Analiza KBN

Nr 6 (86) / 2021 10 maja 2021 r.

Ingerencja służb wywiadowczych Iranu w amerykańskie wybory prezydenckie w 2020 roku

Wiktor Kowalski

15 marca 2021 r. Avril Haines, Dyrektor Wywiadu Narodowego Stanów Zjednoczonych (ang. *Director of National Intelligence*, DNI), odtajniła raport Narodowej Rady Wywiadu (ang. *National Intelligence Council*, NIC) dotyczący prób ingerencji w wybory prezydenckie w USA w 2020 roku. W ocenie Rady nie doszło do bezpośredniej ingerencji podmiotów zagranicznych w poszczególne części procesu wyborczego: rejestrację wyborców, oddawanie głosów, ich liczenie czy ustalenie ostatecznych wyników głosowania. Niewątpliwie, uwaga amerykańskiej opinii publicznej koncentrowała się przede wszystkim na działalności rosyjskich władz, która stała się przedmiotem śledztwa prowadzonego przez prokuratora specjalnego Roberta S. Muellera w latach 2017-2019. Niemniej jednak, obiektem zainteresowania Wspólnoty Wywiadowczej USA (ang. *Intelligence Community*, IC) były również inne państwa ingerujące w proces wyborczy, w tym Iran. Warto przyjrzeć się działalności irańskich władz w cyberprzestrzeni oraz metodom i środkom, jakich używają władze w Teheranie, aby realizować własny program działania.

Wspólnota Wywiadowcza zwraca uwagę na to, że Iran – obok Chińskiej Republiki Ludowej, Federacji Rosyjskiej czy Koreańskiej Republiki Ludowo-Demokratycznej – uważany jest za przeciwnika, którego zdolności w cyberprzestrzeni stanowią poważne zagrożenie dla bezpieczeństwa Stanów

Zjednoczonych. Zauważono, że wraz z upływem czasu działania Irańczyków są coraz bardziej wyszukane, co świadczy o rosnącym zainteresowaniu Teheranu tego typu środkami. Amerykańskie przedsiębiorstwo z branży cyberbezpieczeństwa — FireEye — wymienia kilka APTs (ang. *advanced percistent threat*) powiązanych najprawdopodobniej z rządem Iranu, tj. APT: 33, 34, 35 oraz 39. Ataki takie mogą być przeprowadzone bądź wspierane przez państwa. Ukierunkowane są na konkretne instytucje czy organizacje przy wykorzystaniu złośliwego oprogramowania oraz innych środków i metod (np. zainfekowanych pamięci USB, płyt CD) służących infekcji komputerów, penetracji sieci, pozyskiwaniu wrażliwych danych itp. Celem wspomnianych ataków były instytucje polityczne, wojskowe i bezpieczeństwa związane z rządem Stanów Zjednoczonych, państwami Bliskiego Wschodu (m.in. Arabią Saudyjską) czy Europy Zachodniej. Ponadto, ofiarą tych działań padły podmioty prywatne, w tym przedsiębiorstwa z branży finansowej, zbrojeniowej, telekomunikacyjnej, IT, energetycznej, medialnej, a nawet turystycznej.

We wspomnianym raporcie Narodowa Rada Wywiadu ocenia, że w 2020 r. Teheran starał się podważyć pozycję wyborczą ówczesnego prezydenta Donalda J. Trumpa[1]. Poprzez te działania Irańczycy starali się nie tylko wpłynąć na wynik wyborów, ale także osłabić zaufanie obywateli Stanów Zjednoczonych do instytucji państwowych, mechanizmów demokratycznych oraz pogłębić i tak już wyraźne podziały społeczne wśród Amerykanów. Operacja ta została zatwierdzona przez Najwyższego Przywódcę Iranu ajatollaha Alego Chameneiego, zaś za jej przeprowadzenie odpowiedzialne były instytucje wojskowe oraz służby wywiadowcze Iranu. Autorzy raportu zwracają uwagę na niejako dwutorową działalność Irańczyków. Z jednej strony celem ataków była infrastruktura krytyczna Stanów Zjednoczonych, z drugiej — oddziaływanie na amerykańską opinię publiczną z wykorzystaniem sieci oraz mediów społecznościowych. Zabiegi Irańczyków polegały przede wszystkim na tworzeniu i funkcjonowaniu fikcyjnych kont prowadzonych w mediach społecznościowych, które miały zniechęcać potencjalnych wyborców do oddania głosu na ubiegającego się o reelekcję prezydenta. Motywem przewodnim tych treści była sytuacja społeczna spowodowana pandemią SARS-CoV-2, recesja amerykańskiej gospodarki oraz niepokoje wśród ludności cywilnej. Irańczycy podszywali się pod członków organizacji *Proud Boys*[2], nękając sympatyków i członków Partii Demokratycznej, a także wysyłając wiadomości o możliwych nieprawidłowościach wyborczych. Tym samym irański wywiad aktywnie wykorzystuje wzrost znaczenia krajowego ekstremizmu, który jest uważany przez władze amerykańskie, w tym dyrektora Federalnego Biura Śledczego, za jeden z głównych czynników zagrażających bezpieczeństwu wewnętrznemu USA.

Szacuje się, że do tej operacji podmioty pośrednio i bezpośrednio powiązane z Teheranem utworzyły kilka tysięcy fikcyjnych kont. Irańczycy koncentrowali się głównie na działaniach, które przełożyłyby się na zmianę preferencji politycznych, a w rezultacie — oddanie głosu na kandydata pożądanego przez Teheran. Choć Irańczycy byli świadomi podatności na ataki hakerskie części amerykańskiej infrastruktury niezbędnej w procesie wyborczym, to jednak nie podjęli kroków w celu jej głębszego wykorzystania. W ocenie Wspólnoty Wywiadow-

[1] W odróżnieniu od Moskwy, zainteresowanej utrzymaniem ówczesnego prezydenta na urzędzie.
[2] Organizacja skupiająca białych supremacjonistów, założona w 2016 roku. Brała udział w ataku na Kapitol 6 stycznia 2021 r., w związku z czym postawiono zarzuty czterem liderom grupy.

czej, za użyciem tych środków przemawiała przede wszystkim ekonomia działań operacyjnych. Takie przedsięwzięcie nie wymagało fizycznej obecności irańskich funkcjonariuszy bądź agentów na terytorium Stanów Zjednoczonych, co zmniejszało ryzyko dekonspiracji oraz zwiększało możliwość kontroli. Według raportu powiązany z Iranem libański Hezbollah, który w marcu 2021 r. z pomocą Korpusu Strażników Rewolucji Islamskiej powołał do życia komórkę odpowiedzialną za prowadzenie operacji w cyberprzestrzeni, był zainteresowany ingerencją w amerykański proces wyborczy.

Intensywne próby wykorzystania przez Irańczyków potencjału tkwiącego w cyberprzestrzeni były wynikiem dwóch wydarzeń. Pierwsze z nich to wykorzystanie sieci oraz mediów społecznościowych do mobilizacji zwolenników Mir-Hosejna Musawiego (tzw. Zielona Rewolucja z 2009 r.), co w rezultacie doprowadziło do największych od 1979 r. protestów. Drugie to atak na irańskie instalacje nuklearne w 2010 r. przy użyciu komputerowego robaka *Stuxnet*, który nie miał charakteru bezpośredniego, fizycznego uderzenia z wykorzystaniem konwencjonalnych środków, np. lotnictwa. Doświadczenia samego Iranu, jak i innych państw regionu czyniłyby taką operację dość prawdopodobną. We wrześniu 1980 r., osiem dni po rozpoczęciu konfliktu z Irakiem, Teheran zdecydował się na bezpośredni atak na iracki ośrodek nuklearny pod Bagdadem. Rok później, w 1981 r. nalot na ten sam ośrodek przeprowadzili Izraelczycy. W 2007 r. Izrael zniszczył syryjskie instalacje nuklearne we wschodniej Syrii. Wydarzenia te skłoniły decydentów do instytucjonalizacji wykorzystania środków cybernetycznych oraz przeciwdziałania cyberatakom przez system bezpieczeństwa Iranu.

Od 2010 r. Irańczycy znacznie rozwinęli swoje zdolności w cyberprzestrzeni. Sieć podmiotów powiązana zarówno z defensywnym, jak i ofensywnym wykorzystaniem środków cybernetycznych koncentruje się wokół policji, armii, Ministerstwa Wywiadu, Korpusu Strażników Rewolucji Islamskiej, a nawet Basidżów. Koordynacją ich działań zajmuje się powstała w 2011 r. Najwyższa Rada Cyberprzestrzeni.

W raporcie przygotowanym na potrzeby Kongresu i poświęconym irańskim zdolnościom w cyberprzestrzeni przywołano kilka ataków, które Irańczycy przypuścili na Stany Zjednoczone oraz ich sojuszników. To między innymi atak na Saudi Aramco w 2012 r., który doprowadził do zakłócenia działalności głównej rafinerii saudyjskiego przedsiębiorstwa (w 2017 r. ponownie zaatakowano to przedsiębiorstwo oraz katarski RasGas), a także znajdujące się w Las Vegas kasyna należące do nieżyjącego już Sheldona Adelsona. Znany był on ze swoich republikańskich sympatii, wspierał finansowo kampanie Partii Republikańskiej, a także udzielał poparcia izraelskiemu premierowi Benjaminowi Netanjahu. Ataki te przybierały nie tylko formę jednokrotnego incydentu, lecz były również znacząco rozłożone w czasie (głównie rozproszona odmowa dostępu - DDoS), a ich ofiarą padły amerykańskie banki, w tym Bank of America oraz Wells Fargo. Celem irańskich hakerów stała się również mała zapora wodna położona w miasteczku Rye w stanie Nowy Jork.

W marcu 2018 r. amerykański Departament Sprawiedliwości oskarżył dziewięciu Irańczyków o włamanie w okresie od 2013 do 2017 r. do sieci ponad 144 amerykańskich uniwersytetów oraz 176 innych placówek w ponad 21 państwach (również w Polsce). Hakerzy wykradli ponad 31 terabajtów wrażliwych danych i treści będących własnością intelektualną ośrodków. Celem ataków stały się także podmioty prywatne, federalne (m.in Departament

Pracy) i stanowe (m.in. stan Hawaje). Z cyberszpiegostwem powiązana jest sprawa byłej funkcjonariuszki amerykańskich służb wywiadowczych. Monica Elfriede Witt przeszła na stronę Irańczyków w 2013 roku. Zarzuty o próbę włamania do rządowych sieci komputerowych i kradzież tożsamości postawiono również czterem irańskim hakerom, którzy mieli włamać się do urządzeń wskazanych przez Witt pracowników amerykańskiej wspólnoty wywiadowczej. Ponadto, Iran korzysta z ataków w cyberprzestrzeni do realizacji polityki regionalnej. Celem tych ataków są głównie państwa rywalizujące z Iranem, będące członkami Rady Współpracy Zatoki Perskiej (ang. *Gulf Cooperation Council*, GCC).

Powyższa ocena działalności Teheranu przywodzi na myśl tzw. środki aktywne (ros. *активные мероприятия*), które kojarzone są głównie z działalnością rosyjskich służb wywiadowczych. Interesującą kwestią pozostaje wpływ rosyjskiej doktryny dotyczącej środków aktywnych na wykorzystanie ich przez Irańczyków. W latach 90. XX w., już po rozbudowie aparatu bezpieczeństwa na skutek zmian politycznych i wojny z Irakiem, irańskie Ministerstwo Wywiadu nawiązało współpracę z następczynią KGB — Służbą Wywiadu Zagranicznego FR. Obszarem współpracy obu służb było ograniczenie amerykańskich wpływów w Azji Środkowej, a także wymiana doświadczeń dotycząca zwalczania obecnych na terytorium obu państw separatyzmów etnoreligijnych. W raporcie dotyczącym wspomnianego wyżej resortu wskazuje się, że Ministerstwo Wywiadu korzysta z osiągnięć wojny psychologicznej oraz dezinformacji przeciwko państwom, organizacjom czy środowiskom (głównie dysydentów) uznawanym za przeciwników obecnego systemu.

Analitycy Atlantic Council wskazują, że Irańczycy rozpoczęli działania oparte na tworzeniu fałszywych profili w mediach społecznościowych już w 2010 r., jednak działalność ta nie była obiektem zainteresowania Amerykanów. Sytuacja zmieniła się w 2018 r., kiedy to wykryto siatkę blisko 70 stron internetowych, działających w 15 państwach. Jej głównym celem były działania dezinformacyjne. Działalność Irańczyków skupiała się głównie na obszarze państw Bliskiego Wschodu — Jemenie i Syrii, jednak celem były również państwa Zachodu (np. Wielka Brytania, Stany Zjednoczone) oraz Rosja.

W opublikowanej na początku kwietnia 2021 r. przez amerykańską Wspólnotę Wywiadowczej corocznej ocenie zagrożeń, Iran wciąż pozostanie wyzwaniem dla interesów i bezpieczeństwa Stanów Zjednoczonych oraz jego sojuszników na Bliskim Wschodzie. Ponadto, władze irańskie będą w dalszym ciągu zainteresowane użyciem cyberprzestrzeni do wrogich działań, takich jak: cyberszpiegostwo, ataki na infrastrukturę krytyczną (w kwietniu i lipcu 2020 r. celem ataków stały się izraelskie sieci wodociągowe) oraz operacje wpływu, mające na celu rozprzestrzenianie fałszywych informacji oraz osłabienie zaufania do instytucji państwowych.

Irańskie próby ingerencji w amerykański proces wyborczy należy wpisać w szerszy kontekst dwustronnych relacji pomiędzy Teheranem a Waszyngtonem. Kampania wymierzona w Donalda J. Trumpa była próbą odpowiedzi na twardy kurs obrany przez administrację ówczesnego prezydenta po 2016 roku. W maju 2018 r. amerykańska administracja wycofała się z porozumienia nuklearnego (*Joint Comprehensive Plan of Action*, JCPOA), później nałożono na Iran kolejne sankcje, zaś w styczniu 2020 r. prezydent USA wydał rozkaz zlikwidowania (ang. *targeted killing*) gen. Solejmaniego — wpływowego dowódcy Korpusu Strażników

Rewolucji Islamskiej. Osłabienie jego pozycji wiązało się więc z obawami utrzymania polityki ,,maksymalnej presji'', którą Donald J. Trump mógłby kontynuować w razie reelekcji.

Z punktu widzenia Teheranu kontrkandydat Donalda J. Trumpa — Joseph R. Biden Jr. i jego nowa administracja wywodząca się z Partii Demokratycznej — mógłby dążyć do zmniejszenia napięcia we wzajemnych relacjach i wrócić do rozmów w sprawie kontynuacji porozumienia nuklearnego z 2015 roku. W gabinecie nowego prezydenta zasiadają osoby, które były odpowiedzialne za ich przebieg, ale także politycy, którzy opowiadają się za powrotem do umowy, m.in. sekretarz stanu A. Blinken, W. Sherman — zastępca sekretarza stanu, główny negocjator ze strony amerykańskiej, doradca ds. bezpieczeństwa narodowego J. Sullivan czy dyrektor Centralnej Agencji Wywiadowczej W. J. Burns. Formalnie tylko Stany Zjednoczone wycofały się z JCPOA, w wyniku czego Iran stopniowo odchodził od postanowień porozumienia, informując o tym jego strony i instytucje międzynarodowe.

Zarówno nowa administracja USA, jak i rządy Francji, Niemiec i Wielkiej Brytanii, a także sam rząd w Teheranie, z zastrzeżeniem zniesienia sankcji, są zainteresowane wznowieniem negocjacji w sprawie przywrócenia porozumienia, o czym świadczą chociażby ostatnie próby podjęcia rozmów w Wiedniu. Pomimo zmiany administracji Waszyngton nie może jednak lekceważyć aktywnej polityki Iranu na Bliskim Wschodzie — ingerencji w państwach ościennych, wsparcia szyitów w Iraku czy Jemenie, a także Baszara al-Asada w Syrii. Z drugiej strony, w tym regionie Amerykanie muszą liczyć się także z interesami swoich sojuszników, przede wszystkim Izraela oraz Arabii Saudyjskiej.

W samym Iranie zaufanie do Stanów Zjednoczonych po wycofaniu się z porozumienia JCPOA jest ograniczone. Część sił politycznych (związana z Najwyższym Przywódcą) odrzuca możliwość podjęcia kolejnych rozmów. Należy pamiętać o nadchodzących w czerwcu 2021 r. irańskich wyborach prezydenckich, które mogą wyłonić administrację niechętną utrzymaniu porozumienia i poprawie relacji ze Stanami Zjednoczonymi. Do tego momentu przełom na linii Waszyngton – Teheran wydaje się mało prawdopodobny.

***

Próby ingerencji Irańczyków w funkcjonowanie procesu wyborczego, ale także ograniczone usiłowanie kształtowania nastrojów społecznych pokazuje, iż Iran stara się w ramach swoich możliwości aktywnie oddziaływać na system polityczny państwa uznawanego za głównego przeciwnika. Działania te podporządkowane są przede wszystkim realizacji określonych założeń polityki zagranicznej Iranu, a także mają na celu wzmocnienie potencjału w obszarze bezpieczeństwa zewnętrznego. Przedmiotem zainteresowania Irańczyków są podmioty państwowe, jak i prywatne, uznane przez Teheran za godzące w republikę islamską.