PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 104 (2302), 26 MAJA 2021 © PISM

BIULETYN

# Możliwości wprowadzenia sankcji UE za kampanie dezinformacyjne

Elżbieta Kaca

W UE odnotowano rosnącą liczbę zagranicznych operacji dezinformacyjnych, głównie rosyjskich i chińskich. Komisja Europejska (KE) rozważa opracowanie systemu sankcji w odpowiedzi na takie ataki. Ich stosowanie może być jednak ograniczane przez trudności techniczne w wykrywaniu źródeł operacji oraz różnice poglądów państw członkowskich co do skali działań odwetowych. Z perspektywy Polski, która popiera stosowanie restrykcji, takie rozwiązanie może wzmocnić reakcję Unii wobec agresywnych działań Rosji i Chin.

W grudniu 2020 r. w komunikacie w sprawie europejskiego planu działania na rzecz demokracji KE zaproponowała zbadanie możliwości stosowania sankcji UE w związku z zagranicznymi operacjami w przestrzeni informacyjnej, które działają na szkodę Unii. Dotyczy to ukrytych kampanii podejmowanych przez państwa i ich przedstawicieli przy wykorzystaniu dezinformacji, czyli celowego rozpowszechniania fałszywych lub wprowadzających w błąd treści, a także innych technik manipulacji.

Przyczyną przedstawienia propozycji jest nasilająca się w trakcie pandemii COVID-19 fala dezinformacji w UE, głównie ze strony Rosji i Chin. Działania te m.in. podważają zaufanie do zachodnich szczepionek (głównie mRNA), instytucji UE i strategii szczepień, napędzając ruchy antyszczepionkowe. W przeszłości Rosja przeprowadziła wiele operacji w okresach wyborczych, np. w 2016 r. – w związku z referendum na temat wyjścia Wielkiej Brytanii z UE, czy w 2017 r. – z wyborami prezydenckimi we Francji i parlamentarnymi w Niemczech.

**Charakterystyka zagrożeń i ich wykrywanie.** Celem operacji dezinformacyjnych jest osiągnięcie korzyści politycznych lub gospodarczych w efekcie podważenia zaufania społeczeństw do instytucji demokratycznych, a także zwiększenie podziałów społeczno-politycznych. W kampaniach tego typu podmioty zagraniczne najczęściej oczerniają europejskie demokratyczne wartości, polityków i instytucje, tworzą teorie spiskowe i propagują wizję rozpadu UE. Ich głównym narzędziem jest rozpowszechnianie dezinformacji w mediach społecznościowych za pomocą fałszywych kont, trolli, botów, najczęściej na kilku platformach jednocześnie. Od początku pandemii COVID-19 w UE zidentyfikowano 740 przykładów rosyjskiej dezinformacji, wykorzystujących artykuły skutecznie popularyzowane w mediach społecznościowych (dane East StratCom). W Niemczech w 2017 r. zidentyfikowano blisko 3 tys. kont sponsorowanych przez Rosję, angażujących się w dyskusje na temat wyborów, a 7,4% wpisów na Twitterze na ten temat było generowanych przez boty.

Podmioty prowadzące operacje dezinformacyjne stale ulepszają metody zdobywania popularności wśród odbiorców, a także działania utrudniające wykrycie ich kampanii. Fałszywe konta, strony czy grupy są coraz lepiej profilowane pod kątem docelowych adresatów. Mogą sprawiać wrażenie niezależnych instytucji, think tanków lub inicjatyw badawczych, bądź budować wizerunek osób zaufania publicznego. Działają też na zaszyfrowanych platformach, takich jak WhatsApp, zamkniętych grupach na Facebooku, serwisach internetowych (np. Reddit), wykorzystują ponadto zdjęcia profilowe generowane przez sztuczną inteligencję, utrudniające identyfikację operacji. Państwa coraz częściej zlecają realizację kampanii prywatnym firmom zajmującym się np. marketingiem. W trakcie wyborów w USA w 2020 r. rosyjska operacja dokonała się za pomocą nowo utworzonych firm w Ghanie, Meksyku i Nigerii.

Największe platformy społecznościowe, głównie Facebook i Twitter, wykrywają coraz większą liczbę kampanii dezinformacyjnych oraz usuwają niektóre treści. Działają jednak wybiórczo. Ponieważ czerpią dochody z reklam, w niewielkim stopniu ujawniają operacje realizowane przez państwa istotne dla nich gospodarczo, np. Chiny. Według szacunków Global Disinformation Index 76 mln dolarów wyniosły w 2020 r. dochody z reklam zamieszczanych na witrynach promujących dezinformację skierowaną wobec państw UE. Na poziomie Unii funkcjonuje komórka East StratCom monitorująca głównie rosyjską dezinformację, a coraz więcej państw członkowskich rozbudowuje własne zdolności śledcze w tej dziedzinie, np. Czechy, Estonia, Finlandia, Francja, Litwa, Niemcy, Szwecja. W UE istnieje wiele organizacji pozarządowych i instytucji naukowych zajmujących się wykrywaniem dezinformacji w oparciu o otwarte źródła. KE wspiera finansowo działające w tej sferze Europejskie Obserwatorium Mediów Cyfrowych. Obszar tych analiz jest jednak ograniczony z powodu braku regularnego dostępu do danych platform społecznościowych.

**Możliwy zakres sankcji i wyzwania.** Modelem sankcji ma być wprowadzony w 2019 r. system restrykcji UE stosowany w celu zwalczania cyberataków. Oznacza to możliwość użycia zakazu wjazdu do UE oraz zamrożenia aktywów wobec osób fizycznych i prawnych, które są bezpośrednio odpowiedzialne za realizację kampanii, ale też wspierają takie działania bądź są w nie zaangażowane w inny sposób. Sankcje mogłyby dotyczyć zagranicznych operacji skierowanych przeciw UE i jej państwom członkowskim, które wywołują poważne skutki w Unii. Przykładem mogą być ataki przeprowadzane w okresach wyborczych i/lub przeciw instytucjom społeczno-politycznym. Rozporządzenie powinno umożliwiać użycie restrykcji w przypadku innych naruszeń wykorzystujących dezinformację, bez ich precyzowania – dzięki czemu sankcje będą mogły być przyjęte w przypadku kampanii realizowanych w trakcie kryzysów o nieprzewidzianej naturze. Co więcej, UE powinna móc stosować sankcje w odpowiedzi na poważne operacje wymierzone przeciwko państwom trzecim lub organizacjom międzynarodowym. Przepisy mogą też precyzować czynniki pozwalające ocenić wpływ kampanii. Jest to trudno mierzalne ze względu na brak możliwości zbadania opinii odbiorców dezinformacji, istnieje jednak wiele metod oceny jej skutków, np. za pomocą popularności kont i wpisów czy skali ich powielania przez różne kręgi medialne i społeczne, np. tradycyjne media i decydentów.

Problematyczne jest przypisanie operacji konkretnemu podmiotowi i przedstawienie wystarczających dowodów przez służby prawne Rady UE. Aby potwierdzić źródło działań, potrzebny będzie dostęp do niejawnych informacji na temat działalności podejrzanych podmiotów, które są w posiadaniu służb wywiadowczych państw członkowskich, oraz do danych technicznych platform społecznościowych dotyczących m.in. kont, administratora czy użytego oprogramowania lub infrastruktury. Platformy mogą udostępniać takie informacje na wniosek organów ścigania danego państwa. Służby wywiadowcze państw członkowskich niechętnie współpracują na poziomie UE w zwalczaniu dezinformacji. Choć istnieją kanały wymiany informacji niejawnych, np. w ramach Komórki ds. Syntezy Informacji o Zagrożeniach Hybrydowych przy Centrum Analiz Wywiadowczych UE czy systemu wczesnego ostrzegania o kampaniach dezinformacyjnych, tylko niektóre państwa aktywnie angażują się we współpracę. Nawet jeśli uda się zgromadzić wystarczające dowody potwierdzające operację, problemem będzie jednomyślna decyzja państw członkowskich o przyjęciu sankcji ze względu na różnice podejść do Rosji czy Chin. Niektóre państwa, np. Węgry i Cypr, niechętne stosowaniu restrykcji ze względu na swoje interesy, mogą oficjalnie blokować ten proces. Z kolei Polska, państwa bałtyckie, Czechy i Słowacja, które podkreślają zagrożenia w dziedzinie bezpieczeństwa ze strony Rosji i/lub Chin, będą zapewne wspierać utworzenie takiego instrumentu.

**Wnioski.** Dla poparcia wprowadzenia systemu sankcji przez wszystkie państwa UE kluczowe będą skutki dezinformacji dotyczącej pandemii COVID-19 oraz skala przyszłych operacji w okresach wyborczych w największych państwach UE. Ponieważ restrykcje mają oficjalnie określać źródło ataków, ich zaletą będzie potwierdzenie jedności UE w obliczu nowych zagrożeń oraz zwiększenie świadomości publicznej na temat zagranicznych ingerencji w przestrzeni informacyjnej.

Na poziomie technicznym ważne będzie zwiększenie wykrywania kampanii dezinformacyjnych. W negocjowanym akcie o usługach cyfrowych państwa członkowskie powinny zgodzić się na wprowadzenie obowiązku dla platform internetowych udostępniania Komisji i zweryfikowanym badaczom danych dotyczących nielegalnych treści i celowej manipulacji. Mogą też rozszerzyć mandat East StratCom o monitorowanie dezinformacji ze strony Chin i innych państw trzecich, co wymaga zwiększenia niewielkiego budżetu komórki. Istotna będzie wymiana informacji między państwami członkowskimi, ale też z USA, ze względu na doświadczenie tamtejszych służb w wykrywaniu źródeł operacji, o czym świadczy np. przyjęcie sankcji w tej dziedzinie wobec Rosji w kwietniu 2021 r.

Z perspektywy Polski, będącej obiektem kampanii dezinformacyjnych ze strony Chin i Rosji, restrykcje UE byłyby przydatnym instrumentem nacisku na władze tych państw. Polska może je propagować we współpracy z Komisją Specjalną ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w UE, w tym Dezinformacji (INGE) w Parlamencie Europejskim, która rekomenduje wprowadzenie sankcji.