Komentarz KBN

Nr 8 (80) / 2021 12 sierpnia 2021 r.

Powrót cara i drużyna marzeń – pierwsze decyzje Joe Bidena w zakresie cyberbezpieczeństwa

Dominika Dziwisz

Pierwsze 100 dni w Białym Domu jest traktowane przez komentatorów polityki USA jako prognoza kadencji nowego prezydenta — zarówno w zakresie tego, czego się można po niej spodziewać, jak i tego, co nowa administracja jest w stanie zaproponować i osiągnąć. Jest to najlepszy czas na przebicie się z nowymi, często kontrowersyjnymi, pomysłami i inicjatywami.

Joe Biden, 46. prezydent USA, objął urząd w niełatwych czasach, kiedy Amerykanie, po burzliwym okresie rządów Donalda Trumpa, byli (i nadal są) głęboko podzieleni, a wskaźniki COVID-19 były najgorsze od początku pandemii. Można było założyć, że te i inne palące wyzwania, jak choćby zmiana polityki klimatycznej, redefiniowanie wpływów firm technologicznych, czy ożywienie gospodarki, okażą się ważniejsze niż problemy cyberbezpieczeństwa. Jednak, zgodnie z obietnicami przedwyborczymi Joe Bidena, cyberbezpieczeństwo ma mieć najwyższy priorytet na każdym szczeblu administracji. Po kilku miesiącach spędzonych przez nowego prezydenta w Białym Domu można dokonać pierwszych analiz i ocenić, czy polityka cyberbezpieczeństwa Joe Bidena faktycznie będzie inna niż ta prowadzona przez Donalda Trumpa.

Cyber Biden vs. Cyber Trump – kontynuacja czy nowa polityka cyberbezpieczeństwa?

Zazwyczaj pierwsza kadencja nowego prezydenta USA jest w dużej części kontynuacją kierunku obranego przez jego poprzednika. W przypadku Bidena niekoniecznie jest inaczej.

Z jednej strony są sygnały, że prezydentura Bidena oznacza powrót do polityki jego dawnego szefa, Baracka Obamy. Przejawia się to większym zaangażowaniem w budowanie polityki cyberbezpieczeństwa i międzynarodowego dialogu w tym zakresie, przywróceniem niektórych organizacyjnych struktur cyberbezpieczeństwa oraz, co oczywiste, powrotem do łask zaufanych doradców – weteranów cyberbezpieczeństwa. Wszystko wskazuje też na to, że Biden będzie stosował zwiększoną presję na Rosję. W 2016 r. dokonała ona systematycznej ingerencji w kampanię przed wyborami prezydenckimi w USA[1]. Biden, który był wtedy wiceprezydentem, obiecał, że USA wykorzystają arsenał możliwości działań w cyberprzestrzeni, aby wysłać Władimirowi Putinowi „wiadomość" w najlepszym, wybranym przez USA momencie. Pierwszy taki sygnał ostrzegawczy został wysłany do Rosjan pod koniec 2020 r. po atakach hakerskich na firmę SolarWinds, który pozostawał niewykryty przez wiele miesięcy. Urzędujący wtedy Donald Trump podał w wątpliwość zaangażowanie Rosji i nazwał ataki „znacznie poważniejszymi w 'Fake Newsach' niż w rzeczywistości". Natomiast prezydent-elekt zareagował zdecydowanie, potępiając Rosję i przyrzekając podjęcie postępowania karnego. Swoje obietnice spełnił w kwietniu 2021 r. ogłaszając pakiet sankcji wobec Moskwy, w tym sankcji finansowych i wydaleń dyplomatów. Tym samym Biały Dom jasno dał do zrozumienia, że podjęte kroki są reakcją na szkodliwe działania Rosji, które nie będą tolerowane, co oznacza radykalną zmianę podejścia Białego Domu do cyberbezpieczeństwa, które w ciągu ostatnich czterech lat było niespójne.

Z drugiej strony, przyjęcie bardziej agresywnej polityki wobec Rosji oznacza jednocześnie kontynuację kontrowersyjnej, wprowadzonej w czasie kadencji Trumpa, aktywnej strategii Pentagonu, wyrażonej w koncepcjach „stałego zaangażowania" (*persistent engagement*) oraz „obrony wyprzedzającej" (*defend forward*). Można to wywnioskować z oświadczenia prezydenta Bidena i wiceprezydent Harris, które zostało wydane po ataku SolarWinds, w którym powtórzono, że „dobra obrona nie wystarczy". Innymi słowy, nowe koncepcje agresywnych działań w cyberprzestrzeni będą nadal rozwijane. Bardzo prawdopodobne, że tym samym Trump zrobił Bidenowi przysługę forsując odważne ofensywne rozwiązania, które pomimo kontrowersji są skutecznym narzędziem zwalczania agresji w cyberprzestrzeni oraz odstraszania.

Pomimo rozbieżności w realizacji polityki cyberbezpieczeństwa, porównanie opublikowanych w marcu 2021 r. wytycznych polityki cyberbezpieczeństwa z przyjętą w 2018 r. Strategią Cyberbezpieczeństwa także nie wskazuje na zasadniczą zmianę kursu. W obu dokumentach podkreślono priorytetowe znaczenie cyberbezpieczeństwa dla polityki bezpieczeństwa USA, konieczność współpracy z sektorem prywatnym, zaangażowanie międzynarodowe i odstraszanie cyberprzestępców. Różnice są nieznaczne. Wytyczne Bidena akcentują znaczenie różnorodności w krajowej bazie talentów cybernetycznych, zarówno w rządzie, jak i w sektorze prywatnym,

[1] Śledztwo Roberta Muellera, specjalnego prokuratora do nadzorowania federalnego śledztwa w sprawie zarzutów o ingerencję Rosji w wybory prezydenckie, zakończyło się aktami oskarżenia przeciwko obywatelom rosyjskim za udział w ingerencji, ale nie dostarczyło dowodów na to, że Trump lub jego zespół bezpośrednio pomagali Rosji w jej rzekomych przestępstwach.

podczas gdy dokument Trumpa milczy w tej sprawie. Brak specjalistów w obszarze cyberbezpieczeństwa jest bardziej dotkliwy w przypadku stanowisk rządowych, ponieważ praca dla rządu tradycyjnie jest mniej dochodowa niż zajmowanie podobnych stanowisk w sektorze prywatnym, co skutecznie zniechęca najlepszych kandydatów. Innymi słowy, taka praca oznacza dużą odpowiedzialność przy niewielkiej realnej decyzyjności. W związku z tym administracja Bidena musi zwiększyć fundusze na szkolenia i rekrutację, aby pomóc w obsadzeniu krytycznych stanowisk. Jest to zdanie podzielane przez ekspertów: „Mamy nowego prezydenta, ale niedobór talentów w zakresie cyberbezpieczeństwa (zaostrzony przez pandemię) utrzymuje się. Nowa administracja nie będzie miała luksusu zajmowania się tylko dzisiejszymi wyzwaniami związanymi z cyberbezpieczeństwem i będzie musiała poważnie podejść do rozwoju pracowników i włączenia do pracy większej liczby osób – a to będzie oznaczać więcej nietradycyjnych kandydatów [którzy będą wymagać rozwoju szkoleń - przyp. aut.]".

Ponadto Biden mocno popiera inwestycje rządowe w cyberbezpieczeństwo, podczas gdy dokument Trumpa wskazuje na zminimalizowanie znaczenia inwestycji rządowych w cyberbezpieczeństwo, choć jednocześnie podkreśla rolę rządu w ułatwianiu sektorowi prywatnemu inwestowania w cyberbezpieczeństwo. Warto dodać, że Narodowa Strategia Cybernetyczna Trumpa nie różniła się zbytnio od cyberstrategii Obamy, co może sugerować bardziej ciągłość i ewolucję podejścia do cyberbezpieczeństwa, a nie rewolucyjne zmiany. Sposób realizacji strategii i szczegółowe dokumenty oraz efektywność strategii zależą od tego, jak dobrze administracja Bidena ją wprowadzi w życie. A największy wpływ na to będzie miał zespół doradców.

Powrót cyber-cara i drużyna marzeń

O realnej sile prezydenta decyduje zespół jego doradców. Donald Trump poświęcił sporo czasu i energii na zwalnianie specjalistów ds. cyberbezpieczeństwa i zamykanie agencji cyberbezpieczeństwa. Joe Biden musi zmierzyć z zupełnie innymi wyzwaniami – koordynacją dużej liczby wysoko postawionych, dobrze przygotowanych ludzi na stanowiskach kierowniczych. Jak się powszechnie komentuje, Bidenowi udało się zbudować najbardziej kompetentny zespół doradców jaki kiedykolwiek zgromadzono w rządzie USA. Jednakże, potencjalnie złą wiadomością jest to, że USA mają kilka „nakładających się pozycji i ról, walczących o władzę, ograniczone budżety federalne i wpływy". Innymi słowy, może to doprowadzić do sytuacji odwrotnej do zamierzonej, kiedy rywalizacja silnych charakterów doprowadzi do walki o władzę, sporów o kompetencje i zakres odpowiedzialności, a ostatecznie do atomizacji amerykańskiej polityki cyberbezpieczeństwa.

Dla polityki cyberbezpieczeństwa kluczowe są cztery stanowiska.

Pierwszym z nich jest cyber-koordynator Białego Domu. To stanowisko zostało utworzone za prezydentury Baracka Obamy i zgodnie z założeniami „cyber-car" miał być jednym z najważniejszych doradców prezydenta odpowiedzialnym za ujednolicenie polityki rządu w zakresie cyberbezpieczeństwa i cyberwojny. W praktyce, od momentu utworzenia tego stanowiska koordynator nigdy nie miał żadnej realnej władzy, a zakres jego uprawnień był znacznie węższy. Rola ta ograniczała się do budowania atmosfery zaufania między sektorami i współpracy z sektorem

prywatnym, co *de facto* dublowało kompetencje Departamentu Bezpieczeństwa Krajowego. W 2018 r. Donald Trump zlikwidował stanowisko cyber-koordynatora uznając je za niepotrzebne.

Brak lidera koordynującego politykę federalną w zakresie cyberbezpieczeństwa stał się szczególnie widoczny po atakach rosyjskich hakerów na systemy SolarWinds, a także chińskich na Microsoft Exchange Server. Ostatecznie dopiero w połowie kwietnia 2021 r. Biden mianował Chrisa Inglisa, byłego zastępcę dyrektora Narodowej Agencji Bezpieczeństwa (NSA), na stanowisko krajowego dyrektora ds. cyberprzestrzeni (U.S. National Cyber Director). Zgodnie z zapisami najnowszej National Defense Authorization Act, dyrektor ma mieć większy autorytet i realny wpływ na politykę cyberbezpieczeństwa niż cyber-koordynatorzy za prezydentury Obamy. Ma on doradzać prezydentowi we wszystkich kwestiach związanych z cyberbezpieczeństwem i pomagać w koordynowaniu reakcji rządu na poważne ataki cyfrowe oraz działań dyplomatyczne związanych z cyberbezpieczeństwem. Dyrektor jest jednym z nielicznych urzędników Białego Domu, którego stanowisko wymaga zatwierdzenia przez Senat, co dodaje mu prestiżu.

Kongres nie określił dokładnego zakresu kompetencji i władzy Inglisa i pozostaje niejasne, w jaki sposób będzie on współpracował z Anne Neuberger, zastępczynią prezydenckiego doradcy ds. bezpieczeństwa narodowego w sprawach nowych i cybernetycznych technologii (Deputy National Security Advisor for Cyber and Emerging Technology). Może to zadziałać na korzyść Inglisa, bo mając w dużej mierze nieokreślony mandat, będzie miał wyjątkową okazję do ukształtowania roli dyrektora. Neuberger odpowiedzialna jest za koordynację działań rządu federalnego w zakresie cyberbezpieczeństwa. Jest dobrze przygotowana do tego zadania, mając doświadczenie jako pierwszy dyrektor ds. cyberbezpieczeństwa w NSA, gdzie zarządzała wymianą informacji wywiadowczych związanych z zagrożeniami dla infrastruktury krytycznej pomiędzy NSA a innymi agencjami rządowymi i sektorem prywatnym.

Trzecią osobą decydującą o cyberbezpieczeństwie USA jest Jen Easterly, również była urzędniczka NSA. W rządzie Bidena przydzielono jest stanowisko dyrektor Agencji Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA), najważniejszej krajowej agencji zaangażowanej w ochronę infrastruktury krytycznej przed atakami.

Ostatnim członkiem prezydenckiego cyberkwartetu, obok Inglisa, Neuberger i Easterly, jest Paul Nakasone, dyrektor NSA i jednocześnie szef USCYBERCOM. Ten czterogwiazdkowy generał jest odpowiedzialny zarówno za U.S. Cyber Command, jak i NSA. Innymi słowy, Nakasone jest bezpośrednio odpowiedzialny za zapobieganie kolejnemu niespodziewanemu atakowi, gdziekolwiek i kiedykolwiek on nadejdzie, czy to w świecie fizycznym, czy w wirtualnym. Jako dyrektor NSA dowodzi największą agencją wywiadowczą na świecie, a jako dyrektor U.S. Cyber Command odpowiada nie tylko za obronę USA przed cyberatakami, ale także za przeprowadzanie cyberataków.

Biden obsadził stanowiska doświadczonymi specjalistami z sektora publicznego. Natomiast nie pojawiają się tu żadne nazwiska ekspertów z sektora prywatnego. Zważywszy na to, że większość elementów amerykańskiej infrastruktury krytycznej (od 80 do 90 proc.) jest w rękach prywatnych, może to być zaskakujące. Wygląda na to, że pomimo wielokrotnych zapewnień o konieczności budowania skutecznej i ścisłej współpracy między sektorami publicznym i prywatnym, realne działania w tym obszarze nadal pozostają w sferze obietnic wyborczych. To błąd,

ponieważ połączenie wiedzy specjalistów z obu sektorów oznacza większą pulę wiedzy i większą skuteczność działania.

Jedną z możliwych interpretacji braku realnych zmian w tym obszarze jest to, że Waszyngton z góry zakłada, że dla każdego z rodzajów cyberagresji możliwe są rozwiązania opracowane na poziomie rządowym, a rola sektora prywatnego ogranicza się do bycia ofiarą[2]. Takie myślenie ma jednak realną szansę na zmianę po ogłoszeniu 28 lipca memorandum w sprawie poprawy cyberbezpieczeństwa infrastruktury krytycznej. Zwrócono w nim uwagę na to, że zabezpieczenie infrastruktury krytycznej wymaga podejścia całego narodu i obu sektorów, bo rząd federalny nie może tego zrobić sam.

Podsumowanie

Joe Biden zrekrutował najlepszych specjalistów ds. polityki cyberbezpieczeństwa. Czas pokaże czy stworzą oni równie sprawny zespół. Jest na to szansa, też i z uwagi na to, że w przeciwieństwie do prowadzonej przez Trumpa polityki częstej wymiany ludzi na stanowiskach, nowy prezydent chce realizować spójną politykę i cyberstrategię. Brak przedstawicieli sektora prywatnego w tym gronie jest problemem, ale ogłoszone 28 lipca br. memorandum sygnalizuje, że przynajmniej dostrzeżono konieczność zmian w tym zakresie. Od początku kampanii wyborczej wszystko wskazywało na to, że Biden odetnie się od polityki Trumpa grubą kreską. Tym niemniej w zakresie cyberbezpieczeństwa po kilku miesiącach prezydentury niewiele na to wskazuje. Z drugiej strony, zdecydowana postawa wobec Rosji i powrót do dialogu z najważniejszymi partnerami strategicznymi są oceniane jednoznacznie pozytywnie. Wydaje się, że Biden łączy skuteczne (choć kontrowersyjne) elementy strategii Trumpa z dyplomatycznym podejściem Obamy. Kolejnej oceny będzie można dokonać po zakończeniu jego pierwszego roku urzędowania, gdy nowe regulacje zaczną być wprowadzane w życie.

[2] Rozmowa z Jasonem Healeyem z Atlantic Council nt. kształtowanie polityki cyberbezpieczeństwa [w:] D. Dziwisz, *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne*, Kraków 2015.