Cyberdefence 24

aut. Adam Lelonek 05.10.2017

WYZWANIA DLA KOMUNIKACJI STRATEGICZNEJ POLSKI I UNII EUROPEJSKIEJ [ANALIZA]

Realia wojny informacyjnej i psychologicznej zmieniły środowisko bezpieczeństwa w skali globalnej. Działania hybrydowe, skierowane przeciwko zachodnim organizacjom, instytucjom, ale i ich państwom członkowskim indywidualnie wymagają podjęcia szeregu celowanych działań, jednak wśród zachodnich elit intelektualnych czy politycznych wciąż brakuje elementarnej świadomości zagrożenia i identyfikacji działań przeciwnika. Bez niej nie może być mowy o woli politycznej, której praktycznym i realnym odzwierciedleniem jest zapewnienie odpowiedniego finansowania.

Do tych bardziej widocznych inicjatyw wspieranych rządowo w Europie na odcinku propagandy i dezinformacji należą:

1. zespół zadaniowy East StratCom Task Force przy Europejskiej Służbie Działań Zewnętrznych (European External Action Service, EEAS),
2. Europejskie Centrum Przeciwdziałania Zagrożeniom Hybrydowym (European Center for Countering Hybrid Threats, Hybrid COE),
3. NATO Strategic Communications Centre of Excellence (NATO StratCom COE).

Do tego dochodzi planowana grupa ekspercka przy Komisji Europejskiej, mająca się zajmować tematem fałszywych informacji, która powstaje z inicjatywy nowej komisarz UE ds. gospodarki cyfrowej i społeczeństwa z Bułgarii Mariji Gabriel.

Selektywne porównanie potencjałów

East StratCom Task Force powołany w 2015 r. ma budżet ok. 1 mln euro, Hybrid COE ok. 1,5 mln euro (z czego połowę tej sumy wyłożył kraj przyjmujący, czyli Finlandia), natomiast NATO StratCom COE nie jest finansowane z budżetu NATO, gdyż nie wchodzi w skład struktury dowodzenia Sojuszu. Współpraca opiera się na udziale państw członkowskich w partnerstwie z sektorami: cywilnym, wojskowym i prywatnym. Wśród sponsorów od stycznie 2017 znalazły się: Estonia, Niemcy, Włochy, Litwa, Łotwa, Holandia, Wielka Brytania i Polska. Finlandia oraz Szwecja zostały państwami partnerskimi, a swoich pracowników oddelegowały również Francja i Kanada. Dokładny budżet nie jest oficjalnie znany.

W tym samym czasie budżet dla rządowej telewizji Kremla RT to 18,7 mld rubli, czyli ok. 320 mln dolarów. Prowadzi ona transmisję w języku angielskim, arabskim, hiszpańskim oraz dostępna jest online dodatkowo w rosyjskim, niemieckim i francuskim. Stacja sama deklaruje zasięg 700 mln ludzi na całym świecie, jednak nie do końca wiadomo jak dokonano takich szacunków i w jakim okresie. Według The New York Times realnie można mówić o ok. 70 mln tygodniowo, z czego ok. 35 mln w Europie.

Funkcjonalność i skuteczność narzędzi

Instytucje zagraniczne, wykonujące swoją pracę na bardzo wysokim poziomie i zrzeszające czołowych ekspertów od wojny informacyjnej, psychologicznej, propagandy, dezinformacji, cyberbezpieczeństwa, IT, mediów czy komunikacji, wykonują swoją pracę na różnych płaszczyznach. Część materiałów jest dostępna dla użytku publicznego i znajduje się w otwartym dostępie. Szerokie udostępnianie efektów pracy tych podmiotów jest warunkiem skuteczności ich działań. Po stronie krajowych mediów mainstreamowych w państwach UE i NATO nie ma jednak woli podejmowania tych kwestii w sposób stały, regularny, nie związany z bieżącymi, krótkotrwałymi sensacjami.

Konsekwencją tego jest utrzymywanie niskiego stanu wiedzy społecznej, ale i elit, w tym politycznych, które wciąż nieprawidłowo lub zbyt wąsko identyfikują zagrożenia dla własnej przestrzeni informacyjnej. W tym samym czasie strona rosyjska jest w stanie prowadzić zakrojone na szeroką skalę operacje informacyjne i psychologiczne na poziomie danego kraju lub międzynarodowym, selekcjonując docelowe audytoria i aktywizując radykalne środowiska polityczne, prorosyjskich liderów opinii lub quasi-agencji informacyjnych, symulujących pracę mediów. Oprócz tego wykorzystuje szeroko media społecznościowe, zwłaszcza Twitter, co szczególnie odczuły podczas wyborów Stany Zjednoczone, Francja i Niemcy.

Na chwilę obecną Zachód buduje bazę instytucjonalno-ekspercką z wykorzystaniem niezwykle ograniczonych środków finansowych. Jakkolwiek Sojusz Północnoatlantycki uznał cyberprzestrzeń kolejnym obszarem prowadzenia działań zbrojnych, to nie możemy jeszcze mówić o jednolitej strategii działania w sferze informacyjnej czy psychologicznej. Zachód prowadzi działania analityczne, identyfikacyjne, edukacyjne, operacyjne, szczątkowo także informacyjne, lecz jest to wciąż etap przedsięwzięć o charakterze defensywnym. Nie ma mowy o aktywnym przeciwdziałaniu czy działaniach wyprzedzających z obszaru informacyjnego czy psychologicznego w skali choćby zbliżonej do rosyjskiej. Nie ma do tego zasobów finansowych, eksperckich, instytucjonalnych, kadrowych, instrumentarium prawno-legislacyjnego, ale i woli politycznej.

Poziom polski

Na poziomie polskim na palcach jednej ręki można policzyć instytucje typu NGO zajmujące się systemową identyfikacją, weryfikacją, analizą i/lub neutralizacją wrogich działań z obszaru operacji informacyjnych i psychologicznych w przestrzeni informacyjnej i cyberprzestrzeni wymierzonych w

bezpieczeństwo Polski i polskie społeczeństwo, a tym samy starających się budować spójny przekaz składający się na komunikację strategiczną naszego kraju w tym obszarze. Są to: **Fundacja Bezpieczna Cyberprzestrzeń** z projektem badań i przeciwdziałania manipulacji środowiskiem informacyjnym – **Disinfo_Digest**, **Instytut Kościuszki** z projektem **CYBERSEC** oraz coroczną międzynarodową konferencją o cyberbezpieczeństwie w Europie o tej samej nazwie, a także **Fundacja Centrum Analiz Propagandy i Dezinformacji** podejmująca działania zmierzające do stworzenia platformy do współpracy międzyśrodowiskowej w zakresie budowania systemu odpowiedzi na wrogie wobec Polski działania informacyjne i psychologiczne. Odnotować należy też aktywność **Fundacji Centrum Stosunków Międzynarodowych**, która jako pierwsza w Polsce podjęła współpracę z East StratCom Task Force i stała się pierwszym polskim kontrybutorem Disinformation Review.

Istnieją oczywiście projekty takie jak **StopFake PL** realizowany przez **Stowarzyszenie Dziennikarzy Polskich** we współpracy z ukraińskim inicjatorem projektu StopFake, który analizuje fałszywe informacje i narracje pojawiające się w przestrzeni informacyjnej Polski, a także inne inicjatywy zajmujące się pewnymi elementami związanymi z informacją, jak **OKO.press** czy **demagog.org.pl**. Skupiają się one jednak na działaniach **fact-checkingowych**, które z perspektywy przeciwdziałania zewnętrznym zagrożeniom dla polskiej przestrzeni informacyjnej i budowania komunikacji strategicznej są działaniami wtórnymi do problemu i daleko niewystarczającymi w asymetrycznej wojnie informacyjnej i psychologicznej prowadzonej przeciwko Polsce. Jakkolwiek są to inicjatywy potrzebne, a ich wiedza i doświadczenie doskonale nadają się do wykorzystania przy działaniach edukacyjnych i szkoleniowych.

Następnie należy wymienić indywidualne działania poszczególnych dziennikarzy, blogerów czy anonimowych użytkowników sieci społecznościowych, które stanowią raczej działania doraźne i stanowią przejaw osobistych zainteresowań poszczególnych osób niż ośrodków medialnych, które reprezentują. A jedyna indywidualna inicjatywa, która do tej pory zwalczała rosyjską propagandę w nad Wisłą, czyli **Rosyjska V Kolumna w Polsce Marcina Reya**, sama padła ofiarą ataku kilku dziennikarzy. W tym przypadku na uwagę zasługuje fakt, że pod szyldem jednego z mediów, na łamach którego pojawił się atak, działają osoby o zupełnie innych poglądach i ocenie sytuacji. Innymi słowy nawet w obrębie jednego medium nie ma spójności co do działań w obszarze informacyjnym. Nową jakość na polskim podwórku dziennikarskim może wnieść **Fundacja Reporterów** ze swoim nowym międzynarodowym projektem dziennikarstwa śledczego **Vsquare**, poruszającym m.in. tematy z obszaru propagandy i dezinformacji.

Gorzej na tym polu wypadają polskie państwowe ośrodki analityczno-badawcze, spośród których na uwagę zasługują jedynie analizy **Ośrodka Studiów Wschodnich**. Szereg innych polskich think-tanków oraz fundacji podejmuje również tą tematykę doraźnie w swoich publikacjach oraz wydarzeniach o charakterze eksperckim lub naukowym, a nawet projektowym na poziomie międzynarodowym nie posiadając nawet w swoich szeregach specjalistów w tej dziedzinie. Co ciekawe Polska nie ma nawet swojego przedstawiciela w East StratCom Task Force w Brukseli.

Mimo istnienia różnych inicjatyw i tak wielu wydarzeń naukowych i eksperckich nie ma ani żadnej koordynacji, ani ponadśrodowiskowej współpracy, ani odpowiedniego finansowania czy wsparcia na

etapie formacji, funkcjonowania lub rozwoju dla ludzi pracujących z tymi tematami. Największym problemem wydaje się jednak brak ekspertów w danej dziedzinie: teoretyków, którzy potrafią obiektywnie spojrzeć na zagrożenia bez bycia oskarżonym o poglądy rusofobiczne czy rusofilskie, oraz praktyków, którzy potrafią przekuć posiadaną wiedzę i umiejętności w danym obszarze na realne działania. Znowu ich liczba w sektorze cywilnym nie przekracza dziesięciu.

Polskie główne media, mające największy zasięg, nie okazują większego zainteresowania raportami Disinformation Review wydawanymi regularnie od lat przez brukselską komórkę Europejskiej Służby Działań Zewnętrznych, ukazujących fałszywe przekazy informacyjne wpuszczane do przestrzeni informacyjnej państw UE, w tym Polski. Nie do końca jest zresztą zainteresowanie efektami prac analityków i mówieniem regularnie o kwestiach zagrożeń, z czego wyjątkami od reguły są: **Polskie Radio 24** i **Telewizja Biełsat**. Termin propaganda, dezinformacja czy fake news jest za to szeroko wykorzystywany w doraźnych walkach politycznych lub krótkoterminowych działaniach w polityce zagranicznej, co dalece ułatwia działania zewnętrznym podmiotom i utrudnia odbiorcom informacji w Polsce identyfikację działań ofensywnych infogresorów nie tylko na poziomie semantycznym, ale i funkcjonalnym.

Zalecenia

Wśród czołowych priorytetów są:

1. Edukacja – modyfikacja programów nauczania na poziomie wczesnoszkolnym i dalej, kursy doszkalające dla nauczycieli, zwłaszcza informatyki czy wiedzy o społeczeństwie, adaptacja programów uniwersyteckich i zawodowych do bieżących wyzwań w przestrzeni cybernetycznej i informacyjnej, powołanie specjalnych komórek w ministerstwach edukacji i koordynacja ich działań z innymi resortami (w polskim przypadku w Ministerstwie Edukacji oraz Ministerstwie Oświaty i Szkolnictwa Wyższego współpracujących nad przygotowaniem i wdrażaniem nowych rozwiązań w koordynacji z Ministerstwem Cyfryzacji, Ministerstwem Spraw Wewnętrznych, Ministerstwem Obrony Narodowej i Ministerstwem Spraw Zagranicznych) – działania z tego obszaru powinny być poprzedzone szerokimi konsultacjami społecznymi oraz nawiązaniem współpracy z partnerami zagranicznymi, mającymi doświadczenia w realizacji podobnych przedsięwzięć,

2. Szkolenia – skierowane do pracowników administracji publicznej wszystkich szczebli, ale i polityków, dziennikarzy czy wszystkich innych organizacji, instytucji czy podmiotów pracujących z informacją,

3. Partnerstwo publiczno-prywatne – dostarczanie impulsów do budowania i aktywizacji powiązań oraz interakcji pomiędzy NGOs, biznesem, instytucjami państwowymi, aby móc przejść i w pełni wykorzystać zakrojone na szeroką skalę działania oddolne, tj. potencjał społeczeństwa obywatelskiego, a równolegle przygotowanie mechanizmów implementacji *know how* organizacji pozarządowych do bieżących działań organów państwowych, wykorzystanie zasobów eksperckich przy przygotowaniu planów działań, strategii, nowych rozwiązań legislacyjnych czy innych działań konceptualno-organizacyjnych,

4. Odchodzenie od modelu reaktywnego do aktywnego – w dobie dynamicznego postępu technologicznego działania związane z biernym i wtórnym identyfikowaniem zagrożeń już po określonych zajściach mogą przynieść nieodwracalne skutki i znaczące straty materialne i

niematerialne; wiele sytuacji na poziomie krajowym czy międzynarodowym pozwala na zbudowanie wiarygodnych prognoz odnośnie potencjalnych działań infoagresora, lecz wciąż nie ma modelów neutralizacji czy stosowania własnych przekazów informacyjnych czy systemów ostrzeżeń wobec danego społeczeństwa lub na poziomie międzynarodowym (najlepszym przykładem jak może to wyglądać są działania informacyjne niemieckiego kontrwywiadu, tj. Federalnego Urzędu Ochrony Konstytucji w okresie przedwyborczym),

5. Przygotowanie i formacja ekspertów – przygotowanie kadr znacząco wykracza poza działania w sferze oświaty i wymaga interdyscyplinarnego podejścia różnych organów państwowych, w tym umożliwienia i wspierania przedstawicieli własnego państwa w pracach instytucji i organów międzynarodowych (kluczem jest tu odpolitycznienie kwestii bezpieczeństwa informacyjnego i selekcji osób na poziomie krajowym, w tym w szczególności wobec ekspertów potrzebujących państwowych nominacji na poziomie międzynarodowym), aby następnie móc implementować ich doświadczenia w rozwiązaniach krajowych po skończonej kadencji lub współpracy z zewnętrznym podmiotem; brakuje interdyscyplinarnego podejścia, praktycznej wiedzy i doświadczeń, które są trudne do zdobycia w bieżącej pracy w think tanku lub mediach, bez partnerstwa z podmiotami międzynarodowymi i krajowymi,

6. Identyfikacja zagrożeń i stanu bezpieczeństwa – jest to w zasadzie punkt wyjścia do podjęcia wszystkich wspomnianych wyżej działań, bez którego nie jest możliwe uzyskanie pozytywnych efektów prac; konieczne jest stworzenie bazy analityczno-legislacyjnej, w tym komponentu o charakterze jawnym, publicznym, jako fundamentu do działań organizacyjnych, edukacyjnych, informacyjnych, prawnych i politycznych.

Podsumowanie

Realnym odzwierciedleniem priorytetów politycznych jest zaangażowanie finansowe. Biorąc pod uwagę skalę działań Rosji oraz ponadnarodowych organizacji zachodnich, dysproporcja jest więcej niż znacząca. Jest to odzwierciedleniem nie tylko woli politycznej obu stron. Jest to w zasadzie pochodna świadomości zagrożeń i ewolucji środowiska bezpieczeństwa.

Najsłabszym ogniwem każdego systemu, czy to informacyjnego czy cybernetycznego, pozostaje człowiek. Działania jednostki, np. redaktora zatwierdzającego treści w znanym medium, dziennikarza zamieszczającego publiczny komentarz w medium społecznościowym czy polityka poszerzającego treści propagandowe, dezinformacyjne lub z zewnętrznie narzucanymi narracjami (wpisy lobbystów lub prorosyjskich autorytetów), mogą spowodować więcej szkód niż zaplanowana z rozmachem operacja informacyjna z wykorzystaniem hakerów. Pojedyncze takie zdarzenie może przyczynić się do otwarcia nowego frontu i służyć za narzędzie w rękach propagandystów na całe miesiące. To pokazuje, jak ważna jest edukacja i świadomość zagrożeń.

Obecnie wciąż uczymy się identyfikować to, co zostało zrobione w przestrzeni informacyjnej danego państwa kilka lub kilkanaście miesięcy wstecz. Działania propagandowe i dezinformacyjne są jednak wciąż dopracowywane. Zostaną one zaadaptowane do nowych warunków prawnych dla działania mediów społecznościowych i potencjalnych regulacji na poziomie UE, mających chronić europejską przestrzeń informacyjną przed zewnętrznymi ingerencjami. Liczba zagrożeń i ich skala nieustannie

rosną, podczas gdy liczba ekspertów i ich możliwości zdobywania praktycznych doświadczeń są ściśle ograniczone. Tak samo jak ich możliwość docierania do osób decyzyjnych w strukturach państwowych.

Wielu wciąż utożsamia działania informacyjne czy psychologiczne, jako wrzucanie fake newsów do przestrzeni informacyjnej państwa, a obronę jako opisywanie tego faktu. Niska świadomość społeczna ułatwia wrogie działania infoagresorom. Ograniczona percepcja zagrożenia i reaktywne postrzeganie metod zaradczych są na chwilę obecną głównym wyzwaniem dla Zachodu i Polski. Bez strategii i odpowiednich środków finansowych będziemy jedynie podmiotem, na który się oddziałuje, a inicjatywa będzie leżała po stronie przeciwnika.

Analiza powstała w oparciu o referat i dyskusję podczas panelu „Wyzwania dla unijnej komunikacji strategicznej" na konferencji pt. „Media – Rosja. Nowe zagrożenia propagandowe", zorganizowanej przez Fundację Wolność i Demokracja w dniu 4 października br. w Warszawie.