NASK

11 konkretów w walce z dezinformacją

1. Niezależność polityczna to priorytet

Walka z dezinformacją będzie niezależna od wpływów czy nacisków politycznych. Nie znaczy to, że nie będzie dotyczyć polityki – analiza treści o charakterze politycznym pozostanie jednym z obszarów badań. Zawsze będzie jednak inicjowana przez NASK, a nie przez podmioty zewnętrzne, które chciałyby zlecić jakieś konkretne działania.

2. Komplementarny zespół ekspertów

Stworzymy zespół interdyscyplinarny na wzór francuskiej agencji VIGINUM[1]. W składzie zespołu: fact checkerzy, eksperci w dziedzinie geopolityki, eksperci w dziedzinie nauk politycznych i społecznych, eksperci OSINT, analitycy danych, lingwiści. Dezinformacja to złożone zjawisko, a naszym celem jest stworzenie zespołu, który ma kompetencje, by analizować je całościowo.

3. Analiza wzorców zachowań to skuteczna walka z dezinformacją

Przeniesiemy punkt ciężkości – z analizy treści na wzorce zachowań.

Analiza treści pod kątem językowym i narracyjnym musi być uzupełniona na dwóch poziomach:

- Poprzez zastosowanie metody oznaczania danych (debunking, zgodnie z definicją NATO StratCom[2]), z uwzględnieniem analizy źródeł, autorów i technik manipulacyjnych, w połączeniu z analizą trendów narracyjnych.
- Poprzez badanie OSINT (open-source intelligence, czyli biały wywiad) i analizę tzw. wzorców zachowań i metod autorów dezinformacji (Technics Tactics and Procedures).

Przeciwdziałanie dezinformacji w NASK koncentrowało się na analizie treści i eliminacji fałszywych narracji. Skierowanie uwagi na badanie wzorców zachowań autorów dezinformacji pozwoli skuteczniej oszacować skalę zjawiska. Rozszerzymy także zestaw środków zaradczych – oprócz komunikacji strategicznej skupimy się na współpracy z platformami w celu szybszego reagowania na treści dezinformacyjne oraz obalania wprowadzających w błąd lub fałszywych narracji.

[1] Francuska agencja odpowiedzialna za ochronę przestrzeni informacyjnej przed obcymi zakłóceniami, utworzona 13 lipca 2021 roku. Działa przy Sekretariacie Generalnym Obrony i Bezpieczeństwa Narodowego (SGDSN).
[2] Centrum Łączności Strategicznej NATO (NATO StratCom COE) zaczęło funkcjonować w styczniu 2014 r., a we wrześniu 2014 r. otrzymało akredytację NATO. https://stratcomcoe.org/pdfjs/?file=/publications/download/nato_stratcom_coe_fact-checking_and_debunking_02-02-2021-1.pdf (dostęp 03.04.2024).

NASK-PIB
ul. Kolska 12
01–045 Warszawa

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

NASK

4. Stosowanie technik białego wywiadu

Wykorzystamy metody OSINT-owe do badania dezinformacji, by wykrywać kampanie dezinformacyjne i siatki, przez które jest rozpowszechniana. Wykorzystamy metodologię FIMI Framework[3], DISARM Framework[4] oraz STIX[5]. Przyjęcie tych rozwiązań, które obecnie są wdrażane na poziomie europejskim, pozwoli nam na współpracę z innymi podmiotami i umożliwi badanie zjawiska w skali europejskiej.

5. Rapid Alert System

Częściowo utrzymamy strukturę Rapid Alert System, która obsługuje zgłoszenia obywateli wpływające do NASK oraz cały czas monitoruje treści pochodzące z podejrzanych źródeł. Rozszerzymy jednak zakres badania poprzez analizę innych platform (w szczególności Facebooka) oraz stron internetowych – do tej pory analizowano głównie platformę X (Twitter). Będziemy też badać metadane powiązane z treściami w mediach społecznościowych, takie jak znaczniki czasu, geotagi i identyfikatory użytkowników, by uzyskać wgląd w pochodzenie i wzorce rozpowszechniania dezinformacji.

6. Dokładna analiza dezinformacji zewnętrznej

Pogłębimy analizę dezinformacji pochodzenia zewnętrznego oraz tego, w jaki sposób przenika do polskiej infosfery (jak FIMI czy propaganda rosyjska). Analiza obejmie 8 filarów mechanizmu dezinformacji rosyjskiej, w tym: analizę komunikatów instytucji rządowych, instytucji finansowanych przez rząd, ich proxy (autorów i strony powielające propagandę rosyjską) oraz szkodliwe wykorzystywanie mediów społecznościowych. Opracujemy też analogiczną strukturę do analizy dezinformacji chińskiej i będziemy analizować przenikania tego rodzaju treści do polskiej infosfery.

7. Lepsza analiza dezinformacji wewnętrznej

Pogłębimy analizę dezinformacji pochodzenia wewnętrznego, tworzonej na potrzeby polityczne lub społeczne. Obejmie ona diagnozowanie głównych kanałów, źródeł, przekazów, technik, intencji i motywów. Ustalimy adresatów dezinformujących kampanii, które mogą uderzać w określone grupy (np. osoby LGBT, lekarze czy aktywiści klimatyczni) oraz środowiska, które za tymi kampaniami stoją.

8. Szybka i dobrowolna wymiana informacji

Będziemy wspierać mechanizmy dobrowolnej wymiany informacji, na przykład opierając się na istniejących lub nowych Centrach Analizy i Wymiany Informacji (ang. Information Sharing and Analysis Center, ISAC).

9. Odpowiedź na zagrożenia związane z AI – weryfikacja treści multimedialnych

Będziemy weryfikować autentyczność treści multimedialnych udostępnianych w mediach społecznościowych z wykorzystaniem narzędzi do analizy obrazu i wideo (deepfake) oraz najnowszych technologii – również tych tworzonych w NASK.

---

[3] Struktura i proces przeciwdziałania Foreign Information Manipulation Interference (FIMI), czyli zagranicznym manipulacjom informacjami i ingerencjom w informacje.
[4] Platforma open-source służąca do zwalczania dezinformacji poprzez udostępnianie danych i analiz oraz koordynację działań.
[5] Structured Threat Information Expression (STIX) – format danych wykorzystywany do wymiany informacji o zagrożeniach cybernetycznych (CTI).

10. Edukacja, edukacja, edukacja!

Położymy większy nacisk na edukację społeczną (zwłaszcza grup narażonych, takich jak seniorzy czy młodzież) w zakresie rozpoznawania dezinformacji poprzez dalsze, regularne organizowanie warsztatów i szkoleń dla społeczności lokalnych, w których uczestnicy będą uczyć się identyfikować i krytycznie oceniać informacje. Dodatkowo szkolenia dla urzędników i policjantów.

11. Szybka ścieżka kontaktu z platformami

Stworzymy szybkie, osobowe ścieżki kontaktu i reakcji w najważniejszych portalach społecznościowych (Meta, Google, TikTok) i zaoferujemy wsparcie osobom publicznym, gdy ich wizerunek wykorzystywany będzie bezprawnie, np. do szerzenia dezinformacji.