

Jak przeciwdziałać dezinformacji?

Poradnik dla administracji publicznej



NASK

Jak przeciwdziałać dezinformacji?

Poradnik dla administracji publicznej

NASK

Autorzy

Sylwia Adamczyk
Katarzyna Dziąg
Aleksandra Michałowska-Kubś
Bohdan Pawłowicz
Iwona Prószyńska
Aleksandra Wójtowicz

Wsparcie

Andrzej Kozłowski

Redakcja

Katarzyna Nakonieczna

Koordinacja

Anna Pudłowska

Opracowanie graficzne

Alicja Kaim

ISBN: 978-83-65448-93-4

Licencja udostępniania:

CC BY-NC 4.0



SPIS TREŚCI

5 WSTĘP

7 PODSTAWOWE POJĘCIA

10 CZĘŚĆ I: DEZINFORMACJA W PRZESTRZENI PUBLICZNEJ

11 1.1. Podatność na dezinformację i zagrożenia dla sfery publicznej

14 1.2. Rola platform społecznościowych w rozprzestrzenianiu dezinformacji

15 1.2.1. Algorytmy

16 1.2.2. Boty i trolle

18 1.2.3. Odpowiedzialność za rozpowszechnianie dezinformacji

19 1.3. Aktorzy dezinformacji

22 1.4. Zagraniczne manipulacje informacjami i ingerencje w informację (FIMI)

29 1.5. Wybrane metody i techniki dezinformacji

40 CZĘŚĆ II: STRATEGIE REAGOWANIA NA DEZINFORMACJĘ

41 2.1. Prebunking, debunking, fact-checking

46 2.2. Reagowanie na fałszywe treści w bieżącej komunikacji

48 CZĘŚĆ III: KOMUNIKACJA W OBLICZU KRYZYSU

49 3.1. Komunikacja w samorządach

49 3.1.1. Cele komunikacji

50 3.1.2. Monitorowanie i ewaluacja działań komunikacyjnych

50 3.2. Reagowanie na dezinformację

57 BIBLIOGRAFIA

WSTĘP

Raport Światowego Forum Ekonomicznego o ryzykach globalnych z 2024 roku (Global Risk Report 2024) w perspektywie najbliższych dwóch lat wskazuje dezinformację jako największe zagrożenie dla gospodarki światowej i społeczeństwa. Następne miejsca na liście zajmują: ekstremalne zjawiska pogodowe, polaryzacja społeczna, zagrożenia w cyberprzestrzeni i konflikty zbrojne. Raport zwraca uwagę, że zjawisko dezinformacji eskaluje wraz z rozwojem i popularyzacją coraz bardziej zaawansowanych technologii i osłabianiem zaufania do informacji i instytucji. Zdaniem autorów/autorek raportu, w ciągu najbliższych dwóch lat aktorzy dezinformacyjni będą wykorzystywać syntetyczne treści (generowane automatycznie) by wzmacniać podziały społeczne, przemoc ideologiczną i represje polityczne, a podejmowane przez państwa regulacje dotyczące sztucznej inteligencji, nie będą nadążać za jej rozwojem. Autorzy/autorki spodziewają się także, że niektóre rządy, stojąc przed dylematem, czy zapobiegać dezinformacji, czy chronić wolność słowa, będą działać zbyt wolno¹.

Dezinformacja wiąże się z poważnymi konsekwencjami dla różnych obszarów: życia społecznego, zdrowia publicznego, państwa i jego struktur, a także polityki oraz biznesu. Pogłębia istniejące podziały i utrwala antagonizmy, wpływa na procesy wyborcze i podważa zaufanie do instytucji. Blokując przepływ rzetelnych treści, utrudniając podejmowanie świadomych decyzji. Wprowadza chaos i destabilizację. Wyrządza szkody wizerunkowe i finansowe. Jednocześnie całkowite wyeliminowanie dezinformacji nie jest możliwe. Istnieją jednak sposoby, by jej przeciwdziałać. Jednym z nich jest wzmacnianie świadomości na temat tego zjawiska. Jest to główny cel tego poradnika.

Niniejsze opracowanie prezentuje podstawowe pojęcia z zakresu dezinformacji, objaśnia jej oddziaływanie na społeczeństwo, przedstawia jej aktorów i omawia zagraniczne wpływy w polskiej przestrzeni

1 World Economic Forum (2024). Global Risks Report 2024, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf [dostęp: 05.07.2024 r.]

informacyjnej. Kładąc nacisk na praktyczny wymiar, prezentuje przykłady zagrożeń, a także metody reagowania oraz elementy komunikacji strategicznej, uwzględniające w szczególności potrzeby jednostek samorządu terytorialnego.

Poradnik ma dostarczyć praktycznych wskazówek dotyczących budowania odporności na dezinformację – zarówno w wymiarze indywidualnym, jak i publicznym.

PODSTAWOWE POJĘCIA

Dezinformacja

Fatszywa bądź wprowadzająca w błąd treść, która jest celowo, intencjonalnie tworzona lub rozpowszechniana z zamiarem oszukania odbiorców/odbiorczyń bądź pozyskania określonych korzyści, np. ekonomicznych, politycznych. Dezinformacja może wyrządzić szkodę zarówno jednostkom, grupom, organizacjom, jak i krajom.

Misinformacja

Fatszywa bądź wprowadzająca w błąd treść, która jest tworzona bądź rozpowszechniana bez złych zamiarów, świadomości jej nieprawidłowości – w wyniku pomyłki, lub błędnego przekonania na dany temat. Kluczową różnicą między dezinformacją i misinformacją jest intencja. Warto podkreślić, że misinformacja również może prowadzić do szkodliwych konsekwencji.

Malinformacja

To rodzaj zakłócenia w sferze informacyjnej, w którym wykorzystywane są prawdziwe treści, ale w złej intencji – z zamiarem wyrządzenia szkody, manipulacji. Może to być ujawnienie poufnych informacji w domenie publicznej, publikowanie bądź rozpowszechnianie treści prywatnych, intymnych bez zgody osoby lub instytucji, której dotyczą.

Bot

Bot to automatyczny program, który może wykonywać określone zadania. W kontekście dezinformacji boty rozumiane są głównie jako fałszywe, zautomatyzowane konta, profile, które naśladują ludzkie zachowanie i są wykorzystywane do wzmacniania określonych treści poprzez ich polubienia, udostępnienia, a także komentowanie postów czy artykułów. Wraz z rozwojem technologii rozróżnienie takich kont od profili prawdziwych użytkowników/użytkowniczek staje się coraz większym wyzwaniem. Boty zwykle są wykorzystywane w grupach – nazywanych farmami botów – liczących niekiedy nawet tysiące kont. W rezultacie pozwalają na szybką, a w dodatku taną, manipulację danymi treściami w znaczącym stopniu i na dużą skalę.

Troll

To prawdziwa osoba, użytkownik/użytkowniczka, która swoją aktywnością, zwłaszcza w mediach społecznościowych, prowokuje konflikty, podziały, potęguje chaos i zamieszanie oraz zaburza rzeczową dyskusję. Zorganizowane grupy trolli – nazywane armiami bądź fabrykami – mogą być wykorzystywane do określonych celów geopolitycznych, politycznych lub innych.

**Bańka filtrująca/
informacyjna**

To zjawisko powstające w wyniku działania algorytmów danej witryny internetowej, platformy mediów społecznościowych, które w połączeniu z aktywnością użytkownika/użytkowniczki, dostarczają mu głównie treści wyselekcjonowane i zgodne z jego przekonaniami i światopoglądem. W rezultacie użytkownik/użytkowniczka rzadko ma styczność z materiałami przedstawiającymi odmienny punkt widzenia, co ogranicza jego/jej dostęp do szerszego kontekstu oraz utrudnia zrozumienie innych opinii i perspektyw.

Komora echa

To rodzaj zamkniętego „ekosystemu”, kręgu komunikacyjnego, w którym użytkownicy/ użytkowniczki wymieniają się podobnymi poglądami, poszukują treści potwierdzających ich przekonania i wzmacniają je. Często jest to konsekwencja istnienia baniek informacyjnych.

Manipulacja

To naginanie lub przeinaczanie treści w celu udowodnienia swoich racji lub wpływania na cudze poglądy i zachowania. Treści manipulacyjne nie są wprost fałszywe, lecz zawierają stwierdzenia niepełne, prezentowane w błędnym kontekście, czy wyselekcjonowane, by udowodnić obraną tezę, ignorujące szerszy obraz.



CZĘŚĆ I

Dezinformacja w przestrzeni publicznej

1.1. Podatność na dezinformację i zagrożenia dla sfery publicznej

Podatność na dezinformację jest złożonym zjawiskiem, które wynika z wielu różnych czynników. Należy do nich m.in. brak odpowiedniej edukacji medialnej i świadomości na temat fałszywych lub wprowadzających w błąd treści i płynących z nich zagrożeń. Takim czynnikiem bywa również brak dostępu do rzetelnych informacji. Nie można także pominąć przyczyn psychologicznych, które wpływają na to, jak przyswajamy docierające do nas treści – badacze/badaczki wskazują na różne aspekty oceny prawdziwości informacji przez odbiorców/odbiorczynie. Bardzo ważne są w tym kontekście emocje, które mogą wpływać na zniekształcenie percepcji i obniżenie zdolności krytycznego myślenia².

Istnieje pięć elementów wymienianych jako kluczowe dla oceny, czy informacja jest prawdziwa³. Są to:

1. KOMPATYBILNOŚĆ

Istnieje większe prawdopodobieństwo, że twierdzenie zostanie zaakceptowane jako prawdziwe, gdy jest kompatybilne z innymi informacjami, które zna dana osoba, niż w sytuacji, gdy jest sprzeczne z jej dotychczasową wiedzą.

2. SPÓJNOŚĆ NARRACYJNA

Istnieje większe prawdopodobieństwo, że twierdzenie zostanie zaakceptowane jako prawdziwe, gdy pasuje do szerszej narracji, która nadaje spójność jego poszczególnym elementom.

3. WIARYGODNOŚĆ ŹRÓDŁA

Istnieje większe prawdopodobieństwo, że treść zostanie zaakceptowana jako prawdziwa, jeśli pochodzi z wiarygodnego zdaniem odbiorcy/

-
- 2 C. Martel, G. Pennycook, D.G. Rand (2020). *Reliance on emotion promotes belief in fake news*, *Cogn. Research* 5, 47, <https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-020-00252-3#citeas> [dostęp: 05.07.2024 r.]; <https://www.szko-lazklasa.org.pl/jak-emocje-wplywaja-na-podatnosc-mlodziezy-na-dezinformacje-wystartowal-program-fake-know-more/> [dostęp: 05.07.2024 r.]
 - 3 R. Greifeneder, M. E. Jaffé, E. J. Newman, and N. Schwarz (2020). *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation*, https://www.researchgate.net/publication/345954715_The_Psychology_of_Fake_News_Accepting_Sharing_and_Correcting_Misinformation [dostęp: 05.07.2024 r.]

odbiorczyni źródła. Ocena wiarygodności źródła może opierać się na informacjach deklaracyjnych dotyczących np. wykształcenia czy osiągnięć, ale też np. braku sprzecznych interesów czy poczuciu znajomości – ludzie bardziej ufają osobom, instytucjom, organizacjom itp., które znają.

4. SPOŁECZNY DOWÓD SŁUSZNOŚCI

Aby ocenić prawdziwość twierdzenia, ludzie biorą pod uwagę, czy inne osoby wierzą w daną treść. Są bardziej pewni swoich przekonań, jeśli podzielają je także inni. Podobnie są bardziej skłonni do akceptowania przekazu, jeśli jakaś grupa osób również to zrobiła, a także bardziej ufają pamiętanym treściom, jeśli ktoś przypomina je sobie w podobnym kształcie.

5. DOWODY WSPIERAJĄCE

Pewność co do przekonań wzrasta wraz z liczbą potwierdzających je dowodów. Dowodami mogą być potwierdzenia uzyskane poprzez działania empiryczne (np. poszukiwanie faktów w literaturze naukowej) lub poprzez przywołanie odpowiednich informacji z pamięci. W każdym przypadku pewność wzrasta wraz z liczbą przywoływanych dowodów. Znaczenie ma także łatwość znalezienia potwierdzenia.

Każdy z wymienionych czynników ma przełożenie na podatność osób na fałszywe treści:

- Dezinformacja może być bardziej skuteczna, gdy jest zgodna z przekonaniem odbiorcy/odbiorczyni, co sprawia, że łatwiej ją zaakceptować, pomimo braku rzeczywistych dowodów na jej poparcie. Wiąże się z tym tzw. błąd potwierdzenia (ang. confirmation bias). Jest to skłonność do preferowania informacji zgodnych z przekonaniem i ignorowania tych, które są z nimi sprzeczne.
- Twierdzenia, które pasują do danej historii, są bardziej przekonujące, dlatego przekazy dezinformacyjne tworzone są w taki sposób, aby fałszywe lub wprowadzające w błąd treści były spójne z szerszym kontekstem. Warto przy tym nadmienić, że dezinformacja rzadko oparta jest jedynie na nieprawdziwych treściach, z reguły zawiera w sobie elementy prawdy, właśnie po to, aby odbiorcy/odbiorczynie łatwiej w nią uwierzyli.
- Dezinformacja może wykorzystywać efekt autorytetu – skłonność do polegania na/ zgadzania się z osobami lub instytucjami uznawanymi za autorytet. Aktorzy dezinformacyjni mogą tworzyć fałszywe lub

wprowadzające w błąd treści, podszywając się pod prawdziwe wiarygodne osoby lub instytucje albo kreując rzekome autorytety.

- Dezinformacja może być celowo wzmocniana, pokazywana w taki sposób, aby sprawiać wrażenie, że dana treść cieszy się szerokim poparciem lub akceptacją społeczną. Pomaga to zyskać wiarygodność. Osiąga się to np. poprzez wykorzystanie botów do stworzenia sztucznego tłumu i uzyskania pozorów popularności danego materiału.
- Dezinformacja może polegać na manipulowaniu poprzez selektywne prezentowanie lub całkowite fałszowanie dowodów, które są trudne do zweryfikowania. Może to obejmować wybiórcze przedstawianie faktów, wyciąganie ich z kontekstu, fabrykowanie danych.
- Dezinformacja często wykorzystuje emocje, aby przyciągnąć uwagę i wzbudzić zaangażowanie. Silne emocje, takie jak strach czy gniew, mogą osłabiać zdolność do logicznego myślenia oraz krytycznej analizy treści⁴.

Warto zwrócić również uwagę na problem nadmiaru informacji, które nieustannie docierają do odbiorców/odbiorczyń z wielu źródeł. Prowadzi to często do powierzchownego przetwarzania treści, a użytkownicy/użytkowniczki mają tendencję do preferowania łatwiejszych w odbiorze informacji. W efekcie nadmiar treści utrudnia skuteczne oddzielenie informacji fałszywych lub wprowadzających w błąd od tych rzetelnych.

Opisane czynniki sprawiają, że każdy jest narażony na dezinformację. Dlatego tak ważna jest edukacja i uświadamianie obywateli. Kluczowe jest informowanie o mechanizmach wykorzystywanych przez aktorów dezinformacyjnych oraz rodzajach treści, które są fałszywe lub wprowadzające w błąd. Chodzi o to, by zwiększyć zdolność społeczeństwa do rozpoznawania i przeciwdziałania dezinformacji.

W Raporcie Światowego Forum Ekonomicznego (Global Risk Report 2024)⁵ zwrócono uwagę, że dezinformacja stanowi bardzo poważne zagrożenie również z perspektywy globalnej – zarówno dla gospodarki, jak i społeczeństwa. Fałszywe lub wprowadzające w błąd treści wykorzystywane przez osoby o złych intencjach niosą poważne zagrożenia dla różnych obszarów: życia społecznego, zdrowia publicznego, państwa i jego struktur, a także polityki czy biznesu. Dezinformacja pogłębia

4 C. Martel, G. Pennycook, D.G. Rand (2020). *Reliance on emotion promotes belief in fake news*, *Cogn. Research* 5, 47, <https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-020-00252-3#citeas> [dostęp: 05.07.2024 r.]

5 Op.cit.

podziały i utrwała antagonizmy, wpływa na procesy wyborcze i podważa zaufanie do instytucji. Blokuje przepływ rzetelnych treści, utrudniając podejmowanie świadomych decyzji. Wprowadza chaos i destabilizację.

Z uwagi na złożoność i dynamikę zjawiska, zintegrowane działania różnych podmiotów są niezbędne, aby skutecznie monitorować i identyfikować dezinformację, edukować społeczeństwo i budować jego odporność na fałszywe treści oraz promować prawdziwe i rzetelne przekazy. Podstawą wszystkich przedsięwzięć w tym zakresie jest jednak świadomość zagrożeń i zrozumienie, w jaki sposób dezinformacja może wpływać na interes publiczny.

1.2. Rola platform społecznościowych w rozprzestrzenianiu dezinformacji

Pisząc o podatności na dezinformację warto zwrócić uwagę na kanały, którymi jest rozprzestrzeniana i źródła informacji dominujące w danym społeczeństwie. Według raportu „Dezinformacja oczami Polaków 2024”, podstawowe źródła informacji dla obywateli Polski to: telewizja (64%), internetowe portale informacyjne (58%) oraz radio (50%) i media społecznościowe (46%).

To właśnie na platformach społecznościowych, według Polaków, fałszywe informacje pojawiają się najczęściej. Na kolejnych miejscach respondenci wskazują telewizję oraz przekazy polityków/polityczek⁶.

Platformy społecznościowe mają istotne znaczenie w przekazywaniu informacji oraz w prowadzeniu interakcji społecznych. 57% Polaków/Polek (tj. trzy czwarte użytkowników/użytkowniczek internetu w naszym kraju) – deklaruje, że ma konto w jakimś serwisie społecznościowym⁷. Obok pozytywnych aspektów takich serwisów, należy również

6 DigitalPoland (2024). Dezinformacja oczami Polaków 2024, <https://digitalpoland.org/publikacje/pobierz?id=70f40c4e-3fe1-4abd-9a32-02a26c324f18> [dostęp: 28.06.2024 r.]

7 CBOS (2023). Korzystanie z internetu w 2023 roku, https://www.cbos.pl/SPISKOM.POL/2023/K_072_23.PDF [dostęp: 02.07.2024 r.]

podkreślić ich udział w rozprzestrzenianiu fałszywych bądź wprowadzających w błąd treści.

1.2.1. Algorytmy

Sposób prezentowania i rozprzestrzeniania treści w mediach społecznościowych wyznaczają algorytmy. Odgrywają one podstawową rolę w funkcjonowaniu agregatorów treści i systemów rekomendacyjnych⁸. Algorytmy dopasowania treści rozpoczęły epokę mobilnej personalizacji. Użytkownicy/użytkowniczki, stają się obiektami analizy wyrafinowanych technologii, nieprzerwanego śledzenia i profilowania. Na podstawie historii ich aktywności algorytmy mogą dopasować ofertę odpowiadającą na ich zainteresowania oraz potrzeby, aby optymalizować zyski dostawcy treści⁹.

Choć ten mechanizm ma zalety – pozwala łatwiej znaleźć odbiorcy/odbiorczynie interesujące go/ją treści, to może prowadzić również do ograniczenia jego/jej interakcji z innymi informacjami, punktami widzenia. Może wywołać efekt zamknięcia w tzw. bańce informacyjnej (filtrującej). Użytkownicy/użytkowniczki otrzymują wiadomości głównie związane z zainteresowaniami, zgodne ze światopoglądem, przekonaniami, przez co ich percepcja rzeczywistości może zostać zaburzona, a obiektywna ocena danej sytuacji – utrudniona¹⁰. Warto dodać, że bańki informacyjne są unikalne dla każdego użytkownika/użytkowniczki. Nawet wtedy,

-
- 8 J. Kreft (2018), *Władza algorytmów. U źródeł potęgi Google i Facebooka*, Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, s. 13, https://www.researchgate.net/profile/Jan-Kreft/publication/332752295_Wladza_algorytmow_U_zrodel_potegi_Google_i_Facebooka/links/5ec6b61c458515626cbf1ac7/Wladza-algorytmow-U-zrodel-potegi-Google-i-Facebooka.pdf, [dostęp: 28.06.2024 r.]
 - 9 J. Skorus, *Komunikacja we władzy algorytmów – szansa czy zagrożenie?*, [w:] *Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach*, Nr 1(16)/2020, s. 79, https://wzop.edu.pl/wp-content/uploads/2021/06/05_Komunikacja_we_wladzy_J_Skorus-1.pdf [dostęp: 01.07.2024 r.]
 - 10 S. Juszczyk (2023). *Funkcjonowanie młodzieży w świecie postcyfrowym na podstawie wielodyscyplinowych badań w ramach paradygmatów: Przemysł 4.0, Edukacja 4.0 oraz Społeczeństwo 5.0*, [w:] E. Widawska (red.), *Młode pokolenie w (nie)przyjaznym świecie – konteksty teoretyczne, metodologiczne i praktyczne*, s. 166-167.

kiedy istnieje grono osób o podobnych zainteresowaniach, to każda z nich otrzyma nieco inny zestaw treści –przeznaczony dla konkretnego użytkownika/użytkowniczkich strumień informacji¹¹.

Architektura platform społecznościowych sprzyja występowaniu efektu komory echa (nazywanej także komorą pogłosową, ang. echo chamber). To rodzaj „ekosystemu”, w którym użytkownicy/użytkowniczki napotykają, poszukują i wzmacniają takie treści, które potwierdzają ich przekonania na dany temat. Stają się oni częścią różnych grup (niekiedy zamkniętych), które dzielą się informacjami zgodnymi z ich preferencjami. Pozornie grupy te mogą stwarzać wrażenie wymiany poglądów, ale w rzeczywistości dyskusje odbywają się tylko w obrębie ustalonych wartości. W związku z tym ich uczestnicy/uczestniczki radykalizują się w swoich przekonaniach i wzajemnie utwierdzają w ich słuszności. Zamknięci na informacje „z zewnątrz” konsumują ciągle te same przekazy, powracające jak echo.

1.2.2. Boty i trolle

Szczególną rolę w kontekście rozprzestrzeniania dezinformacji w mediach społecznościowych odgrywają również trolle i boty.

Trolle to użytkownicy/użytkowniczki, którzy poprzez zamieszczanie kontrowersyjnych czy napastliwych treści, komentarzy prowokują innych do reakcji. Swoją aktywnością wywołują konflikty, podziały, potęgują chaos i zamieszanie oraz zaburzają rzeczową dyskusję. Osoby takie przejawiają antyspołeczne zachowania, obrażają lub ośmieszają innych. Są przeciętnie znacznie bardziej aktywne od zwykłych użytkowników/użytkowniczek sieci, generując do 12 razy więcej treści. Według badań 50% osób zajmujących się tego rodzaju działalnością posiada cechy psychopatyczne¹². Trolle mogą działać w zorganizowanych grupach (nazywanych

11 M. Szpunar (2018), *Koncepcja bańki filtrującej a hipernarcyzm nowych mediów* [w:] *Zeszyty prasoznawcze*, s. 194, https://www.magdalenaszpunar.com/_publikacje/2018/4-Magdalena%20Szpunar-1.pdf [dostęp: 01.07.2024 r.]

12 K. Bąkiewicz (2023), *Dezinformacja – instrukcja obsługi*, Warszawa: Wydawnictwo CeDeWu Sp. z o.o., s. 112-113.

farmami lub fabrykami trolli), w sposób skoordynowany po to, by jeszcze skuteczniej wprowadzać chaos w przestrzeni informacyjnej.

Obok trolli, bardzo poważne zagrożenie związane z rozprzestrzenianiem dezinformacji, stanowią boty. W przeciwieństwie do trolla, który jest człowiekiem – bot jest automatycznym programem wykonującym określone zadania. W kontekście dezinformacji boty definiowane są głównie jako fałszywe, zautomatyzowane konta, profile, które naśladują ludzkie zachowanie. Mogą one publikować i udostępniać wpisy, reagować na nie w określony sposób, wchodzić w interakcję z użytkownikami lub innymi botami. Treści rozpowszechniane przez boty mogą być tworzone przez ludzi, ale też generowane w pełni automatycznie, np. przy wykorzystaniu sztucznej inteligencji¹³. Łatwość i niskie koszty tworzenia botów sprawiają, że często powstają tzw. farmy botów. Są to konta generowane w bardzo dużych ilościach – tysiącach, dziesiątkach, setkach tysięcy. Często są wykorzystywane do amplifikowania określonych treści. Dodatkowym zagrożeniem jest fakt, że wraz z rozwojem technologii rozróżnienie kont botów od profili prawdziwych użytkowników/użytkowniczek staje się coraz większym wyzwaniem.

Poprzez swoje działanie boty i trolle mogą tworzyć „sztuczny tłum”, mający sprawiać wrażenie, że dane informacje, czyjeś wpisy są popularne, a przez to ważne czy bardziej wiarygodne. Ponadto, algorytmy mediów społecznościowych potęgują możliwości trolli i botów (a co za tym idzie – rozprzestrzenianie dezinformacji), poprzez promowanie treści kontrowersyjnych, sensacyjnych lub emocjonalnych, które generują większe zaangażowanie użytkowników/użytkowniczek. Równocześnie boty mogą manipulować algorytmami. W 2023 roku eksperci/ekspertki NASK zaobserwowali nienaturalne aktywności w mediach społecznościowych, których celami były konta biorące udział w debacie publicznej dotyczącej bezpieczeństwa strategicznego w Polsce. Działania te nosiły znamiona złośliwego wykorzystania algorytmów przez boty. Ostabiły zasięgi kont w mediach społecznościowych należących m.in. do analityka wojskowego Jarostawa Wolskiego, dziennikarzy: Jakuba Wiecha i Bartłomieja Wypartowicza czy analityka ekonomicznego i militarnego Marka Meissnera. Opisany atak wykorzystywał technikę „follow-unfollow”: boty najpierw masowo zaobserwowały wybrane profile (follow), a następnie równocześnie wycofały swoje obserwowanie (unfollow). To sprawiło, że algorytmy platformy X przestały promować wpisy osób,

13 Ł. Olejnik (2024). *Propaganda – od dezinformacji i wpływu do operacji i wojny informacyjnej*, Warszawa: Wydawnictwo Naukowe PWN SA, s. 94.

których dotyczył ten ruch. W efekcie ich posty stały się mniej widoczne, straciły zasięg.

Pisząc o działalności botów i trolli w mediach społecznościowych, warto również wspomnieć o pojęciu „skoordynowanego nieautentycznego zachowania” (ang. Coordinated Inauthentic Behaviour, w skrócie CIB). Ogólnie rzecz ujmując, pojęcie to odnosi się do grupy profili lub stron – zarządzanych przez boty, bądź prawdziwych użytkowników/użytkowniczki – których skoordynowane działanie ma na celu wprowadzenie innych w błąd co do tego kim są albo co robią i manipulację percepcją danej treści (nie ma tu znaczenia, czy jest ona fałszywa, czy prawdziwa)¹⁴.

1.2.3. Odpowiedzialność za rozpowszechnianie dezinformacji

Według raportu „Dezinformacja oczami Polaków”¹⁵, zdaniem obywateli/obywaterek do odpowiedzialności za rozpowszechnianie fałszywych treści powinni być przede wszystkim pociągani administratorzy/administratorki stron, portali i aplikacji (53%), właściciele dużych platform internetowych, tj. Apple, ByteDance, Google, Meta, Microsoft (50%), eksperci w danej dziedzinie (44%), dziennikarze/dziennikarki i pracownicy/pracowniczki mediów (44%) oraz rząd i podległe mu urzędy (43%), a także policja i prokuratura (42%)¹⁶. Podejmowane są działania legislacyjne, mające pomagać w egzekwowaniu takiej odpowiedzialności. Przykładem jest Akt o usługach cyfrowych (Digital Service Act, DSA) – nowe prawo unijne, które ma na celu stworzenie bardziej bezpiecznego i transparentnego internetu. Nakłada ono nowe obowiązki na platformy internetowe i wszystkich pośredników w Unii Europejskiej w zakresie usuwania nielegalnych treści, ochrony prywatności użytkowników/użytkowniczek

14 N. Gleicher, Meta (2018), *Coordinated Inauthentic Behavior Explained*, [Coordinated Inauthentic Behavior Explained | Meta \(fb.com\)](#) [dostęp: 05.07.2024 r.]

15 Op.cit.

16 DigitalPoland (2024). *Dezinformacja oczami Polaków 2024*, <https://digitalpoland.org/publikacje/pobierz?id=70f40c4e-3fe1-4abd-9a32-02a26c324f18> [dostęp: 05.07.2024 r.]

i walki z dezinformacją właśnie po to, by działały w sposób odpowiedzialny i nie nadużywały swojej pozycji na rynku¹⁷.

1.3. Aktorzy dezinformacji

Przekazy dezinformacyjne pochodzą od podmiotów zaangażowanych, czyli tzw. aktorów dezinformacji. Mogą nimi być zarówno konkretne osoby, jak i całe instytucje, grupy czy organizacje np.:

- Państwa, służby specjalne państw – mogą prowadzić operacje dezinformacyjne w celu osiągnięcia celów strategicznych, takich jak wpływanie na politykę, gospodarkę, bezpieczeństwo lub kulturę innych krajów lub regionów.
- Trolle – prawdziwi użytkownicy/użytkowniczki, publikujący złośliwe lub nieprawdziwe informacje, by wywołać negatywne reakcje, zakłócić dyskusje lub wpływać na nastroje społeczne, mogą działać na zlecenie lub pod wpływem innych podmiotów, które mają interes we wpływaniu na opinię publiczną lub zakłócaniu porządku publicznego.
- Boty – automatyczne programy, które mogą kreować, rozpowszechniać, amplifikować dezinformację na dowolny temat, w zależności decyzji osób nimi dysponujących.
- Armie (fabryki, farmy) botów/trolli – szczególnie niepokojące w kontekście szerzenia dezinformacji mogą być działania wspomnianych już armii trolli lub fabryk botów – zorganizowanych struktur, które mogą w usystematyzowany sposób wprowadzać do debaty określone treści, promować pewne narracje, dyskredytować osoby, produkty, marki czy konkretne poglądy. Ich działalność może być skierowana

17 Komisja Europejska, Akt o usługach cyfrowych: Pytania i odpowiedzi, <https://digital-strategy.ec.europa.eu/pl/faqs/digital-services-act-questions-and-answers> [dostęp: 05.07.2024 r.]

do wewnątrz państwa, ale także na zewnątrz – w kierunku innych krajów¹⁸.

- Politycy/polityczki, osoby publiczne – mogą szerzyć dezinformację m.in. poprzez postępowanie się nierzetelnymi danymi lub wykorzystywanie nieprawdziwych informacji jako narzędzia wpływu politycznego.
- Media – mogą szerzyć dezinformację poprzez publikowanie fałszywych lub wprowadzających w błąd treści, ale też niesprawdzonych lub niezweryfikowanych informacji. W drugim przypadku, po uzyskaniu wiedzy na temat swojej pomyłki, powinny opublikować odpowiednie sprostowanie.
- Liderzy/liderki opinii – osoby, które mają wpływ na poglądy, postawy i zachowania innych ludzi, np. celebryci/celebrytki czy aktywiści/aktywistki, także mogą rozpowszechniać dezinformację. Może to wynikać z ograniczonej wiedzy w danej dziedzinie, postępowania się błędnymi lub niesprawdzonymi danymi, z osobistych przekonań i poglądów, ale także ukrytych motywacji i interesów. Warto podkreślić ogromny zasięg i wpływ osób z tej grupy na ich odbiorców/odbiorczynie.
- Zwyczajni użytkownicy/użytkowniczki – każdy może przyczynić się do szerzenia dezinformacji poprzez udostępnianie niesprawdzonych informacji lub zwiększanie ich zasięgu przez wchodzenie z nimi w różne interakcje. Rola każdego użytkownika/użytkowniczki w zatrzymywaniu dezinformacji jest kluczowa, gdyż to on jest pierwszym ogniwem w łańcuchu jej rozprzestrzeniania. Od jego decyzji zależy, czy fałszywe lub wprowadzające w błąd treści zostaną przekazane dalej i potencjalnie zyskają zasięg i wpływ na innych ludzi. Świadomość i odpowiedzialność każdego użytkownika/użytkowniczki w tym zakresie jest zatem bardzo ważna.



Jedną z najbardziej znanych armii trolli była rosyjska Internet Research Agency (IRA), której korzenie sięgały 2012 roku¹⁹. Prowadzone przy jej wykorzystaniu kampanie wpływu informacyjnego, manipulacje w mediach społecznościowych, zostały odnotowane w wielu krajach. Do szerzenia dezinformacji i określonych narracji wykorzystywano różne metody



18 Ł. Olejnik (2024). *Propaganda – od dezinformacji i wpływu do operacji i wojny informacyjnej*, Warszawa: Wydawnictwo Naukowe PWN SA, s. 247.

19 S. Walker (2015). *The Russian troll factory at the heart of the meddling allegations*, The Guardian, <https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house> [dostęp: 02.07.2024 r.]

i kanały. Często publikowano bardzo duże ilości treści na różnych platformach. Trolle należące do IRA pisały tysiące komentarzy, wiadomości i dystrybuowały prokremlowską narrację dzięki siatce powiązanych kont w większości dostępnych platform społecznościowych. Ponadto treści, produkowane przez armię trolli były tłumaczone na wiele języków²⁰. Przykładem działalności rosyjskich trolli w Polsce może być sytuacja z 2022 roku. Na początku rosyjskiej inwazji na Ukrainę w sieci pojawiły się doniesienia o tym, że na stacjach może zabraknąć paliw. Braki miały wynikać z odcięcia dostaw przez Rosję oraz przejęcia zapasów przez wojsko. Konsekwencją tych doniesień były kolejki aut na stacjach w całej Polsce. Wprowadzano nawet limity tankowania wynikające z nagłego podwyższonego popytu. Instytut Badań Internetu i Mediów Społecznościowych poinformował, że w sieci został wówczas przeprowadzony zmasowany rosyjski atak dezinformacyjny, w którym uczestniczyło około 300 kont, zalewając polski internet przekazem mającym wywołać kryzys i destabilizację²¹. Warto dodać, że choć najstynniejsza rosyjska farma trolli – IRA oficjalnie zakończyła swoją działalność w związku ze śmiercią jej założyciela – Jewgienija Prigożyna, to w praktyce jej aktywność jest kontynuowana i wywiera wpływ na obywateli różnych krajów oraz procesy globalne.

1.4. Zagraniczne manipulacje informacjami i ingerencje w informacje (FIMI)

FIMI (ang. Foreign Information Manipulation and Interference) to zagraniczne manipulacje informacjami i ingerencje w informacje. Jest to nowy termin, który przenosi punkt ciężkości z treści na zachowanie aktorów dezinformacyjnych. FIMI opisuje wzorzec zachowań, zwykle

20 K. Bąkiewicz (2023). *Dezinformacja – instrukcja obsługi*, Warszawa: Wydawnictwo CeDeWu Sp. z o.o., s. 170.

21 Instytut Badań Internetu i Mediów Społecznościowych (2022). <https://x.com/ibimspl/status/1496815247402938371> [dostęp: 02.07.2024 r.]

legalnych, który ma potencjał negatywnego wpływu na wartości, procedury i procesy polityczne. Działalność taka ma charakter manipulacyjny, jest prowadzona w sposób celowy i skoordynowany. Aktorami takich działań mogą być państwa lub podmioty niepaństwowe, w tym ich pełnomocnicy/pełnomocniczki działający wewnątrz i poza własnym terytorium²². Choć zachowanie, o którym mowa, zazwyczaj nie jest nielegalne, to ma szkodliwy charakter. Nie ogranicza się przy tym do sfery polityki, ale dotyczy wszelkiej manipulacji, która może wyrządzić szkodę społeczeństwu, np. dotyczącej zdrowia czy klimatu.

Warto zwrócić uwagę na rozróżnienie między FIMI a dezinformacją. Jak wspomniano, FIMI kładzie nacisk na zachowanie, w przeciwieństwie do dezinformacji, która odnosi się do treści. Ponadto FIMI zarezerwowane jest dla zagranicznej niepożądanego ingerencji w sferę informacyjną. Tym, co wyróżnia FIMI jest także czerpanie z dorobku analizy zagrożeń cybernetycznych. Zatem dezinformacja i FIMI do pewnego stopnia się zająbiają, jednak nie są tożsame – nie każda dezinformacja będzie częścią FIMI, a FIMI nie ogranicza się jedynie do dezinformacji²³.

Europejska Służba Działań Zewnętrznych (ESDZ, ang. EEAS) zauważa, że FIMI jest wykorzystywane do podważania zaufania publicznego co do legalności i skuteczności instytucji demokratycznych. Może przyczyniać się do zwiększenia polaryzacji i podziałów w ramach Unii Europejskiej. Jednocześnie wpływa na zdolność UE do wdrażania polityk zarówno wewnątrz, jak i poza Unią. FIMI może również eskalować przemoc polityczną w regionach już narażonych na konflikty, podważając w ten sposób wysiłki pokojowe UE i społeczności międzynarodowej na całym świecie. Podmioty FIMI używają różnorodnych, stale ewoluujących taktyk, technik i procedur (TTPs)²⁴. Działania te rozpatrywane są w kategorii zagrożeń hybrydowych.

ESDZ przygotowała kilka raportów związanych z FIMI. Jeden z nich dotyczy analizy 750 incydentów FIMI zaobserwowanych w przestrzeni

-
- 22 EEAS (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf [dostęp: 04.07.2024 r.]
- 23 N. Hénin, EU DisinfoLab (2023). FIIM: towards the European redefinition of foreign interference, https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [dostęp: 03.09.2024 r.]
- 24 EEAS (2024). Tackling Disinformation, Foreign Information Manipulation & Interference, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en#81218 [dostęp: 05.07.2024 r.]

informacyjnej pomiędzy 1 grudnia 2022 a 30 listopada 2023 roku²⁵. Z raportu wynika, że analizowane działania były ukierunkowane w szczególności na Ukrainę. Próbowano podważyć jej stabilność i osłabiać poparcie dla niej. Celami ataków FIMI były w tym czasie także m.in. państwa członkowskie UE, NATO, a także organizacje medialne, takie jak: Euronews, Reuters, Deutsche Welle i New York Times. Wykazano również, że celami FIMI były poszczególne osoby, m.in. prezydent Ukrainy Wołodymyr Zełenski i pierwsza dama Ołena Zełenska, wysoki przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa Josep Borrell oraz prezydent Francji Emmanuel Macron. W działaniach FIMI wykorzystywano ponadto wizerunki znanych na świecie osobistości filmowych, takich jak np. Nicolas Cage i Margot Robbie – celem tych zabiegów było dotarcie z fałszywym przekazem do szerszej publiczności. Raport wykazał także, że ważnymi katalizatorami dla działań FIMI są aktualne wydarzenia. W 21,3% analizowanych incydentów wykorzystywano zainteresowanie opinii publicznej okolicznościami takimi jak: szczyty polityczne, wybory, oficjalne wizyty i inne. To pokazuje, że aktorzy FIMI bacznie śledzą działalność instytucji i mediów oraz strategicznie wykorzystują do realizacji swoich interesów uwagę skupianą wokół poszczególnych wydarzeń. Najczęściej stosowanymi w analizowanych incydentach FIMI kanałami przekazu były Telegram i X, jednak szkodliwą działalność zaobserwowano na praktycznie wszystkich dostępnych platformach.

Jedną ze zidentyfikowanych w infosferze kampanii FIMI jest operacja Doppelganger (ang. „sobowtór”). Została ujawniona w 2022 roku. Twórcy kampanii podszywają się pod media, tworząc strony internetowe łudząco podobne do autentycznych portali informacyjnych (czasem także stron rządowych). Podobieństwo to dotyczy nie tylko warstwy wizualnej, ale też samej nazwy domeny, która koresponduje z prawdziwą, np. podszywająca się domena to „theguardian.co[.]com”, a prawdziwa: theguardian.com. Twórcy kampanii wykorzystują takie „klony” do umieszczania na nich dezinformacyjnych artykułów czy filmów. Następnie dystrybuują je w mediach społecznościowych. Wiele elementów wskazuje na zaangażowanie w operację aktorów z siedzibą w Rosji. Ponadto w ramach operacji tworzone są treści zgodne z prokremlowską narracją²⁶.

25 EEAS (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf [dostęp: 04.07.2024 r.]

26 A. Alaphilippe, G. Machado, R. Miguel, F. Poldi (2022). Doppelganger. Media clones serving Russian propaganda, <https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf> [dostęp: 10.07.2024 r.]

ESDZ przyjrzała się działaniom prowadzonym w ramach operacji Doppelganger w kontekście wyborów do Parlamentu Europejskiego w 2024 roku²⁷. Działania te miały na celu zakłócenie procesu wyborczego. Skierowane były głównie do odbiorców/odbiorczyń we Francji i Niemczech, ale także w Polsce, we Włoszech i w Hiszpanii. Treści były dopasowane indywidualnie do specyfiki każdego kraju. Koncentrowały się na tematach takich jak: migracja, energia i klimat oraz wojna na Ukrainie. Jeśli chodzi o działania wymierzone w Polskę, to w kwietniu 2024 roku, twórcy/twórczynie kampanii podszyli się pod portale internetowe Polityki oraz Polskiego Radia.

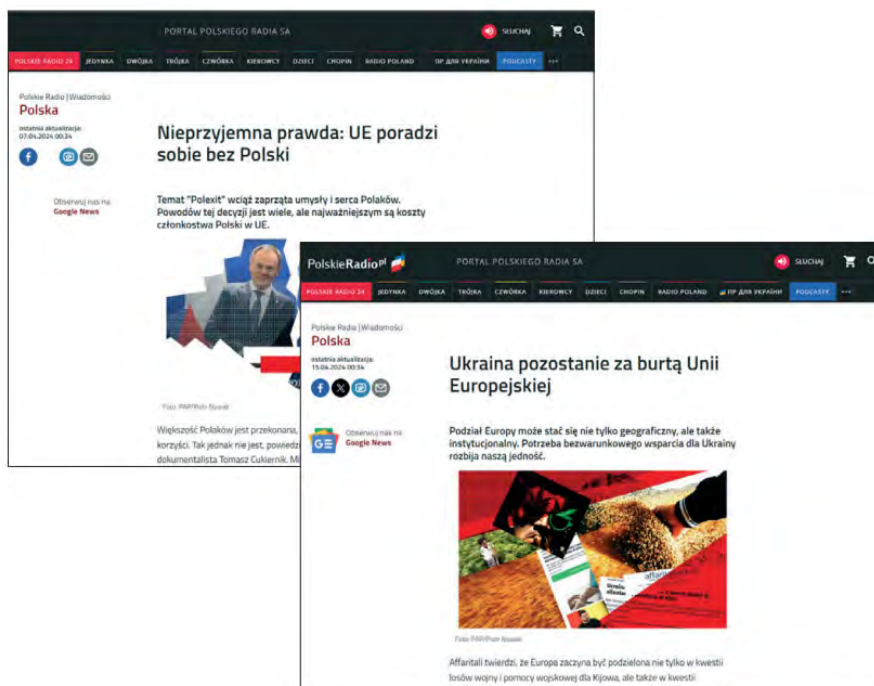
Rys. 1. Strona internetowa podszywająca się pod portal Polityki.



Źródło: ESDZ (2024). Doppelganger strikes back: FIMI activities in the context of the EE24, https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf [dostęp: 10.07.2024 r.]

27 ESDZ (2024). Doppelganger strikes back: FIMI activities in the context of the EE24, https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf [dostęp: 10.07.2024 r.]

Rys. 2. Strona internetowa podszywająca się pod portal Polskiego Radia.



Źródło: ESDZ (2024). Doppelganger strikes back: FIMI activities in the context of the EE24, <https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24-June2024.pdf> [dostęp: 10.07.2024 r.]

W raporcie Europejskiej Służby Działań Zewnętrznych (ESDZ) opisano kluczowe etapy nagłaśniania fałszywego przekazu w mediach społecznościowych, na przykładzie działań na platformie X:

1. PUBLIKOWANIE TREŚCI

Grupa 8-12 kont w serwisie X rozpoczyna proces dystrybucji treści, publikując posty zawierające podpis tekstowy, link prowadzący użytkowników do fałszywej strony oraz obrazek z miniaturą artykułu. Krok ten stanowi podstawę dla kolejnych etapów działania.

2. WZMACNIANIE PRZEKAZU POPRZEZ CYTOWANIE

Krótko po publikacji pierwszych postów, większa grupa nieautentycznych kont (około 1000) zwana „wzmacniaczami”, rozpoczyna powielanie przekazu, udostępniając wpisy.

3. WZMACNIANIE PRZEKAZU POPRZEZ KOMENTOWANIE

Fałszywe treści powielane są w komentarzach na profilach użytkowników posiadających dużą liczbę obserwatorów. Wykorzystywane do takich działań konta stają się nieaktywne po ukończeniu swoich zadań.

4. DYSTRYBUCJA POPRZEZ ZMYLENIE PRZEKIEROWAŃ URL

Aby uniknąć ograniczeń platformy dotyczących publikowania linków do domen umieszczonych na czarnej liście, stosowana jest technika wieloetapowego przekierowania URL. Link przekierowuje użytkowników przez kilka pośrednich stron internetowych przed dotarciem do docelowego miejsca – artykułu opublikowanego na fałszywej stronie – sobowtórze.

Na Facebooku fałszywy przekaz rozpowszechniany był ponadto za pomocą postów sponsorowanych.

Innym przykładem FIMI, zaobserwowanym w polskojęzycznej przestrzeni informacyjnej, jest tzw. operacja Ghostwriter. Została ona ujawniona w 2020 roku. Stoi za nią, przynajmniej częściowo, grupa cyberprzestępców UNC1151 (nazywana także grupą Ghostwriter), powiązana najpewniej z rządem Białorusi²⁸. Jej działania wymierzone są m.in. w Polskę. Między październikiem 2020 a styczniem 2021 roku doszło do incydentów, w ramach których konta w mediach społecznościowych kilku polskich polityków zostały przejęte i wykorzystane do rozpowszechniania narracji mających na celu zdyskredytowanie polskiego rządu oraz pogłębienie istniejących wewnętrznych podziałów politycznych. Skompromitowano wówczas konta:

- postanki PiS Joanny Borowiak – zamieszczono z jej profilu wpis o treści: „Możecie sobie protestować ile chcecie. Jak powiedział Jarosław Kaczyński, zdanie narkomanek-prostytutek i zabójców dzieci nie będzie mieć wpływu na podejmowane decyzje”;
- posta PiS Marcina Duszka – na należącym do niego profilu zamieszczono jego zdjęcie z kobietą i podpisano: „Poznajcie tę ślicznotkę! Izabela (...) będzie moją nową sekretarką. Udowodniła już swój profesjonalizm i będzie moją prawą ręką we wszystkich sprawach. Moi koledzy postowie będą zazdrościć”, ponadto w komentarzach pojawiły się opublikowane z tego samego konta zdjęcia rozneglizowanych kobiet;
- ówczesnej ministry rodziny i polityki społecznej Marleny Małąg – zamieszczono wpis o treści: „Jako kobieta, jako matka nigdy nie zrozumieć ani nie poprę protestujących. Wulgarnie i chamskie zachowanie nie zdoła kobiet, przypominają mi watahy Papuasów i bezmózgich dzikusów zdolnych jedynie do bicia i bezrozumnego

28 Mandiant (2021). UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests, <https://cloud.google.com/blog/topics/threat-intelligence/unc1151-linked-to-belarus-government/> [dostęp: 11.07.2024 r.]

uprawiania seksu. Niektórym wogóle strach dać zapałki do ręki. Dla wszystkich bluzgających pseudo kobiet należy stworzyć specjalne rezerwy, w których będą wykorzystane jako inkubatory” [pisownia oryginalna przyp. red.];

- posta PiS Marka Suskiego – na jego profilu ukazały się zdjęcia ukazujące roznegliżowaną kobietę przypominającą Ewę Szarzyńską – wiceprzewodniczącą rady miasta w Mogilnie – oraz cztery wpisy, m.in.: „Będę wykorzystywał wszystkie moje polityczne możliwości, będę zwracał się osobiście do Kaczyńskiego, żeby Szarzyńska już nigdy nie pojawiła się na polskiej scenie politycznej. Dziś opublikowała na Instagram, nowe zdjęcia, „Takie wulgarne zachowanie osoby publicznej jest niedopuszczalne. Nie zdziwiłbym się, gdyby taką rozwiązłość seksualną wykazywali politycy w KO lub w otoczeniu Marty Lempart” [pisownia oryginalna przyp. red.];
- ówczesnej wiceministry rozwoju, pracy i technologii Iwony Michątek – zamieszczono grafikę z wizerunkiem Jarosława Kaczyńskiego za kratami i podpisano: „Gang PiS na czele z Kaczyńskim przekroczył wszelkie możliwe granice. Okrucieństwo i bezkarność stały się normą dla rządzącego establishmentu. Nie chcę już być po tej samej stronie z mordercami, katami i złodziejami. PiS to typowa dyktatorska, antydemokratyczna organizacja przestępcza, która skoncentrowana na bogaceniu się w sposób nieuczciwy” [pisownia oryginalna – przyp. red.]²⁹.

29 Mandiant (2021). *Ghostwriter update: Cyber Espionage Group UNC1151 Likely Conducts Ghostriter Influence Activity*, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf [dostęp: 11.07.2024 r.]

Rys. 3. Wpis ze skompromitowanego profilu Iwony Michałek.



Źródło: Mandiant (2021). Ghostwriter update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf [dostęp: 11.07.2024 r.]

Grupa UNC1151 odpowiedzialna jest także m.in. za przeprowadzoną w 2023 roku kampanię e-mailową, w której podszywano się pod Ministerstwo Spraw Wewnętrznych i Administracji. Wiadomość zawierająca logotyp MSWiA, rozsyłana do obywateli z adresu mailowego przypominającego adres ministerstwa, sugerowała konieczność zgłaszania organom państwowym uchodźców z Ukrainy według załączonego do e-maila formularza. Autorzy fałszywej wiadomości grozili rzekomymi karami grzywny za niedostarczenie odpowiednich informacji³⁰.

Warto dodać, że opisane kampanie nie zakończyły się, a ataki co jakiś czas powracają.

30 Gov.pl (2023). [AKTUALIZACJA] UWAGA! CSIRT NASK ostrzega przed kampanią e-mailową podszywającą się pod Ministerstwo Spraw Wewnętrznych i Administracji!, <https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostzega-przed-kampania-e-mailowa-podszywajaca-sie-pod-ministerstwo-spraw-wewnetrznych-i-administracji> [dostęp: 11.07.2024 r.]



Przykłady pokazują, że działalność cyberprzestępców bywa nieodłącznym elementem kampanii dezinformacyjnych. Tym istotniejsza staje się konieczność zadbania o poprawne zabezpieczenie profili w mediach społecznościowych czy kont mailowych, m.in. poprzez stosowanie silnych hasł oraz dwuskładnikowego uwierzytelniania.

1.5. Wybrane metody i techniki dezinformacji

Podmioty zajmujące się dezinformacją stosują różnorodne metody i techniki mające na celu wprowadzenie odbiorcy/odbiorczynie w błąd. Znajomość tych metod jest kluczowa dla skutecznego weryfikowania prawdziwości treści oraz lepszego zrozumienia mechanizmów dezinformacji.

Poniżej przedstawiono opis wybranych metod i technik dezinformacyjnych wraz z sugerowanymi sposobami weryfikacji treści, które pozwalają identyfikować i przeciwdziałać konkretnym zagrożeniom.

A. DEEPPFAKE

Deepfake to wygenerowany lub zmanipulowany materiał audio lub wideo, który do złudzenia przypomina prawdziwe osoby, obiekty, miejsca, dźwięki, głos czy zdarzenia. Nazwa pochodzi od połączenia terminów „deep learning” (głębokie uczenie maszynowe) oraz „fake” (fałsz). Tworzenie deepfake’ów opiera się na wykorzystaniu narzędzi sztucznej inteligencji (AI).

Technika ta została wykorzystana np. w lipcu 2024 roku do rozpowszechnienia fałszywej informacji o rzekomej transakcji, jakiej miała dokonać żona prezydenta Ukrainy, Ołena Zełenska. Pierwsza dama miała kupić w paryskim salonie najnowsze luksusowe Bugatti Tourbillon, wydając na nie 4,5 mln euro z publicznych pieniędzy. Pojawiające się w mediach społecznościowych wpisy na ten temat

miały charakter antyukraiński. Zaprezentowanie rzekomej rozrzutności Ołeny Zeleńskiej w obliczu toczącej się w jej kraju wojny, miało na celu nie tylko zaszkodzenie wizerunkowi pary prezydenckiej, ale także podważenie zasadności niesienia pomocy finansowej Ukrainie. W fałszywym przekazie wykorzystano m.in. deepfake w postaci wideo prezentującego rzekomego przedstawiciela marki Bugatti opowiadającego w języku francuskim o prezentacji luksusowego samochodu parze prezydenckiej oraz transakcji, jaka miała zostać przeprowadzona.

Rys. 4. Wpis na platformie X zawierający deepfake w formacie wideo.



Źródło: www.x.com [dostęp: 15.07.2024 r.]

Przykładowe sposoby weryfikacji:

- W przypadku wideo: zwrócenie uwagi, czy ruch ust jest zgodny z momentem usłyszenia wypowiedzi i czy zgadza się z wypowiadanymi słowami; czy występują nienaturalne odstępy czasu lub brak mrugania oczami; czy podczas ruchów głową położenie włosów ulega zmianie; czy ułożenie ciała postaci przybiera nienaturalną formę.
- W przypadku zdjęć: zwrócenie uwagi czy przedstawione postaci wglądają naturalnie, np. czy nie posiadają za dużo rąk, nóg lub palców.

Warto pamiętać, że technologia tworzenia deepfake'ów jest stale udoskonalana, co sprawia, że ich weryfikacja staje się coraz trudniejsza.

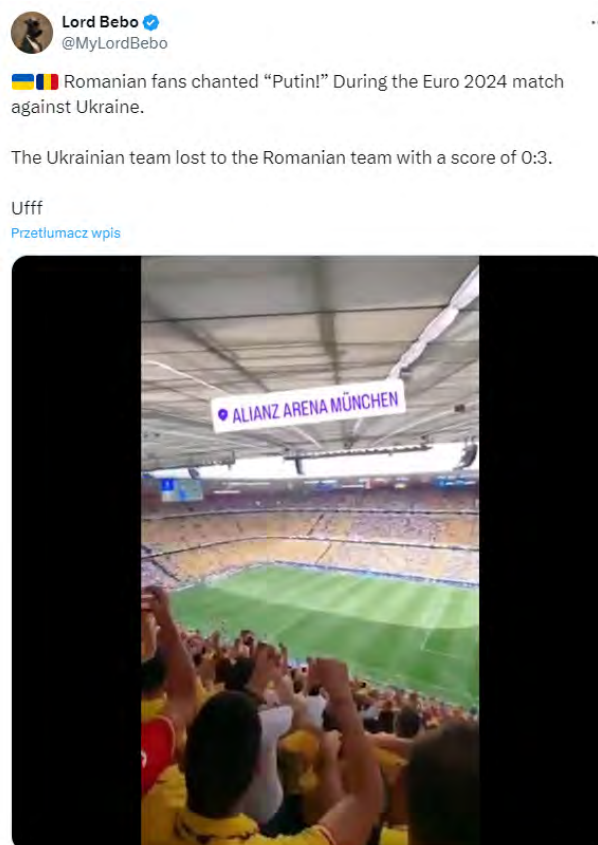
Starannie wykonane deepfaki mogą być niemal nieodróżnialne od autentycznych zdjęć czy filmów.

B. CHEAPFAKE

Cheapfake z języka angielskiego oznacza dosłownie „tanie oszustwo”. Oznacza proste manipulowanie obrazem, dźwiękiem lub wideo za pomocą powszechnie dostępnych narzędzi. Mimo, że daje nieprofesjonalne efekty, może być skuteczną metodą dezinformacji, szczególnie gdy użytkownik ma jedynie szybki i przelotny kontakt z daną treścią.

W czerwcu 2024 roku sieć obiegło nagranie, na którym mieli być widoczni rumuńscy kibice, rzekomo skandujący nazwisko „Putin” podczas meczu Rumunia-Ukraina rozgrywanego w ramach mistrzostw Europy w piłce nożnej. W rzeczywistości było to przerobione nagranie, do którego podłożono dźwięk³¹.

Rys. 5. Wpis na platformie X: przykład cheapfake'u.



Źródło: www.x.com [dostęp: 15.07.2024 r.]

31 Demagog.org (2024). Rumuńscy kibice skandują „Putin” w trakcie Euro? To przeróbka, https://demagog.org.pl/fake_news/rumunscy-kibice-skanduja-putin-w-trakcie-euro-to-przerobka/ [dostęp: 15.07.2024 r.]

Przykładowe sposoby weryfikacji:

- Uważne przyjrzenie się nagraniu czy zdjęciu. Ocena, czy widoczne są nienaturalne przejścia i cięcia.
- Sprawdzenie autora/autorki oraz kontekstu publikacji.
- W przypadku zdjęcia: weryfikacja za pomocą funkcji wyszukiwania obrazem w wyszukiwarce.
- Porównanie z innymi źródłami dokumentującymi te same wydarzenia.

C. PODSZYWANIE SIĘ

Metoda podszywania się oparta jest o wykorzystanie rozpoznawalnego wizerunku konkretnej instytucji lub osoby do szerzenia fałszywych informacji. Podmioty stosujące tę technikę używają nazwy i logotypu danej instytucji lub danych i wizerunku danej osoby, w celu wprowadzenia odbiorców/odbiorczyń w błąd. Działanie takie może przyczynić się nie tylko to wzmocnienia zasięgów fałszywych treści, ale też do obniżenia zaufania i podważania wiarygodność podmiotów, pod które następuje podszywanie.

Przykładem wykorzystania omawianej techniki może być sytuacja z dnia wyborów parlamentarnych w 2023 roku. W serwisie X podszyto się pod Państwową Komisję Wyborczą, informując o rzekomym unieważnieniu głosowania z uwagi na „oszustwa na masową skalę”. Wykorzystano logotyp i nazwę PKW, a do wpisu dołączono przykuwającą wzrok grafikę.

Rys. 6. Wpis na platformie X opublikowany na koncie podszywającym się pod PKW.



Przykładowe sposoby weryfikacji:

- W przypadku mediów społecznościowych – zwrócenie szczególnej uwagi na nazwę profilu: zweryfikowanie, czy nie występują literówki lub inne błędy w nazwie mogące wskazywać na fałszywe konto.
- Zwrócenie uwagi na opis profilu (zdarza się, że w opisie podszywającego się konta jest informacja o tym, że ma ono charakter satyryczny).
- Sprawdzenie, jakie wpisy publikowane były wcześniej z danego konta – może okazać się, że wiele z nich nie miało nic wspólnego z osobą czy instytucją, do której przypisuje się dany profil.
- W przypadku platformy X – zwrócenie uwagi na identyfikator użytkownika zaczynający się od „@”, znajdujący się pod nazwą profilu. Identyfikator niezbieżny z nazwą użytkownika może sugerować fałszywe konto.
- W przypadku stron internetowych – sprawdzenie, czy ich adres URL jest poprawny.

D. FAŁSZYWY KONTEKST

Fałszywy kontekst dotyczy przekazów, które przedstawiają prawdziwe zdjęcia, wideo czy opisy autentycznych wydarzeń, w nieprawdziwym lub niepełnym świetle, zmieniając tym samym ich znaczenie.

Technikę tę wykorzystano do zbudowania fałszywej tezy wokół wyborów samorządowych w Polsce, głoszącej, że kandydują w nich Ukraińcy. Postulowano się zdjęciem prezentującym żółto-niebieski plakat wyborczy Anny Tymoshenko, kandydatki na radną Częstochowy. Sugerowano, że jest ona Ukrainką, a w kampanii postuguje się barwami Ukrainy. Miało to świadczyć o rzekomej „ukrainizacji Polski”. Tymczasem, choć sam plakat wyborczy kandydatki był autentyczny, zaprezentowano go w fałszywym kontekście. W rzeczywistości kandydatka była Polką (nazwisko przejęta od męża Ukraińca), a zastosowane na jej plakacie kolory, to oficjalne barwy Częstochowy.

Rys. 7. Wpis na platformie X: przykład fałszywego kontekstu.



Źródło: www.x.com [dostęp: 9.04.2024 r.]

Przykładowe sposoby weryfikacji:

- Wyszukanie w innym źródle informacji na ten sam temat – sprawdzenie, jak inni autorzy/autorki relacjonują to samo wydarzenie lub, jak omawiają daną kwestię.
- W przypadku mediów społecznościowych – weryfikacja konta, które przekazuje daną informację – sprawdzenie, jakie inne treści publikuje.
- W razie wątpliwości co do tego, czy dana fotografia obrazuje opisywane wydarzenie – odnalezienie oryginalnego źródła zdjęcia (np. poprzez skorzystanie z funkcji wyszukiwania obrazem w wyszukiwarce).
- Odnalezienie pełnego tekstu lub nagrania, z którego pochodzi dany fragment, jeśli nie jest przedstawiona całość materiału.

E. MANIPULACJA PRAWDZIWYMI DANymi

Metoda ta polega na wyciąganiu fałszywych wniosków z prawdziwych danych poprzez zaprezentowanie ich niepoprawnej interpretacji. Samo użycie danych służy uwiarygodnieniu fałszywej tezy.

Manipulacja prawdziwymi danymi została wykorzystana do przedstawienia fałszywej informacji o rzekomym „wyprzedawaniu” zmagazynowanego gazu, które miałyby wpływać negatywnie na bezpieczeństwo energetyczne Polski. W rzeczywistości zmiana poziomu zapętnienia magazynów to efekt normalnego działania systemu magazynowania gazu³².

Rys. 7. Wpis na Facebooku: przykład manipulacji prawdziwymi danymi.



Źródło: www.facebook.com [dostęp 02.04.2024 r.]

32 K. Jabłonowski, „Tusk wyprzedaje zapasy gazu”? To manipulacyjny przekaz, <https://konkret24.tvn24.pl/polska/tusk-wyprzedaje-zapasy-gazu-to-manipulacyjny-przekaz-st7833597> [dostęp: 16.07.2024 r.]

Przykładowe sposoby weryfikacji:

- Sprawdzenie źródła informacji, czy jest wiarygodne, czy autor lub autorka może posiadać ekspercką wiedzę w dziedzinie, w której zabiera głos.
- Zweryfikowanie, czy inne wiarygodne źródła (np. specjalistyczne media branżowe lub zaufani eksperci/ekspertki) potwierdzają tę samą interpretację.
- Ocena, czy przedstawione dane i zaprezentowane wnioski są spójne logicznie.

F. FAŁSZYWE BADANIA



Kolejną metodą stosowaną w rozpowszechnianiu dezinformacji jest powoływanie się na pseudonaukowe badania. Ich źródłem są m.in. predatory journals, czyli „drapieżne czasopisma”, które nie przestrzegają standardów etyki publikacyjnej oraz charakteryzują się wprowadzającymi w błąd informacjami i brakiem przejrzystości. Za opłatą można w nich opublikować praktycznie każdą pracę. Predatory journals podają nieprawdziwe informacje o rzekomym zaangażowaniu wybitnych naukowców w proces recenzencki, a redaktorzy publikacji są często nieweryfikowalni³³.

Poniżej zaprezentowano przykład użycia fałszywych badań we wpisie opublikowanym w serwisie X. Autor sugeruje, że emisja CO₂ przez człowieka w ciągu ostatnich kilku dekad miała „marginalny wpływ na klimat”, powołując się przy tym na artykuł opublikowany przez czasopismo „Sci”. Twierdzenie takie stoi w sprzeczności z innymi badaniami naukowymi, a samo czasopismo wykazuje cechy tzw. predatory journal³⁴.

33 Biblioteka Główna AGH, Predatory journals, <https://bg.agh.edu.pl/otwarta-nauka/open-access/drapiezne-czasopisma> [dostęp: 16.07.2024 r.]

34 Demagog.org (2024), Emisja CO₂ nie wpływa na klimat? Rzetelne źródła mówią inaczej, https://demagog.org.pl/fake_news/emisja-co%E2%82%82-nie-wplywa-na-klimat-rzetelne-zrodla-mowia-inaczej/ [dostęp: 16.07.2024 r.]

Rys. 8. Wpis na platformie X: przykład użycia fałszywych badań.

 **Piotr Witzczak** 
@PiotrWitzczak

Wg nowego badania opublikowanego na łamach periodyku "Sci" emisja CO₂ przez człowieka w ciągu ostatnich kilku dekad miała marginalny wpływ na klimat [1]

Wg @jakubwiech udział człowieka w ociepleniu klimatu wynosi...100% (!) [2]

Wybierz źródło, które stanowi prymitywną propagandę

@krzysztofbosak
@lkwarzecha

1 [mdpi.com/2413-4155/6/1/...](https://doi.org/10.1002/2413-4155/6/1/)
"These findings confirm the major role of the biosphere in the carbon cycle and a non-discernible signature of humans"

2 [twitter.com/jakubwiech/sta...](https://twitter.com/jakubwiech/status/1824134155617123456)

7. Conclusions

The results of the analyses in this paper provide negative answers to the research questions posed in the Introduction. Specifically:

1. From modern instrumental carbon isotopic data of the last 40 years, no signs of human (fossil fuel) CO₂ emissions can be discerned.
2. Proxy data since the Little Ice Age suggest that the modern period of instrumental data does not differ, in terms of the net isotopic signature of atmospheric CO₂ sources and sinks, from earlier centuries.

Combined with earlier studies, namely [2,3,4,5,31], these findings allow for the following line of thought to be formulated, which contrasts the dominant climate narrative, on the basis that different lines of thought are beneficial for the progress of science, even though they are not welcomed by those with political agendas promoting the narratives (whose representatives declare that they "own the science", as can be seen in the motto in the beginning of the paper).

1. In the 15th century, Earth entered a cool climatic period, known as the Little Ice Age, which ended at the beginning of the 19th century.
2. Immediately after, a warming period began, which has lasted until now. The causes of the warming must be analogous to those that resulted in the Medieval Warm Period around 1000 AD, the Roman Climate Optimum around the first centuries BC and AD, the Minus Climate Optimum at around 1500 BC, and other warming periods throughout the Holocene.
3. As a result of the recent warming, and as explained in [5], the biosphere has expanded and become more productive, leading to increased CO₂ concentration in the atmosphere and greening of the Earth [17, 18, 19, 32].
4. As a result of the increased CO₂ concentration, the isotopic signature δ¹³C in the atmosphere has decreased.
5. The greenhouse effect on the Earth remained stable in the last century, as it is dominated by the water vapour in the atmosphere [31].
6. Human CO₂ emissions have played a minor role in the recent climatic evolution, which is hardly discernible in observational data and unnecessary to invoke in modelling the observed behaviours, including the change in the isotopic signature δ¹³C in the atmosphere.

Overall, the findings in this paper confirm the major role of the biosphere in the carbon cycle (and through this in climate) and a non-discernible signature of humans.

One may associate the findings of the paper with several questions related to international policies. Do these results relate the hypothesis that CO₂ emissions contribute to global warming through the greenhouse effect? Do these findings, by suggesting a minimal human impact on the isotopic composition of atmospheric carbon, contradict the need to reduce CO₂ emissions? Are human carbon emissions independent from other forms of pollution, such as emissions of fine particles and nitrogen oxides, which can have harmful effects on human health and the environment? These questions are not posed at all in the paper and certainly are not studied in it. Therefore, they cannot be answered on a scientific basis within the paper's confined scope but require further research. The reader may feel free to study such questions and provide sensible replies. It is relevant to note that a reviewer implied these questions and suggested negative replies to each of them.

Ostatnia zmiana: 10:55 AM · 19 mar 2024 · 47,4 tys. Wyświetlenia

66 262 790 62

Źródło: www.x.com, [dostęp 19.03.2024 r.]

Przykładowe sposoby weryfikacji:

- Weryfikacja autora/autorki treści powołującej się na badania, sprawdzenie, jakie inne treści publikuje.
- Sprawdzenie, czy źródło przywołanych badań ma cechy tzw. predatory journal. Można to zweryfikować korzystając z utworzonych w tym celu baz, takich jak np. www.beallist.net.

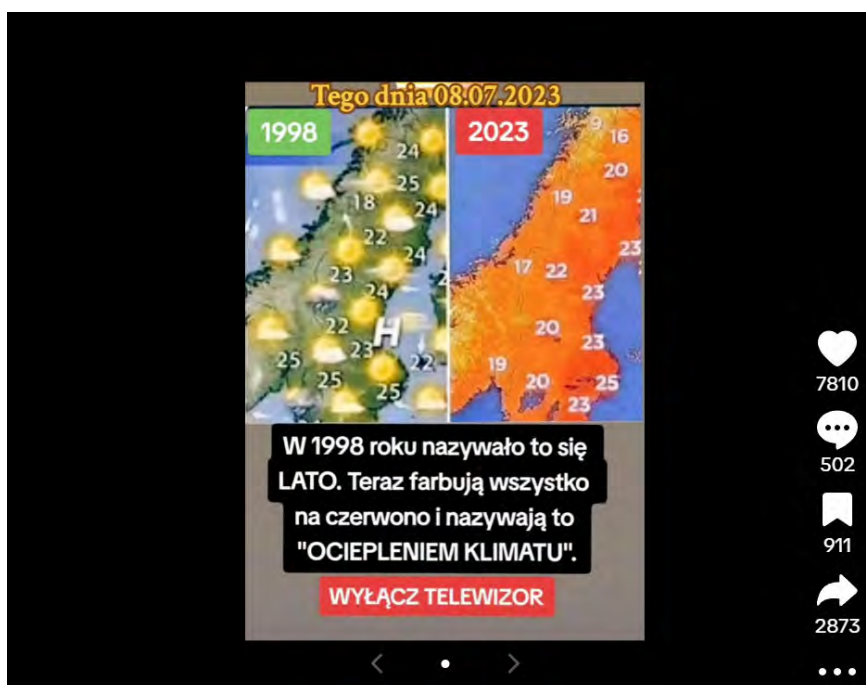
G. FAŁSZYWE POWIĄZANIE

Fałszywe powiązanie polega na tworzeniu pozornych zależności między informacjami w rzeczywistości niezwiązanymi ze sobą. Celem jest więc wprowadzenie odbiorcy/odbiorczynie w błąd poprzez wywołanie wrażenia, że dwa czynniki są od siebie zależne.

Przykładem fałszywego powiązania jest przekaz umieszczony na grafice, która zdobyła popularność w mediach społecznościowych

w lipcu 2024 roku. Zestawiono na niej dwie mapy z prognozą pogody. Jedna z nich była zielona, a na drugiej dominował kolor pomarańczowy. Autor grafiki sugerował, że klimat się nie ociepla, tylko media w dzisiejszych czasach celowo manipulują przekazem. W tym przypadku rzekoma manipulacja mediów miałyby polegać na stosowaniu odpowiednich kolorów, pozornie sugerujących wyższe temperatury. W rzeczywistości mapy te pochodzą z różnych źródeł medialnych, które stosują różne metody wizualizacji prognozy pogody. Ich zestawienie nie jest w żaden sposób uzasadnione. Jest to zatem fałszywe powiązanie. Na grafice podano ponadto fałszywe daty – mapy pochodzą w rzeczywistości z innych lat, niż podane³⁵.

Rys. 9. Materiał na TikToku: przykład fałszywego powiązania.



Źródło: www.tiktok.com [dostęp: 18.07.2024 r.]

Przykładowe sposoby weryfikacji:

- Analiza grafik, zdjęć lub wideo: sprawdzenie ich źródła oraz próba oceny, czy zostały zaprezentowane w pełnym i poprawnym kontekście.
- Sprawdzenie, czy istnieją badania naukowe, które potwierdzają lub obalają zaprezentowane tezy.

35 Demagog.org (2024). Manipulacja przekazem o pogodzie i klimacie? Te mapy to nie dowód, https://demagog.org.pl/fake_news/manipulacja-przekazem-o-pogodzie-i-klimacie-te-mapy-to-nie-dowod/ [dostęp: 18.07.2024 r.]

- Sprawdzenie, czy przywołana kwestia została przeanalizowana i oceniona przez ekspertów w danej dziedzinie.
- Próba odróżnienia korelacji (współwystępowania, pojawienia się dwóch zjawisk jednocześnie) od przyczynowości (gdy coś wynika z czegoś, jedno zjawisko powoduje drugie). Fałszywe powiązanie może błędnie sugerować, że korelacja między dwoma zdarzeniami to ich przyczynowość.



Należy pamiętać, że obecnie praktycznie każda treść w infosferze wymaga od odbiorców/odbiorczyń zachowania ostrożności i krytycznego myślenia. Poza przytoczonymi powyżej sposobami weryfikacji informacji, uniwersalną pomocą w ocenie prawdziwości treści są portale fact-checkingowe, na przykład takie jak: www.demagog.org.pl, www.sprawdzam.afp.com czy www.fake-hunter.pap.pl (więcej o fact-checkingu w części II).



CZĘŚĆ II

Strategie reagowania na dezinformację

2.1. Prebunking, debunking, fact-checking

A. PREBUNKING

Prebunking to strategia przeciwdziałania dezinformacji polegająca na przygotowaniu odbiorców/odbiorczyń na możliwe fałszywe lub wprowadzające w błąd treści, jeszcze zanim użytkownicy się z nimi zetkną oraz obalaniu ich na wczesnym etapie. To swego rodzaju szczepionka przeciwko dezinformacji. Idea prebunkingu oparta jest na teorii psychologicznej inokulacji (zaszczepienia), opracowanej w latach 60. przez psychologa społecznego Williama McGuire'a³⁶. Tak jak szczepionka daje odporność na infekcje dzięki wprowadzeniu do organizmu osłabionej lub martwej formy patogenu, tak prebunking chroni odbiorców przed nieprawdziwymi informacjami przez ich wcześniejszą ekspozycję na nieprawdziwe informacje.

Strategia ta uczy użytkowników/użytkowniczkę, jak rozpoznawać dezinformację, pokazuje mechanizmy, jakie ona wykorzystuje, wyjaśnia, w jaki sposób mogą zostać zmanipulowani. Prebunking nie ma na celu dementowania poszczególnych nieprawdziwych informacji, ale edukację użytkowników na temat ogólnych prawidłowości dotyczących dezinformacji. Badacze wyróżniają dwa główne obszary zastosowania prebunkingu. Jeden koncentruje się na głównych, „szerokich” narracjach dezinformacyjnych i ich obalaniu. Drugi dotyczy najważniejszych technik wykorzystywanych regularnie przez aktorów dezinformacyjnych do wprowadzania odbiorców/odbiorczyń w błąd³⁷.

Instytucje i organizacje zajmujące się przeciwdziałaniem dezinformacji, prowadzą kampanie prebunkingowe, mające na celu budowanie odporności społeczeństw na fałszywe przekazy. Badania wykazują ich

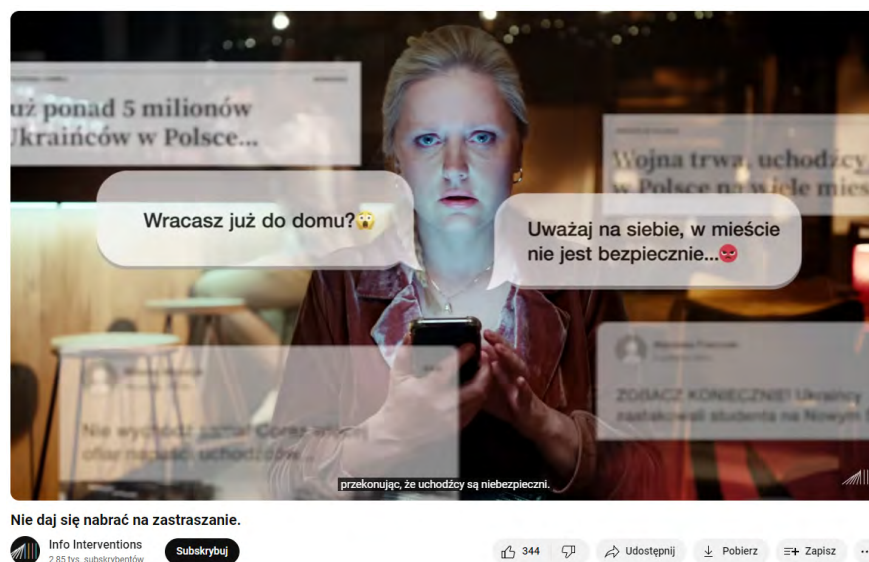
36 J. Roozenbeek, S. Van Der Linden, T. Nygren (2020). *Prebunking interventions based on “inoculation” theory can reduce susceptibility to misinformation across cultures*, <https://misinformation.hks.harvard.edu/article/global-vaccination-badnews/> [dostęp: 03.07.2024 r.]

37 M. Biddlestone, T. Harjani, S. Van der Linden, J. Roozenbeek, A. Stuart, B. Goldberg, M. Graham, M. Iwahara, B. Piri, P. Weigand, R. Xu. (2022). *Obalanie mitów na wczesnym etapie – przewodnik praktyczny*, https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation_pl.pdf [dostęp: 03.07.2024 r.]

skuteczność. Dla przykładu, specjaliści z Uniwersytetu w Cambridge, Uniwersytetu Bristolskiego i Google Jigsaw opracowali 5 krótkich animacji, które były prezentowane użytkownikom jako 30 lub 90-sekundowe reklamy w filmach w serwisie YouTube. Ostrzegały one przez kilkoma technikami manipulacji często stosowanymi w dezinformacji. Okazało się, że animacje te poprawiły zdolność odbiorców/odbiorczyń do wykrywania prób manipulacji oraz odróżniania treści godnych zaufania od nieprawdziwych, a także korzystnie wpłynęły na decyzje o niedostępnieniu dalej fałszywych treści³⁸.

W 2022 roku Google Jigsaw we współpracy z portalem Demagogi oraz NASK-iem, przeprowadził kampanię prebunkingową dotyczącą fałszywych narracji na temat uchodźców z Ukrainy. Aby obalić pojawiające się fałszywe tezy, stworzono serię krótkich filmów. W kampanii uwzględniono kontekst Polski, Czech oraz Słowacji. Po obejrzeniu jednego z filmów o 8% wzrósł odsetek widzów, którzy potrafili prawidłowo rozpoznać omówione techniki manipulacyjne stosowane w kontekście migrantów – sianie strachu lub szukanie kozła³⁹.

Rys. 10. Kadr z filmu w wyprodukowanego w ramach kampanii prebunkingowej Google Jigsaw, NASK i Demagog.



Źródło: www.youtube.com [dostęp: 18.07.2024 r.]

-
- 38 J. Roozenbeek, S. van der Linden, B. Goldberg, S. Rathje, S. Lewandowsky (2022), *Psychological inoculation improves resilience against misinformation on social media*, <https://www.science.org/doi/epdf/10.1126/sciadv.abo6254> [dostęp: 18.07.2024 r.]
- 39 B. Goldberg (2023). *Defanging Disinformation's Threat to Ukrainian Refugees*, <https://medium.com/jigsaw/defanging-disinformations-threat-to-ukrainian-refugees-b164dbbc1c60> [dostęp: 18.07.2024 r.]

Prebunking stosowany w odniesieniu do szerokiej narracji jako prewencyjna strategia przeciwdziałania dezinformacji, może pomóc w podejmowaniu strategicznych działań i promowaniu prawdziwych treści, zanim fałszywy wątek zacznie się rozprzestrzeniać na dużą skalę. Gdy nieprawdziwy przekaz zostanie już powielony tysiące razy, przeciwdziałanie staje się trudniejsze, ponieważ osoby, które miały kontakt z fałszywą informacją mogą być mniej skłonne do uwierzenia w alternatywną wersję opartą na dowodach⁴⁰. Interwencja w takiej sytuacji jest jednak nadal potrzebna. Gdy zatem fałszywa treść zdobyła już popularność, przekonania na dany temat u odbiorców/ odbiorczyń są już silnie ukształtowane lub społeczeństwo jest już wyraźnie podzielone w związku z zaobserwowaną narracją, wówczas zasadne jest zastosowanie strategii debunkingu.

B. DEBUNKING

Debunking (z ang. „obalanie”, „demaskowanie”) odnosi się do procesu ujawniania fałszu i manipulacji⁴¹. Jego celem jest zminimalizowanie wpływu potencjalnie szkodliwych, fałszywych informacji. W przeciwieństwie do prebunkingu, który ma charakter prewencyjny i odnosi się do szerokiej narracji i ogólnych sposobów manipulacji, debunking jest ukierunkowany na konkretny przekaz – podmiot lub temat i demaskuje fałsz w obszarze informacji, które zdobyły już pewną popularność. Ma więc charakter reaktywny.

Należy podkreślić, że debunking nie ogranicza się do samego zaprzeczania, ale zawiera w sobie uzasadnienie, dlaczego dane twierdzenie jest fałszywe, przy jednoczesnym wykazaniu wątpliwej wiarygodności źródła fałszywych tez, jeśli to możliwe⁴².

Skuteczność debunkingu również potwierdzają badania – na przykład seria eksperymentów testujących 52 kontrowersyjne przekonania wśród 10 000 osób podczas wyborów w USA w 2016 roku wykazała jednoznacznie, że osoby, które zobaczyły korekty fałszywych informacji, były znacznie bardziej skłonne do wyrażania zgodnych

40 P. Butcher, A.-H. Neidhardt (2021). *From debunking to prebunking: How to get ahead of disinformation on migration in the EU*, <https://feps-europe.eu/wp-content/uploads/2021/11/From-debunking-to-prebunking-How-to-get-ahead-of-disinformation-on-migration-in-the-EU.pdf> [dostęp: 03.07.2024 r.]

41 NATO Strategic Communications Centre of Excellence (2021). *Fact-checking and debunking. A best practice guide to dealing with disinformation*, https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_fact-checking_and_debunking_02-02-2021-1.pdf [dostęp: 18.07.2024 r.]

42 Global Engagement Center (2020). *GEC Counter-Disinformation Dispatches #4. What Works in Debunking*, <https://apps.dtic.mil/sti/trecms/pdf/AD1137356.pdf> [dostęp: 18.07.2024 r.]

z faktami przekonań niż te, które nie widziały takich korekt⁴³. Choć demaskowanie dezinformacji powoduje powtórzenie również fałszywej bądź wprowadzającej w błąd treści, to gdy odbywa się to wraz ze sprostowaniem, nie prowadzi do znacznych szkód, nawet jeśli odbiorcy/odbiorczynie wcześniej się z nią nie spotkali⁴⁴.

C. FACT-CHECKING

W ogólnym ujęciu, fact-checking (z ang. „weryfikacja faktów”), to proces weryfikacji informacji w celu sprawdzenia ich prawdziwości⁴⁵. Fact-checkingu można dokonać przed lub po publikacji danej informacji.

Fact-checkingu przed publikacją powinni dokonywać dziennikarze w procesie pracy nad materiałem – powinno to być, co do zasady, integralną częścią ich pracy. Niektóre redakcje zatrudniają przeznaczonych do tego zadania analityków weryfikujących informacje zebrane przez dziennikarzy. Nie jest to jednak rozwiązanie popularne w Polsce. W badaniu PressInstitute, w którym wzięli udział polscy dziennikarze/dziennikarki, niemal połowa respondentów (46%) zadeklarowała, że ich pracodawca „nie zabezpiecza dziennikarzy, nie narzuca rozwiązań, sami dbają o weryfikację informacji”. 29% dziennikarzy/dziennikarek wskazało, że pracodawca „sformułował wewnętrzne procedury weryfikacji informacji zabezpieczające dziennikarzy”. 15% respondentów stwierdziło, że redakcja posiada „własny dział fact-checkingu”. 7% nie wie, jakie działania w tym zakresie podejmuje pracodawca, a wg 3% redakcja współpracuje w tym obszarze z zewnętrznym podmiotem⁴⁶. Tymczasem, jak wspomniano, raport Instytutu Reutersa z 2024 roku pokazuje, że zaufanie publiczne do mediów informacyjnych w Polsce spadło od 2015 roku o 17 punktów procentowych (z 56% do 39%)⁴⁷. Nie ulega wątpliwości, że rola weryfikacji treści przez media

43 T. Wood, E. Porter (2019). *The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence*, <https://link.springer.com/article/10.1007/s11109-018-9443-y> [dostęp: 22.07.2024 r.]

44 U.K.H. Ecker, S. Lewandowsky, M. Chadwick (2020). *Can corrections spread misinformation to new audiences? Testing for the elusive familiarity backfire effect*, <https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-020-00241-6> [dostęp: 22.07.2024 r.]

45 K. Wolny-Zmorzyński, K. Doktorowicz, P. Płaneta, R. Filas (red.) (2024). *Leksykon terminów medialnych A-L*, Wydawnictwo Adam Marszałek, s. 224.

46 Press (2022). *Problem dezinformacji w ocenie polskich dziennikarzy*, <https://www.press.pl/pobierz/problem-dezinformacji-2022> [dostęp: 19.07.2024 r.]

47 N. Newman, R. Fletcher, C. T. Robertson, A. Ross Arguedas, R. Kleis Nielsen (2024). *Reuters Institute Digital News Report 2024*, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf [dostęp: 19.07.2024 r.]

jest fundamentalna, szczególnie w kontekście współczesnego, dynamicznego środowiska informacyjnego. Presja czasu i szybkie tempo pracy, a przy tym rozwój technologii ułatwiających produkowanie i szerzenie fałszywych treści sprawiają, że skrupulatna weryfikacja faktów przez redakcje, staje się bardziej wymagająca, a jednocześnie jeszcze bardziej istotna.

Fact-checking dokonywany po publikacji informacji jest domeną analityków/analiticzek działających w na rzecz serwisów lub całych organizacji fact-checkingowych. Analitycy/analiticzki sprawdzają, czy wszystkie informacje w tekście, artykule prasowym czy wypowiedzi lub przemówieniu, są prawdziwe. Następnie publikują swoje wnioski, wskazując na ewentualne manipulacje, nieścisłości i fałszywe wątki. Działalność taka ma na celu poprawę jakości debaty publicznej oraz zwiększenie dostępności rzetelnych i bezstronnych informacji. Korzenie aktywności serwisów i organizacji fact-checkingowych sięgają lat 90. Już w 1994 roku w Stanach Zjednoczonych powstał serwis Snopes.com – pierwotnie jego twórcy koncentrowali się na analizie miejskich legend, a z czasem, w miarę wzrostu zapotrzebowania na rzetelną weryfikację faktów w sieci, rozszerzali swoją działalność. Pierwszą polską organizacją fact-checkingową był z kolei Demagog. Powstał w 2014 roku. Zespół Demagoga weryfikuje m.in. wypowiedzi i obietnice wyborcze polityków/polityczek. Publikuje swoje analizy na portalu demagog.org.pl. Prowadzi także działalność edukacyjną.



Choć fact-checking i debunking mają ze sobą wiele wspólnego, występują między nimi pewne różnice. NATO StratCom COE (Centrum Ekspertyki NATO ds. Komunikacji Strategicznej) wymienia następujące⁴⁸:

- Fact-checking jest prowadzony w duchu bezstronności i apolityczności. Celem jest sprawdzenie poprawności informacji bez względu na źródło. Tymczasem debunking nie musi być apolityczny, ponieważ może być prowadzony przez rządy lub organizacje w celu ujawnienia wrogiego aktora. Może przybierać formę kampanii.
- Fact-checking, w ujęciu całościowym, ma szeroki zakres i dotyczy różnorodnych tematów i źródeł.



48 NATO Strategic Communications Centre of Excellence (2021). Fact-checking and debunking. A best practice guide to dealing with disinformation, https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_fact-checking_and_debunking_02-02-2021-1.pdf [dostęp: 19.07.2024 r.]

Debunking zawsze jest ukierunkowany na konkretnego aktora lub temat.

- Fact-checking ma charakter ogólny. Debunking ma charakter strategiczny, koncentruje się na obaleniu tezy w celu zmniejszenia szkód, jest stosowany głównie względem tematów mających wpływ na kluczowe dla danego podmiotu kwestie.

2.2. Reagowanie na fałszywe treści w bieżącej komunikacji

Reakcja w odpowiednim czasie na zaobserwowaną dezinformację może znacząco zmniejszyć jej wpływ na społeczeństwo i wzmocnić zaufanie publiczne. Aby skutecznie zareagować na fałszywe treści, warto rozważyć uwzględnienie następujących praktyk:

- **Nazwać i zawstydzić („name & shame”).** Powstrzymanie dezinformacji wymaga mówienia o niej wprost na podstawie wiedzy pochodzącej z rzetelnych źródeł. Używając solidnych argumentów przedstawionych w sposób merytoryczny, można efektywnie podważyć wiarygodność fałszywych informacji i zdemaskować ich autorów/autorki.
- **Pokazać, na czym polega dezinformacja.** Skuteczna reakcja na fałszywą treść wymaga ujawnienia sposobów manipulacji oraz ukazania jej celów. Kluczowe jest zademonstrowanie, jak fałszywa treść została zmanipulowana oraz jakie mogą być konsekwencje jej oddziaływania na opinię publiczną.
- **Stosować odpowiedzialną komunikację.** Istotną kwestią jest sposób komunikowania o dezinformacji. Należy używać bezemocjonalnych, prostych sformułowań, przejrzystych przykładów, a w razie niejasności – przedstawiać kolejne szczegółowe informacje. Używanie jasnych komunikatów minimalizuje ryzyko błędnej interpretacji i zwiększa zrozumiałość przekazu.
- **Budować zaufanie poprzez wskazywanie prawdy.** Reagując na dezinformację, należy przedstawić prawdziwy przekaz na dany

temat. Dzięki temu zapobiega się przeświadczeniu, że nie można dotrzeć do rzetelnych źródeł, a przez to również do prawdziwych treści.

- **W uzasadnionych przypadkach – ignorować.** Niektóre fałszywe wątki lepiej pozostawić bez odpowiedzi, aby nie przyciągać do nich dodatkowej uwagi. Wskazanie szerokiego gronu odbiorców/ odbiorczyń fałszywej treści, która nie zdobyła popularności i nie ma wysokiej szkodliwości, może jedynie rozszerzyć zasięg nieprawdziwej narracji.

Dobre praktyki w reagowaniu na dezinformację:

1. REAGOWANIE TAK SZYBKO, JAK TO MOŻLIWE

Na dezinformację należy odpowiadać możliwie szybko, by nie pozwolić szkodliwej treści eskalować.

2. UŻYWANIE ZRZUTÓW EKRANU, A NIE LINKÓW

Dzięki postugiwaniu się zrzutami ekranu prezentującymi obalane tezy, zamiast udostępniania linków, nie zwiększa się zasięgu szkodliwych treści. Warto jednak pamiętać o archiwizacji dowodów w związku z łatwością spreparowania zrzutu ekranu (poprzez zapis w chmurze, na dysku lub innym urządzeniu zewnętrznym).

3. NAZYWANIE DEZINFORMACJI PO IMIENIU

W walce z dezinformacją istotne jest jasne zaprzeczanie nieprawdziwym stwierdzeniom. Należy stanowczo i konkretnie, ale bez emocji dementować fałszywe informacje.

4. POWOŁYWANIE SIĘ NA RZETELNE DANE

Podpieranie prezentowanych twierdzeń dowodami – konkretne liczby, badania i wyliczenia dodają wiarygodności przekazowi.

5. PRZYZNANIE SIĘ DO BŁĘDU

Każdy może popełnić błąd. W przypadku podania fałszywej informacji, należy się do tego przyznać i sprostować nieprawidłowe dane. Pozwala to zachować klarowność komunikacji.



CZĘŚĆ III

Komunikacja w obliczu kryzysu

3.1. Komunikacja w samorządach

Jednostki samorządu terytorialnego (JST) to organy administracyjne najbliższe codziennemu życiu obywateli. Właśnie dlatego istotne jest właściwe prowadzenie efektywnej komunikacji zarówno na co dzień, jak i w sytuacjach kryzysowych.

Misją samorządu terytorialnego są działania na rzecz wszystkich podmiotów z danego obszaru. Dlatego konieczne jest zapewnienie inkluzywnego podejścia w kwestii zapewnienia dostępu do informacji. Oznacza to właściwy dobór języka i kanałów komunikacji, tak aby skutecznie docierać do różnych grup interesariuszy, którymi mogą być np.: mieszkańcy, przedsiębiorcy, organizacje społeczne czy media.

Odpowiednio poprowadzona komunikacja, czyli taka która dostosowuje język, zrozumiałość, nacechowanie emocjonalne i kanały komunikacji przekazu do odbiorców, podnosi poziom publicznego zaufania, a to jest szczególnie ważne w sytuacjach kryzysowych.

3.1.1. Cele komunikacji

Określenie celów komunikacji to kluczowy element na etapie jej planowania.

Przykładowe cele komunikacji to:

- poprawa wizerunku jednostki samorządowej;
- zwiększenie zaangażowania mieszkańców;
- reagowanie na kryzysy informacyjne;
- zapewnienie transparentności dla działań podejmowanych przez jednostkę.

Należy pamiętać, że cele komunikacyjne wynikają z potrzeb danej JST i powinny być ustalane indywidualnie.

Wyznaczenie celów powinno wiązać się z identyfikacją kluczowych odbiorców i odbiorczyń i zrozumieniem ich potrzeb informacyjnych. Tylko w ten sposób można skutecznie wybrać odpowiednie kanały komunikacji, takie jak: media tradycyjne, media społecznościowe, bannery, ale też spotkania czy biuletyny.

3.1.2. Monitorowanie i ewaluacja działań komunikacyjnych

Regularne monitorowanie i analiza efektywności działań komunikacyjnych są niezbędne do oceny, czy założone cele są w odpowiedni sposób realizowane. Wykorzystanie takich wskaźników, jak: zasięg komunikatów, zaangażowanie odbiorców i odbiorczyń czy liczba pozytywnych interakcji, pozwala na bieżąco dostosowywać strategię komunikacyjną do potrzeb społeczności i je modyfikować, jeśli nie przynoszą odpowiednich rezultatów. Dlatego oprócz monitoringu kluczowe jest wyciąganie wniosków dotyczących skuteczności przeprowadzonych działań.

3.2. Reagowanie na dezinformację

Dezinformacja może prowadzić do spadku zaufania do instytucji publicznych, także do JST. Przestępcy wykorzystują coraz doskonalsze narzędzia wspierane przez rozwój sztucznej inteligencji. Pozwalają one na tworzenie fałszywych, ale sprawiających niezwykle realistyczne wrażenie komunikatów – w formie tekstu, zdjęć, nagrań głosowych czy wideo. Warto sobie uświadomić, że dezinformacja jest powszechna

w przestrzeni publicznej, wszyscy jesteśmy na nią narażeni i musimy się nauczyć ją skutecznie rozpoznawać i neutralizować. Dlatego tak istotna jest szybka korekta błędnych informacji oraz identyfikacja jej źródeł.

Budowanie zaufania mieszkańców do JST i skuteczną walkę z dezinformacją warto prowadzić w oparciu o następujące działania:

1. IDENTYFIKACJA ŹRÓDEŁ DEZINFORMACJI

Monitorowanie mediów i platform społecznościowych pozwala na wczesne wykrycie fałszywych informacji. Warto wykorzystać nowoczesne narzędzia do monitoringu mediów i znaleźć w budżecie JST środki umożliwiające korzystanie z przeznaczonych do tego serwisów. Profesjonalny monitoring zapewnia wyszukiwanie informacji we wszystkich typach mediów, pod kątem zdefiniowanych wcześniej określonych słów kluczowych, np. nazwy instytucji, produktu, zjawiska.

Niezbędne jest także powołanie osoby/zespołu, który odpowiada za dynamiczną i adekwatną reakcję na pojawiającą się komunikację kryzysową, w tym dezinformację.

Jedną z metod mających na celu zapobieganiu dezinformacji jest wprowadzenie systemu wczesnego ostrzegania, który umożliwia szybkie reagowanie na pojawiające się fałszywe informacje.

System wczesnego ostrzegania przed dezinformacją powinien zawierać:

- Monitoring: z wykorzystaniem narzędzi do monitoringu mediów oraz portali społecznościowych (większość narzędzi pozwala na obserwowanie pojawiających się wzmianek w czasie rzeczywistym, raz dziennie pojawiają się natomiast raporty zbiorcze umożliwiające ocenę reakcje na daną informację – np. poprzez liczbę jej odbiorców).
- Analizę i ocenę ryzyka, która pomoże odpowiedzieć na pytania o skutki zdarzenia. Istotne jest także utworzenie komórki składającej się z wykwalifikowanych osób, odpowiedzialnych za raportowanie danych i ich ocenę.
- System dynamicznego reagowania: powinien być opracowany obieg przetwarzania informacji i procedury zgłaszania do odpowiednich organów i społeczności.
- System zarządzania kryzysowego: planowanie i wdrażanie działań prewencyjnych oraz odpowiednich reakcji na dezinformację.

2. KOREKTA BŁĘDNYCH INFORMACJI

Szybka korekta błędnych informacji oraz dotarcie z rzetelnym przekazem do mieszkańców są kluczowe dla zapobiegania rozprzestrzenianiu się dezinformacji i minimalizowania jej skutków. Komunikat korygujący nieprawdziwe lub zmanipulowane treści powinien w prosty sposób wyjaśniać fakty dotyczące konkretnej sprawy.

Warto stworzyć gotowe szablony komunikatów, które można szybko dostosować i użyć w przypadku potrzeby wystosowania sprostowania dotyczącego fałszywych informacji.

Komunikat powinien zawierać:

- treść i źródło fałszywej informacji;
- jasne wyjaśnienie realnej sytuacji;
- opis podjętych działań;
- wszystkie niezbędne elementy oficjalnego pisma (logo, stopkę, i inne elementy identyfikacji JST).

Rys. 11. Przykład komunikatu korygującego fałszywą treść.

KOMUNIKATY

Sprostowanie – fake news

W mediach społecznościowych oraz za pośrednictwem poczty elektronicznej dystrybuowany jest skan pisma rzekomo podpisanego nazwiskiem marszałka województwa mazowieckiego Adama Struzika. Pismo dotyczyć ma zatrzymywania obywateli Ukrainy w wieku poborowym.

Informujemy, że pismo to jest sfalszowane, a sama informacja jest przykładem fake newsa i próbą dezinformacji. Marszałek województwa nigdy nie podpisywał żadnego pisma w tej sprawie. Takie pismo nie powstało również w urzędzie marszałkowskim województwa mazowieckiego.

W obliczu zaistniałej sytuacji dziś marszałek województwa poinformuje o zajęciu stosowne służby.

O działaniach dezinformacyjnych i fałszywych pismach informuje również Konsulat Generalny Ukrainy w Krakowie i Rządowe Centrum Bezpieczeństwa.

Źródło: <https://bip.mazovia.pl/pl/bip/komunikaty/sprostowanie-fake-news.html> [dostęp: 11.10.2024 r.]

3. EDUKACJA MIESZKAŃCÓW

Edukacja mieszkańców w zakresie rozpoznawania dezinformacji, przygotowanie ich na narracje, techniki i metody wykorzystywane przez aktorów dezinformacyjnych zwiększają społeczną odporność na dezinformację. Kampanie edukacyjne, kursy i szkolenia mieszkańców, powinny stanowić stały element działalności JST i zawierać takie elementy jak: zrozumienie zjawiska dezinformacji i związanych z nią zagrożeń, dostarczenie wiedzy na temat sposobów rozpoznawania źródeł dezinformacji, ćwiczenie i podkreślenie znaczenia umiejętności krytycznego myślenia.

JST posiada wszelkie, niezbędne narzędzia do edukacji mieszkańców. Oprócz organizacji regularnych szkoleń czy webinarów można także zaproponować mieszkańcom aktywności, które łączą edukację z rozrywką, np. grę terenową lub konkurs.

4. WSPÓŁPRACA Z MEDIAMI

Współpraca z mediami realizowana poprzez np. organizację spotkań prasowych czy wywiadów pozwala na szybkie dotarcie z rzetelnymi informacjami do mieszkańców, co może być niezwykle istotne w ograniczaniu rozprzestrzeniania się dezinformacji. Pracując z lokalnymi mediami, JST ma szansę na zbudowanie zaufania publicznego poprzez wykorzystanie szerokich zasięgów lokalnych rozgłośni radiowych, telewizji czy dzienników, a także kanałów w mediach społecznościowych. Warto podkreślić, że efektywna współpraca to współpraca otwarta, taka która budowana jest systematycznie (także w czasach „bez kryzysów”) oraz proaktywnie. Należy więc pamiętać o szanowaniu pracy mediów, regularnym odpowiadaniu na zapytania czy prośby o wywiad, otwartość w komunikacji i transparentność w przekazywaniu informacji.

5. KOMUNIKACJA KRYZYSOWA

Komunikacja kryzysowa powinna być zawsze uwzględniona w planach kryzysowych, które mają na celu nie tylko usprawnienie działań w sytuacjach kryzysowych, ale również zapewnienie poczucie bezpieczeństwa pracownikom JST. Każdy kryzys jest inny i wymaga odpowiedzi dostosowane do danej sytuacji. W zarządzaniu sytuacją kryzysową kluczową rolę powinien odgrywać powołany do tego zadania zespół. Ważne, aby znalazły się w nim także osoby odpowiedzialne za komunikację. Zespół powinien działać w oparciu o przygotowany wcześniej plan, który należy dostosować każdorazowo do sytuacji.

W praktyce plan zawiera takie elementy jak: mapę ryzyk wraz z szacunkiem ich wystąpienia i opisem scenariuszy postępowania. Wskazuje m.in. łańcuch dowodzenia, czyli osoby odpowiedzialne za poszczególne działania, ich zadania i obowiązki. Warto podkreślić, że wśród potencjalnych scenariuszy w planie powinny być uwzględnione także takie, które mówią o reakcji na dezinformację, cyberzagrożenia. Plan powinien podlegać regularnej aktualizacji (np. raz w roku). W obliczu kryzysu (także jeśli jest wywołany przez dezinformację) do ważnych działań należą między innymi:

1. Analiza sytuacji (umożliwia ocenę aktualnych problemów. Do jej przeprowadzenia możemy wykorzystać np. dane pozyskane dzięki monitoringowi mediów i platform społecznościowych).
2. Określenie celów komunikacji (po co ją uruchamiamy?).
3. Wybór odpowiednich kanałów (determinuje je grupa docelowa – w niektórych przypadkach skuteczniejsze niż poinformowanie poprzez media może okazać się zorganizowanie spotkania z mieszkańcami).

Sugerowane kanały według grupy docelowej:

- **Rodziny:** media społecznościowe, newslettery, spotkania publiczne.
- **Seniorzy:** media tradycyjne (lokalne), tablice ogłoszeniowe, spotkania publiczne.
- **Młodzież:** media społecznościowe, aplikacje mobilne.
- **Przedsiębiorcy:** strona internetowa, newslettery, spotkania publiczne, LinkedIn.
- **NGO:** spotkania publiczne, e-maile, media społecznościowe.
- **Media:** konferencje prasowe, komunikaty prasowe, media społecznościowe.
- **Instytucje edukacyjne i kulturalne:** biuletyny, media.

4. Opracowanie przekazu (dobór języka)

Jak widać istnieje wiele różnych grup, do których może być skierowany komunikat. Ważne jest, aby odpowiednio przygotować wiadomość, tak by była ona zrozumiała dla grupy docelowej. Inaczej należy mówić do przedsiębiorców, inaczej do młodzieży.

5. Uruchomienie komunikacji

To moment, w którym wychodzimy z komunikatem „do ludzi”, może to oznaczać zwołanie konferencji prasowej, publikację biuletynu, lub zaproszenie mieszkańców na spotkanie. Bardzo ważne jest, by w sytuacji kryzysowej nie zwlekać z uruchomieniem komunikacji – czas ma tu często znaczenie.

6. Monitorowanie i analiza publikacji

Ocena czy nasze działania są zrozumiałe i przynoszą cel, który sobie założyliśmy. Komunikacja powinna być dwustronna. To nie tylko mówienie czy pisanie do ludzi, ale także, a może przed wszystkim słuchanie i wchodzenie w dialog. Dlatego tak ważne jest monitorowanie reakcji na komunikację i odpowiednie reagowanie.

7. Reagowanie na bieżąco we współpracy z zespołem zarządzania kryzysowego.

8. Ocena i wnioski (to ważny element, bo pozwala lepiej przygotować się na kolejny kryzys).

PODSUMOWANIE

Warto pamiętać, że efektywna komunikacja kryzysowa przynosi wiele korzyści dla JST. Właściwie prowadzona – zrozumiała, rzetelna i dostarczona we odpowiednim czasie – wzmacnia zaufanie społeczności oraz postrzeganie samorządu jako odpowiedzialnego partnera, gotowego mierzyć się z kluczowymi dla mieszkańców wyzwaniami.

Przykłady komunikacji kryzysowej w obliczu dezinformacji w wykonaniu jednostek samorządu terytorialnego

GMINA MICHAŁOWO

Jednym z samorządów w Polsce, który podjął aktywną walkę z fałszywymi przekazami, jest Gmina Michałowo w województwie podlaskim. W 2021 roku, w czasie kryzysu migracyjnego na granicy polsko-białoruskiej, Michałowo stało się miejscem, które szczególnie doświadczyło problemu dezinformacji. W przestrzeni informacyjnej pojawiały się m.in. przekazy o rzekomym zagrożeniu dla mieszkańców oraz nieprawdzie doniesienia na temat działań podejmowanych przez lokalne władze. Samorząd Michałowa zdecydował się na podjęcie kroków mających na celu zapewnienie mieszkańcom dostępu do rzetelnych informacji.

Jednym z fałszywych wątków, który zaobserwowano w związku z sytuacją w Michałowie, była informacja dotycząca rzekomej działalności

przestępczej migrantów na terenie gminy. W mediach społecznościowych oraz na łamach portali internetowych zaczęły krążyć nieprawdziwe doniesienia o tym, że migranci, którzy przebywali w okolicach Michałowa, mieli dokonywać włamań do domów i atakować mieszkańców. Dezinformacja wywołała niepokój w społeczności Michałowa i okolicznych miejscowości, wzmacniając napięcia i prowadząc do zwiększonego poczucia zagrożenia.

W odpowiedzi na te doniesienia, władze Gminy Michałowo oraz lokalne służby porządkowe wydały oficjalne komunikaty, w których stanowczo zaprzeczyły nieprawdziwym informacjom. Podkreślono, że nie odnotowano żadnych przypadków przestępstw popełnionych przez migrantów na terenie gminy, a rozpowszechniane w mediach społecznościowych doniesienia są fałszywe.

Władze Michałowa zorganizowały również spotkania z mieszkańcami oraz współpracowały z mediami lokalnymi, aby zapewnić dostęp do sprawdzonych informacji i uspokoić nastroje społeczne. Dzięki tym działaniom udało się obalić rozpowszechniane fałszywe tezy i zredukować obawy mieszkańców.

WROCŁAW

Miasto Wrocław stoczyło walkę z dezinformacją dotyczącą rzekomych celowych zakażeń wirusem HIV. Za sprawą TikToka, wiosną 2024 roku, powróciła legenda miejska, jakoby we wrocławskich klubach dochodziło do zakażeń za pomocą wkłuc zakażonymi strzykawkami.

Informacja błyskawicznie rozprzestrzeniła się w mediach społecznościowych. W odpowiedzi, władze miasta oraz Komenda Miejska Policji informowały, że nie pojawiły się żadne zgłoszenia o tego rodzaju incydentach.

Miasto, udzielając informacji lokalnym mediom uspokoiło mieszkańców Wrocławia. Szybko rozprzestrzeniająca się plotka została zdementowana, a w mediach społecznościowych przekazywano sobie informacje o tym, iż rzekome zakażenia podczas Juwenaliów to klasyczny przykład dezinformacji.

Bibliografia

- B. Goldberg (2023). Defanging Disinformation's Threat to Ukrainian Refugees, <https://medium.com/jigsaw/defanging-disinformations-threat-to-ukrainian-refugees-b164dbbc1c60> [dostęp: 18.07.2024 r.]
- B. Gulla Kinga Tucholska, A. Ziernicka-Wojtaszek (2020). Psychologia kryzysu klimatycznego, <https://ruj.uj.edu.pl/server/api/core/bitstreams/0d-d30446-c8eb-4ea0-bd50-52eba8d0dce2/content> [dostęp: 18.07.2024 r.]
- Biblioteka Główna AGH, Predatory journals, <https://bg.agh.edu.pl/otwarta-nauka/open-access/drapieżne-czasopisma> [dostęp: 16.07.2024 r.]
- C. Martel, G. Pennycook, D.G. Rand (2020). Reliance on emotion promotes belief in fake news, *Cogn. Research* 5, 47, <https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-020-00252-3#citeas> [dostęp: 05.07.2024 r.]; <https://www.szkołazklasa.org.pl/jak-emocje-wplywaja-na-podatnosc-mlodziezy-na-dezinformacje-wystartowal-program-fake-know-more/> [dostęp: 05.07.2024 r.]
- Demagog.org (2024), Emisja CO₂ nie wpływa na klimat? Rzetelne źródła mówią inaczej, https://demagog.org.pl/fake_news/emisja-co%E2%82%-82-nie-wplywa-na-klimat-rzetelne-zrodla-mowia-inaczej/ [dostęp: 16.07.2024 r.]
- Demagog.org (2024). Manipulacja przekazem o pogodzie i klimacie? Te mapy to nie dowód, https://demagog.org.pl/fake_news/manipulacja-przekazem-o-pogodzie-i-klimacie-te-mapy-to-nie-dowod/ [dostęp: 18.07.2024 r.]
- Demagog.org (2024). Rumuńscy kibice skandują „Putin” w trakcie Euro? To przeróbka, https://demagog.org.pl/fake_news/rumunscy-kibice-skanduja-putin-w-trakcie-euro-to-przerobka/ [dostęp: 15.07.2024 r.]
- DigitalPoland (2024). Dezinformacja oczami Polaków 2024, <https://digitalpoland.org/publikacje/pobierz?id=70f40c4e-3fe1-4abd-9a-32-02a26c324f18> [dostęp: 28.06.2024 r.]
- EEAS (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf [dostęp: 04.07.2024 r.]

EEAS (2024). Tackling Disinformation, Foreign Information Manipulation & Interference, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en#81218 [dostęp: 05.07.2024 r.]

Global Engagement Center (2020). GEC Counter-Disinformation Dispatches #4. What Works in Debunking, <https://apps.dtic.mil/sti/trecms/pdf/AD1137356.pdf> [dostęp: 18.07.2024 r.]

Gov.pl (2023). [AKTUALIZACJA] UWAGA! CSIRT NASK ostrzega przed kampanią e-mailową podszywającą się pod Ministerstwo Spraw Wewnętrznych i Administracji!, <https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostrzega-przed-kampania-e-mailowa-podszywajaca-sie-pod-ministerstwo-spraw-wewnetrznych-i-administracji>

Instytut Badań Internetu i Mediów Społecznościowych (2022). <https://x.com/ibimspl/status/1496815247402938371> [dostęp: 02.07.2024 r.]

J. Kreft (2018), Władza algorytmów. U źródeł potęgi Google i Facebooka, Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, s. 13, https://www.researchgate.net/profile/Jan-Kreft/publication/332752295_Wladza_algorytmow_U_zrodel_potegi_Google_i_Facebooka/links/5ec6b61c458515626cbf1ac7/Wladza-algorytmow-U-zrodel-potegi-Google-i-Facebooka.pdf, [dostęp: 28.06.2024 r.]

J. Roozenbeek, S. van der Linden, B. Goldberg, S. Rathje, S. Lewandowsky (2022), Psychological inoculation improves resilience against misinformation on social media, <https://www.science.org/doi/epdf/10.1126/sciadv.abo6254> [dostęp: 18.07.2024 r.]

J. Roozenbeek, S. Van Der Linden, T. Nygren (2020). Prebunking interventions based on “inoculation” theory can reduce susceptibility to misinformation across cultures, <https://misinfoeview.hks.harvard.edu/article/global-vaccination-badnews/> [dostęp: 03.07.2024 r.]

J. Skorus, Komunikacja we władzy algorytmów – szansa czy zagrożenie?, [w:] Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach, Nr 1(16)/2020, s. 79, https://wszop.edu.pl/wp-content/uploads/2021/06/05_Komunikacja_we_wladzy_J_Skorus-1.pdf [dostęp: 01.07.2024 r.]

K. Bąkowicz (2023), Dezinformacja – instrukcja obsługi, Warszawa: Wydawnictwo CeDeWu Sp. z o.o.

K. Jabłonowski, „Tusk wyprzedaje zapasy gazu”? To manipulacyjny przekaz, <https://konkret24.tvn24.pl/polska/tusk-wyprzedaje-zapasy-gazu-to-manipulacyjny-przekaz-st7833597> [dostęp: 16.07.2024 r.]

K. Wolny-Zmorzyński, K. Doktorowicz, P. Płaneta, R. Filas (red.) (2024). Leksykon terminów medialnych A-L, Wydawnictwo Adam Marszałek, s. 224.

Komisja Europejska, Akt o usługach cyfrowych: Pytania i odpowiedzi, <https://digital-strategy.ec.europa.eu/pl/faqs/digital-services-act-questions-and-answers> [dostęp: 05.07.2024 r.]

Ł. Olejnik (2024). Propaganda – od dezinformacji i wpływu do operacji i wojny informacyjnej, Warszawa: Wydawnictwo Naukowe PWN SA.

M. Biddlestone, T. Harjani, S. Van der Linden, J. Roozenbeek, A. Stuart, B. Goldberg, M.

Graham, M. Iwahara, B. Piri, P. Weigand, R. Xu. (2022). Obalanie mitów na wczesnym etapie – przewodnik praktyczny, https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation_pl.pdf [dostęp: 03.07.2024 r.]

M. Szpunar (2018), Koncepcja bańki filtrującej a hipernarcyzm nowych mediów [w:] Zeszyty prasoznawcze, s. 194, https://www.magdalenaszpunar.com/_publikacje/2018/4-Magdalena%20Szpunar-1.pdf [dostęp: 01.07.2024 r.]

Mandiant (2021). Ghostwriter update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf [dostęp: 11.07.2024 r.]

Mandiant (2021). UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests, <https://cloud.google.com/blog/topics/threat-intelligence/unc-1151-linked-to-belarus-government/> [dostęp: 11.07.2024 r.]

N. Gleicher, Meta (2018), Coordinated Inauthentic Behavior Explained, [Coordinated Inauthentic Behavior Explained | Meta \(fb.com\)](https://www.facebook.com/notes/meta/coordinated-inauthentic-behavior-explained/) [dostęp: 05.07.2024 r.]

N. Hénin, EU DisinfoLab (2023). FIMI: towards the European redefinition of foreign interference, https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [dostęp: 03.09.2024 r.]

N. Newman, R. Fletcher, C. T. Robertson, A. Ross Arguedas, R. Kleis Nielsen (2024). Reuters Institute Digital News Report 2024, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf [dostęp: 19.07.2024 r.]

NATO Strategic Communications Centre of Excellence (2021). Fact-checking and debunking. A best practice guide to dealing with disinformation, https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_fact-checking_and_debunking_02-02-2021-1.pdf [dostęp: 18.07.2024 r.]

P. Butcher, A.-H. Neidhardt (2021). From debunking to prebunking: How to get ahead of disinformation on migration in the EU, <https://feps-europe.eu/wp-content/uploads/2021/11/>

[From-debunking-to-prebunking-How-to-get-ahead-of-disinformation-on-migration-in-the-EU.pdf](#) [dostęp: 03.07.2024 r.]

P. Sobiesiak-Penszko, M. Kopka-Piątek (2022), Szaleńcy spod szyldu agend klimatycznych. Dezinformacja i propaganda w sprawach zmiany klimatu i polityki klimatycznej. Raport z monitoringu mediów, <https://www.isp.org.pl/pl/publikacje/szalen-cy-spod-szyldu-agend-klimatycznych-dezinformacja-i-propaganda-w-sprawach-zmiany-klimatu-i-polityki-klimatycznej-raport-z-monitoringu-medio-w> [dostęp: 18.07.2024 r.]

Press (2022). Problem dezinformacji w ocenie polskich dziennikarzy, <https://www.press.pl/pobierz/problem-dezinformacji-2022> [dostęp: 19.07.2024 r.]

R. Greifeneder, M. E. Jaffé, E. J. Newman, and N. Schwarz (2020). The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation, https://www.researchgate.net/publication/345954715_The_Psychology_of_Fake_News_Accepting_Sharing_and_Correcting_Misinformation [dostęp: 05.07.2024 r.]

Reuters Institute (2024). Digital News Report. Poland, <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024/poland> [dostęp: 05.09.2024 r.]

S. Juszczyk (2023). Funkcjonowanie młodzieży w świecie postcyfrowym na podstawie wielodyscyplinowych badań w ramach paradygmatów: Przemysł 4.0, Edukacja 4.0 oraz Społeczeństwo 5.0, [w:] E. Widawska (red.), Młode pokolenie w (nie)przyjaznym świecie – konteksty teoretyczne, metodologiczne i praktyczne, s. 166-167.

S. Walker (2015). The Russian troll factory at the heart of the meddling allegations, The Guardian, <https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house> [dostęp: 02.07.2024 r.]

T. Wood, E. Porter (2019). The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence, <https://link.springer.com/article/10.1007/s11109-018-9443-y> [dostęp: 22.07.2024 r.]

U.K.H. Ecker, S. Lewandowsky, M. Chadwick (2020). Can corrections spread misinformation to new audiences? Testing for the elusive familiarity backfire effect, <https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-020-00241-6> [dostęp: 22.07.2024 r.]

World Economic Forum (2024). Global Risks Report 2024, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf [dostęp: 05.07.2024 r.]

NASK