Polska potrzebuje komunikacji strategicznej, a społeczeństwo - większej świadomości

Konferencję zatytułowaną „Jak przygotować Polskę do zewnętrznej ingerencji w wybory? Stan polskiego cyberbezpieczeństwa" otworzył prezes Stowarzyszenia Euro-Atlantyckiego (SEA) - Marek Goliszewski, wskazując, że Internet udostępniony światu przez Pentagon, rozprzestrzenił się bardzo szeroko i wszyscy byliśmy szczęśliwi, że możemy wymieniać między sobą informacje, poznać się nawzajem i nawiązywać kontakty.

Podchodziliśmy do tego narzędzia z pełną ufnością. Jednak z biegiem czasu okazało się, że Internet to nie tylko cudowne narzędzie pomagające nam wszystkim, ale także środek do tego, żeby ci, którzy chcą zaatakować i zaszkodzić firmom lub instytucjom, mają takie możliwości. Dzisiaj, niekontrolowany zalew informacji, często pełen inwektyw i pomówień, zaczął nam szkodzić. Problemem zajęła się UE w sposób metodyczny. W międzyczasie uwidoczniły się niepokojące zjawiska, które mogliśmy obserwować, jak manipulowanie wyborami w Stanach Zjednoczonych, w Niemczech, czy we Francji stawiają pod znakiem zapytania, co dalej z tą dziedziną rewolucji przemysłowej oraz z naszym bezpieczeństwem. Czy Polska jest dziś bezpieczna w tym kontekście? Czy podjęliśmy jakieś działania, które będą chronić nas, nasze państwo i społeczeństwo przez tym negatywnymi zjawiskami, z którymi mamy dzisiaj do czynienia?

Dyrektor biura zarządu SEA - Antoni Wierzejski, moderator konferencji, zaznaczył, że omawiany problem został szczególnie zauważony w polskiej przestrzeni informacyjnej po aneksji Krymu przez Rosję, co wiązało się m.in. ze zwiększoną i zauważalną aktywnością rosyjskich trolli. Moderator dyskusji zwrócił uwagę na raport Centrum Stosunków Międzynarodowych na temat dezinformacji i propagandy, opracowany z partnerami z Grupy Wyszehradzkiej oraz Mołdawii i Ukrainy. Dzięki projektowi nawiązany został kontakt z

zespołem East Stratcom, który działa w ramach unijnej dyplomacji - Europejskiej Służby Działań Zewnętrznych (ESDZ). Zespół ten zebrał dotychczas ponad 3 tys. przypadków pro-kremlowskiej dezinformacji i propagandy w 18 językach, co pokazuje, że nie tylko Polska jest na celowniku działań propagandowo-dezinformacyjnych, ale cały region euro-atlantycki. Dlatego Stowarzyszenie Euro-Atlantyckie, którego jedną z misji jest działanie na rzecz promocji więzi transatlantyckich, jest doskonałym miejscem na taką debatę.

Wskazując na przykłady ingerencji w proces wyborczy w USA oraz we Francji, poprzez zhackowanie skrzynek mailowy sztabów wyborczych poszczególnych kandydatów, moderator dyskusji zwrócił się z pytaniem do Kamila Basaja, kierownika projektu INFOOPS w Fundacji Bezpieczna Cyberprzestrzeń oraz założyciela konta na Twitterze @Disinfo_Digest, czy Polska jest przygotowana do podobnej ingerencji oraz co należy zrobić, aby się do niej przygotować.

Kamil Basaj podkreślił, że cyberprzestrzeń jest środowiskiem, w którym tego typu działania są prowadzone, z tego względu, że dają one możliwość oddziaływania w dosyć złożony sposób. Identyfikację operacji wpływu może prowadzić w wielu wymiarach: począwszy od części retorycznych, czyli tym, co jest istotą przekazu oraz w wymiarze technicznym. W przypadku walki informacyjnej w cyberprzestrzeni, te dwa wymiary się wzajemnie przenikają. Nie tylko ze względu na to, że używa się narzędzi, które są w istocie oprogramowaniem, aby dystrybuować daną treść, ale również w tym sensie, że ludzie, którzy funkcjonują w cyberprzestrzeni: w mediach społecznościowych, czerpią informacje ze stron internetowych, blogów, kształtując wokół siebie pewien ograniczony krąg poznawczy, z którego czerpią informacje. Z perspektywy ośrodka państwowego, który prowadzi agresję informacyjną, identyfikacja tych grup społecznych, ich obszarów i podatności pozwala zaplanować i rozpocząć operacje wpływu na środowisku, w którym one funkcjonują.

Inne wymiary operacji wpływu to: trolling, narracja kontekstowa, botnet - to są wszystko elementy techniczne, które wspomagają proces oddziaływania informacyjnego. Żaden człowiek nie jest przygotowany na proces manipulacji informacją. Badania nad sposobem, w jaki człowiek przetwarza informacje dowodzą, że ciągłe poddanie go oddziaływaniu określonymi informacjami (a w przypadku Rosji tych wektorów jest wiele i są one zmienne, np. dezawuacja relacji sojuszniczych, negatywne obrazowanie Unii Europejskiej, Ukrainy, dążenie do polaryzacji społecznej) może kształtować jego pogląd. Są to często informacje,

które są dla niego wcześniej spreparowane i dystrybuowane. Zamykanie odbiorców w tych kręgach poznawczych nazywamy intoksykacją środowiska poznawczego.

Odnośnie *modus operandi* zastosowanego w USA oraz Francji, każdy z nas, nie tylko partie polityczne, powinien dbać o to, aby uniemożliwić lub utrudnić możliwość podmiotowi zewnętrznemu posługiwania się materiałem w skutek kradzieży ze skrzynki mailowej. W przypadku zhackowania skrzynki mailowej, chodzi o uzyskanie efektu informacyjnego, czyli takiego posługiwania się tymi materiałami, aby np. zdezawuować określoną osobę, której się te maile wykradło. Mailami zdobytymi w ten sposób można także manipulować. Bardzo trudno jest się w takiej sytuacji aktywnie bronić w środowisku informacyjnym, gdyż można dementować, ale do momentu dopóki posiada się zdolność przekazu tej informacji w sieci. A w tej chwili dla większości ludzi do 44 roku życia Internet stanowi podstawowe źródło pozyskiwania informacji. Tym samym, incydenty polegające np. na kształtowaniu teorii spiskowych podczas procesu wyborczego w Stanach Zjednoczonych (np. tzw. *pizza gate,* czy bardziej złożone teorie spiskowe) mają coraz większy wpływ. Warto także dodać, że teorie spiskowe mogą prowadzić do wydarzeń w wymiarze rzeczywistym, co mogliśmy obserwować w USA.

Ważne zalecenia dla Polski w kontekście tematu konferencji, to budowanie i umacnianie świadomości polskiego społeczeństwa, wzmacnianie zdolności społeczeństwa w kwestii pozyskiwania i analizowania informacji, zaangażowanie podmiotów odpowiedzialnych za bezpieczeństwo, szkolenia dla dziennikarzy, samorządowców i polityków. Powinno się również zaangażować przedstawicieli innych nauk społecznych do badania tego zjawiska (socjologów, antropologów, psychologów), gdyż jest ono wielowymiarowe. Jest to istotne m.in. ze względu na poznanie natury problemu, czy też wybranie odpowiedniego języka komunikacji ze społeczeństwem. Niezwykle ważnym aspektem, na który uwagę zwrócił dr Adam Lelonek, prezes fundacji Centrum Analiz Deziformacji i Propagandy, jest stworzenie mechanizmów weryfikacyjnych w mediach, a przede wszystkim w Polskiej Agencji Prasowej, z której w polskich mediach internetowych pochodzi ok. 50 % informacji. Dobrym rozwiązaniem byłoby też korzystanie z doświadczeń innych państw. W ciągu ostatniego roku, niestety niewiele z powyżej wymienionych rekomendacji udało się wdrożyć w Polsce.

Z podobnymi problemami mają do czynienie inne państwa europejskie. Dla Hiszpanii np. kwestia rosyjska mogła jeszcze do niedawna się wydawać egzotyczna, jednak wydarzenia w

Katalonii pokazały, że tak nie jest i Hiszpania radykalnie zmieniła swoje podejście do działań Rosji w tym obszarze.

W Polsce mamy problem z funkcjonowaniem trzeciego sektora, czyli organizacji pozarządowych. Przykładowo na Słowacji podejmowane są działania nie tylko identyfikujące dezinformację i propagandę, ale także podejmujące kwestię pozytywnego przekazu np. na temat NATO, czy UE. Robi to nie państwo, lecz organizacje pozarządowe. Zakres współpracy w ramach relacji państwo - trzeci sektor jest tam dużo wyższy niż w Polsce. Dlatego wzmocnienia wymaga koordynacja relacji państwo - trzeci sektor - społeczeństwo obywatelskie. Jednym z najważniejszych komponentów tego mechanizmu są media (dziennikarze).

W Czechach z kolei, wprowadzono model, w którym to Ministerstwo Spraw Wewnętrznych zajmuje się identyfikacją zagrożeń wynikających z dezinformacji i propagandy. Nie wyklucza to jednak kontaktów z organizacjami pozarządowymi. W Polsce te sprawy weszły w kompetencje MON. Państwo, w przeciwieństwie do organizacji pozarządowych, ma instrumenty, aby decydować, co jest największym zagrożeniem oraz jakie działania należy podejmować w celu ochrony bezpieczeństwa informacyjnego państwa. Z tego względu komunikacja strategiczna (tzw. stratcom) jest dla Polski konieczny. Część działań z zakresu wojny dezinformacyjnej można bowiem szybko korygować poprzez szybką reakcję informacyjną. Jednak bez ośrodka koordynującego tego typu działania jest to bardzo trudne. Bardzo często brakuje zaprzeczenia wobec fałszywych informacji ze strony Polski. Nie można doprowadzać do sytuacji, w której użytkownik nie znajduje zaprzeczenia dla fałszywych informacji lub narracji zewnętrznych. Poszczególne ministerstwa nie powinny działać oddzielnie w konstruowaniu przekazu. Konieczna jest koordynacja komunikacji na poziomie rządowym. Taki spójny przekaz powinien trafiać do PAP i poprzez PAP być powielany za granicą. Aby działanie było skuteczne, często kluczowy jest szybki czas reakcji.

Poprzez wspieranie społeczeństwa obywatelskiego, wspieramy je także przed zagrożeniami wewnętrznymi. Świadomi odbiorcy informacji, widząc wewnętrzną manipulację wzmacniają bowiem krytyczne myślenie wobec przekazu, który wypływa również z wewnątrz państwa.

Wyzwaniem w Polsce pozostaje niewystarczająca ilość ekspertów od tematyki dezinformacji i propagandy, którzy byliby w stanie monitorować zjawisko, nie tylko retrospektywnie, ale również, albo przede wszystkim, poprzez prognozowanie.

Innym problemem, na który zwrócił uwagę dr Lelonek jest fakt, iż powstające analizy na temat zjawiska dezinformacji i propagandy nie są w wystarczający sposób komunikowane wobec społeczeństwa, które nie jest świadome zagrożenia. Podobnie jednak jak z cyberbezpieczeństwem, to od nas samych zależy, na ile będziemy przestrzegać higieny korzystania z informacji, czyli obiektywnego pozyskiwania informacji. Świadomość społeczna jest procesem na lata i Polsce niestety wciąż daleko jeszcze do państw skandynawskich, które już na wczesnoszkolnym etapie edukacji wprowadziły książeczki, uczące dzieci krytycznego myślenia, gdyż to jest podstawą: krytyczny stosunek do przyjmowanych informacji.

Piotr Niemczyk, były dyrektor Biura Analiz i Informacji oraz zastępca dyrektora Zarządu Wywiadu Urzędu Ochrony Państwa, zauważył, że najważniejsza jest identyfikacja informacji nieprawdziwych od prawdziwych oraz umiejętność rozróżniania fałszywych profili w mediach społecznościowych od prawdziwych. Według niego, to nie państwo jest na pierwszej linii frontu, tylko społeczeństwo obywatelskie. Analizując kwestię dotarcia do społeczeństwa z przekazem uświadamiającym zagrożenia związane z dezinformacją i propagandą, panelista zaproponował rozwiązania uwzględniające wpływ mediów publicznych na społeczeństwo. Elementem misji mediów publicznych mogłoby być umieszczaniu wątków związanych z zagrożeniem dezinformacja oraz propagandą np. w telenowelach (jako swoisty *product placement*). W zakresie systemu edukacji zaś, wskazane byłyby zajęcia dla uczniów, które pokazywałyby im, w jaki sposób np. odróżnić fałszywy profil w mediach społecznościowych od prawdziwego.

Społeczność internetowa działa skutecznie w kontekście para-cenzury w przypadku pornografii pedofilskiej. Coraz lepiej świat radzi sobie także z propagandą dżihadystyczną. To wynika bardziej z reakcji świadomych użytkowników Internetu, którzy reagują na te treści. Problemem jest jednak brak woli ze strony moderatorów stron internetowych, by usuwać treści będące np. mową nienawiści, co często jest spowodowane słabą sytuacją finansową mediów.

Nie ma już żadnych wątpliwości, że dystrybucja fałszywych wiadomości w Internecie miała wpływ na wybory w USA. Prawdopodobnie miałaby we Francji, gdyby nie warta odnotowania reakcja francuskiej Państwowej Komisji Wyborczej, która zakomunikowała, aby nie rozpowszechniać informacji zdobytych nielegalnie, gdyż jest to przestępstwo. Większość

mediów zareagowała na ten apel. Okazuje się zatem, że rozsądne zachowanie instytucji państwowej może mieć właściwy efekt.

W przypadku, w którym obywatel dotknięty jest nieprawdziwą informację na jego temat, zawsze należy reagować. Pytaniem, z którym borykają się jednak takie osoby, jest do kogo powinny one zgłosić z takim problemem. Rozwiązaniem mogłoby być państwowe wsparcie dla organizacji pozarządowej, która by się tym zajmowała, aby osoby indywidualne dotknięte fałszywymi informacjami wiedziały, jakie kroki prawne powinny podjąć, aby walczyć z zaistniałą sytuacją. Ważnym elementem odpowiedzi na fałszywe informacje jest sprostowanie. Nie należy fałszywych informacji zostawiać bez odpowiedzi. RODO uniemożliwia dowolny sposób stosowania targetowania behawioralnego - to bardzo dużo zmieni.

Analizując problem odpowiedzi na zewnętrzną ingerencję w proces wyborczy, czy też w ogóle w polską przestrzeń informacyjną, najpierw należy ją właściwie rozpoznać, co nie jest prostym zadaniem. Jednak bez odpowiedniego przeanalizowania, jakie obiekty są implementowane do polskiej infosfery oraz wedle jakiego wzorca działania, trudno jest ocenić skalę zagrożenia. Odpowiedź na taką ingerencję można podzielić na poziom społeczny, techniczny oraz prawny.

Kolejnym wyzwaniem jest ustalenie atrybucji, czyli źródła, z którego pochodzą treści wprowadzające w błąd lub narzucające narracje zgodne ze strategią podmiotu zewnętrznego (np. podgrzewanie nastrojów antyukraińskich w Polsce, czy też poważanie roli NATO w polityce bezpieczeństwa Polski). Są przynajmniej trzy wymiary, w których można starać sie analizować atrybucję: warstwa techniczna, w której pozostają ślady, które można przypisać do przeciwnika informacyjnego, drugą warstwą jest warstwa retoryczna, czyli przekaz (np. w komentarzach pod artykułami internetowymi, czy też w publicystyce). Żeby skłonić osobę lub grupę do podjęcia określonej decyzji, nie trzeba posługiwać się informacjami nieprawdziwymi. Taką osobę lub grupę trzeba mieć dobrze rozpoznaną oraz dobrać do niej odpowiednie informacje. Według dr Lelonka, Rosjanie konstruują przekazy pozornie racjonalne, aby np. teorie spiskowe docierały do jak najszerszego kręgu odbiorców.

Atrybucja może być również zidentyfikowana poprzez rozpoznanie wzorca działania, poprzez elementy retoryczne, czyli, czy np. na stronach internetowych, kontach w mediach

społecznościowych, czy blogach, są elementy wspólne w warstwie retorycznej oraz technicznej - gdyż tego typu błędy się zdarzają, choć nie są powszechne.

Inną metodą na identyfikację działań propagandowo - dezifornacyjnych jest wyszukiwanie w przeglądarce internetowej związków frazeologicznych i wyszukiwanie ich w Internecie, oraz weryfikacja poprzez czas publikacji - może to wskazać, czy było to działanie człowieka, czy robota.

Według dr Kazimierza Wóycickiego, ze Studium Europy Wschodniej Uniwersytetu Warszawskiego, w polskim Internecie jest zidentyfikowanych ok. 80-100 agentów wpływu, a ludzi którzy rozpędzili nienawiść antyukraińską jest raptem kilkanaście. Ostatecznie w wojnie informacyjnej iluś ludzi musi ujawnić twarz. To jest wewnętrzna sprzeczność tego, co robi Putin - w końcu przecież te twarze zostaną ujawnione. Polska nie posiada żadnych środków prawnych, aby tych ludzi po prostu zaaresztować. Antypolska działalność tych ludzi ma ogromny wpływ na cały Internet i jest tolerowana. Nazwanie konkretnej osoby "agentem wpływu" skutkuje często pozwami i sytuacja się odwraca. Słowem: brakuje skutecznych środków prawnych, by walczyć z takimi osobami. Z tym poglądem nie zgodził się dr Lelonek, zauważając, że tak jak *fake newsy* stały się wygodnym pojęciem, tak samo określenie "agent wpływu" nie jest do końca prawdziwe, gdyż trudno jest ustalić, że dana osoba jest opłacana z zewnątrz za swoją aktywność w sieci.

Dr Wóycicki zwrócił uwagę, że skoro istnieją trolle, to ktoś za nie zapłacił. Dlatego należy stosować zasadę "*follow the money*" i skupić się na dotarciu do źródeł finansowania działań deziformacyjno-propagandowych. Wiadomość w Internecie mająca 20 tys. tzw. lajków kosztuje i gdzieś jest karta płatnicza, którą zostało to opłacone. Jeśli państwo nie jest w stanie tego wyłapać, to możemy uczenie dyskutować na ten temat, ale nic z tym nie zrobimy. Innym istotnym problemem jest brak woli politycznej, zarówno w ramach obozu rządzącego, jak i opozycji, aby podjąć działania wobec tego problemu.

Media społecznościowe zostały stworzone jako utopia cudownej opinii publicznej. Niestety brakuje w Internecie gremiów społecznych, które skądinąd powinny być wspomagane przez państwo, takich jak Wikipedia, w ramach której 3000 polskich wikipedystów stworzyło tysiące haseł, których jakość jest wzajemnie kontrolowana przez uczestników. Zaangażowanie się w takie gremia jest kwestią odpowiedzialności obywatelskiej i samo w

sobie odgrywałoby pewną role edukacyjną. Państwo powinno być życzliwe tego typu inicjatywom społecznym.

Kolejnym wyzwaniem jest m.in. to, że polscy decydenci są 40 i 50 plus, a osoby targetowane przez infoagresora poruszają sie swobodnie w mediach społecznościowych oraz Internecie.

W zakresie instrumentarium rosyjskiej machiny propagandowej, dr Wóycicki zwrócił uwagę na infiltrację mediów społecznościowych przez fałszywe profile, w celu dystrybucji treści zbieżnych z rosyjską dezinformacją/propagandą. W obecnej sytuacji politycznej dr Wóycicki nie wierzy w działanie państwa w przeciwdziałanie tym zjawiskom. W kontekście wyborów parlamentarnych w Polsce, pojawił sie pogląd, iż propaganda pro-kremlowska w Polsce może próbować wpłynąć na proces wyborczy poprzez wspieranie skrajnych sił nacjonalistyczne, jednocześnie zwalczając PIS.

Podsumowując, paneliści podkreśli dwie kluczowe kwestie, na których powinno skupić się państwo, media, społeczeństwo obywatelskie oraz sektor edukacyjny. Z jednej strony na poziomie państwowym konieczna jest budowa ośrodka, który zajmowałby sie komunikacją strategiczną w Polsce, z drugiej zaś, należy pilnie podjąć działania, mające na celu poniesienie świadomości społeczeństwa na temat problemu dezinformacji i propagandy, które mogą prowadzić do wpłynięcia na wynik wyborów w Polsce.

Opracował: Antoni Wierzejski