

DYREKTOR STRATCOM: NOWOCZESNA TECHNOLOGIA A DEZINFORMACJA - PRZYJACIEL CZY WRÓG ? [WYWIAD]

Rosyjskie działania zakończyły się sukcesem, ponieważ byliśmy nieprzygotowani mówi Jānis Sārts, dyrektor Centrum Eksperckiego NATO ds. Komunikacji Strategicznej. W wywiadzie ekspert mówi również o ewolucji działań Rosji w sferze informacyjnej, zagrożeniu ze strony deepfake i innowacyjnych pomysłach na walkę z dezinformacją.

Jakie są obecnie największe wyzwania w sferze informacyjnej?

Sfera informacyjna, w której wszyscy jesteśmy zmienia się niezwykle dynamicznie. Sytuacja ta ma miejsce poprzez ciągłą transformację technologiczną. Wymaga to zrozumienia zmian, które mają obecnie miejsce oraz znalezienia ludzi z odpowiednimi umiejętnościami, co nie jest łatwe. Potrzebujemy analityków danych, osób zajmujących się sztuczną inteligencją, inżynierów oprogramowania w celu poznania i zrozumienia środowiska komunikacyjnego i odpowiedzi na wrogie kampanie wpływu prowadzone w cyberprzestrzeni. Największym wyzwaniem jest zmierzenie się z dynamiką tych zmian oraz posiadanie odpowiednich narzędzi, żeby zrozumieć jakie konsekwencje one przyniosą i jak się do nich dostosować. Większość z tych narzędzi NATO nie posiada. Zawsze się pytam, ilu analityków danych i ekspertów od sztucznej inteligencji jest w tej czy innej organizacji. Rzadko kiedy otrzymuje satysfakcjonującą odpowiedź.

Jednym z zagrożeń są rosyjskie działania propagandowe, które były szczególnie widoczne w 2016 roku podczas wyborów prezydenckich w Stanach Zjednoczonych. Jak rosyjska aktywność zmieniła się od tego czasu i czy wciąż musimy się obawiać Rosjan?

Po pierwsze, jeśli spojrzemy na doktryny wojskowe i to co w nich się znajduje na temat operacji informacyjnych, to jest to jeden z najważniejszych elementów postrzegania przez Rosję konfliktu z Zachodem. Ponadto w wielu wypowiedziach rosyjskich wojskowych i polityków można znaleźć odwołania do tego sposobu prowadzenia działań, co daje nam do myślenia jak ważne jest to zagadnienie.

Po drugie, rosyjskie działania w 2016 roku zakończyły się sukcesem, ponieważ byliśmy nieprzygotowani. Mam nadzieję, że to się zmienia i nie mówię tu tylko o Polsce i państwach Bałtyckich, ale również o innych krajach, które w przeszłości nie przykładały odpowiedniej uwagi do ryzyka związanego z działalnością Rosji w sferze informacyjnej.

W 2016 roku, Rosjanie działali ze swojej sfery geolokalizacyjnej, ich skrypty były napisane w cyrylicy, więc łatwo było je wykryć, a reklamy polityczne były wykupione za ruble. Nie były to działania, które ukrywano. Obecnie uważam, że Rosjanie skuteczniej zacierają swoje ślady i o wiele trudniej jest powiedzieć do kogo należy dane konto i czy pochodzi z Rosji czy z innego państwa. To jest jedna

sprawa. Wciąż też Rosjanie stosują metody starej szkoły wykorzystania siatki wpływu, czyli sieci kont rozpowszechniających prorosyjską propagandę. Bardzo trudno jest stwierdzić jakie zależności pomiędzy nimi występują.

W przestrzeni informacyjnej Łotwy mamy "boty", które promują prorosyjskie treści cały czas. Wymaga to wiele czasu i zasobów aby wyśledzić takie działania. Ponadto bardzo trudno jest nam wykazać, że osoby odpowiadające za rozpowszechnianie treści prorosyjskich w mediach społecznościowych biorą pieniądze czy przyjmują polecenia od np. dziennikarzy Sputnika. Starają się to ukryć.

Nie wydaje mi się, że są jednak bardziej efektywni. To co ulega zmianie to fakt, że w ramach naszych społeczeństw mamy więcej słabych punktów, ponieważ obserwujemy coraz większą polaryzację społeczeństw i podział ideologiczny, który można bardzo łatwo wykorzystać. W ten sposób dajemy możliwości działania rosyjskiej dezinformacji.

Łotwa wydaje się być łatwym celem dla rosyjskiej dezinformacji. Jakie są różnice i podobieństwa pomiędzy rosyjskimi kampaniami informacyjnymi w Europie Wschodniej i Zachodniej.

Oczywiście widzimy różnice, ale nie dzieliłbym ich na Europę Zachodnią i Wschodnią. Mamy podział wewnątrz Europy Zachodniej i Europy Wschodniej, jeśli chodzi o prowadzenie operacji informacyjnych. Rosjanie próbują zaadaptować się do specyfiki danego kraju i wykorzystać problemy, które trapią dane państwo. Obecnie w NATO StratCom COE mamy projekt w ramach, którego porównujemy rosyjską dezinformację. Możemy zobaczyć, co oni robią w państwach bałtyckich i nordyckich oraz znaleźć różnice i podobieństwa.

Część z technik jest do siebie podobna, ale cele są zupełnie inne. W państwach bałtyckich, wykorzystuje się fakt, że większość populacji w państwach bałtyckich zna język rosyjski. Można na nich bezpośrednio wpływać poprzez działania informacyjne prowadzone w tym języku przy użyciu rosyjskich, tradycyjnych mediów, które są również transmitowane dla mieszkańców Rosji.

Jeśli chodzi o państwa nordyckie rosyjska propaganda używa ich jako przykładu jak zły jest Zachód. Mamy teorie konspiracyjne o wszechobecnej korupcji. Rosjanie starają się przedstawić obraz Danii, Szwecji czy Finlandii jako skorumpowanych moralnie państw. Ta narracja jest szerzona w Europie Środkowo-Wschodniej. Starają się również wmówić obywatelom, że Zachód jest zły, skorumpowany moralnie a Rosja jest bastionem moralności.

W obszarze symboliki, Rosjanie próbują wykorzystać Europę Wschodnią w narracjach na Zachodzie, mówiąc o tym, że jest zła i nie zasługuje na wsparcie państw zachodnich. Stosują takie figury retoryczne jak np. to, że imigranci z Europy Wschodniej odbierają pracę itp. Są grupy w tych państwach, które chcą wierzyć w takie historie i Rosja wykorzystuje to do własnych celów. Dla osób rosyjskojęzycznych też są adresowane kampanie i ma to miejsce nie tylko w państwach bałtyckich, ale również w Niemczech, gdzie mamy bardzo dużą mniejszość rosyjską liczącą około 2 miliony osób.

Dezinformacja to nie tylko broń, która jest stosowana przez Rosję. Jacy inni aktorzy angażują się w działania informacyjne wymierzone w NATO i jak oni to robią?

Nie jestem pewien czy są jakieś inne podmioty, które atakują NATO, jako organizację. Bardzo trudno jest je zidentyfikować. Raczej możemy mówić o atakach na naszych sojuszników. Chiny stają coraz poważniejszym graczem, ale większość operacji informacyjnych prowadzonych przez to państwo ma miejsce wokół peryferii Chiny i ich sąsiadów. Stosowane taktyki nie są zupełnie różne od tych wykorzystywanych przez Rosję w przestrzeni informacyjnej, ale Państwo Środka jest o wiele ostrożniejsze i planuje swoje działania w perspektywie długookresowej. Zdecydowanie również woli

kłaść nacisk na miękkie środki oddziaływania. Chiny są jednak bardziej zaawansowane technologicznie niż Rosja. Rosjanie używają naszej własnej technologii w celu realizacji swoich interesów, a Chińczycy rozwijają swoją rodzimą technologię. Mamy jednak również innych aktorów, którzy odgrywają ważną rolę w środowisku informacyjnym jak np. Iran. Są również podmioty półpaństwowe. W Meksyku, Brazylii, Wenezueli, Indiach istnieją silne i dobrze zorganizowane sieci organizacji zajmujących się dezinformacją. Nie możemy przypisać ich do rządu konkretnego państwa, ale mają one duże zdolności. Raczej ich działalność nie skupia się na NATO. Od czasu do czasu organizują jednak działania wymierzone w naszych sojuszników. Przykładowo podczas referendum w Katalonii, siatki wenezuelskich trolli były bardzo aktywne.

Jak sytuacja wygląda w przypadku Korei Północnej?

Państwo to nie jest zbyt aktywne w Europie. W Stanach Zjednoczonych wygląda to troszkę inaczej, ale z pewnością nie jest to zagrożenie, na którym powinniśmy się koncentrować w przestrzeni informacyjnej. Korea Północna skupia się raczej na tradycyjnych cyberatakach, a nie na operacjach wpływu.

Jednym z najczęściej wymienianych zagrożeń przyszłości jest deepfake? W jaki sposób może zagrozić demokracji i państwom Zachodu?

Jeżeli grupka ludzi jest w stanie stworzyć wideo, w którym umieszczają jakąś realną postać np. w jakichkolwiek okolicznościach, które są wymyślone, to jest to duże zagrożenie. Z perspektywy technologii nie jesteśmy w stanie odróżnić co jest fałszywe a co prawdziwe. To oznacza, że nie tylko możemy powiedzieć każde kłamstwo, ale teraz możemy je przedstawić wizualnie, a ludzie łatwiej ulegają manipulacji wizualnej. Tak pracuje ludzki mózg. Deepfake zdecydowanie skomplikuje środowisko informacyjne, pogłębi polaryzację procesów politycznych, ponieważ ludzie zaczną wierzyć w to co chcą wierzyć i przykładowo będą nagrania, gdzie jestem przedstawiany jako dobry człowiek, i inne w których robi się ze mnie złoczyńcę. Obie grupy będą przedstawiały nagrania jako prawdziwe. Jeśli nie ma nawet podstawowej zgody co jest prawdą a co fałszem to stworzy to strasznie podzielone społeczeństwo. Musimy natychmiast zainwestować w technologie, które będą w stanie pomóc zapobiec temu co może się stać. Możemy dodawać znaki wodne, użyć technologii blockchain do weryfikacji tożsamości itp. Musimy też zdać sobie sprawę, że pojawią się kryzysy związane z deepfake zanim będzie mieli odpowiednie rozwiązania. Zbliżają się wybory prezydenckie w 2020 roku, będzie co obserwować.

Mówiąc o środkach, które pozwalają walczyć z dezinformacją wydaje się, że edukacja jest kluczowa. Jest to jednak proces, który zajmuje dużo czasu. Mamy jakieś inne narzędzia, które służą walce z dezinformacją?

Mamy wiele narzędzi. Po pierwsze, ludzie muszą dokonać wyboru czy chcą być wykształceni w obszarze walki z dezinformacją. Jeden z problemów nie leży w tym, że mamy do czynienia z propagandą, ale w tym że ludzie chcą w nią wierzyć. Oferujemy różnego rodzaju treningi i kursy, ale ludzie nie zawsze są nimi zainteresowani. Musimy znaleźć sposób, żeby ich zmotywować, aby chcieli się doksztalać w tym obszarze oraz aby w swoich opiniach bazowali na faktach. Należy ich tego nauczyć, dlatego tak ważne jest odróżnianie opinii od faktów. Po drugie, systemy edukacyjne w poszczególnych państwach trzeba przekształcić w taki sposób, aby bardziej odpowiadały wyzwaniom współczesnego świata. Muszą one być bardziej elastyczne, ponieważ świat, a za nim potrzeby edukacyjne będą zmieniały się o wiele szybciej niż wcześniej.

Jeśli mówimy o narzędziach, to gry komputerowe mogą być dobrym rozwiązaniem, w szczególności dla młodych osób. Obecnie rozwijamy aplikację, która będzie pozwalała na wcielenie się w rolę wydawcy i decydowania czy dana informacja jest prawdziwa czy fałszywa. Jest to jeden z naszych

pomysłów, żeby myśleć nieschematycznie i odejść od tradycyjnego podejścia, że trzeba zapisać się na jakiś kurs czy pójść do jakiejś klasy. Musimy spowodować, że nowoczesna technologia stanie się naszym przyjacielem, a nie naszym wrogiem.

Opracowali: Piotr Jaszczuk i Andrzej Kozłowski