NOWA STRATEGIA KONTRWYWIADOWCZA USA

Łukasz Kobierski

21 LUTEGO 2020

Źródło: http://ine.org.pl/nowa-strategia-kontrwywiadowcza-usa/?preview_id=16331&preview_nonce=9e9f308944&preview=true&_thumbnail_id=16343

Artykuł w skrócie

1. Nowa Strategia kontrwywiadowcza USA, stawia nacisk na przeciwdziałania zagrożeniom, które zdaniem autorów, znacznie się zmieniły od czasu ostatniej strategii.

2. Nie tylko inne państwa są zagrożeniem dla USA. Wymieniono też ponadnarodowe organizacje przestępcze i podmioty motywowane ideologicznie.

3. Celem ataków są nie tylko agencje rządowe, ale także jednostki amerykańskiej administracji niezwiązane bezpośrednio z bezpieczeństwem państwa.

4. Adwersarze stosują coraz cześciej wyrafinowane zestawy zdolności wywiadowczych przy użyciu nowych technologii. Wskazano na pięć celów Strategii – ochronę państwowej infrastruktury krytycznej, zmniejszenie zagrożenia dla kluczowych łańcuchów dostaw, przeciwdziałanie drenażowi amerykańskiej gospodarki, ochrona instytucji i procesów demokratycznych, przeciwdziałanie operacjom cybernetycznym.

W pierwszej połowie lutego 2020 roku Narodowe Centrum Kontrwywiadu i Bezpieczeństwa (NCSC) podległe pod Biuro Dyrektora Wywiadu Narodowego (DNI) opublikowało Strategię kontrwywiadowczą USA na lata 2020-2022. Przedstawia ona, zdaniem autorów, nowe podejście do kontrwywiadu w celu przeciwdziałania zagrożeniom, które znacznie się zmieniły od czasu ostatniej strategii w 2016 roku.

Jak powiedział dyrektor NCSC William Evanina – ,,Dzisiejsza strategia stanowi zmianę paradygmatu w reagowaniu na zagrożenia związane z obcym wywiadem jako narodem. Podczas gdy poprzednie strategie kontrwywiadu klasyfikowały zagrożenie przez naszych największych przeciwników z obcych państw narodowych, ta koncentruje się na pięciu kluczowych obszarach, w których zagraniczne jednostki wywiadowcze uderzają nas najmocniej i gdzie musimy poświęcić większą uwagę – infrastruktura krytyczna, kluczowe łańcuchy dostaw USA, gospodarka, amerykańskie instytucje demokratyczne oraz operacje cybernetyczne i techniczne”[1].
Jak zauważają analitycy DNI zagrożenia dla Stanów Zjednoczonych ze strony zagranicznych podmiotów wywiadowczych (rozumianych szeroko, zarówno jako aktorów państwowych i pozapaństwowych) stają się coraz bardziej

złożone, różnorodne i szkodliwe dla interesów USA. Trzy główne trendy charakteryzują obecne i nadchodzące środowisko kontrwywiadowcze:

1. Wzrastająca liczba podmiotów zagrażających USA. Jako pierwsze wymieniono Rosję i Chiny. Wśród kolejnych przeciwników państwowych znajdowały się państwa takie jak Kuba, Iran i Korea Północna. Wymienieni aktorzy niepaństwowi to libański Hezbollah, tzw. Państwo Islamskie (ISIS) i al-Kaida. Wskazano także na ponadnarodowe organizacje przestępcze i podmioty motywowane ideologicznie, takie jak hakerzy, osoby publikujący tajne dokumenty (leaktivists), oraz cudzoziemcy bez formalnego powiązania z zagranicznymi służbami wywiadowczymi, kradnący wrażliwe dane i własność intelektualną.

2.Adwersarze mają coraz bardziej wyrafinowany zestaw zdolności wywiadowczych przy użyciu technologii. Wymieniono tutaj m.in. urządzenia biometryczne, systemy bezzałogowe, zdjęcia w wysokiej rozdzielczości, zaawansowane szyfrowanie, analizę dużych zbiorów danych oraz nieautoryzowane ujawnianie amerykańskich narzędzi cybernetycznych.

3.Zagraniczne jednostki wywiadowcze, atakują większość departamentów rządowych i agencje USA, ale także jednostki amerykańskiej administracji niezwiązane z bezpieczeństwem państwa – laboratoria, sektor finansowy, bazy przemysłowe oraz inne podmioty prywatne i akademickie. Część przeciwników próbuje atakować i zakłócać infrastrukturę krytyczną, zdolności wojskowe w czasie kryzysu oraz wpływać na interes gospodarczy USA. Opinia publiczna jest również celem akcji wywiadowczych.

Podkreślono, że ciągle zmieniający się krajobraz technologiczny prawdopodobnie przyspieszy te trendy, zagrażając bezpieczeństwu oraz dobrobytowi narodu amerykańskiego, prowadząc do osłabienia gospodarczego, militarnego i przewagi technologicznej USA. Rozwijane nowe technologie, takie jak sztuczna inteligencja, informatyka kwantowa, nanotechnologia, zaawansowane materiały, ulepszone szyfrowanie, robotyka i Internet rzeczy, pozwolą przeciwnikom USA na bardziej wysublimowane ataki wywiadowcze. W związku z powyższymi, rząd, sektor publiczny i prywatny, zagraniczni sojusznicy i instytucje oraz społeczeństwo amerykańskie musi przyjąć bardziej proaktywną postawę kontrwywiadowczą w sferze bezpieczeństwa oraz odstraszać potencjalnych oponentów.

Dalej wyróżniono pięć celów Strategii:

1) Ochrona państwowej infrastruktury krytycznej.

2) Zmniejszenie zagrożenia dla kluczowych łańcuchów dostaw towarów i usług, zarówno w sektorze zbrojeniowym jak i prywatnym.

3) Przeciwdziałanie drenażowi amerykańskiej gospodarki i zabezpieczenie przewagi konkurencyjnej na światowych rynkach.

4) Ochrona instytucji i procesów demokratycznych oraz zachowania kultury otwartości.

5) Przeciwdziałanie cybernetycznym operacjom obcych wywiadów.

Autorzy podkreśli, że powyższe cele mają równą wagę i reprezentują obszary, gdzie zagrożenie wywiadowcze najbardziej szkodzi interesom bezpieczeństwa narodowego USA.

W kolejnej części przedstawiono plan, na podstawie którego uda się zrealizować pięć celów strategicznych.

Dla ochrony państwowej infrastruktury krytycznej:

– rozszerzanie wymiany informacji o infrastrukturze krytycznej z departamentami federalnymi i agencjami, z władzami stanowymi, lokalnymi, plemiennymi oraz z sektorem prywatnym partnerami i sojusznikami,

– utrzymać, szkolić i rozszerzyć grono ekspertów, którzy mogą identyfikować i przeciwdziałać zagrożeniom dla infrastruktury krytycznej w USA,

– rozwinąć nowe narzędzie analityczne, aby poprawić system ostrzegania oraz umożliwić akcje ofensywne i defensywne.

Dla zmniejszenia zagrożenia dla kluczowych łańcuchów dostaw:

– zwiększenie możliwości wykrywania zagrożeń w łańcuchu dostaw poprzez dostęp do nowych źródeł informacji, zrozumienia i oceny zamiarów przeciwników, wprowadzenie nowych procesów identyfikacji podejrzanych lub dostawców wysokiego ryzyka, produktów, oprogramowania i usług,

– zwiększenie integralność i zarządzanie ryzykiem łańcucha dostaw w całym rządzie federalnym,

– rozszerzenie obszarów/zakresu zagrożeń łańcuchów dostaw, zarządzania ryzykiem i najlepszych praktyk.

Dla przeciwdziałania drenażowi amerykańskiej gospodarki:

– poprawa wykrywania zagranicznych zagrożeń dla krajowej bazy innowacji,

– zwiększenie świadomości zagrożenia wywiadu zagranicznego dla gospodarki USA,

– identyfikacja i przeciwdziałanie inwestycjom zagranicznym w Stanach Zjednoczonych, które mogą stanowić zagrożenie bezpieczeństwa dla państwa, poprzez współpracę z sektorem prywatnym w celu opracowania lepszych procedur śledzenia inwestycji zagranicznych.

Dla ochrony instytucji i procesów demokratycznych:

– rozwinięcia możliwości działania kontrwywiadowczego w celu wykrywania, odstraszania i przeciwdziałaniu zagranicznym wpływom,

– wzmocnienie partnerstwa między departamentami i agencjami rządowymi USA oraz szczególnie z firmami z branżny mediów społecznościowych, firmami technologicznymi i środowiskiem akademickim w celu podniesienia świadomości na temat działalności obcych wpływów,

– wzmocnienie współpracy z zagranicznymi partnerami w celu podnoszenia świadomości na temat działalności obcych wywiadów, dzielenia się doświadczeniami oraz dobrymi praktykami.

Dla przeciwdziałania cybernetycznym operacjom:

– polepszenie integracji społeczności kontrwywiadowczej, bezpieczeństwa i sfery cybernetyczne,

– rozwijanie, szkolenie i utrzymanie kadry kontrwywiadu cybernetycznego i technicznego,

– ulepszenie zestawu narzędzi do kontrwywiadu cybernetycznego we współpracy z sektorem prywatnym,

Pod koniec raportu podsumowano zasady, którymi powinno kierować się USA, w celu osiąganięcia swoich celów:

– partnerstwo i wymiana informacji,

– innowacyjność, aby opracowywać i wdrażać technologie i rozwiązania, aby poszerzyć możliwości kontrwywiadowcze,

– dostosowanie strategii, planów i wytycznych do pięciu celów niniejszej strategii

– zidentyfikowanie wymagań dotyczące zasobów, by zostały odpowiednio odzwierciedlone i uszeregowane według priorytetów w cyklu planowania i budżetowania.

– ocena skuteczności zamierzonych postępów

Wnioski i rekomendacje

Strategia przedstawia ogólnikowo cele i zagrożenia przed którymi stoją Stany Zjednoczone w sferze kontrwywiadowczej. W dokumencie, często odwoływano się do ochrony gospodarki państwa. Można powiedzieć, że to jedno z najważniejszych wyzwań nowej Strategii. Trump w swojej retoryce, często odwołuje się do kwestii gospodarczych, co ma odzwierciedlenie w dokumencie strategicznym.

W Strategii podkreślono, że rząd USA nie jest w stanie samodzielnie stawić czoła wszystkim wyzwaniom i wzywa do przyjęcia podejścia opartego na współpracy całego społeczeństwa USA, pomocy sektora prywatnego, dobrze poinformowanej opinii publicznej oraz zagranicznych sojuszników.

Większość nowych priorytetów kontrwywiadu USA związanych jest z negatywnymi dla Ameryki działaniami Chińskiej Republiki Ludowej – kradzieży własności intelektualnej, zagrożenia ze strony nowych technologii, zaburzenia kluczowych łańcuchów dostaw. Elity Stanów Zjednoczonych próbują balansować siłę Chin i przy każdej możliwej okazji przypominać, o niebezpieczeństwie dla bezpieczeństwa państw ze strony Pekinu.

Polska, czy szerzej Unia Europejska, również mogłaby zintensyfikować wzajemną wymianę informacji kontrwywiadowczych, o zagrożeniach ze strony różnych aktorów. Należy też włączyć w tę sferę sektor prywatny. Współpraca na tym polu mogłaby być swoistą sytuacją win-win.

Podobnie jak w USA, powinniśmy wskazać strategiczne priorytety i podstawowe obszary działań służby kontrwywiadowczych, dostosowanych do obecnych, dynamicznie zmieniających się realiów. Pozwoli to na lepsze przygotowanie się możliwych ataków oraz rozsądnego rozdysponowania środków finansowych.

Konieczne jest szkolenie obecnej i przyszłej kadry kontrwywiadowczej, która jest świadoma wyzwań ich służby w XXI wieku. Należy też finansować narzędzia, które będą wspomagać ich pracę, przede wszystkim w obszarze nowych technologii.

---

[1] https://www.dni.gov/index.php/ncsc-newsroom/item/2099-press-release-ncsc-unveils-the-national-counterintelligence-strategy-of-the-u-s-2020-2022

Sfinansowano przez Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018-2030.

O AUTORZE

Łukasz Kobierski

Prezes Zarządu Instytutu Nowej Europy. Absolwent stosunków międzynarodowych Uniwersytetu Warszawskiego oraz Uniwersytetu Mikołaja Kopernika. Stypendysta programu z zakresu bezpieczeństwa narodowego, wywiadu i operacji informacyjnych na Daniel Morgan Graduate School of National Security w Waszyngtonie oraz rocznego stypendium w ramach programu Erasmus na Carl von Ossietzky Universität Oldenburg. Doświadczenie analityczne zdobywał podczas staży m.in. w Departamencie Polityki Bezpieczeństwa Międzynarodowego Ministerstwa Obrony Narodowej oraz Departamencie Analiz Strategicznych Biura Bezpieczeństwa Narodowego.

Kontakt:
lukasz.kobierski@ine.org.pl
https://twitter.com/LukasKobierski