



Francuski model przeciwdziałania zagranicznym operacjom informacyjnym

Amanda Dziubińska, Aleksandra Wójtowicz

Przed wyborami prezydenckimi, które odbędą się w 2027 r., Francja wzmacnia system przeciwdziałania zagranicznym operacjom informacyjnym. Wyspecjalizowana struktura (VIGINUM) i międzyinstytucjonalna koordynacja ułatwiają wykrywanie ingerencji i szybkie reagowanie. Wyzwaniem pozostaje jednak ograniczenie wpływu narracji dezinformacyjnych na debatę publiczną. Francuskie doświadczenia mogą pomóc innym państwom, w tym Polsce, w usprawnianiu współpracy między instytucjami i stworzeniu kompleksowego mechanizmu ochrony wyborów.

Ewolucja kampanii dezinformacyjnych we Francji. Od czasu tzw. Macron Leaks (dwa dni przed drugą turą wyborów prezydenckich w 2017 r. w wyniku ataku przeprowadzonego przez powiązaną z rosyjskim wywiadem grupę hakerską do sieci wyciekło ponad 20 tys. wiadomości e-mail powiązanych z kampanią wyborczą Emmanuela Macrona) w każdym kolejnym ogólnokrajowym głosowaniu we Francji odnotowano próby zagranicznej ingerencji. Zmienił się jednak ich charakter. Pojedyncze incydenty zostały zastąpione trwałymi, wielokanałowymi operacjami wpływu. Od 2022 r. działa operacja „Doppelgänger”, za którą odpowiada rosyjska Agencja Projektów Społecznych. Kampania ta polega na podszywaniu się pod francuskie media (m.in. „Le Monde”, „Le Parisien”) i instytucje. Od 2023 r. rozwija się „Matrioszka/Overload” – jedna z największych prorosyjskich operacji, która uderza w różne kraje europejskie, w szczególności we Francję – większość wpisów publikowanych w jej ramach dotyczy francuskich polityków i polityczek. Fałszywe materiały są masowo zgłaszane redakcjom i fact-checkerom, aby przeciążyć ich zdolności weryfikacyjne. Przy okazji wyborów w ramach tej operacji generowane są z użyciem AI nagrania podszywające się pod znane redakcje, np. „Euronews”, a także osoby – w tym aktorów czy piosenkarzy, którzy rzekomo komentują wydarzenia polityczne. Równolegle działa sieć „Portal Kombat” („Operacja Pravda”), zalewająca internet treściami z rosyjskich źródeł, by zanieczyszczać dane treningowe modeli AI, oraz Storm-1516, który tworzy „śledztwa” wymierzone we francuskich polityków. Storm-1516 uderza w wybory w krajach

demokratycznych – w 2024 r. najintensywniej działał w Stanach Zjednoczonych, gdzie publikował materiały oczerniające Kamalę Harris i Tima Waltza, a obecnie jest aktywny głównie we Francji. Okresami szczególnej intensyfikacji dezinformacji skierowanej przeciw Francji były wybory do Parlamentu Europejskiego oraz igrzyska olimpijskie w 2024 r., a także kampania samorządowa w 2026 r. W tym czasie zintensyfikowały się też działania dezinformacyjne, m.in. w ramach „Operacji Overload”, w tym ataki na mniejsze partie i lokalnych polityków. Poza zainteresowaniem kampanii dezinformacyjnych pozostają właściwie wyłącznie politycy skrajnej prawicy, którzy sprzeciwiają się dalszemu wspieraniu Ukrainy bądź otwarcie popierają Rosję.

Francuski model odpowiedzi. Działania państwa porządkuje pierwsza francuska strategia przeciwdziałania zagranicznym manipulacjom informacyjnym (FIMI) na lata 2026–2030, przyjęta w lutym br. przez prezydenta. Jej realizację koordynuje Sekretariat Generalny Obrony i Bezpieczeństwa Narodowego (SGDSN), który odpowiada za projektowanie, koordynację i wdrażanie polityki obronnej oraz bezpieczeństwa narodowego. Strategia skupia się na czterech obszarach: wykrywaniu i reagowaniu na FIMI, edukacji, regulacji AI oraz współpracy międzynarodowej. Za wykrywanie FIMI odpowiada VIGINUM, agencja utworzona w lipcu 2021 r. w strukturze SGDSN. Na podstawie publicznie dostępnych danych bada ona powiązania kont, infrastrukturę i sposoby rozpowszechniania treści. Jej mandat obejmuje analizę operacji z udziałem podmiotów zagranicznych, które celowo i masowo

rozpowszechniają fałszywe lub mylące informacje, m.in. za pomocą fikcyjnych kont i automatyzacji. W lutym br. rozszerzono możliwość zbierania danych przez VIGINUM także z mniejszych serwisów. VIGINUM nie może nakazać usunięcia treści ani nałożyć sankcji, dlatego przełożenie jej ustaleń na ograniczenie wrogich operacji wymaga działań innych instytucji i dostawców usług internetowych. Agencja informuje decydentów o wykrytych operacjach, część analiz jest też dostępna publicznie. Na tej podstawie tworzona jest komunikacja strategiczna. Często obejmuje ona odpowiedzi na narracje dezinformacyjne, do czego wykorzystywana jest publiczna atrybucja wykrytych operacji wskazująca na konkretne podmioty, lub oświadczenia skoordynowane z partnerami. Powstają także memy, które mają za zadanie ośmieszyć rosyjskie narracje.

W styczniu br. została uruchomiona sieć koordynacji i ochrony wyborów (RCPE), kierowana przez SGDSN i obejmująca m.in. VIGINUM, regulatora mediów Arcom, MSW i komisję kontroli finansowania kampanii partii politycznych (CNCCFP). Jej członkowie wspólnie oceniają zagrożenia i uzgadniają reakcję. Podczas wyborów samorządowych sieć publikowała cotygodniowe biuletyny. Arcom, krajowy koordynator ds. usług cyfrowych, współpracuje z Komisją Europejską przy egzekwowaniu aktu o usługach cyfrowych (DSA). KE nadzoruje wypełnianie obowiązków przez największe platformy w zakresie ograniczania ryzyk systemowych, w tym zagrożeń dla wyborów. Ochronę uzupełniają działania agencji cyberbezpieczeństwa ANSSI i policyjnego urzędu zwalczania cyberprzestępczości OFAC. Odrębnym instrumentem jest wprowadzony ustawą z grudnia 2018 r. przyspieszony tryb sądowy, stosowany m.in. przy wyborach prezydenckich i parlamentarnych. Sąd orzeka w ciągu 48 godzin o środkach powstrzymujących rozpowszechnianie fałszywych treści, które zagrażają rzetelności głosowania, jeżeli ich dystrybucja jest celowa, masowa oraz sztucznie wzmacniana lub zautomatyzowana.

Francja aktywnie uczestniczy w europejskim systemie przeciwdziałania FIMI. Podczas prezydentury w Radzie UE w 2022 r. doprowadziła do porozumienia w sprawie DSA, a jej nacisk na egzekwowanie prawa wobec największych platform wpływa na tempo postępowań KE wobec X, Mety i TikToka. Komisje specjalne PE ds. obcych ingerencji (INGE/ING2, 2020–2023), kierowane przez Raphaëla Glucksmanna, były w dużej mierze francuską inicjatywą polityczną i utrwaliły w Brukseli traktowanie dezinformacji jako problemu bezpieczeństwa. Raporty techniczne VIGINUM („Portal Kombat”, „Matroszka”) ustaliły ramy debaty o FIMI w UE. Francja wraz z innymi państwami UE, w tym Polską, aktywnie współtworzy też [Europejską Tarczę Demokratyczną](#). Działalność analityczna uruchomionego w lutym br. Europejskiego Centrum Odporności Demokratycznej, inicjatywy promowanej przez Polskę w trakcie jej prezydentury, ma opierać się na metodologiach wypracowanych przez francuskie VIGINUM.

Skuteczność i ograniczenia. Działania francuskich instytucji usprawniają wykrywanie ingerencji i koordynację reakcji, ale trudno ocenić ich wpływ na zachowania wyborców. Podczas

wyborów samorządowych VIGINUM zidentyfikowało cztery zagraniczne incydenty. Współpraca z dostawcami usług internetowych pozwoliła zablokować niemal 200 kont, choć zaangażowanie dostawców było nierówne. Niewielki zasięg operacji dezinformacyjnych nie pozwala także ocenić, jak system poradziłby sobie z atakami docierającymi do szerokiej publiczności. System relatywnie dobrze radzi sobie z pojedynczymi operacjami, ale wyzwaniem może być wzrost ich skali i tempa – zwłaszcza podczas wyborów prezydenckich. Odpowiedzią rządu na zidentyfikowane słabości jest złożony w lipcu br. projekt ustawy, która ma rozszerzyć przyspieszoną procedurę na wszystkie rodzaje wyborów i zaostrzyć kary za manipulowanie głosowaniem. Przewiduje też interwencję poza wyborami w razie zagrożenia poważnym i bezpośrednim naruszeniem interesów państwa, niezależnie od pochodzenia operacji.

Wnioski i rekomendacje. Największym testem rozwijanego systemu będą wybory prezydenckie w 2027 r. Doświadczenia francuskie wskazują, że skuteczne przeciwdziałanie zagranicznym operacjom informacyjnym wymaga traktowania ich jako zagrożenia dla bezpieczeństwa państwa. Istotna jest też koordynacja, w czym pomóc może ustanowienie wyspecjalizowanej instytucji z określonym mandatem. Polska może wykorzystać te praktyki i, bazując także na doświadczeniach z poprzednich wyborów, utworzyć np. stały międzyinstytucjonalny mechanizm ochrony wyborów z udziałem PKW, określonym trybem pracy i ścieżką komunikacji publicznej oraz wsparciem wszystkich sił politycznych w okresie kampanii. Można także rozważyć poszerzenie mandatu NASK, tak aby stał się główną polską instytucją koordynującą walkę z dezinformacją, a jednocześnie usprawnić komunikację między pozostałymi organizacjami, które zajmują się kwestiami dezinformacji – zbyt duże rozproszenie negatywnie wpływa na skuteczność działań.

Polska powinna rozważyć politykę jawnej atrybucji wykrytych operacji wpływu wraz z publikacją analiz FIMI w polskiej infosferze. Francuska praktyka pokazuje, że publiczne nazywanie operacji i wskazywanie ich autorów może pozytywnie wpływać na odporność społeczną. Podobnie działa też Europejska Służba Działań Zewnętrznych, która publikuje coroczny raport o FIMI w krajach UE.

Dezinformacyjne ataki na partie i kandydatów warto uwzględnić w przygotowaniach do kampanii wyborczych w państwach europejskich w 2027 r., m.in. poprzez prowadzenie briefingów dla sztabów oraz ustanowienie mechanizmu szybkiego reagowania na treści generowane przez AI, podszywające się pod polityków i media. Polska powinna w dalszym ciągu współkształtować Europejską Tarczę Demokratyczną, by uwzględniała perspektywę państw wschodniej flanki. W ramach Tarczy Polska ma odpowiadać za współpracę z organizacjami pozarządowymi, ale i platformami społecznościowymi – w tym przypadku kluczowe jest wdrożenie DSA, ponieważ bez krajowych regulacji prawnych trudniej będzie efektywnie na nie wpływać i wymagać np. przeciwdziałania ryzykom systemowym związanym z wyborami.