



Temat 3 .

Dezinformacja,
propaganda i inżynieria
społeczna

dr inż. Michał Malinowski

<https://www.drmalinowski.edu.pl>

BEZPIECZEŃSTWO
INFORMACJI



- Dezinformacja
- Propaganda
- FakeNews
- Systemy rekomendacji
- Bańka informacyjna
- Wojna hybrydowa
- Inżynieria społeczna
- Fake influencers
- Techniki obrony

Zadanie

Treść

Prezentacja zadania podczas zajęć.

Okolo 9 osób podczas zajęć

(0-2 pkt)



Dezinformacja

Dezinformacja

celowe rozpowszechnianie fałszywych lub wprowadzających w błąd informacji w celu manipulacji opinią publiczną, osiągnięcia korzyści politycznych, ekonomicznych lub społecznych.

Cechy

Celowe działanie

nie jest to przypadkowy błąd, lecz świadome wprowadzanie w błąd.

Ukryty cel

manipulacja odbiorcami dla osiągnięcia określonych korzyści.

Szeroki zasięg

często rozpowszechniana przez media, internet, media społecznościowe.

Wzmacnianie emocji

odwoływanie się do strachu, złości, kontrowersji.

Nieprawdziwe informacje o politykach mający wpłynąć na wybory

Fałszywe informacje o szczepionkach prowadzące do paniki.

Dezinformacja

Błędna informacja

nieprawdziwa lub niedokładna informacja rozpowszechniana **nieświadomie**, bez zamiaru manipulacji lub wprowadzenia w błąd.

Różnice między dezinformacją a błędną informacją

 Cecha	 Dezinformacja	 Błędna informacja
 Intencja	Celowe wprowadzanie w błąd w określonym celu (np. politycznym, społecznym, ekonomicznym).	Brak złej intencji – wynika z nieświadomego błędu lub braku wiedzy.
 Źródło i sposób rozpowszechniania	Tworzona i rozpowszechniana w sposób zorganizowany (np. przez rządy, grupy propagandowe, fałszywe media).	Często przekazywana przypadkowo przez zwykłych użytkowników, którzy wierzą w jej prawdziwość.
 Możliwość korekty	Trudna do zweryfikowania i często powielana pomimo dowodów na jej fałszywość.	Może być stosunkowo łatwo skorygowana po sprawdzeniu wiarygodnych źródeł.

Dezinformacja

Główne zasady przetwarzania informacji przez mózg

Mózg selekcjonuje informacje nie analizujemy wszystkiego, tylko to, co uznajemy za istotne.

Preferujemy szybkie, intuicyjne osądy zamiast głębokiej analizy (myślenie heurystyczne).

Silne emocje (strach, gniew) zwiększają podatność na manipulację i zmniejszają zdolność krytycznego myślenia.



Wrażenie
znajomości

Impuls
zakupowy

System 1

Szybki ale impulsywny

Racjonalizacja
decyzji

System 2

Leniwy ale analityczny

Dezinformacja

Efekt potwierdzenia (confirmation bias)

Skłonność do szukania, interpretowania i zapamiętywania informacji w sposób potwierdzający nasze wcześniejsze przekonania.

Ignorowanie lub odrzucanie dowodów sprzecznych z naszymi poglądami.

Osoba wierząca w teorię spiskową będzie ignorować fakty naukowe, a szukać treści potwierdzających jej przekonanie.



Dezinformacja

Podatność na manipulację

Bańki informacyjne (filter bubbles)

- algorytmy mediów społecznościowych pokazują nam tylko treści zgodne z naszymi zainteresowaniami, zamykając nas w wąskiej perspektywie.

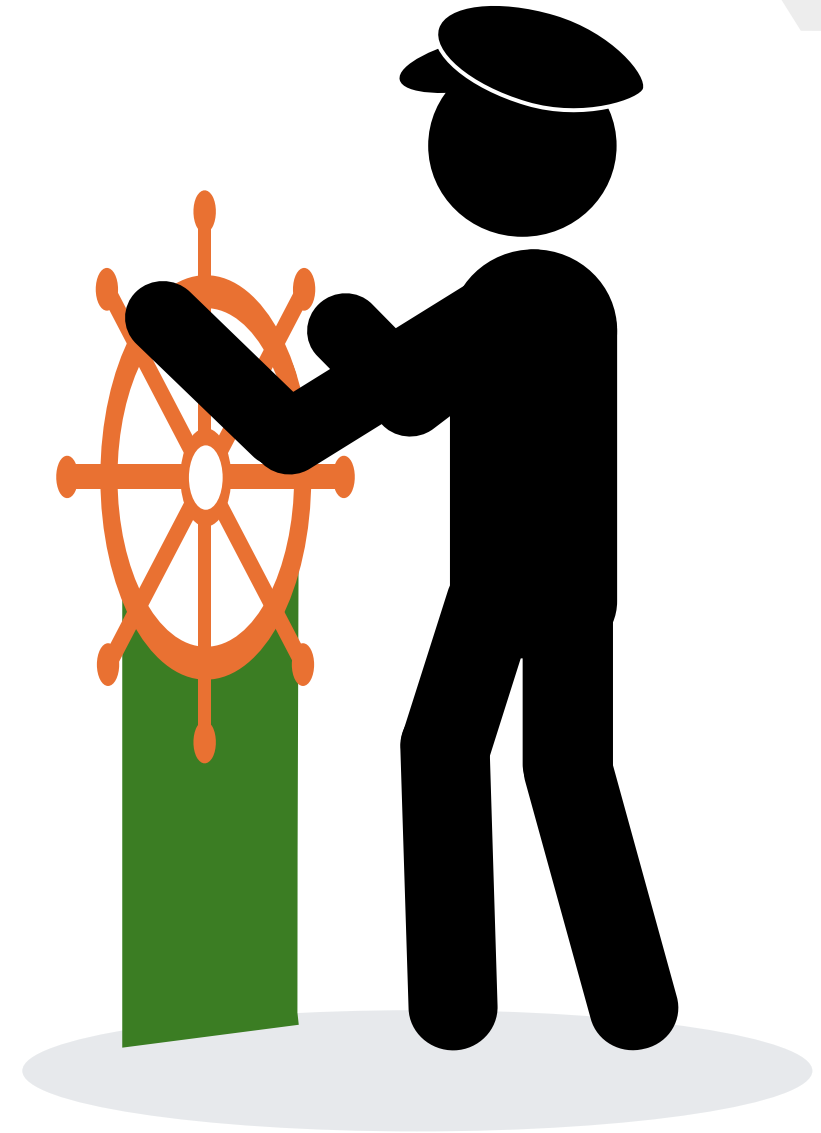
Efekt pierwszeństwa i efekt świeżości

- pierwsze i ostatnie informacje, które usłyszymy, najbardziej wpływają na nasze zdanie.

Zjawisko iluzorycznej prawdy (illusory truth effect)

- im częściej słyszymy daną informację, tym bardziej wydaje nam się prawdziwa, nawet jeśli jest fałszywa.

Po ile zwierząt każdego gatunku
zabrał Mojżesz do Arki?



Dezinformacja

Clickbait (pułapki klikalności)

- ✓ Sensacyjne, często przesadzone nagłówki mające wzbudzić ciekawość i emocje.
- ✓ Treść artykułu często nie odpowiada nagłówkowi.

Powód: zwiększenie liczby kliknięć, generowanie przychodów z reklam.

Zmanipulowane zdjęcia i filmy

- ✓ Fotomontaże, filtry i retusz zmieniające kontekst obrazu.
- ✓ Deepfake – fałszywe nagrania audio/video przedstawiające osoby w sytuacjach, które nigdy nie miały miejsca.
- ✓ Manipulacja perspektywą – zmiana znaczenia zdjęcia poprzez kadrowanie lub pominięcie istotnych szczegółów.

Szok! Naukowcy odkryli coś, co zmieni twoje życie na zawsze!

Zmiana kolejności klatek nagrania, by wyglądało na atak zamiast samoobrony.

Dezinformacja

Wyrwanie cytatów z kontekstu

- ✓ Manipulacja polegająca na wyrwaniu fragmentu wypowiedzi i przedstawieniu go w innym świetle.
- ✓ Może zmienić całkowite znaczenie wypowiedzi.
- ✓ Często wykorzystywane w polityce i mediach sensacyjnych

 **Oryginał:** „Nie popieram tego pomysłu, ale rozumiem jego zwolenników.”

 **Manipulacja:** „Popieram ten pomysł.”

Propaganda

Propaganda

systematyczne i celowe rozpowszechnianie informacji (często zmanipulowanych) w celu ukształtowania opinii i postaw społecznych.

Charakter

polityczny

ideologiczny

militarny

religijny

komercyjny



Opiera się na emocjach, nie na faktach.
Często wykorzystuje strach, nadzieję,
dumą lub wrogość.

Propaganda

Rola propagandy w historii

II wojna światowa

- plakaty antywojenne, demonizowanie przeciwników, nawoływanie do patriotyzmu.

Zimna wojna

- kampanie medialne USA i ZSRR przedstawiające przeciwnika jako zagrożenie dla świata.

Reżimy totalitarne

- np. propaganda nazistowska, komunistyczna – kontrolowanie mediów i edukacji, aby kształtować ideologię.



Naziści wykorzystywali propagandę do budowania kultu Hitlera i uzasadniania działań wojennych.

Propaganda

Propaganda we współczesnym świecie

Media i polityka

- kreowanie narracji przez telewizję, internet, media społecznościowe.

Reklamy i marketing

- tworzenie wizerunku marki przez emocje, a nie fakty (np. „ten produkt uczyni cię szczęśliwym”).

Dezinformacja w internecie

- fake news, deepfake, manipulacja danymi statystycznymi.

Kwiecień 2020 !



Współczesne kampanie polityczne wykorzystujące social media do manipulacji wyborcami.

Propaganda

Fake news

celowo fałszywa lub wprowadzająca w błąd informacja przedstawiana jako prawdziwa wiadomość, mająca na celu manipulację opinią publiczną, osiągnięcie korzyści politycznych, finansowych lub społecznych

- ✓ Sprawdź źródło informacji – czy pochodzi z wiarygodnego medium?
- ✓ Zweryfikuj, czy inne rzetelne źródła podają tę samą wiadomość.
- ✓ Analizuj emocjonalny ton – czy tekst ma na celu wzbudzenie strachu lub sensacji?
- ✓ Sprawdź datę publikacji – czy informacja nie jest stara lub wyrwana z kontekstu?

Deepfake

technologia wykorzystująca sztuczną inteligencję (AI) i algorytmy uczenia maszynowego do tworzenia realistycznie wyglądających, ale fałszywych nagrań wideo, audio lub obrazów, które mogą przedstawiać osoby mówiące lub robiące rzeczy, których nigdy nie powiedziały ani nie zrobiły.

- ✓ Nienaturalne mruganie, ruchy ust lub mimika twarzy.
- ✓ Artefakty wizualne – nienaturalne oświetlenie lub rozmazania w okolicy twarzy.
- ✓ Nienaturalne ruchy głowy i ciała w stosunku do tła.
- ✓ Analiza dźwięku – błędy w synchronizacji głosu i warg.

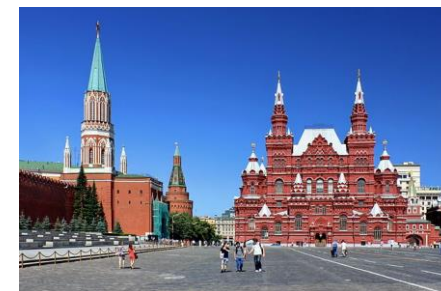
Jak rozpoznać... ?

FakeNews

Eksperyment z dnia 2 marca 2025r.

Treść prompta:

„Zaproponuj krótką treść komunikatu prasowego mówiącego o odbytej wizycie prezydenta Stanów Zjednoczonych z rodziną w Rosji w kontekście ostatnich wydarzeń geopolitycznych związanych z planem pokojowym względem wojny na Ukrainie. Wizyta była nieoficjalna.”



FakeNews



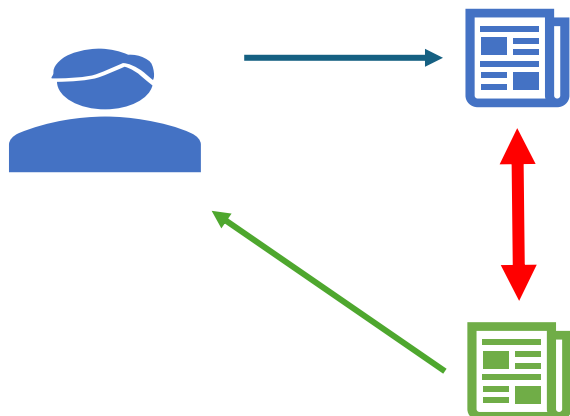
Model	Ocena	Faktograficzna poprawność	Brak halucynacji	Jakość struktury
ChatGPT 4o	Poprawny	Tak	Tak	Dobra
Gemini 2.0 Flash	Niepoprawny	Brak odpowiedzi	Brak odpowiedzi	Brak odpowiedzi
Copilot	Niepoprawny	Nie (fałszywe informacje)	Nie (chiński wątek)	Słaba (nieadekwatna treść)
Bielik	Niepoprawny	Nie (Biden jako prezydent)	Nie (błędny prezydent)	Średnia (błędne dane)
PLLuM 8x7B	Niepoprawny	Nie (Biden jako prezydent)	Nie (błędny prezydent)	Średnia (błędne dane)
Claude 3.7 Sonnet	Poprawny	Tak	Tak	Dobra
Deepseek (R1)	Poprawny	Tak	Tak	Dobra

Systemy rekomendacji

System rekomendacji

to algorytmiczne narzędzie służące do przewidywania preferencji użytkownika i sugerowania mu najbardziej odpowiednich treści, produktów lub usług. Wykorzystuje techniki analizy danych, uczenia maszynowego i sztucznej inteligencji w celu personalizacji rekomendacji.

Oparte o treść



Podobny artykuł jest rekomendowany dla użytkownika

Oparte o sąsiedztwo



Artykuł przeczytany przez jednego użytkownika jest rekomendowany dla drugiego

Systemy rekomendacji

Działania i efekty

Pokazują nam treści, które pasują do naszych wcześniejszych zainteresowań i poglądów.

Ograniczają dostęp do odmiennych punktów widzenia.

Efekt echo chambers
(komór echa)

W efekcie użytkownicy utwierdzają się w swoich przekonaniach, nawet jeśli są oparte na fałszywych informacjach.

Paradoks!!
Pomimo ogromnej ilości informacji i łatwego dostępu do niej, jesteśmy ograniczeni informacyjnie.

Systemy rekomendacji

Wykorzystanie przez organizacje

Wzmacnianie narracji

- Algorytmy promują treści korzystne dla danej organizacji, jednocześnie ograniczając dostęp do alternatywnych źródeł.

Bańki informacyjne

- Użytkownicy otrzymują tylko treści zgodne z ich poglądami, co wzmacnia podziały społeczne.

Dezinformacja polityczna i ekonomiczna

- Organizacje mogą wykorzystywać systemy rekomendacji do manipulowania opinią publiczną i destabilizacji przeciwników.

Fake news wzmacniane przez algorytmy

- Treści wzbudzające emocje (np. strach) są chętniej polecane, co sprzyja szerzeniu dezinformacji.

Wybory prezydenckie w USA (2016)

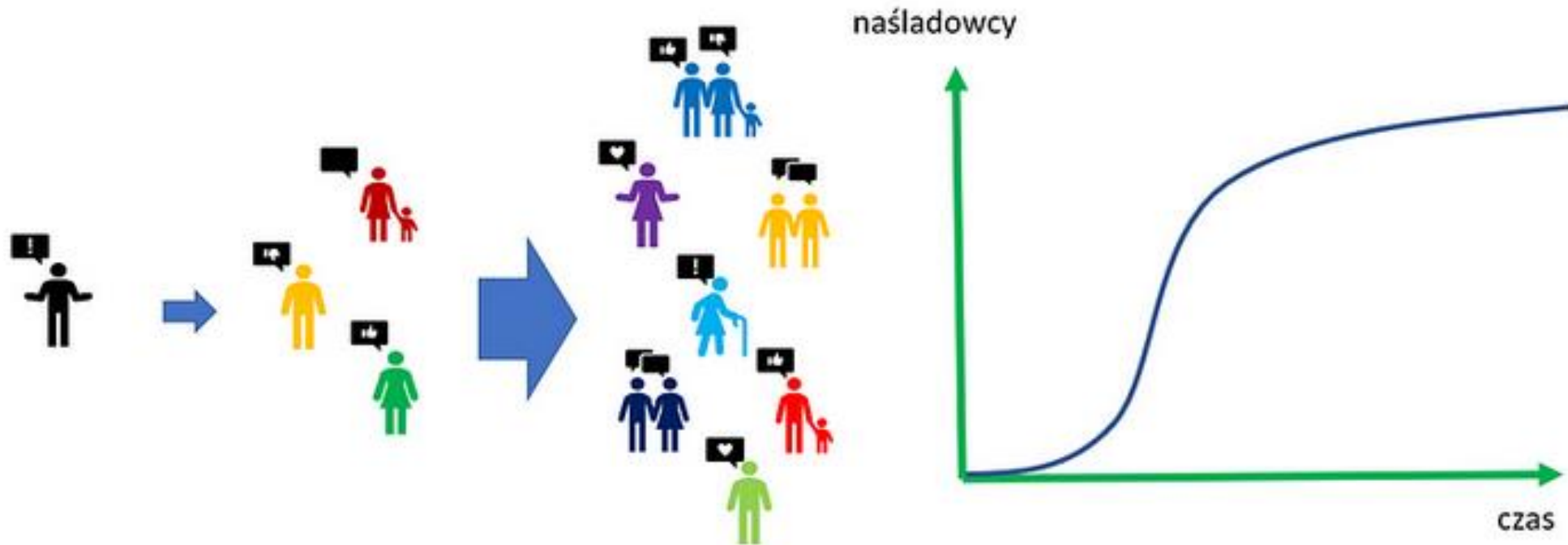
Rosyjskie farmy trolli i boty na Facebooku oraz Twitterze szerzyły fake newsy, które były wzmacniane przez algorytmy, wpływając na wyborców.

Pandemia COVID-19 i dezinformacja

Facebook i TikTok promowały fake newsy o „szkodliwości” szczepionek, które zdobywały miliony wyświetleń, mimo że były nieprawdziwe.

Systemy rekomendacji

Dyfuzja informacji



Bańka informacyjna

Bańka informacyjna

sytuacja, w której użytkownik Internetu jest otoczony treściami zgodnymi z jego poglądami i zainteresowaniami, ponieważ algorytmy rekomendacyjne filtrują informacje tak, by pasowały do jego wcześniejszych wyborów.



Ekstremizacja poglądów

- osoby narażone wyłącznie na jednostronne treści mogą radykalizować swoje przekonania, np. popadając w fanatyzm polityczny, religijny czy ideologiczny.

Manipulacja społeczeństwem

- rządy, korporacje i grupy interesu mogą wykorzystywać algorytmy do sterowania opinią publiczną i wpływania na wybory polityczne.

Łatwość szerzenia dezinformacji

- fake newsy rozprzestrzeniają się szybciej i skuteczniej w zamkniętych grupach, gdzie nie ma dostępu do alternatywnych informacji.

Zanik zdolności krytycznego myślenia

- osoby w bańce informacyjnej zaczynają bezrefleksyjnie wierzyć w podawane im treści, odrzucając wszelkie kontrargumenty.

Polaryzacja i konflikty społeczne

- podziały między grupami o różnych poglądach mogą prowadzić do agresji, protestów, a nawet zamieszek czy aktów przemocy.

Wojna hybrydowa

Wojna hybrydowa

strategia konfliktu, w której agresor łączy różne metody działań – zarówno militarne, jak i niemilitarne – w celu osłabienia przeciwnika bez formalnego wypowiedzenia wojny.

Brak jednoznacznego frontu

- działania prowadzone jednocześnie w różnych obszarach (cyberprzestrzeń, propaganda, ekonomia, polityka).

Użycie dezinformacji

- szerzenie fake newsów i manipulowanie opinią publiczną.

Wykorzystywanie cyberataków

- hakowanie systemów informatycznych, ataki na infrastrukturę krytyczną.

Działania militarne pod przykrywką

- np. „zielone ludziki” na Krymie w 2014 r.

Destabilizacja społeczeństwa

- wywoływanie chaosu, protestów, osłabianie zaufania do rządu.

Rosja – aneksja Krymu (2014) – użycie nieoznakowanych żołnierzy, propaganda i cyberataki.

Cyberataki na Estonię (2007) – rosyjskie ataki na systemy bankowe i rządowe po usunięciu sowieckiego pomnika.

Kryzys migracyjny na granicy polsko-białoruskiej (2021) – reżim Białorusi sprowadzał migrantów z Bliskiego Wschodu i Afryki,

Wojna hybrydowa

Wojna informacyjna

działania polegające na manipulowaniu informacją w celu wpływania na opinię publiczną, destabilizowania społeczeństw i osłabiania przeciwnika. Może obejmować dezinformację, propagandę, cenzurę oraz cyberataki na systemy informacyjne.

- 1 Dezinformacja
- 2 Propaganda
- 3 Manipulacja mediami
- 4 Cenzura i kontrola informacji
- 5 Cyberataki na infrastrukturę krytyczną
- 6 Kreowanie fake newsów
- 7 Sfabrykowane dowody i deepfake
- 8 Podszywanie się pod źródła informacji
- 9 Wpływanie na algorytmy rekomendacyjne
- 10 Destabilizacja społeczna poprzez media społecznościowe

 **Wojna informacyjna** jest jednym z głównych narzędzi wojny hybrydowej – poprzez dezinformację, propagandę i manipulację społeczną wspiera inne działania, np. operacje wojskowe czy destabilizację polityczną.

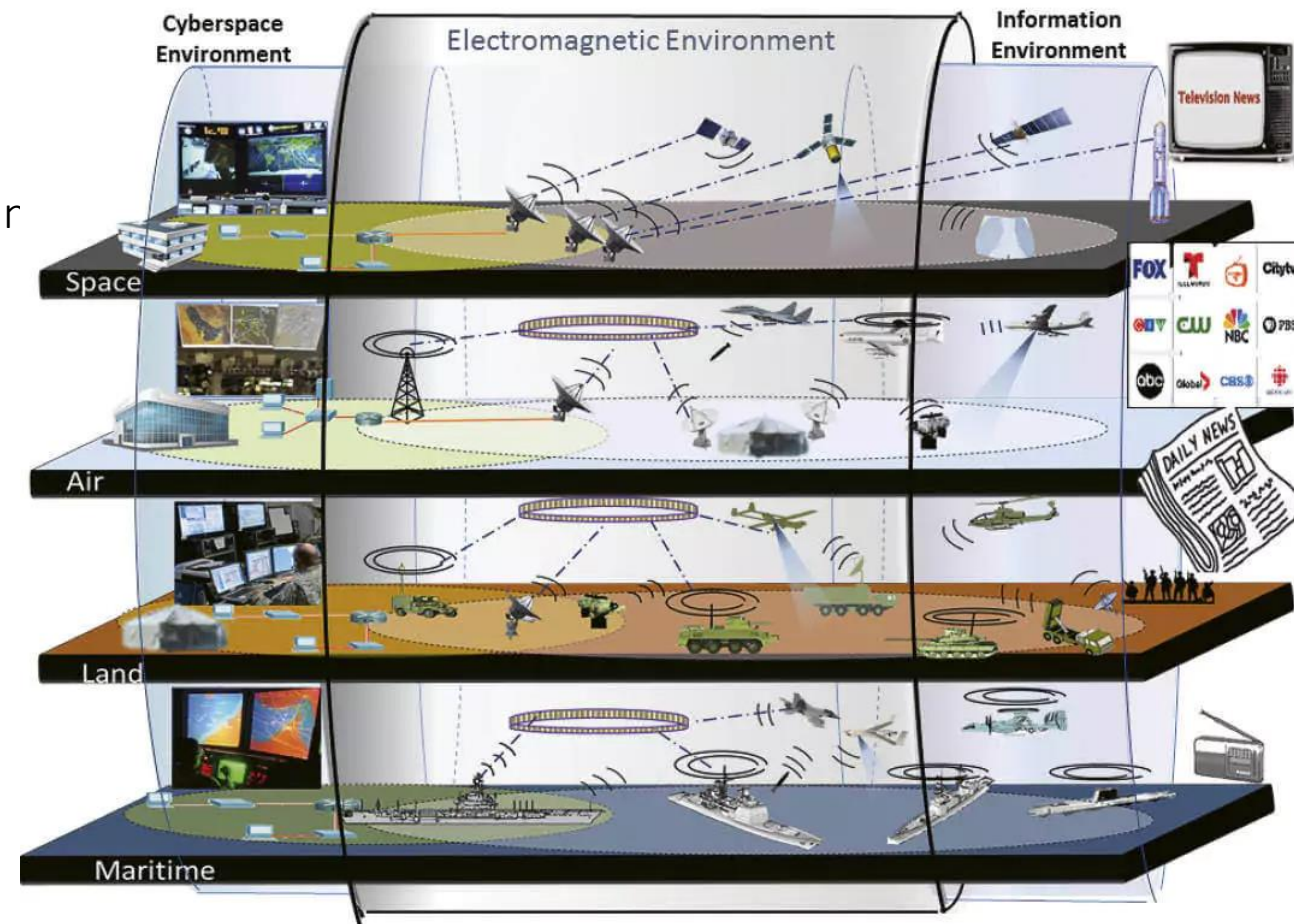
Wojna hybrydowa

Walka elektroniczna (EW – Electronic Warfare)

użycie systemów elektronicznych do zakłócania, przechwytywania i manipulowania sygnałami w celu uzyskania przewagi operacyjnej.

- ✓ Obejmuje działania ofensywne (zakłócanie, hakowanie) i defensywne (ochrona infrastruktury).
- ✓ Jest wykorzystywana w wojnie informacyjnej do manipulowania przepływem informacji i zakłócania komunikacji przeciwnika.

Zakłócanie sygnału GPS w czasie operacji wojskowych w celu dezorientacji przeciwnika



Wojna hybrydowa

FIMI – Manipulacja i ingerencja w informacje z zagranicy

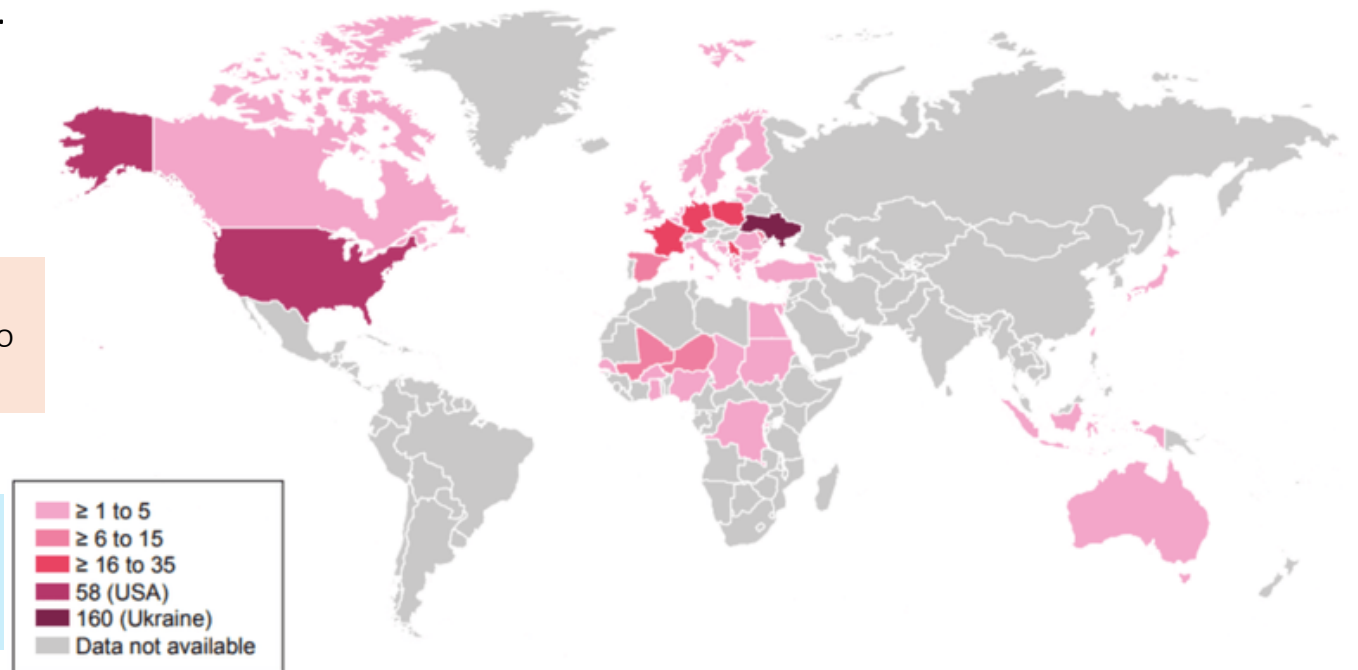
to zagraniczne operacje manipulacyjne, które wpływają na środowisko informacyjne danego kraju.

Takie działania mogą być prowadzone przez rządy, grupy polityczne lub inne podmioty dążące do destabilizacji społeczeństw i instytucji.

Chiny prowadziły kampanię dezinformacyjną, sugerując, że wirus SARS-CoV-2 pochodzi z amerykańskiego laboratorium wojskowego w Fort Detrick.

Iran wykorzystywał fałszywe konta na Twitterze do szerzenia antyizraelskiej i antyamerykańskiej propagandy w krajach UE.

Kraje dotknięte przez FIMI w 2023 r.



Wojna hybrydowa

Operacje FIMI Rosji przeciwko Polsce

Nazwa operacji	Opis działań	Lata	Źródło
Operacja "Doppelgänger"	Tworzenie fałszywych stron internetowych imitujących renomowane media, takie jak "Polityka" czy Polskie Radio, w celu rozpowszechniania dezinformacji i osłabienia poparcia dla Ukrainy.	2022–2024	Demagog
Operacja "Podcięcie"	Wykorzystanie sztucznej inteligencji do tworzenia i rozpowszechniania fałszywych nagrań w różnych językach, w tym po polsku, mających na celu osłabienie wsparcia dla Ukrainy i wzmacnianie napięć społecznych.	2023–2024	Konkret24
Kampania dezinformacyjna podczas pandemii COVID-19	Szerzenie fałszywych informacji dotyczących pandemii, mających na celu wywołanie paniki, chaosu informacyjnego oraz podważenie zaufania do instytucji państwowych.	2020	Gov.pl
Ataki klonów	Podszywanie się pod strony internetowe renomowanych mediów w celu szerzenia dezinformacji i manipulacji opinią publiczną.	2022–2024	Demagog

Wojna hybrydowa

Sojusznicza Wspólna Doktryna Operacji w Cyberprzestrzeni

Sojusznicza Wspólna Doktryna Operacji w Cyberprzestrzeni (AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)) to dokument opracowany przez NATO, który definiuje zasady i wytyczne dotyczące planowania, prowadzenia oraz oceny operacji w cyberprzestrzeni w kontekście operacji sojuszniczych.

https://www.drmalinowski.edu.pl/media_files/11915

Typy operacji w cyberprzestrzeni

- Operacje obronne (Defensive Cyberspace Operations - DCO): Mają na celu ochronę wolności działania w cyberprzestrzeni poprzez zapobieganie, wykrywanie oraz neutralizowanie zagrożeń.
- Operacje ofensywne (Offensive Cyberspace Operations - OCO): Służą do projekcji siły i osiągnięcia celów militarnych poprzez tworzenie efektów w cyberprzestrzeni.



Inżynieria społeczna

Inżynieria społeczna

to technika manipulacji psychologicznej, której celem jest nakłonienie ludzi do ujawnienia poufnych informacji lub wykonania określonych działań na korzyść atakującego.

Wykorzystuje ludzką ufność, emocje i nawyki zamiast technologicznych metod ataku.

Stosowana w cyberprzestępczości, szpiegostwie i oszustwach finansowych.

Może prowadzić do wycieku haseł, danych bankowych czy dostępu do systemów IT.

Oszust podszywa się pod pracownika IT i telefonicznie prosi o resetowanie hasła.

Wygrałeś darmowy dostęp do premium!
Wystarczy, że podasz swoje dane.”

10 000 osób już dołączyło – nie przegap okazji!

Inżynieria społeczna

Psychologia podatności na manipulację

Autorytet (Authority bias)

- Ludzie ufają osobom o wysokim statusie, więc oszuści podszywają się pod ekspertów lub instytucje.

Reguła wzajemności (Reciprocity rule)

- Jeśli ktoś zrobi nam przysługę, czujemy się zobowiązani do odwzajemnienia.

Społeczny dowód słuszności (Social proof)

- Ufamy temu, co robi większość, co ułatwia szerzenie manipulacji przez fałszywe rekomendacje.

Reguła niedostępności (Scarcity effect)

- Ludzie bardziej pożądamy rzeczy, które wydają się rzadkie lub ograniczone czasowo.

Efekt sympatii (Liking bias)

- Jesteśmy bardziej skłonni pomagać osobom, które lubimy lub które są do nas podobne.

Strach i pilność (Fear & urgency manipulation)

- Presja czasu i wzbudzanie paniki powodują, że podejmujemy pochopne decyzje.

Czy podasz mi swój PESEL?



<https://youtu.be/Advj0Zlo5nQ?si=kZmeramlpwFIjhvg>

Fake influencers

Fake influencers

osoby budujące fałszywy autorytet w mediach społecznościowych, często kupując obserwujących i lajki, aby wpływać na decyzje odbiorców.



Kupowanie followersów i interakcji

- sztuczne budowanie wiarygodności poprzez fałszywe konta.

Manipulacja emocjami

- stosowanie sensacyjnych nagłówków i szokujących treści, by zwiększyć zasięg.

Fake reviews (fałszywe recenzje)

- pisanie sponsorowanych opinii bez oznaczenia reklamy.

Podszywanie się pod ekspertów

- używanie tytułów i terminologii naukowej bez faktycznych kwalifikacji.

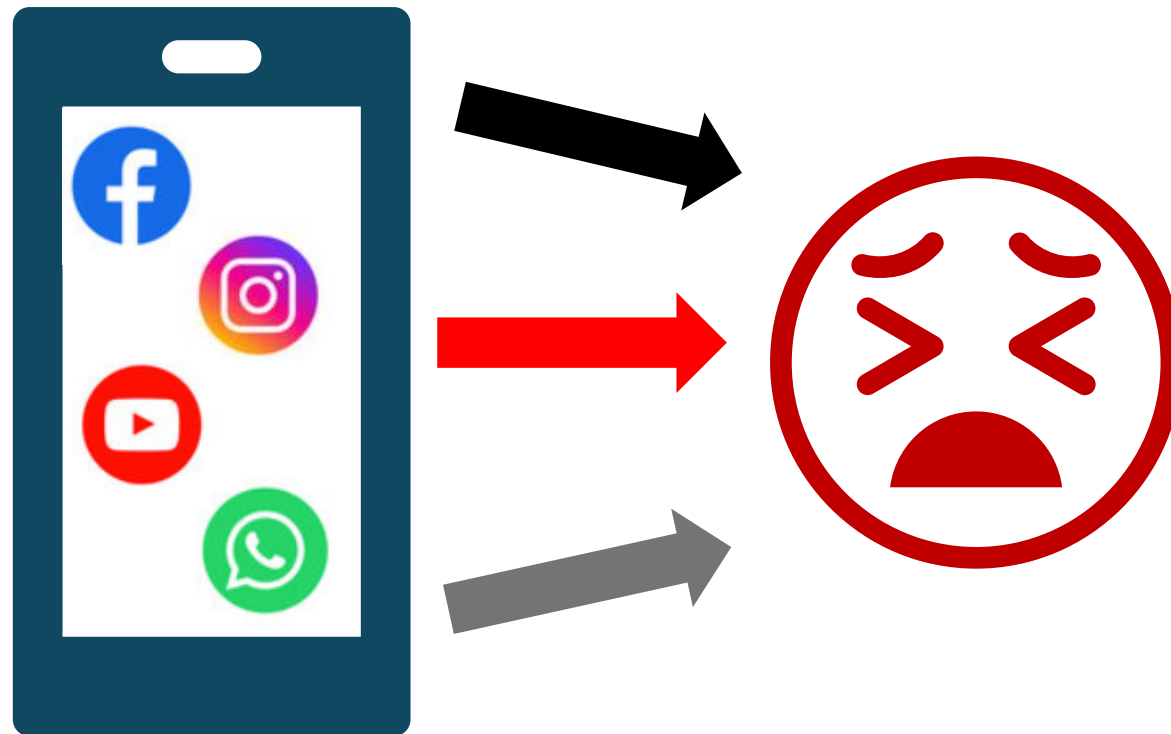
Współpraca z botami

- automatyczne komentarze i udostępnienia zwiększające zasięg.

Strach i FOMO (fear of missing out)

- presja, że odbiorca „coś straci”, jeśli nie skorzysta z oferty.

FOMO – Strach przed przegapieniem



FOMO 2.0 – Lęk przed niedokumentowaniem

Techniki obrony

Weryfikacja źródeł

- sprawdzaj, kto jest autorem informacji i czy inne wiarygodne media ją potwierdzają.

Fact-checking

- korzystaj z narzędzi takich jak Snopes, PolitiFact, Demagog, aby analizować prawdziwość treści.

Unikanie emocjonalnych reakcji

- manipulacje bazują na strachu i gniewie, dlatego zachowaj spokój przed udostępnieniem informacji.

Sprawdzanie daty i kontekstu

- stare lub wyrwane z kontekstu treści mogą być przedstawiane jako aktualne.

Unikanie baniek informacyjnych

- korzystaj z różnych źródeł, aby uniknąć jednostronnej perspektywy narzuconej przez algorytmy.

Techniki obrony

Nieujawnianie poufnych danych

- nie podawaj haseł, numerów kart czy danych osobowych przez telefon, e-mail ani SMS.

Analiza podejrzanych wiadomości

- sprawdzaj nadawcę, adres e-mail i linki w treściach mogących zawierać phishing.

Ostrożność wobec autorytetów

- oszuści podszywają się pod instytucje (np. banki, policję) w celu wyłudzenia danych.

Ograniczanie wpływu algorytmów

- modyfikuj ustawienia prywatności, wyczyść historię wyszukiwania i sprawdzaj, jak działają rekomendacje.

Edukacja cyfrowa

- rozwijaj umiejętność krytycznego myślenia i ucz innych, jak rozpoznawać manipulacje w sieci.

Fact-checking

Fact-checking

proces weryfikacji faktów, mający na celu ocenę prawdziwości informacji poprzez analizę źródeł, danych oraz kontekstu, w którym została przedstawiona.

Strategie skutecznego fact-checkingu

Weryfikacja źródeł

- sprawdzanie, kto stoi za daną informacją i jakie ma intencje.

Krytyczne myślenie

- unikanie emocjonalnych reakcji i analizowanie kontekstu.

Porównywanie różnych źródeł

- czy inne media potwierdzają tę samą informację?

Sprawdzanie daty publikacji

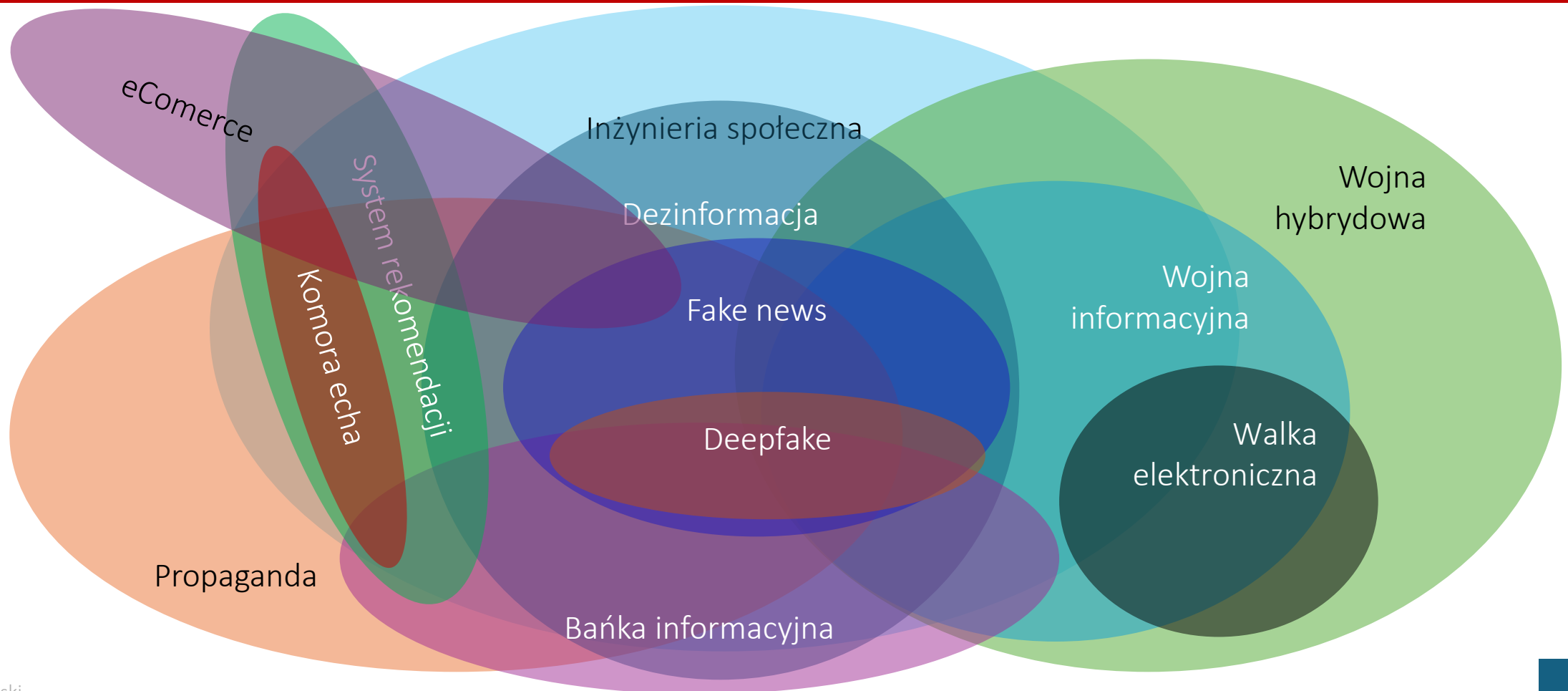
- czy informacja nie jest wyrwana z kontekstu lub przestarzała?

Analiza języka

- fake newsy często używają emocjonalnych, sensacyjnych zwrotów.

Narzędzie	Opis	Link
Snopes	Jedna z najstarszych stron weryfikujących fake newsy i teorie spiskowe.	https://www.snopes.com/
PolitiFact	Amerykańska organizacja oceniająca prawdziwość wypowiedzi polityków w skali od „prawdy” do „kłamstwa”.	https://www.politifact.com/
Fake News Detector	Narzędzie AI analizujące treści pod kątem wiarygodności.	https://www.fakenewsdetector.org/
Demagog	Polska platforma fact-checkingowa skupiająca się na polityce i mediach.	https://demagog.org.pl/
Google Fact Check Tools	Narzędzie Google do sprawdzania rzetelności informacji w wyszukiwarce.	https://toolbox.google.com/factcheck/explorer

Domeny



Zadanie

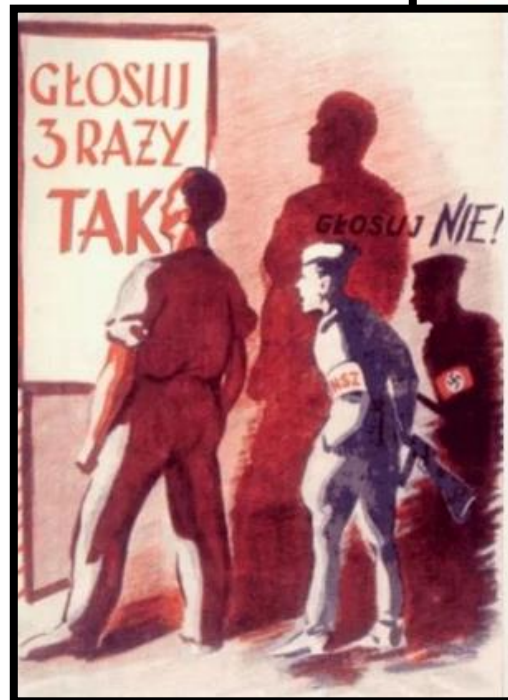
Treść

Przedstaw tło historyczne dwóch wydarzeń związanych z tymi plakatami.

Wskaż techniki manipulacji informacją zastosowane na tych plakatach.

Wielkość treści: ~ 1 strona A4

(0-2 pkt)



Termin przestania sprawozdania, wskazany w zadaniu w Moodle.

