bezpieczne
wybory

Osłona kampanii wyborczej

Przeciwdziałanie dezinformacji na przykładzie wybranych kampanii dezinformacyjnych

NASK

NASK

Osłona kampanii wyborczej. Przeciwdziałanie dezinformacji na przykładzie wybranych kampanii dezinformacyjnych

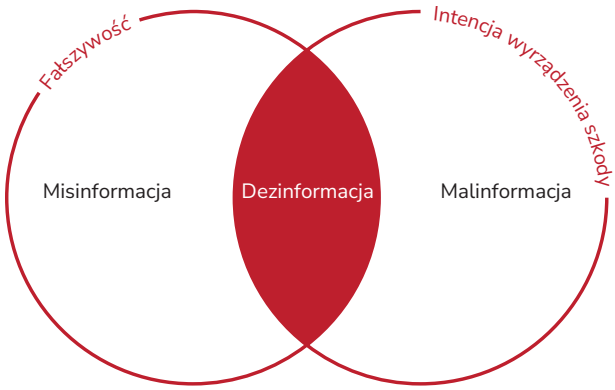
AUTORZY:
Sylwia Adamczyk
Izabela Jarka
Andrzej Kozłowski
Anna Kwaśnik
Michał Marek
OPIEKA MERYTORYCZNA:
Magdalena Wilczyńska
KOORDYNACJA:
Anna Pudłowska
OPRAWA GRAFICZNA:
Magdalena Mazur

ISBN:
978-83-65448-92-7

LICENCJA:
CC BY-NC 4.0

Spis treści

Dezinformacja



Oprac. na podstawie: Council of Europe, Claire Wardle, Hossein Derakhshan, *Information disorder: Toward an interdisciplinary framework for research and policy making.*

Zgodnie z przyjętą metodologią, NASK-PIB przez **dezinformację** rozumie „wszystkie formy fałszywych, niedokładnych lub wprowadzających w błąd informacji zaprojektowanych, prezentowanych i promowanych w celu umyślnego wyrządzenia szkody publicznej lub osiągnięcia zysku”[1].

Dopełnieniem tego pojęcia są definicje malinformacji (ang. malinformation) i misinformacji (ang. misinformation).

Eksperci Rady Europy opisują malinformację jako zakłócenie przekazu informacyjnego posługujące się informacją prawdziwą, ale publikowaną w celu wyrządzenia szkody. Misinformacja, zgodnie z definicją, posługuje się natomiast informacją nieprawdziwą, publikowaną jednak bez intencji wyrządzenia szkody. Misinformacja może być np. wynikiem błędu lub braku rzetelności dziennikarskiej. Brak zamierzonego działania szkodliwego jest zatem istotnym elementem odróżniającym misinformację od dezinformacji.

Dezinformacja jest rodzajem zakłócenia przekazu informacyjnego szczególnie trudnym do wykrycia, ponieważ intencja autora/autorki jest ukryta. Choć można domniemywać cel twórcy/twórczyni.

---

1 Definicja opracowana przez Grupę Ekspertów Wysokiego Szczebla Komisji Europejskiej ds. Fałszywych Wiadomości i Dezinformacji w Internecie (HLEG), https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation [dostęp: 18.09.2024].

Wybrane techniki manipulacyjne używane w przekazach dezinformacyjnych

W przekazach dezinformacyjnych powszechnie wykorzystywane są różnego rodzaju techniki manipulacyjne, mające na celu zniekształcenie rzeczywistości i wpłynięcie na opinię odbiorców. Są to między innymi:

Źródło: Wpis w serwisie X.com

- **Podszywanie się** – używanie logotypu lub wizerunku w celu wykorzystania wiarygodności danego podmiotu lub osoby do szerzenia szkodliwych informacji.

Przykład: Konto o nazwie „@Masakra_Witam" podszyło się pod Polską Agencję Prasową, wykorzystując jej logotyp, grafikę oraz zmieniając nazwę w serwisie X.

Źródło: Wpis w serwisie X.com

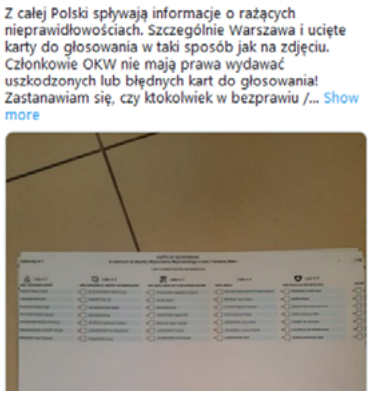
- **Manipulowanie danymi** – wyciąganie fałszywych wniosków z danych, ich niepoprawna interpretacja lub wycinanie z kontekstu w celu wprowadzenia w błąd.

Przykład: Manipulację danymi wykorzystano do polaryzacji społecznej poprzez łączenie sympatii politycznych z aspektem walorów intelektualnych wyborców.

Źródło: Wpis w serwisie X.com

- **Cherry-picking** – wykorzystywanie wybiórczych dowodów lub danych na potwierdzenie określonej tezy, przy jednoczesnym ignorowaniu pozostałych materiałów, które przeczyłyby temu twierdzeniu.

Przykład: Kandydat na europosła, sugerując rzekomą „kampanię oczerniającą" wymierzoną m.in. w jego stronę, odniósł się tylko do części materiału opublikowanego w jednym z serwisów internetowych. Pominął m.in. przychylne komentarze wobec polityków PiS oraz negatywne względem KO. Całość nie nosiła znamion oczerniania.



Źródło: Wpis w serwisie X.com

- **Fałszywy kontekst** – przedstawianie informacji w ujęciu, które wprowadza odbiorcę w błąd.

Przykład: Autor wpisu na platformie X sugerował, że członkowie PKW wydają wyborcom uszkodzone karty do głosowania. W rzeczywistości przedstawione na zdjęciu karty nie zostały wydane. Na etapie sprawdzania przez komisje wyborcze zostały one wycofane.

Źródło: Wpis w serwisie X.com

- **Teoria spiskowa** –alternatywne wyjaśnienie zdarzenia, zakładające istotny udział grupy konspiratorów, próbujących zataić prawdę przed opinią publiczną.

Przykład: Pojawiało się wiele sugestii, że kolejka osób chcących oddać głos w wyborach parlamentarnych, która zgromadziła się przed komisją wyborczą nr 148 we Wrocławiu, nie była efektem obywatelskiego zrywu, a rezultatem spisku mającego na celu zwycięstwo konkretnej frakcji.

Źródło: Wpis w serwisie X.com

- **Dowód anegdotyczny** – argument opierający się na osobistych doświadczeniach lub pojedynczych przykładach, niepoparty badaniami lub danymi statystycznymi. Prowadzi do błędnych wniosków, zakładając przeniesienie indywidualnego doświadczenia na ogólny trend.

Przykład: Po wybuchu wojny w Ukrainie w mediach społecznościowych opublikowano wpis oparty na relacji anonimowej „znajomej z Ząbek". Opisywał on sytuację, do jakiej miało rzekomo dojść w szpitalu, gdzie nie udzielono pomocy „Kasi" (w domyśle córce kobiety z Ząbek), która skręciła nogę. Opisane zdarzenie miało być dowodem na to, że osoby pochodzące z Ukrainy są lepiej traktowane przez instytucje państwowe niż polscy obywatele. Po weryfikacji okazało się, że żaden ze szpitali w Ząbkach, ani też żadna z placówek w całej w Polsce, nie wprowadziły takiej polityki.

Jednym z narzędzi demaskujących techniki manipulacyjne stosowane w dezinformacji jest fact-checking (z ang. weryfikacja faktów), czyli proces sprawdzania informacji w celu zweryfikowania ich prawdziwości.

Co sprzyja rozprzestrzenianiu dezinformacji?

Rozpowszechnianiu fałszywych treści sprzyja szereg mechanizmów technologicznych i społecznych. Mogą one znacząco zwiększać zasięg i skuteczność dezinformacji. Są to między innymi:

- **Algorytmy** – zawężają ukazywane treści jedynie do zbieżnych z poprzednimi wyszukiwaniami. Dotyczy to usług, które są oferowane w ramach jednej platformy.

- **Bańki informacyjne** – polegają na spersonalizowanym ukazywaniu treści w internecie, które są dopasowane do użytkownika na podstawie jego wcześniejszych aktywności w sieci.

- **Komory echa** – to zjawisko zamkniętej przestrzeni komunikacyjnej, w której odbiorca spotyka się głównie z opiniami zgodnymi z jego własnymi. Wzmacnia to jego poglądy oraz daje poczucie,

że większość osób mówi o tym samym i myśli w podobny do niego sposób, a poglądy przeciwne występują niezwykle rzadko.

- **Udostępnienia** – rozprzestrzenianie dezinformacji zależy także od użytkowników. Udostępnianie fałszywych treści wzmacnia ich zasięgi.

Zagraniczne ingerencje

Działania dezinformacyjne prowadzone przeciwko państwu polskiemu przez podmioty zewnętrzne odgrywają coraz większą rolę w funkcjonowaniu społeczeństwa. Mają one na celu między innymi destabilizację sytuacji społeczno-politycznej w kraju oraz stymulowanie polaryzacji społecznej. Najaktywniejszymi adwersarzami Polski są państwa prowadzące wojnę informacyjną, która jest elementem szerokich działań hybrydowych, realizowanych przez Federację Rosyjską i Białoruś.

Wrogie kampanie informacyjne obserwowane w polskiej infosferze realizowane są nie tylko poprzez emisję treści propagandowych. Obejmują kompleksowe działania dezinformacyjne oraz zaawansowane operacje wpływu, prowadzone przy zastosowaniu nowoczesnych środków technicznych oraz działań stricte wywiadowczych i dywersyjnych. Mogą skutkować także atakami fizycznymi (na co szczególnie narażeni są żołnierze Wojska Polskiego na granicy polsko-białoruskiej).

W sytuacji ataków w przestrzeni informacyjnej ze strony Federacji Rosyjskiej i Białorusi, ważne jest, aby identyfikować prowokacje oraz czynniki, służące deprecjonowaniu wizerunku RP poza granicami kraju i wzmacniające działania dezinformacyjne. Czynniki te mogą zaistnieć na różnych poziomach rozpowszechniania informacji, także na poziomie lokalnym.

Świadomość zagrożeń pozwala na neutralizację szkodliwego wpływu działań podmiotów ztewnętrznych. Warto przy tym dostrzegać, iż szczególnie ważne pozostaje budowanie zdolności do reagowania na dezinformację pojawiającą się na poziomie lokalnym. Często przedstawiciele struktur państwowych pracujący na poziomie samorządowym mogą być „pierwszą linią obrony” przed rozpowszechnianym przekazem dezinformacyjnym.

Przykładowe narzędzia do weryfikacji treści

- **WayBack Machine** – archiwum internetowe umożliwiające dostęp do usuniętych lub zmodyfikowanych witryn, także wpisów w mediach społecznościowych.
  https://web.archive.org/

- **Rejestr IO** – rejestr organizacji i firm, pozwalający na sprawdzenie powiązań osobowych i kapitałowych.
  https://rejestr.io/

- **Google Grafika** – narzędzie, w którym po załadowaniu zdjęcia lub grafiki można zobaczyć podobne obrazy, zbadać pochodzenie oryginału lub sprawdzić, na jakich stronach został opublikowany.
  https://www.google.com/imghp

- **Tin Eye** – zaawansowane narzędzie do wyszukiwania obrazów - pozwala sprawdzić źródło obrazu, a także miejsca w internecie, gdzie obraz został opublikowany.
  https://tineye.com/

- **Fotoforenics** – narzędzie do wykrywania edytowanych cyfrowo elementów fotografii.
  https://fotoforensics.com/

- **Anilyzer.com** – narzędzie do analizowania materiałów wideo.
  https://anilyzer.com/

- **InVID-WeVerify** – bezpłatna wtyczka, która umożliwia m.in.: dostęp do metadanych, przeglądanie klatek filmu, przybliżenie elementów.
  https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

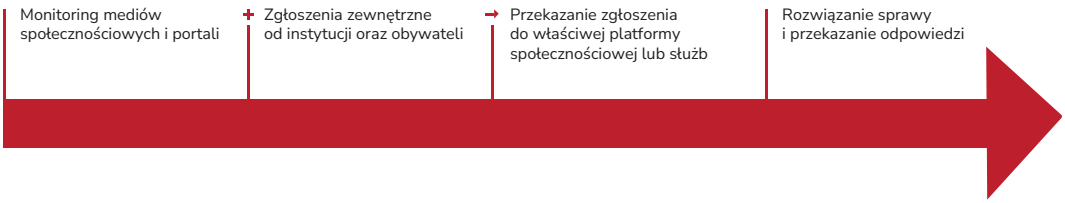
- **Deepware –** narzędzie do weryfikowania i wykrywania fałszywych materiałów wideo. Po wprowadzeniu adresu URL lub załadowaniu pliku, można uzyskać informacje na temat ewentualnych modyfikacji materiału.
  https://deepware.ai/

Działania NASK

NASK podejmuje szereg działań mających na celu przeciwdziałanie dezinformacji:

- monitoruje media społecznościowe i portale;
- przyjmuje zgłoszenia przekazywane na adres mailowy: dezinformacja@nask.pl;
- wyodrębnienia wątki o charakterze dezinformacyjnym;
- tworzy analizy narracji, profili i ich powiązań oraz raporty tematyczne;
- przekazuje szkodliwe treści do służb lub platform społecznościowych.

Obsługa zgłoszeń



Projekt Bezpieczne Wybory

Portal BezpieczneWybory.pl stanowi ogólnodostępną platformę zgłaszania incydentów związanych z cyberbezpieczeństwem oraz szkodliwymi treściami w okresie kampanii wyborczej i wyborów, a także jest kompendium wiedzy wyborczej. Głównym celem tej inicjatywy jest długoterminowe zapewnienie cyfrowego bezpieczeństwa wyborów w Polsce oraz opracowanie mechanizmów przeciwdziałania dezinformacji w przestrzeni informacyjnej.

Na portalu dostępne są aktualne i zweryfikowane informacje dotyczące procesu wyborczego oraz praktyczne porady w zakresie cyberbezpieczeństwa. Projekt jest realizowany przez Dział Przeciwdziałania Dezinformacji NASK, we współpracy z CERT Polska.

Na stronie BezpieczneWybory.pl można znaleźć:

- informacje dotyczące wyborów i głosowania;
- materiały edukacyjne z zakresu cyberbezpieczeństwa;
- zakładkę do przesyłania zgłoszeń incydentów cyberbezpieczeństwa lub potencjalnych działań dezinformacyjnych i szkodliwych związanych z wyborami.

W ramach projektu Bezpieczne Wybory NASK aktywnie wspierał procesy wyborcze podczas wyborów parlamentarnych w październiku 2023 roku, wyborów samorządowych w kwietniu 2024 roku oraz wyborów europejskich w czerwcu 2024 roku, przyczyniając się do podniesienia poziomu bezpieczeństwa cyfrowego i zaufania społecznego do systemu wyborczego.

Cyberhigiena

W dobie dynamicznie rozwijającej się technologii, ochrona danych oraz dbałość o bezpieczeństwo w sieci powinny być priorytetami każdej organizacji. Ataki socjotechniczne, szkodliwe oprogramowanie, wycieki danych, dezinformacja – to tylko wybrane przykłady cyberzagrożeń, z jakimi mierzą się nie tylko firmy i organizacje, ale także wszyscy użytkownicy internetu.

Cyberhigiena, czyli zbiór najlepszych praktyk, działań i nawyków w zakresie ochrony danych i bezpieczeństwa w środowisku cyfrowym, to jeden z podstawowych elementów skutecznej ochrony przed zagrożeniami.

Przestrzeganie podstawowych zasad cyberhigieny może pomóc w minimalizowaniu ryzyka związanego z cyberatakami oraz uchronić przed ich konsekwencjami.

Bezpieczne hasła i uwierzytelnianie dwuskładnikowe

- W trosce o bezpieczeństwo danych zarówno prywatnych, jak i służbowych, należy zadbać o silne hasła, za pomocą których użytkownik loguje się na swoje urządzenia, a także usługi internetowe (np. poczta elektroniczna, bankowość, social media). Hasło powinno składać się z co najmniej 14 znaków. Dobrą praktyką jest tworzenie haseł, które składają się z całych fraz lub zdań. Hasła nie powinny zawierać żadnych informacji o użytkowniku (np. imienia, nazwiska, daty urodzenia) ani być powiązane z jego nazwą.

- Należy zadbać o to, by hasło było unikalne – do każdej usługi inne.

- Warto rozważyć korzystanie z menadżerów haseł, które nie tylko pomagają w ich przechowywaniu, ale również ich tworzeniu.

- Weryfikacja dwuetapowa (ang. two-factor authentication, 2FA) to metoda ochrony kont, która opiera się na potwierdzaniu tożsamości użytkownika za pomocą dwóch odrębnych czynników. Pierwszym z nich jest zazwyczaj hasło wpisywane podczas logowania. Drugi czynnik może przybierać różne formy np. kodu wysłanego na numer telefonu, adres e-mail lub wygenerowanego przez aplikację lub np. odcisk palca (biometria). Dopiero po wprowadzeniu obu składników, użytkownik otrzymuje dostęp do konta.

Wprowadzenie weryfikacji dwuetapowej znacząco podnosi poziom ochrony konta, zmniejszając ryzyko udanych ataków ze strony cyberprzestępców.

- Najskuteczniejszą metodą uwierzytelniania dwuskładnikowego są tokeny sprzętowe, podłączane do komputera przez USB. Uznawane są za bardzo bezpieczne i łatwe w użyciu, ponieważ eliminują potrzebę wpisywania kodów z SMS-ów lub aplikacji uwierzytelniających. W przypadku braku możliwości zakupienia klucza U2F, warto rozważyć korzystanie z przeznaczonych do tego aplikacji.

Aktualizacje sprzętu i oprogramowania

Wykonywanie regularnych aktualizacji daje pewność, że wszystkie systemy, programy i aplikacje są wyposażone w najnowsze poprawki bezpieczeństwa, co minimalizuje ryzyko podatności na cyberataki. Dynamicznie zmieniające się środowisko zagrożeń, sprzyja cyberprzestępcom, którzy nieustannie poszukują luk w oprogramowaniu, które mogą być wykorzystane do przeprowadzenia ataków. Nieaktualizowane systemy stają się łatwym celem, co w przypadku skutecznego ataku może prowadzić do poważnych naruszeń bezpieczeństwa danych, utraty zaufania klientów, a także znaczących strat finansowych.

Regularne aktualizacje często usprawniają także funkcjonowanie i wydajność oprogramowania oraz sprzętu, zatem mogą przyczynić się do zwiększenia efektywności operacyjnej organizacji. Nowe funkcje i ulepszenia mogą poprawić wydajność procesów, a także zapewnić zgodność z obowiązującymi standardami i przepisami. Rekomenduje się włączenie automatycznych aktualizacji.

Zasada ograniczonego zaufania i zdrowy rozsądek

Ochrona przed atakami phishingowymi to przede wszystkim czujność i zasada ograniczonego zaufania. Rekomenduje się zachowanie szczególnej ostrożności przy otwieraniu wiadomości od nieznanych nadawców, w których mowa jest o konieczności podjęcia szybkich działań lub które zawierają linki bądź załączniki. Zaleca się dokładne zweryfikowanie adresu e-mail nadawcy oraz potwierdzenia autentyczności treści.

Rozdzielenie kont służbowych od kont prywatnych

Rozdzielenie kont służbowych od kont prywatnych jest fundamentalną zasadą w zakresie zarządzania bezpieczeństwem informacji w organizacji. Polega ono na wyraźnym oddzieleniu zasobów, danych oraz komunikacji związanych z pracą zawodową od tych wykorzystywanych do celów osobistych.

Kopie zapasowe

W przypadku organizacji posiadanie kopii zapasowych jest kluczowe dla zachowania ciągłości działania i minimalizowania strat w razie awarii lub ataków.

Przy tworzeniu kopii zapasowych warto odnieść się do zasady 3-2-1, którą łatwo zapamiętać:

- 3 kopie ważnych danych,
- 2 kopie na różnych nośnikach danych – tak aby nie były podatne na te same zagrożenia; może to być chmura albo dysk zewnętrzny czy inny nośnik danych odpięty od głównego urządzenia,
- 1 kopia powinna znajdować się w innej lokalizacji tj. poza domem lub firmą.

Stosowanie dobrych praktyk z zakresu cyberhigieny to podstawa bezpieczeństwa cyfrowego – zarówno na poziomie organizacji, jak i w życiu prywatnym.

Gdzie i jak zgłosić incydent?

Dział Przeciwdziałania Dezinformacji – incydenty związane z fałszywymi treściami

- E-mail: dezinformacja@nask.pl
- Formularz zgłaszania dezinformacji w kontekście wyborczym: https://www.bezpiecznewybory.pl/zglos-incydent/formularz

Zespół Dyżurnet.pl – nielegalne i szkodliwe treści

- E-mail: dyzurnet@dyzurnet.pl
- Formularz zgłoszeniowy: https://dyzurnet.pl/zglos-nielegalne-tresci
- Infolinia: 801-615-005

CERT Polska – incydenty związane z bezpieczeństwem internetowym

- Formularz zgłoszeniowy na stronie: https://incydent.cert.pl/ lub w aplikacji mObywatel (usługa „Bezpiecznie w sieci")
- Zgłaszanie podejrzanych wiadomości SMS w formie tekstowej poprzez funkcję „przekaż" na numer 8080

Inne przydatne linki

- NASK: https://www.nask.pl/
- CERT Polska: https://cert.pl/
- Bezpieczne Wybory: https://www.bezpiecznewybory.pl/
- Bezpieczny Miesiąc: https://bezpiecznymiesiac.pl/

NASK