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

BIULETYN

Nr 175 (1748), 21 grudnia 2018 © PISM

Infrastruktura wyborcza Stanów Zjednoczonych: zagrożenia i ochrona przed rosyjską ingerencją

Andrzej Dąbrowski

Ingerencja Rosji w wybory w Stanach Zjednoczonych w 2016 r. uwidoczniła podatność amerykańskiego społeczeństwa oraz systemu politycznego i wyborczego na cyberataki. Mimo podjętych przez Kongres i branżę mediów społecznościowych kroków zaradczych, nie udało się wyeliminować wad infrastruktury wyborczej i środków przekazu, co udowodnił przebieg tegorocznych wyborów do Kongresu. Czynniki te mogą mieć wpływ także na kolejne wybory, w związku z czym USA prawdopodobnie zintensyfikują działania zapobiegające atakom i próbom manipulacji. Polska może skorzystać z doświadczeń USA dla zabezpieczenia własnego procesu wyborczego.

Do kluczowych zagrożeń procesu wyborczego w USA należą nie tylko wadliwa infrastruktura techniczna, np. systemy gromadzenia i przetwarzania danych o wyborcach, czy psujące się maszyny liczące głosy, lecz przede wszystkim podatność opinii publicznej na manipulacje przez podmioty zagraniczne. Zjawiska te odnotowano po raz pierwszy na dużą skalę w trakcie wyborów prezydenckich w 2016 r. Ostatnie wybory do Kongresu, przeprowadzone w listopadzie 2018 r., pokazały, że problemy z infrastrukturą oraz wpływem zagranicznych podmiotów pozostają aktualne.

Zagrożenia dla infrastruktury wyborczej. Procedurę głosowania w wyborach powszechnych reguluje ustawa Help America Vote (HAVA) z 2002 r. Miała zreformować przestarzały system liczenia głosów, wykorzystujący karty perforowane. W tym celu powołana została Komisja Wspierania Wyborów (Election Assistance Commission, EAC). Zgodnie z HAVA stany mają obowiązek stworzenia skomputeryzowanego rejestru wyborców oraz korzystania z maszyn wyborczych skanujących karty do głosowania lub wykorzystujących technologię dotykową. W ostatnich wyborach do Kongresu zawiodła część przestarzałych urządzeń liczących głosy, co utrudniło wyborcom w wielu stanach oddanie głosu (m.in. Floryda, Nowy Jork, Georgia) oraz doprowadziło do ponownego liczenia głosów w wyborach do Senatu na Florydzie. Osobnym problemem jest zagrożenie infiltracją oprogramowania zliczającego głosy. Przed wyborami w 2016 r. rosyjskim hakerom udało się przeniknąć zabezpieczenia jednej z firm dostarczających oprogramowanie tego typu (VR Systems). Hakerzy zdobyli częściowy dostęp do systemów wyborczych i rejestrów wyborców w co najmniej 21 stanach. W 2017 r. ujawniono również, że maszyny do głosowania używane w kilku stanach posiadają kluczowe komponenty produkcji chińskiej, a jedna z firm zajmujących się produkcją oprogramowania wyborczego była dofinansowywana przez fundusz kontrolowany przez rosyjskiego oligarchę Władimira Potanina, objętego amerykańskimi sankcjami. Władze federalne zdecydowały w ubiegłym roku o usunięciu z rządowych komputerów oprogramowania rosyjskiej firmy Kaspersky, jako zagrażającego systemom zabezpieczeń. EAC bada zabezpieczenia dostawców oprogramowania, ale tylko na wniosek stanów, które nie muszą korzystać z certyfikowanych systemów.

Odrębnym zagrożeniem dla procesu wyborczego są fałszywe treści w Internecie. Portale społecznościowe, mimo doświadczeń kampanii wyborczej z 2016 r., pozostają podatne na

rozprzestrzenianie celowej dezinformacji. Podobnie jak w 2016 r., przed wyborami z listopada br. masowo rozprowadzano w mediach społecznościowych fałszywe informacje przy użyciu fikcyjnych kont.

Działania administracji i Kongresu. W maju 2017 r. Donald Trump podpisał rozporządzenie ws. cyberbezpieczeństwa, a we wrześniu 2018 r. administracja opublikowała pierwszą od 2003 r. strategię cyberbezpieczeństwa. W dokumentach tych nie podjęto tematu ochrony infrastruktury wyborczej. Doradca prezydenta ds. bezpieczeństwa, John Bolton, zlikwidował także podlegające mu stanowisko koordynatora ds. cyberbezpieczeństwa, który miał za zadanie m.in. uzgadniać strategię w zakresie ochrony procesów wyborczych. We wrześniu br. prezydent Trump wydał jednak rozporządzenie o możliwości nakładania sankcji na podmioty zagraniczne, które według amerykańskich służb wywiadowczych „starały się ingerować w wybory oraz podważać publiczne zaufanie do procesu wyborczego". W październiku br. Cyber Command, dowództwo odpowiedzialne za prowadzenie działań w cyberprzestrzeni w ramach Departamentu Obrony, przeprowadziło ofensywną operację wymierzoną w rosyjskich hakerów. Było to pierwsze w historii ujawnione przedsięwzięcie amerykańskich służb, które, działając w cyberprzestrzeni wobec obcego państwa, miały na celu zapobiegnięcie próbie oddziaływania na wybory.

Również Kongres podjął działania w celu zabezpieczenia wyborów, przeznaczając w marcu br. 380 mln dol. na modernizację infrastruktury wyborczej, m.in. na przeprowadzenie audytów procedur i systemów wyborczych, zakup nowoczesnych maszyn do głosowania oraz nowych i zabezpieczonych programów komputerowych do obsługi wyborów. Rozpoczął również prace nad ustawą Secure Elections Act (SEA), zgodnie z którą Departament Bezpieczeństwa Krajowego (Department of Homeland Security, DHS) stałby się centralnym ośrodkiem odpowiedzialnym za bezpieczeństwo procesu wyborczego. DHS mógłby współpracować z agencjami wywiadowczymi w celu identyfikowania zagrożeń i koordynacji działań organów stanowych w przypadku ataku na infrastrukturę wyborczą. Na mocy ustawy urzędnicy stanowi, odpowiedzialni za przeprowadzenie wyborów, otrzymaliby dostęp do informacji zastrzeżonych, co do tej pory stanowiło problem, wymagając współpracy władz stanowych ze służbami specjalnymi. Mimo ponadpartyjnego poparcia w Kongresie, prace nad ustawą trwają.

Opinia publiczna w niebezpieczeństwie. Według amerykańskich służb (FBI, CIA i NSA), większość działań Rosji, mających na celu oddziaływanie na wybory w 2016 r., odbywało się w Internecie. Pod wpływem nacisków opinii publicznej, która obarczyła media społecznościowe odpowiedzialnością za brak kontroli nad umieszczanymi tam treściami, oraz w obawie o spadek zaufania użytkowników i, co za tym idzie, wartości giełdowej, władze platform takich jak Facebook i Twitter podjęły działania na rzecz przeciwstawienia się propagandzie, dezinformacji i tzw. *fake news*. Facebook udoskonalił algorytmy, które utrudniają wysyłanie niezamówionych informacji, weryfikują konta publikujące *fake news*, a także stworzył narzędzia umożliwiające zgłaszanie do administratorów podejrzanych treści. Portal ten podjął również współpracę z rządami państw, z których pochodzą fałszywe informacje. Twitter i Facebook, współpracując ze stanowymi komisjami wyborczymi, zlikwidowały też dużą liczbę kont rozprzestrzeniających dezinformację. Tylko w 2018 r. udało się skasować 652 fałszywe konta na Facebooku, publikujące treści polityczne i społeczne. Wśród nich co najmniej 32 wykazywały podobną aktywność jak te, które były powiązane z rosyjską Agencją Badania Internetu, główną organizacją odpowiedzialną za szerzenie dezinformacji na zlecenie władz Rosji. Facebook przyznał też, że zidentyfikował i usunął ponad 300 kont związanych z Iranem, które, działając już od 2011 r., docierały do ok. 800 tys. odbiorców. We wrześniu br. główne firmy branży mediów społecznościowych ogłosiły plan zwalczania *fake news* w USA i Unii Europejskiej.

Wnioski. USA mogą być zainteresowane pogłębieniem współpracy z sojusznikami w dziedzinie ochrony infrastruktury wyborczej i zwalczania dezinformacji. Państwa NATO, zwłaszcza wschodniej flanki, powinny uwzględniać cyberzagrożenia i dezinformację w Internecie jako istotne ryzyka dla środowiska bezpieczeństwa. W interesie Polski leży korzystanie z doświadczeń amerykańskich, które mogą posłużyć do zwalczania dezinformacji i zabezpieczenia własnej infrastruktury wyborczej.

Mimo udowodnienia przez służby wywiadowcze rosyjskiej ingerencji w wybory w 2016 r. oraz prób ponownego wpływania na wyniki głosowania w 2018 r., Kongres i administracja nie podjęły jeszcze wystarczających działań w celu ochrony infrastruktury wyborczej. Może to wynikać z konstytucyjnej zasady ochrony wolności wypowiedzi i braku możliwości wpływania przez władze na treści publikowane w Internecie. Pod naciskiem opinii publicznej Facebook i Twitter zaczęły jednak wprowadzać kolejne mechanizmy ograniczające dystrybucję nieprawdziwych informacji. Amerykańska branża mediów społecznościowych, pod wpływem rządu i opinii publicznej, rozpocznie proces zmian mechanizmów i zasad publikowania treści w serwisach. Posiadając globalny zasięg, będzie tym samym w stanie wpływać na kształt i jakość debaty publicznej, w tym w państwach NATO.