PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

POLICY PAPER

NR 3 (216), CZERWIEC 2024 © PISM

Redakcja: Sławomir Dębski, Wojciech Lorenz

Podejście UE do zwalczania obcych manipulacji informacyjnych i ingerencji

Filip Bryjka

Skuteczne reagowanie na obce manipulacje informacyjne i ingerencje (FIMI) jest jednym z priorytetów UE w zakresie przeciwdziałania zagrożeniom hybrydowym. Od przyjęcia Kompasu Strategicznego w marcu 2022 r. państwom członkowskim i instytucjom unijnym udało się ustalić wspólne zasady definiowania, wykrywania i analizy incydentów FIMI, co ma ułatwić wymianę informacji. Wyzwaniem pozostaje utworzenie systemu skoordynowanej odpowiedzi na poziomie UE. Bardziej proaktywne działania w ramach FIMI Toolbox, skuteczniejsze egzekwowanie sankcji oraz operacjonalizacja systemu reagowania będą miały kluczowe znaczenie dla przeciwdziałania systemowemu zagrożeniu ze strony Rosji, ale także innych państw i podmiotów niepaństwowych.

Od czasu aneksji Krymu przez Rosję w 2014 r. państwa UE są poddawane nasilonym rosyjskim operacjom informacyjnym, których celem jest wywieranie wpływu na procesy i decyzje polityczne, pogłębianie podziałów społecznych oraz zakłócanie debaty opartej na wolności słowa. By przeciwdziałać FIMI (*Foreign Information Manipulations and Interference*), państwa Unii tworzą odpowiednie struktury w administracji publicznej, angażują społeczeństwo obywatelskie oraz współpracują z platformami internetowymi i mediami. Muszą przy tym stale adaptować się do zmieniających się taktyk, technik i procedur (TTPs), które są stosowane przez aktorów stanowiących zagrożenie (threat actors). Operacje FIMI charakteryzują się coraz większym poziomem automatyzacji, co wynika z postępu technologicznego. Używając farm botów – programów naśladujących ludzkie działania w sieci, atakujący rozpowszechniają na masową skalę zmanipulowane treści i zwiększają zasięgi szkodliwego oddziaływania. Często stosowaną metodą jest podszywanie się pod polityków lub instytucje poprzez klonowanie ich stron internetowych i oficjalnych kont w mediach społecznościowych. Operacje FIMI są realizowane za pomocą rozbudowanej infrastruktury i programów umożliwiających ich maskowanie, co utrudnia wykrycie atakującego i przypisanie mu odpowiedzialności. W działaniach tych coraz większą rolę pełni wykorzystywanie sztucznej inteligencji (AI), która w przyszłości nie tylko będzie służyć do kreowania zmanipulowanych treści, ale także do planowania całych kampanii (w tym wyboru narracji i grup docelowych). Nowe technologie dają przewagę atakującemu, ponieważ umożliwiają rozpowszechnianie zmanipulowanych treści na masową skalę przy pomocy nieautentycznych metod (botów). Obecnie atakujący nie ponosi niemal żadnych konsekwencji nieetycznego działania.

Operacje FIMI charakteryzują się coraz większym poziomem automatyzacji, co wynika z postępu technologicznego.

FIMI jako nowe ramy pojęciowe w UE

Kategoria obcych manipulacji informacyjnych i ingerencji została wprowadzona do oficjalnego języka UE w marcu 2022 r. Jest to pojęcie szersze niż dezinformacja rozumiana jako fałszywe lub wprowadzające w błąd treści, które są rozpowszechniane z zamiarem oszukania lub zapewnienia korzyści ekonomicznych lub politycznych, i które mogą wyrządzić szkodę publiczną. FIMI opisuje z kolei wzorzec zachowania, który przeważnie nie jest nielegalny (*non-illegal*), ale zagraża lub może potencjalnie negatywnie wpłynąć na demokratyczne wartości i procesy polityczne. Takie działania mają charakter manipulacyjny, są prowadzone w sposób celowy i skoordynowany przez podmioty państwowe lub niepaństwowe, w tym przez ich pełnomocników (*proxies*) na ich własnym terytorium i poza nim. Ramy pojęciowe FIMI nie ograniczają się zatem do *fake news*, propagandy czy dezinformacji, lecz koncentrują się na ingerowaniu w procesy polityczne państw poddawanych wrogiemu oddziaływaniu informacyjnemu. Obejmują ten problem szerzej, uwzględniając ewoluujące TTPs stosowane m.in. przez Rosję, Chiny i Białoruś, także w domenie cyber (np. ataki na spisy wyborców, *deep fake* czy operacje typu *hack and leak* polegające na wykradaniu i publikowaniu poufnych informacji lub korespondencji).

FIMI opisuje wzorzec zachowania, który przeważnie nie jest nielegalny (*non-illegal*), ale zagraża lub może potencjalnie negatywnie wpłynąć na demokratyczne wartości i procesy polityczne.

Państwa członkowskie UE stosują różne kryteria kwalifikujące incydenty w sferze informacyjnej jako FIMI. Szwecja, która jest uważana za jednego z liderów odporności, za FIMI uważa zdarzenia, które 1) mają zagraniczne pochodzenie; 2) zawierają treści wprowadzające w błąd odbiorcę; 3) mają zamiar wywoływać szkody; 4) niosą za sobą potencjalne ryzyko dla bezpieczeństwa. Podobne kryteria cyfrowych ingerencji uwzględnia francuska agencja VIGINUM: 1) zaangażowanie aktorów zagranicznych; 2) nieautentyczność działania; 3) treści wprowadzające w błąd; 4) określony cel.

Wyzwania związane z rozwojem unijnego systemu reagowania na FIMI

Podobnie jak w przypadku innych zagrożeń hybrydowych, odpowiedzialność za przeciwdziałanie FIMI należy do kompetencji państw członkowskich. Skuteczność zapobiegania zależy jednak od współpracy państw i organizacji. Instytucje odpowiedzialne za przeciwdziałanie FIMI w państwach UE są ulokowane w różnych strukturach rządowych (np. ministerstwach spraw zagranicznych, spraw wewnętrznych, obrony), w wyniku czego mają inne mandaty, sposób organizacji i zakres zadań. Stosują także odmienną metodologię analizy incydentów FIMI, co utrudnia wymianę informacji.

UE dąży do standaryzacji sposobów wykrywania i reagowania na FIMI, opierając się na metodzie DISARM-STIX.

Od przyjęcia Kompasu Strategicznego w marcu 2022 r. UE dąży do standaryzacji sposobów wykrywania i reagowania na FIMI, opierając się na metodzie DISARM-STIX, która jest stosowana m.in. przez Zespół Analizy Danych (*Data Analysis Team*) działający w Wydziale Komunikacji Strategicznej, Grup Zadaniowych i Analiz Informacyjnych (SG.STRAT.2) Europejskiej Służby Działań Zewnętrznych (ESDZ). Metoda ta pozwala m.in. na wprowadzanie do wspólnej bazy danych analizy stosowanych taktyk, technik i procedur, a także informacji na temat infrastruktury wykorzystywanej do przeprowadzenia operacji wpływu (np. domen, serwerów, nieautentycznych kont itd.).

Dotychczasowe prace koncepcyjne UE pozwoliły m.in. na określenie wspólnych ram definicyjnych oraz standardów metodologicznych, które chociaż nie są obowiązkowe dla państw Unii, są uznawane za najlepsze z dostępnych praktyk. Decyzja o ich wprowadzeniu należy do poszczególnych państw członkowskich. Dalsza standaryzacja metod pracy analityków w instytucjach państw UE, a także organizacjach pozarządowych zajmujących się zwalczaniem FIMI, znacznie poszerzyłaby świadomość sytuacyjną państw członkowskich i usprawniłaby wymianę informacji w ramach unijnego Systemu Wczesnego Ostrzegania (Rapid Alert System, RAS) oraz Centrum Wymiany i Analizy Informacji (Information Sharing and Analysis Center, ISAC).

Standaryzacja metod analizy FIMI ułatwiłaby też przypisanie atrybucji atakującemu, co z kolei powinno usprawnić na poziomie politycznym podejmowanie decyzji dotyczących wspólnych (skoordynowanych) odpowiedzi. Możliwość przypisania odpowiedzialności za atak jest także niezbędnym elementem odstraszania takich działań, ponieważ wiąże się z różnymi kosztami dla agresora, np. wizerunkowymi, politycznymi, a w przypadku wprowadzenia sankcji – nawet finansowymi.

Standaryzacja metod analizy FIMI ułatwiłaby też przypisanie atrybucji atakującemu, co z kolei powinno usprawnić na poziomie politycznym podejmowanie decyzji dotyczących wspólnych (skoordynowanych) odpowiedzi.

Europejska Służba Działań Zewnętrznych (ESDZ) zaproponowała cztery sposoby reagowania na incydenty FIMI w zależności od ich szkodliwości: 1) ignorowanie (*ignore*) – czasami lepiej zignorować incydent niż na niego reagować, ponieważ reakcja może prowadzić do nagłośnienia manipulacji i być kontrproduktywna; 2) powstrzymanie (*contain*) – informowanie platform internetowych o wykryciu nieautentycznej sieci lub o szkodliwych treściach; 3) minimalizowanie (*minimize*) – usuwanie nieautentycznych kont i rozpowszechnianych przez nie treści; 4) przekierowanie (*redirect*) – przekierowanie uwagi odbiorcy na rzetelne informacje za pomocą komunikatu na odpowiednim szczeblu.

Dotychczasowe reakcje UE na FIMI koncentrowały się na prowadzeniu aktywnej komunikacji strategicznej (StratCom), demaskowaniu (tzw. *debunking* lub *naming and shaming*), a także wzmacnianiu odporności społecznej (*societal resilience*) poprzez edukację i współpracę z sektorem pozarządowym. Chociaż działania te są istotne i powinny być rozwijane, nie są wystarczające, by skutecznie zwalczać ataki FIMI, które z uwagi na rozwój nowych technologii są stosowane na masową skalę. UE nie nakłada na podmioty używające FIMI przeciwko państwom członkowskim niemal żadnych

UE nie nakłada na podmioty używające FIMI przeciwko państwom członkowskim niemal żadnych kosztów związanych z ich szkodliwym oddziaływaniem.

kosztów związanych z ich szkodliwym oddziaływaniem. Przykładem braku właściwej odpowiedzi jest możliwość przeglądania na terytorium UE rosyjskich stron internetowych (np. RT czy Sputnik) mimo unijnych sankcji nałożonych na te media w marcu 2022 r. Po inwazji Rosji na Ukrainę niektóre państwa (np. Czechy i Polska) przez krótki czas (ok. 3–6 miesięcy) utrzymywały blokadę stron internetowych rozpowszechniających prorosyjską propagandę i dezinformację, jednak sądy krajowe uznały, że nie ma wystarczających podstaw prawnych do stosowania takich środków. Skuteczne działania podjęły natomiast władze Estonii, gdzie zablokowano 53 kanały telewizyjne i ok. 300 stron internetowych, korzystając z prawa zakazującego promowania wojny napastniczej.

Nieskuteczność unijnego systemu reagowania na FIMI wynika m.in. z różnego stopnia zaawansowania poszczególnych państw Unii w zakresie przeciwdziałania FIMI, różnych regulacji prawnych na poziomie krajowym, braku woli politycznej do bardziej proaktywnych działań, ograniczeń związanych z ochroną wolności słowa czy przepisów RODO. Do zmiany tego stanu rzeczy przyczynić ma się wdrożenie w tym roku Aktu o usługach cyfrowych (*Digital Service Act*, DSA), który ma zwiększyć możliwości oddziaływania państw na platformy internetowe w zakresie zwalczania i usuwania nielegalnych treści.

Nieskuteczność unijnego systemu reagowania na FIMI wynika m.in. z różnego stopnia zaawansowania państw w zakresie przeciwdziałania FIMI, różnych regulacji prawnych, braku woli politycznej do bardziej proaktywnych działań, ograniczeń związanych z ochroną wolności słowa czy przepisów RODO.

Wnioski i rekomendacje

W celu zwiększenia skuteczności zwalczania FIMI państwa UE powinny rozwijać krajowe zdolności do obrony i odstraszania informacyjnych agresorów poprzez podwyższanie kosztów prowadzonych przez nich operacji. Wdrożenie przez państwa członkowskie standardów UE usprawni wymianę informacji i ułatwi wspólne reagowanie na FIMI, czyli usuwanie przez platformy internetowe nieautentycznych sieci kont, blokowanie domen i serwerów wykorzystywanych do operacji FIMI czy nakładanie i egzekwowanie sankcji na osoby oraz podmioty w nie zaangażowane. Istotne jest także ujawnianie informacji na temat wykorzystywanej infrastruktury, co utrudnia jej ponowne zastosowanie, a stworzenie nowych kanałów oddziaływania wymaga znacznych nakładów.

Polska powinna dysponować wyspecjalizowaną instytucją zajmującą się wykrywaniem, analizą i reagowaniem na FIMI zgodnie ze standardami obowiązującymi w ESDZ.

Polska powinna dysponować wyspecjalizowaną instytucją zajmującą się wykrywaniem, analizą i reagowaniem na FIMI zgodnie ze standardami obowiązującymi w ESDZ. Ze względu na zagraniczne pochodzenie incydentów FIMI taka struktura mogłaby powstać w MSZ i podlegać powołanemu w maju br. pełnomocnikowi ministra spraw zagranicznych ds. przeciwdziałania dezinformacji międzynarodowej. By właściwie realizować zadanie, taka instytucja musi dysponować budżetem i wyszkolonymi zasobami kadrowymi umożliwiającymi stałe monitorowanie przestrzeni informacyjnej. Mandat takiej instytucji powinien umożliwiać jej koordynację działań innych podmiotów zajmujących się przeciwdziałaniem FIMI (np. Instytutu NASK, służb wywiadowczych i kontrwywiadowczych), a także odpowiednich komórek w innych resortach (zwłaszcza RCB, MON, MSWiA czy Ministerstwie Cyfryzacji). W instytucjach tych powinny obowiązywać takie same standardy wykrywania i analizy incydentów FIMI, co umożliwi sprawną wymianę informacji oraz jej operacjonalizację na poziomie państwa i UE.

Docelowo w Polsce powinien powstać kompleksowy system przeciwdziałania FIMI oparty na podejściu angażującym całe społeczeństwo (*whole society approach*), który dzięki utworzeniu organu umożliwiającego systematyczne konsultacje i wymianę informacji ze strukturami państwowymi zwiększy rolę organizacji pozarządowych (zwłaszcza fact-checkingowych i demaskujących dezinformację), inicjatyw obywatelskich oraz sektora prywatnego (zwłaszcza dostawców usług cyfrowych). W znacznym stopniu odciążyłoby to struktury państwowe i pozwoliło szerzej przeciwstawić się problemowi FIMI, który ma powszechny charakter z uwagi na rozwój nowych technologii. By zachować ciągłość działania, państwo może rozważyć współfinansowanie działalności NGO poprzez granty. Kluczowe przy tym będzie określenie obiektywnych kryteriów doboru partnerów oraz sposobu wyznaczania zakresu zadań (sektorów odpowiedzialności), które w ramach tej współpracy mieliby realizować. Współpraca z administracją państwową nie powinna bowiem ograniczać autonomii ich działania w pozostałych sferach. Dla skuteczności systemu kluczowe będzie jednak, by organizacje partnerskie były wyszkolone zgodnie ze standardami ESDZ.

Docelowo w Polsce powinien powstać kompleksowy system przeciwdziałania FIMI oparty na podejściu angażującym całe społeczeństwo (whole society approach).

Jednym z priorytetów polskiej prezydencji w UE może być też zainicjowanie debaty na temat bardziej proaktywnych działań wobec państw i podmiotów pozapaństwowych, które stosują FIMI. Odpowiedni system reagowania w postaci skutecznego nakładania sankcji i blokowania domen można rozwinąć w ramach Cyber Toolbox lub FIMI Toolbox. Część pracy w zakresie ochrony przed FIMI powinna być przekierowana na platformy, które czerpią zyski finansowe ze sponsorowanej dezinformacji. W trakcie prezydencji w UE Polska może także proponować, by w ramach wdrażania Aktu o usługach cyfrowych platformy miały obowiązek posiadania wyspecjalizowanych struktur do wykrywania i reagowania na incydenty FIMI.

Jednym z priorytetów polskiej prezydencji w UE może być też zainicjowanie debaty na temat bardziej proaktywnych działań wobec państw i podmiotów pozapaństwowych, które stosują FIMI.