PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 128 (2938), 2 WRZEŚNIA 2024 © PISM

BIULETYN

Ingerencje Rosji i Iranu w wybory prezydenckie w USA

Filip Bryjka

Rosja i Iran prowadzą w mediach społecznościowych operacje informacyjne, które mają wpłynąć na postawy wyborcze Amerykanów w nadchodzących wyborach prezydenckich. Rosyjskie ingerencje stanowią największe zagrożenie dla przebiegu głosowania, a rosnąca aktywność Iranu w tym obszarze stanowi dodatkowe wyzwanie dla amerykańskich służb bezpieczeństwa. Chociaż wspólnym celem autorytarnych reżimów jest podważenie wiarygodności demokratycznych instytucji i pogłębienie polaryzacji politycznej w USA, różnią się pod względem preferowanych kandydatów – Rosja wspiera Donalda Trumpa, zaś celem Iranu jest niedopuszczenie do jego reelekcji.

Przedstawiciele służb wywiadowczych i administracji USA ostrzegają, że Rosja i Iran próbują wpłynąć na wynik listopadowych wyborów prezydenckich. Autorytarne reżimy wykorzystują do tego m.in. grupy hakerskie i specjalnie przygotowaną infrastrukturę internetową. By skuteczniej oddziaływać na odbiorców, korzystają ze sztucznej inteligencji (AI) oraz usług wyspecjalizowanych firm zajmujących się marketingiem politycznym, komunikacją i public relations. Dotychczasowe zaangażowanie Chin jest niewielkie, ogranicza się do podważania amerykańskiej demokracji i pozycji międzynarodowej.

Cele i metody rosyjskich ingerencji – Trump 2.0. Podobnie jak w trakcie wyborów w 2016 r. i 2020 r. Rosja wspiera kandydaturę Donalda Trumpa, licząc, że jego nieprzewidywalność i transakcyjne podejście w polityce międzynarodowej pozwolą narzucić Ukrainie pokój na preferowanych przez Rosję warunkach. Do takich kalkulacji mogą skłaniać kontrowersyjne wypowiedzi Trumpa na temat kosztów wspierania Ukrainy, planu zaprowadzenia pokoju w 48 godzin po objęciu prezydentury czy podważanie sensu istnienia NATO. Jego reelekcja jest zatem uznawana za korzystniejszą dla rosyjskich interesów niż zwycięstwo Kamali Harris, która zapowiada kontynuację wsparcia Ukrainy.

Do promowania określonych narracji i rozpowszechniania teorii spiskowych Rosja na coraz większą skalę wykorzystuje AI, grupy hakerskie (m.in. Ruza Flood/Doppelganger, Storm-1516, Storm-1841/Rybar) i infrastrukturę przygotowaną do operacji wpływu. Firma Newsguard, która zajmuje się wykrywaniem i analizą operacji dezinformacyjnych, zidentyfikowała 170 fałszywych stron internetowych podszywających się pod (zmyślone lub istniejące w przeszłości) lokalne amerykańskie gazety o nazwach zbliżonych do prawdziwych tytułów (np. „Houston Post", „Chicago Crier", „Boston Times", „DC Weekly" itp.). W rzeczywistości zostały one utworzone przez Rosję, która stosuje metodę „prania informacji" (*information laundring*) polegającą na uwiarygodnianiu fałszywego źródła informacji. Autorami tekstów są pracownicy podszywający się pod dziennikarzy, niekiedy wykorzystujący zdjęcia prawdziwych osób. Dla zwiększenia wiarygodności zmanipulowanych treści powstają filmy na YouTube, w których rzekomi informatorzy i sygnaliści mają utwierdzać odbiorców w przekonaniu o wiarygodności sensacyjnych informacji. Tworzone są także fałszywe dokumenty, np. faktura mająca dowodzić, że żona prezydenta Ukrainy kupiła luksusowy samochód ze środków pochodzących z amerykańskiej pomocy wojskowej. W ten sposób Rosja stara się zarówno wpłynąć na postawy wyborcze Amerykanów, jak i osłabić ich poparcie dla wspierania Ukrainy przez USA.

Prawdziwe zdarzenia lub historie są manipulowane przy użyciu narzędzi opartych na AI, które przedstawiają je tak, by były zgodne z określonym (konserwatywnym) stanowiskiem. Często są wykorzystywane także teorie spiskowe, w które wierzy ok. 25% elektoratu Republikanów (badania PRRI z 2022 r.). Przykładem takich działań są różne interpretacje

zamachu na Trumpa czy też fałszywa informacja o podsłuchiwaniu przez FBI jego rezydencji na Florydzie. Wpisuje się to w narrację głoszoną przez byłego prezydenta, który podważa uczciwość wymiaru sprawiedliwości w USA i twierdzi, że istnieje spisek, który ma nie dopuścić do jego reelekcji.

Do tej pory nie odnotowano poważnych cyberataków (np. na sztab demokratów) czy operacji typu *hack-and-leak* (polegających na wykradaniu i upublicznianiu korespondencji lub dokumentów oczerniających osobę lub partię polityczną), jakie w poprzednich latach stosowały rosyjskie służby wywiadowcze. Działania te pomogły Trumpowi zwyciężyć w 2016 r., co wykazało śledztwo specjalnego prokuratora (tzw. raport Mullera). Na tej podstawie Departament Sprawiedliwości oskarżył 12 osób pracujących dla 85. Centrum Łączności Specjalnej (JW. 26165) i cyberjednostki nr 74455 rosyjskiego wywiadu wojskowego GRU.

Cele i metody irańskich ingerencji – byle nie Trump. Podobnie jak Rosja Iran podsyca wewnętrzne podziały w USA i podważa zaufanie Amerykanów do instytucji publicznych. W odróżnieniu od Rosji celem Iranu jest jednak niedopuszczenie do reelekcji Trumpa, którego pierwsza kadencja (2016–2020) jest negatywnie oceniana przez Irańczyków. W tym okresie USA m.in. wycofały się z porozumienia nuklearnego z Iranem (JCPOA), prowokacyjnie uznały Jerozolimę za oficjalną stolicę Izraela, a także zabiły w Iraku gen. Kasema Solejmaniego – dowódcę korpusu strażników rewolucji islamskiej (IRGC). Ponowne zwycięstwo Trumpa może oznaczać poparcie dla ofensywnej polityki Benjamina Natanjahu wobec Iranu i wspieranych przez niego grup zbrojnych (m.in. Hamas, Hezbollah, Huti). Kamala Harris, jako polityczka bardziej lewicowa niż Joe Biden, może natomiast dążyć do zrównoważenia podejścia USA do Izraela i wojny z Hamasem, co jest w interesie Iranu.

Metody ingerowania w proces wyborczy w USA nie zmieniły się od 2020 r., gdy Iran uruchomił wiele cybernetycznych operacji wpływu, siejących niezgodę w społeczeństwie i podżegających do przemocy wobec amerykańskich urzędników państwowych. Za rozpowszechnianie treści skrajnie prawicowej grupy Proud Boys i wysyłanie gróźb mailowych wobec polityków w USA skazano w 2021 r. dwóch irańskich hakerów.

Do prowadzonych obecnie operacji wpływu Iran wykorzystuje grupy hakerskie (m.in. Sefid Flood, APT-42/Mint Sandstorm, APT-33/Peach Sandstorm). Stosując metodę podszywania się (*phishing*), usiłują uzyskać dostęp do skrzynek mailowych i kont polityków w mediach społecznościowych, by wykraść, a następnie upublicznić wrażliwe informacje (*hack-and-leak*). Grupy te są także zaangażowane w szerzenie zmanipulowanych i nieprawdziwych informacji za pomocą sieci fałszywych stron internetowych Storm-2035 (np. „Nio Thinker", „Savannah Time"), farm trolli i botów. Podobnie jak Rosja do manipulacji informacyjnych Iran wykorzystuje sztuczną inteligencję, która przekształca prawdziwe artykuły w treści zawierające określone tezy i narracje mające wywrzeć wpływ na grupę docelową. Narzędzia AI są także wykorzystywane do kreowania fałszywych obrazów i filmów (tzw. *deep fake*), których wykrycie przez zwykłych odbiorców jest coraz trudniejsze, co zwiększa skuteczność wpływania na postawy wyborcze. Działania te są prowadzone m.in. wokół kwestii polaryzujących amerykańskie społeczeństwo, np. praw osób LGBTQ+, napięć na tle rasowym czy konfliktu izraelsko-palestyńskiego. Śledztwo Microsoft Threat Analysis Center (MTAC) ujawniło, że za pomocą fałszywych profili aktywistów i niejawnego finansowania Iran (przy udziale chińskich grup hakerskich) wspierał propalestyńskie protesty na amerykańskich uniwersytetach, które wybuchły przeciwko operacji wojskowej Izraela w Strefie Gazy. W połowie sierpnia Federalne Biuro Śledcze (FBI), Biuro Dyrektora Wywiadu Narodowego (ODNI) oraz Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) we wspólnym oświadczeniu oskarżyły Iran o „podsycanie niezgody".

Wnioski i perspektywy. Chociaż Rosja i Iran mają sprzeczne preferencje co do kandydatów, a rosyjska ingerencja w wybory jest znacznie bardziej rozległa i zaawansowana, skutkiem działań obu państw jest pogłębianie wewnętrznych podziałów w USA, szerzenie chaosu i osłabianie zaufania do amerykańskich instytucji państwowych. W najbliższych tygodniach należy spodziewać się intensyfikacji rosyjskich i irańskich operacji informacyjnych polegających na szerzeniu fałszywych historii i narzucaniu narracji mającej wspierać preferowanego kandydata lub oczerniać drugiego. Rosja może przy tym wywierać presję na Iran, by zaprzestał lub ograniczył działania mogące zaszkodzić wizerunkowi Trumpa. W okresie poprzedzającym głosowanie hakerzy mogą dokonywać cyberataków na infrastrukturę wyborczą (np. listy ze spisami wyborców). W przypadku porażki preferowanego kandydata Rosja lub Iran mogą przeprowadzić kampanię dezinformacyjną ukierunkowaną na podważenie legitymizacji wyborów, której celem może być wywołanie chaosu (w tym zamieszek na wzór ataku na Kapitol w 2020 r.).

Skuteczność przeciwdziałania manipulacjom informacyjnym i ingerencjom (FIMI) mogłoby zwiększyć zacieśnienie współpracy na linii USA–UE, a także w formacie dwustronnym między USA a państwami Unii. Wymiana informacji poszerzyłaby świadomość sytuacyjną (m.in. w zakresie identyfikowania infrastruktury wykorzystywanej do operacji wpływu), co pozwoliłoby na szybszą reakcję. Agencje rządowe USA mogłyby także odegrać ważną rolę w wywieraniu presji na platformy internetowe (w większości amerykańskie) w zakresie wykrywania i usuwania szkodliwych treści, a także reagowania na zgłaszane incydenty.

Redakcja: Sławomir Dębski, Rafał Tarnogórski,
Jędrzej Czerep, Wojciech Lorenz, Patrycja Sasnal, Justyna Szczudlik, Daniel Szeligowski, Jolanta Szymańska, Marcin Terlikowski, Damian Wnukowski, Szymon Zaręba, Tomasz Żornaczuk