PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BIULETYN

Nr 67 (1815), 23 maja 2019 © PISM

Polityka Litwy na rzecz walki z dezinformacją

Kinga Raś

Aby przeciwstawić się rosyjskim działaniom dezinformacyjnym i atakom cybernetycznym, Litwa dostosowuje struktury administracyjne i modyfikuje ustawodawstwo krajowe. Jednocześnie mobilizuje pozostałe państwa Unii Europejskiej do systemowej walki z fake newsami używanymi do manipulowania opinią publiczną. Polska, która również jest narażona na rosyjskie kampanie dezinformacyjne, może skorzystać z litewskich doświadczeń.

Cele i metody działań rosyjskich. Inspirowana przez Rosję dezinformacja jest wykorzystywana do ingerencji w procesy społeczne i polityczne innych państw. Przybiera formę zamierzonych działań, których celem jest manipulowanie opinią publiczną. Od listopada 2015 r. zespół EU vs Disinfo (działający w ramach East StratCom Task Force) zidentyfikował w Europie ponad 5 tys. przypadków dezinformacji sprzyjającej rosyjskim interesom.

Obecnie rosyjska aktywność wymierzona w Litwę koncentruje się na sprawach społecznie wrażliwych i o znaczeniu strategicznym, jak pamięć historyczna czy kwestie społeczne i gospodarcze (w tym dotyczące sektora energetycznego). W szerszym kontekście odzwierciedla długoterminowe interesy Rosji, jak też jej aspiracje do utrzymania kontroli oraz wpływu w przestrzeni informacyjnej państw postsowieckich.

Rosja chce przede wszystkim podważyć zaufanie społeczne do polityki obronnej i bezpieczeństwa Litwy. Potwierdzają to oficjalne raporty litewskich służb, które podkreślają, że choć w 2018 r. zmniejszyła się liczba nieprawdziwych informacji dotyczących wojskowej obecności NATO na Litwie, to Rosja utrzymywała stały przekaz wymierzony przeciwko Sojuszowi i litewskim siłom zbrojnym.

Celem działań dezinformacyjnych – często zintegrowanych z atakami cybernetycznymi, jak zamierzone rozprzestrzenianie szkodliwego oprogramowania w sieciach instytucji państwowych – jest też kradzież wrażliwych danych. Na przykład w 2018 r. po hakerskim włamaniu z platformy informacyjnego kanału telewizyjnego TV3 została rozpowszechniona fałszywa informacja na temat orientacji seksualnej ministra obrony Raimundasa Karoblisa. Następnie wiadomość ta, wraz z linkiem oraz zainfekowanym plikiem, przekazywana była drogą mailową do mediów i instytucji państwowych.

Jednocześnie Rosja prowadzi działania wywiadowcze (cyberszpiegostwo), m.in. poprzez rozprzestrzenianie wirusów Agent.btz/Snake. Ich najnowsze wersje zostały wykryte w systemach przetwarzania danych litewskich instytucji państwowych. Ataki przeprowadzane są np. przez APT28 – grupę hakerską bezpośrednio łączoną z rosyjskim wywiadem, której aktywność została zidentyfikowana w litewskiej przestrzeni cybernetycznej.

Litewskie metody zwalczania dezinformacji. Litwa, ze względu na podłoże historyczne, bliskość geograficzną i mieszkającą tam mniejszość rosyjską (ok. 5%), jest szczególnie narażona na rosyjskie działania dezinformacyjne. Zostały one wyraźnie zintensyfikowane po rosyjskiej agresji na Ukrainę w 2014 r. Jednym z powodów była polityka Litwy, należącej do państw w sposób najbardziej pryncypialny sprzeciwiających się agresywnym działaniom Rosji w regionie. Litwa pośrednio wspierała środowiska krytyczne wobec rosyjskich władz, np. po protestach społecznych z grudnia 2011 r. W rezultacie jest zdecydowanym orędownikiem

antyrosyjskich sankcji, mimo kosztów ponoszonych zwłaszcza w wymiarze gospodarczym. Dodatkowo rosyjskie władze wciąż postrzegają Litwę (i pozostałe państwa bałtyckie) jako część swojej strefy uprzywilejowanych interesów.

Litwa podejmuje działania w kilku wymiarach. Zmodyfikowała model zarządzania krajowym systemem cyberbezpieczeństwa, zakładający współpracę organów państwa, w tym służb mundurowych oraz instytucji i podmiotów zaliczanych do infrastruktury krytycznej (jak m.in. firmy energetyczne). W tym celu w 2015 r. utworzono Narodowe Centrum Cyberbezpieczeństwa (NCC), a w 2017 r. znowelizowano ustawę o cyberbezpieczeństwie, m.in. by scentralizować zarządzanie bezpieczeństwem zasobów informacyjnych oraz zintegrować monitoring krajowych sieci łączności elektronicznej.

Litwa stara się też dostosowywać obowiązujące procedury do nowych zagrożeń, co ma ułatwić wykrywanie i zwalczanie dezinformacji. Służy temu m.in. regulacja pozwalająca uprawnionym organom państwa (m.in. NCC) na krótkoterminowe zablokowanie serwerów podmiotu, który jest wykorzystywany do szerzenia fake newsów lub uczestniczy w cyberatakach. Takie rozwiązania sprzyjają też usprawnieniu systemu reagowania na bieżące zagrożenia w internecie.

Władze Litwy podjęły próbę ograniczenia wpływu rosyjskich mediów w swojej przestrzeni publicznej. W tym celu, choć tylko czasowo, blokowały możliwość nadawania rosyjskiej telewizji na Litwie (nadal jednak dostępnej w internecie). W kwietniu br. litewski parlament przegłosował zmiany przepisów, które zezwolą Litewskiej Komisji ds. Telewizji i Radiofonii (LRTK) na pilne zaprzestanie nadawania kanałów telewizyjnych w przypadku zagrożenia bezpieczeństwa narodowego.

Litwini dążą do zwiększenia społecznej świadomości zagrożeń. Wysokie kompetencje i szerokie uprawnienia administracji nie są wystarczające do samodzielnego zwalczania dezinformacji. Dlatego pomocne są oddolne inicjatywy, jak tzw. ruch elfów. Tworzą go głównie wolontariusze litewscy, skupiający się na identyfikacji i zwalczaniu rosyjskich trolli. Mają oni demaskować fałszywe konta, by uniemożliwić rozprzestrzenianie się nieprawdziwych informacji. W tym celu utworzono też platformę Demaskuok.lt, zrzeszającą przedstawicieli instytucji państwowych, ale także dziennikarzy i specjalistów IT.

Wymiernym dowodem efektywności litewskich działań jest rosnąca liczba zdemaskowanych fake newsów *i* fałszywych kont (które następnie były blokowane). Potwierdziła to błyskawiczna akcja wymierzona przeciwko niemieckiemu producentowi odzieży sportowej, który pod wpływem działań społecznych i litewskiej dyplomacji wycofał jubileuszową kolekcję nawiązującą do czasów ZSRR.

Wnioski i perspektywy. Mechanizmy stosowane przez Rosję wobec Litwy są praktykowane także w stosunku do innych państw UE i NATO (np. Niemiec czy Polski). Skoordynowane podejście litewskich władz do problemu dezinformacji okazuje się skuteczną receptą na działania rosyjskie. Sprzyjają temu rozwiązania organizacyjne i instytucjonalne oraz wysoki poziom świadomości społecznej i tocząca się debata publiczna.

Litewscy eksperci sygnalizowali wzrost rosyjskiej aktywności dezinformacyjnej w związku z wyborami do Parlamentu Europejskiego i wzywali do zacieśnienia współpracy państw członkowskich oraz przedsiębiorstw z branży medialnej i informacyjnej działających na terenie UE. Przykład Litwy może stanowić skuteczny model w walce z dezinformacją.

Wspólne działania Polski i Litwy na rzecz wzmocnienia bezpieczeństwa energetycznego i wojskowego będą jednym z głównych i coraz bardziej eksponowanych przedmiotów rosyjskiej dezinformacji. Można oczekiwać, że Rosja będzie się starała utrudniać polskie i litewskie zabiegi o wzmocnienie wschodniej flanki NATO i o zwiększenie wojskowej obecności amerykańskich żołnierzy w regionie. Będzie też chciała zakłócić współpracę Polski i Litwy w sektorze energetycznym, zwłaszcza że oba państwa nie tylko sprzeciwiają się budowie Nord Stream 2, ale też same realizują projekty mające zwiększyć ich niezależność od rosyjskich dostaw, jak rozbudowa własnych gazoportów czy międzysystemowych połączeń gazowych (GIPL). Dlatego Polska może wykorzystać nie tylko litewski model włączenia walki z dezinformacją w szerszy kontekst cyberbezpieczeństwa, ale również scentralizowane rozwiązania organizacyjne czy procedury stosowane w razie wykrycia ataków cybernetycznych.

Wspólna walka z dezinformacją daje obu państwom pole do zwiększenia współpracy w tym zakresie zarówno na poziomie instytucjonalnym, jak i wśród ekspertów IT czy dziennikarzy, np. w ramach specjalnych warsztatów szkoleniowych poświęconych analizie treści. Polska może też zacieśniać współpracę w ramach unijnego zespołu szybkiego reagowania (European Union Cyber Rapid Response Teams, CRRTs) oraz wspierać Litwę w realizacji inicjatywy tworzenia strefy „cyber-Schengen". W praktyce miałoby to usprawnić reakcję na cyberataki, m.in. poprzez umożliwienie szybkiej wymiany danych i informacji. Litwa podkreśla, że wówczas UE mogłaby bardziej skutecznie wspierać we wzmacnianiu cyberbezpieczeństwa i w walce z dezinformacją także państwa w swoim sąsiedztwie, w tym Ukrainę.