeciwko Ukrainie*, *Biuletyn PISM, 46*(2856).
5. Bryjka, F. (2024). *Podejście UE do zwalczania obcych manipulacji informacyjnych i ingerencji*, Polski Instytut Spraw Międzynarodowych, nr 3.
6. Cześnik, M., Miśta, R., Żerkowska-Balas, M. (2020). Uczestnictwo i mobilizacja w wyborach parlamentarnych 2019 roku, *Studia Socjologiczne, 4*(239), 91-121.
7. Dziwak, E. (2019). Od egalitarności do inkluzywności. Hejt jako następstwo komercjalizacji internetu. *Zeszyty prasoznawcze*, t. *62*, nr 1, Kraków.
8. Fundacja DigitalPoland. (2024). Raport Dezinformacja oczami Polaków. Warszawa.
9. Gałek, B. (2022). Cyfrowy astroturfing jako instrument kreowania procesów politycznych. Zarys problematyki. *Studia Społeczno-Polityczne,* 19/2022, Siedlce.
10. Gov.pl. (b.d). *Rozpoznawanie nieprawdziwych informacji*. Pobrano z: https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych--informacji (dostęp: 20.03.2026).

11. Gov.pl. (2023). *Walka z dezinformacją w mediach społecznościowych: O czym należy wiedzieć?* Pobrano z: https://www.gov.pl/web/5g/walka-zdezinformacja-w-mediach-spolecznosciowych-o-czym-nalezy-wiedziec (dostęp: 20.03.2026).
12. Hetmański, M. (2003). *Społeczny charakter informacji, Społeczeństwo informatyczne, Szansa czy zagrożenie?*, Lublin.
13. Kaczmarek, K. (2024). Konsekwencje dezinformacji: Przegląd wybranych narzędzi i technik manipulacji. *Bezpieczeństwo narodowe*, 2024/45, Koszalin.
14. Kmiecik, P. (2019). *Bezpieczeństwo informacyjne Rzeczypospolitej w dobie fake news – przykłady wykorzystania mediów cyfrowych w szerzeniu dezinformacji*, Warszawa.
15. *Komunikat ws. dezinformacji ws. sytuacji na Ukrainie w internecie, Instytut Badań Internetu i Mediów Społecznościowych*. Pobrano z: https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ (dostęp: 02.11.2025).
16. Kuczma, K. (2016). *Dezinformacja jako instrument zwalczania polskich planów dywersyfikacji źródeł energii*, Securitologia, nr 2.
17. Legucka, A. (2024). Kampanie dezinformacyjne Rosji przed wyborami do Parlamentu Europejskiego. *PISM*, Nr 82 (2892).
18. Materska, K. (2007). *Informacja w organizacjach społeczeństwa wiedz*, Warszawa.
19. NASK Państwowy Instytut Badawczy. (2024). *Zjawisko dezinformacji w dobie rewolucji cyfrowej,* Warszawa.
20. NASK. (2024). *Jak przeciwdziałać dezinformacji? Poradnik dla administracji publicznej*.
21. NASK. (b.d.). *Przeciwdziałym dezinformacji*. https://www.nask.pl/weryfikuje?utm_source (dostęp: 20.03.2026).
22. Pelc, P. (2024). *Cyberprzestrzeń jako element walki informacyjnej – doświadczenie z konfliktu w Ukrainie*, Akademickie Centrum Polityki Cyberbezpieczeństwa, Akademia Sztuki Wojennej.
23. *Rozporządzenie Parlamentu Europejskiego i Rady sprawie przejrzystości i targetowania reklamy politycznej*, 2021.
24. Stelmaszczyk, Ł., Chrząszcz, A. (2023). Zagrożenia w Internecie, *Studia Społeczne*.
25. Urban, A. (2009). *Bezpieczeństwo społeczności lokalnych*, Warszawa.

26. Włodyka, E. M. (2024). *Polaryzacja, kohabitacja czy integracja? Wyzwania dla cyberbezpieczeństwa procesów wyborczych w Polsce*. Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe. Akademia Sztuki Wojennej.
27. Wójtowicz, A. (2025). Wpływ sztucznej inteligencji na dezinformację, *PISM*, NR 63 (3066).
28. Wolska, A. (2024). *Fejk tygodnia: UE jest na krawędzi bankructwa, więc będą zajmowane oszczędności obywateli*, EURACTIV.pl.
29. *Zjawisko dezinformacji w dobie rewolucji cyfrowej*. Raport Cyberprofilaktyka.pl. 2023.