PROJEKT

PRZECIWDZIAŁANIE ROSYJSKIEJ DEZINFORMACJI I PROPAGANDZIE

RAPORT

Rozpoznanie otoczenia i uwarunkowań systemowych Organizacji Społeczeństwa Obywatelskiego w Polsce: wprowadzenie, luki, potrzeby i rekomendacje.

Autorzy: dr Aleksander Olech, Natalia Matiaszczyk

Warszawa, Grupa Defence24, Grudzień 2022

Raport został opracowany w ramach finansowanego przez USAID i koordynowanego przez International Republican Institute's (IRI) Beacon Project, międzynarodowego projektu badawczego poświęconego przeciwdziałaniu rosyjskiej dezinformacji i propagandzie. Opinie w nim wyrażone należą wyłącznie do jego autorów i nie należy ich utożsamiać ze stanowiskiem IRI.

Spis treści

1. Wprowadzenie

Cel raportu

Grupa Defence24 uczestniczy w finansowanym przez USAID międzynarodowym projekcie badawczym, koordynowanym przez International Republican Institute's (IRI) Beacon Project nt. Przeciwdziałania rosyjskiej dezinformacji i propagandzie. Projekt realizowany jest od 1 listopada 2022 roku do 28 lutego 2023 roku we współpracy z podmiotami administracji państwowej i organizacjami pozarządowymi.

Celem projektu jest wspieranie systemowych rozwiązań dotyczących przeciwdziałania rosyjskiej dezinformacji i propagandzie wymierzonej w Polskę, w tym w polskie społeczeństwo. Projekt ma również na celu wskazanie mechanizmów, których wdrożenie w administracji państwowej i rządowej oraz organizacjach pozarządowych, powinno przyczynić się do wzmacniania odporności państw na zagrożenia związane z dezinformacją, jaką Rosja prowadzi m.in. w Polsce, w celu podważenia demokratycznych procesów.

Problematyka zwalczania dezinformacji oraz rosnące zaangażowanie Federacji Rosyjskiej są wyzwaniem dla organizacji międzynarodowych, państw i społeczeństwa obywatelskiego od blisko dwóch dekad. Bezpieczeństwo informacyjne wraz z jego integralną częścią, jaką jest cyberbezpieczeństwo, jest jednym z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, mającym charakter transsektorowy i wpływającym na efektywność funkcjonowania całego systemu bezpieczeństwa. W związku z tym, na rzecz podtrzymania swojej integralności, aparat państwowy powinien reagować, poszukując narzędzi do przeciwdziałania niebezpieczeństwom. W sferze informacyjnej, gdzie główną rolę odgrywa jednostka (obywatel), tym łącznikiem pomiędzy administracją państwową a społeczeństwem będą organizacje pozarządowe.

Zagrożenia w przestrzeni informacyjnej, takie jak operacje informacyjne i psychologiczne, w tym o charakterze dezinformacyjnym i propagandowym, są wyzwaniem globalnym. W swoich działaniach wykorzystuje je szerokie grono podmiotów – od władz różnych państw, przez organizacje terrorystyczne, po grupy hakerskie. Wśród celów tego typu operacji można wyróżnić między innymi wywieranie presji na rządach, samorządach, społeczeństwie, opinii publicznej, jak i również celowe sianie paniki czy wywoływanie konfliktów społecznych.

Jednym z przykładów prowadzenia wojny hybrydowej jest wykorzystanie Internetu w celu szerzenia dezinformacji. Należy podkreślić, że bardzo powszechne jest stosowanie takich

taktyk przez Federację Rosyjską i grupy z nią powiązane Jest to przykład wskazujący na wykorzystanie narzędzi pierwotnie postrzeganych jako pokojowe (np. media społecznościowe), do prowadzenia lub wspierania taktyk wojny hybrydowej[1]. Należy wziąć pod uwagę, że Rosja jest również postrzegana jako „państwo terrorystyczne", które jest w stanie sukcesywnie realizować swoje operacje, chociażby poprzez znaczną ekspansję militarną i terytorialną w Ukrainie, utrzymując kilkadziesiąt zagranicznych baz wojskowych[2], a także wykorzystując grupy najemników (m.in. Grupa Wagnera[3]). Oprócz tego, aktywna obecność rosyjskich polityków i dziennikarzy w mediach społecznościowych w celach propagandowych również stanowi ważny element działalności hybrydowej i dezinformacyjnej[4].

Trzeba zaznaczyć, że Internet i sieci internetowe pozwalają podmiotom państwowym i niepaństwowym prowadzić nowe operacje. Sieć internetowa może być wykorzystywana do hakowania infrastruktury krytycznej, wpływania na procesy wyborcze, przeprowadzania kampanii dezinformacyjnych i propagandowych, kradzieży informacji i udostępniania wrażliwych danych w przestrzeni publicznej. W najgorszych przypadkach cyberprzestępca przejmuje kontrolę nad zasobami, takimi jak systemy wojskowe i struktury dowodzenia[5].

Nie sposób przeanalizować wszystkich celowych działań dezinformacyjnych Federacji Rosyjskiej, a także częściowo Chin, które są realizowane w Polsce w ostatnich latach. Po rosyjskiej inwazji na Ukrainę w 2014 roku nastąpił znaczny wzrost liczby publikowanych treści uderzających w Polskę i jej sojuszników, a w obliczu rosyjskiego ataku na Ukrainę w lutym 2022 roku doszło do skumulowania działań przeciwko państwom NATO, które bardzo mocno wspierają Kijów. Obecnie jednym z głównych celów rosyjskiej dezinformacji jest Polska, a z uwagi na rosnącą potrzebę budowania odporności, kluczowe jest określenie zagrożeń i zaplanowanie strategii przeciwdziałania im.

---

[1] S. Bachmann, *Hybrid wars: the 21st-century's new threats to global peace and security*, Scientia Milita-ria, South African Journal of Military Studies, Vol 43, No. 1, 2015
R. Cohen-Almagor, *Jihad Online: How Do Terrorists Use the Internet?,* Advances in Intelligent Systems and Computing, Hull 2017.
B. Salama, *The Resilience of the Islamic State,* Institut für Friedenssicherung und Konflikt management, Vienna 2016.

[2] A. Olech, A. Rogozińska, *Zagraniczne obiekty wojskowe jako system wzmacniania międzynarodowego potencjału militarnego Federacji Rosyjskiej*, Warszawa 2021.

[3] A. Olech, *Francja wycofuje się z Mali i idzie na zachód Afryki*, https://defence24.pl/geopolityka/francja-wycofuje-sie-z-mali-i-idzie-na-zachod-afryki-analiza, dostęp: 14.12.2022.

[4] S. Taillat, *Un mode de guerre hybride dissymétrique ? Le cyberespace*, Stratégique, No 111, Paris 2016, ss. 89, 95.

[5] D. Fiott, R. Parkes, *Protecting Europe. The EU's response to hybrid threats*, European Union Institute for Security Studies, Paris 2019, s. 5.

Realizowane kampanie dezinformacyjne wymierzone w Polskę to długofalowy, wielopłaszczyznowy i kompleksowy proces, który ma na celu głównie dezorientację społeczeństwa oraz wywołanie chaosu. Zamęt kreuje polityczne i ekonomiczne problemy, ale również wpływa na ogólne bezpieczeństwo państwa. Dezinformacja wykorzystywana przez państwo trzecie jako broń pozwala na osiąganie oczekiwanych wyników wyborów, określonych decyzji politycznych czy wywołanie niepokojów w społeczeństwie – wykreowanie chaosu jest strategią na osłabienie i destabilizację systemu politycznego, co z kolei może prowadzić do wywoływania nacisków przez obywateli na władzę państwową. Co ważne, działania podejmowane w sferze informacyjnej mają również na celu kreowanie stosunków międzynarodowych – tworzenie animozji i napięć w kontaktach międzypaństwowych, czy też tworzenie lub niszczenie sojuszy. Zarówno polskie, jak i inne społeczeństwa w ramach sojuszy, powinny być świadome współczesnych zagrożeń, aby chronić i utrzymać multilateralne relacje, które są w obecnych czasach bezcenne, w szczególności mając na uwadze dotychczas pojawiające się wyzwania w regionie Europy Środkowo-Wschodniej[6].

Nakreślenie problemu

Działalność dezinformacyjna, którą prowadzi Federacja Rosyjska, jest dostrzegalna niemalże w każdym państwie, w którym Kreml widzi potencjał na realizację własnych interesów. Stanem na grudzień 2022 roku trzeba podkreślić, że Polska stała się jednym z głównych celów szkodliwych rosyjskich działań, a realizowane kampanie są w szczególności dostrzegane w kwestii sprawy ukraińskiej[7]. Dezinformacja wywołuje nie tylko liczne problemy natury prawnej i organizacyjnej powiązanej z koniecznością prowadzenia specjalnych czynności zwalczających szkodliwe narracje, ale również zmusza rządy państw do podjęcia dyskusji na temat naruszania podstaw demokracji oraz stosunków międzynarodowych. Negatywne działania w obszarze informacyjnym wykroczyły poza obszar naukowych rozważań i stały się elementem politycznych reakcji. Mimo że nie jest to nowe zagrożenie, to dla poszczególnych rządów oraz organizacji pozarządowych w Unii Europejskiej i NATO stało się niezwykle trudne do wyeliminowania, bezpośrednio oraz pośrednio oddziałując na społeczeństwo.

[6] S. Gliwa, A. Olech, *Relacje polsko-czeskie i próby ich zakłócenia podejmowane w ramach rosyjskiej kampanii dezinformacyjnej – polska perspektywa,* https://ine.org.pl/relacje-polsko-czeskie-i-proby-ich-zaklocenia-podejmowane-w-ramach-rosyjskiej-kampanii-dezinformacyjnej-polska-perspektywa, dostęp: 13.12.2022.
[7] J. Dobrowolska, A. Olech, *#CyberMagazyn: Relacje polsko-ukraińskie. Rosyjskie próby dezinformacji,* https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-relacje-polsko-ukrainskie-rosyjskie-proby-dezinformacji, dostęp: 10.12.2022.

Rola organizacji pozarządowych jest szczególnie ważna w trakcie kryzysów i zagrożeń. Dotyczy to sytuacji na każdym poziomie organizacyjnym tj. lokalnym, wojewódzkim, państwowym i międzynarodowym. Wówczas to te podmioty także realizują działania na rzecz informowania obywateli. Nie dotyczy to zawsze newsów, które są podawane natychmiast – tuż pod zdarzeniu, ponieważ kluczowe jest, w jakiej formie oraz jak szczegółowo opisano zagadnienie. Przykładów zaangażowania organizacji pozarządowych na rzecz budowania sfery informacyjnej jest wiele, ale zyskały one na znaczeniu w ostatnich kilku latach, osiągając największe zainteresowanie na przełomie 2021 i 2022; w trakcie kryzysu na granicy polsko-białoruskiej[8] i litewsko-białoruskiej[9], wybuchu wojny w Ukrainie[10], czy też regularnie prowadząc warsztaty dotyczące historii i sytuacji międzynarodowej, zwłaszcza dla obywateli zamieszkujących tereny przygraniczne[11], organizując zbiórki[12] oraz pomagając Ukraińcom uciekającym przed wojną[13]. Misją samą w sobie stało się relacjonowanie sytuacji w kraju lub za granicą – w bardzo przystępnej formie – dla obywateli. Co więcej, bardzo wiele tematów, które dotyczą bezpośrednio Polski (i jej sąsiadów) było opisywanych w języku angielskim oraz częściowo rosyjskim i ukraińskim[14], co pozwalało również zagranicznym czytelnikom na zrozumienie sytuacji w regionie. Tym samym pojawiający się kryzys to z jednej strony wyzwanie dla administracji państwowej, a z drugiej nowa, ekspercka rola organizacji pozarządowych, wyjaśniających pojawiające się wątki.

Nie bez znaczenia jest zasięg oraz liczba organizacji pozarządowych w skali kraju. W Polsce w grudniu 2021 roku było zarejestrowanych 138 tys. organizacji pozarządowych, w tym 107 tys. stowarzyszeń oraz 31 tys. fundacji, ale tak naprawdę aktywnie działa około 70 tysięcy stowarzyszeń i fundacji[15]. Niemniej jednak, przedmiotem analizy niniejszego raportu są jedynie

[8] Z. Śliwa, A. Olech, *Migracje i kryzys na granicy polsko-białoruskiej*, https://ine.org.pl/migracje-i-kryzys-na-granicy-polsko-bialoruskiej, dostęp: 10.12.2022.
[9] M. Gibała, A. Olech, *Dezinformacja rosyjska i chińska na Litwie nie ustaje,* https://cyberdefence24.pl/cyberbezpieczenstwo/dezinformacja-rosyjska-i-chinska-na-litwie-nie-ustaje, dostęp: 10.12.2022.
[10] A. Wilk, P. Żochowski, *Jedna armia rosyjsko-białoruska. 284. dzień wojny,* https://www.osw.waw.pl/pl/publikacje/analizy/2022-12-05/jedna-armia-rosyjsko-bialoruska-284-dzien-wojny. Analizy publikowane z każdego dnia konfliktu.
[11] Fundacja Misji Obywatelskiej, "Polskie drogi do Niepodległości", https://www.facebook.com/FundacjaMisjiObywatelskiej/posts/pfbid02eRcfTjhbXweBBdNaJrprKQLE5ur8RuhD8iXznHKPDSEis17FP1D8ahJa5UxaXdDbl, dostęp: 10.12.2022.
[12] Fundacja Misji Obywatelskiej, https://www.facebook.com/story.php?story_fbid=pfbid02mc2v6WWFQmxM8VM6NY7Xm1wLcsX7yDgyMPpBKqFqHcdfo1CoznWrCTviHG54NPngl&id=106710257776777&sfnsn=mo, dostęp: 14.12.2022.
[13] Fundacja Misji Obywatelskiej, https://www.facebook.com/story.php?story_fbid=pfbid02NCt1RC44QEtjEmb9sobbvfeSigPbpxmfwsMqdN3PhRn7hMfYPJzhvfWNajZ2pk2hl&id=106710257776777&sfnsn=mo, dostęp: 14.12.2022.
[14] Więcej m.in. na: https://defence24.com, https://demagog.org.pl/tematy/english/, https://www.pism.pl.
[15] NGO, *Fakty o NGO,* https://fakty.ngo.pl/fakt/liczba-ngo-w-polsce, dostęp: 10.12.2022.

te organizacje, które zajmują się szeroko pojmowanym bezpieczeństwem. Co ważne, bardzo wiele z NGOsów, nawet nie mając profilu ukierunkowanego na tematykę bezpieczeństwa, stosunków międzynarodowych lub konkretnie dezinformację, było zaangażowanych w szeroko zakrojone działania, gdy w lutym 2022 roku Rosja dokonała inwazji na Ukrainę. Działo się tak z powodu różnych aspektów tego konfliktu, które miały m.in. charakter militarny, informacyjny, energetyczny, społeczny, humanitarny, psychologiczny, medyczny i prawny. Co więcej, Polska była państwem najbardziej zaangażowanym i odczuwającym skutki konfliktu. To oznacza, że działania organizacji pozarządowych wynikały nie tylko z ich statusowych przedsięwzięć, ale także z uwagi na osoby zrzeszone lub śledzące funkcjonowanie NGOsów, które w różnych formatach relacjonowały lub nawiązywały do konfliktu rosyjsko-ukraińskiego.

W Polsce funkcjonuje co najmniej kilkaset organizacji pozarządowych, które w ramach swojego profilu mogłyby realizować zadania w ramach platformy współpracy z administracją rządową. W związku z tym, autorzy nie wybierają, nie klasyfikują oraz nie faworyzują konkretnych stowarzyszeń lub fundacji, które mogą zostać zaangażowane w dalsze etapy współpracy na rzecz wsparcia polskiej racji stanu w przeciwdziałaniu dezinformacji. Prawdą jest, że w konsultacjach – w trakcie powstawania raportu – wzięło udział kilkunastu przedstawicieli oraz współpracowników organizacji pozarządowych, think-tanków oraz świata akademickiego. Jednakże niniejszy raport ma jednak służyć rozwinięciu współpracy między administracją publiczną a NGOsami oraz zaproponowaniu nowych rozwiązań, a selekcja organizacji rządowych do realizacji kolejnych projektów nastąpi na późniejszych etapach i w procesie wielopłaszczyznowej konsultacji. Grupa organizacji pozarządowych w Polsce jest bardzo liczna, a zatem nie należy wykluczyć tych podmiotów, które będą chciały się zaangażować, mając właściwy profil do współpracy.

Publikowanie treści przez NGOsy to ogromna odpowiedzialność. Są to podmioty, teoretycznie, najbliżej obywatela, a co ważniejsze – dla obywatela. To oznacza, że powinny dostarczać sprawdzone i prawdziwe treści, które pozwolą na zwiększenie świadomości obywatela oraz jego edukację. Jest to proces niezwykle trudny, długotrwały i narażony na działania zewnętrzne, niemniej, opłacalny również dla drugiej strony. Organizacje pozarządowe chcą, aby ich działalność była zauważona, udostępniana i obserwowana. To oznacza, że budują – przez lata – sieć swoich (wiernych) odbiorców, którzy cenią treści i materiały. Jest to współpraca, która ma swoje korzyści nie tylko dla obywateli i NGOsów, ale także dla administracji publicznej, która częściowo wspiera oraz horyzontalnie nadzoruje ich funkcjonowanie.

Trzeba zaznaczyć, że opisywana problematyka w niniejszym raporcie stanowi ramy dla budowania współpracy pomiędzy organizacjami pozarządowymi i administracją publiczną. Ponadto jest to perspektywa NGOsów, a zatem przedstawione są wyzwania oraz kwestie, które są istotniejsze dla fundacji i stowarzyszeń, niż dla podmiotów rządowych. Autorzy postulują w swoich rozważaniach o wzmocnienie lub nawiązanie nowych relacji w ramach zwalczania dezinformacji, które mają się przysłużyć administracji publicznej oraz organizacjom pozarządowym. Sugerowane działania mają posłużyć jako zalecenia na rzecz poprawy obecnych regulacji i rozwiązań, ponieważ zmiany w procesie dwustronnej współpracy będą wymagać dalszych konsultacji oraz zostaną rozłożone w czasie. Innymi słowami, autorzy wypełniają lukę w dotychczasowych opracowaniach obejmujących kwestię kooperacji, także w ramach regularnych projektów, z zakresu bezpieczeństwa informacyjnego.

2. Współpraca pomiędzy NGOsami a administracją publiczną w zakresie zwalczania operacji informacyjnych i psychologicznych, w tym o charakterze dezinformacyjnym i propagandowym

Stan obecny

Cyberbezpieczeństwo oraz przestrzeń informacyjna w „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej" z 2020 roku zostały zaliczone do pierwszego z czterech filarów bezpieczeństwa narodowego. Wśród celów i priorytetów znalazło się podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym. Z punktu widzenia organizacji pozarządowych niezwykle istotne jest wspomnienie o roli promowania wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Ważnym dla NGOsów celem jest również rozwój kompetencji, wiedzy oraz świadomości zagrożeń i wyzwań w obszarze cyberbezpieczeństwa zarówno wśród kadr administracji publicznej, jak i w społeczeństwie. Co więcej, dokument wspomina również o aktywnym przeciwdziałaniu dezinformacji poprzez budowę zdolności i stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych, jak również dążeniu do zwiększenia świadomości społecznej o zagrożeniach związanych z manipulacją informacją poprzez edukację w zakresie bezpieczeństwa informacyjnego.

Dużą wagę do roli bezpieczeństwa informacyjnego i cyberbezpieczeństwa przywiązuje także NATO. Konieczność wzmocnienia zdolności do obrony przed atakami cybernetycznymi po raz

pierwszy została uznana podczas szczytu w Pradze w 2002 roku. W 2014 roku członkowie Sojuszu Północnoatlantyckiego uznali cyberobronę za częścią obrony zbiorowej deklarując, że cyberataki mogą prowadzić do powołania się na Artykuł 5. Co więcej, w 2016 roku członkowie Sojuszu uznali przestrzeń cybernetyczną za obszar działań zbrojnych i w większym stopniu zobowiązali się do wzmacniania cyberobrony w odniesieniu do swoich krajowych sieci i infrastruktury oraz traktowania jej jako priorytet. Z kolei w 2018 roku członkowie Sojuszu przyjęli „Wizję i strategię w odniesieniu do cyberprzestrzeni, jako domeny operacyjnej" (Vision and Strategy on Cyberspace as a Domain of Operations)[16]. Obecnie w ramach NATO funkcjonują dwa centra doskonałości zajmujące się cyberbezpieczeństwem i bezpieczeństwem informacyjnym, w tym zwalczaniem dezinformacji. Są to CCD COE w Tallinnie oraz Strategic Communications COE w Rydze.

Internet oraz media społecznościowe powstały w górnolotnym celu – łączenia ze sobą ludzi. Dość szybko okazało się jednak, że pomimo swoich niezliczonych zalet, stały się one również obszarem działań wrogich państw, przestępców i terrorystów. Jak pokazują liczne przykłady rosyjskiej propagandy, działalność w obszarze informacyjnym, poprzez oddziaływanie na opinię i nastroje społeczne, przekłada się także na działania w świecie „offline" przejawiające się, jako naruszenia bezpieczeństwa i porządku publicznego. Pomimo licznych inicjatyw mających zwalczać szkodliwą działalność w sieci, warto wyraźnie podkreślić, że wdrażane rozwiązania wciąż pozostają o krok za działalnością dezinformacyjną nie tylko Federacji Rosyjskiej, ale również zwykłych przestępców.

Należy stwierdzić, że chociaż w „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej" rola i możliwości, jakie w zakresie zwalczania operacji informacyjnych i psychologicznych wymierzonych przeciwko Polsce, a także w budowaniu bezpieczeństwa informacyjnego mogą odegrać organizacje pozarządowe są relatywnie szerokie, to nie są one zaangażowane przez podmioty administracji publicznej na tyle, na ile by mogły. Oznacza to, że nie są wykorzystywane potencjały organizacji pozarządowych, ich doświadczenie, wiedza oraz zasięgi, rozumiane poprzez kręgi instytucji i osób, do których są w stanie dotrzeć.

Ze względu na tę niezwykle strategiczną kooperację na linii NGOsy – administracja publiczna, bez której nie będzie możliwości rozwijania organizacji pozarządowych, tak ważne jest regularne weryfikowanie, czy obie strony mają spójną wizję na rzecz dobrobytu

[16] L. Brent, *Rola NATO w cyberprzestrzeni,* https://www.nato.int/docu/review/pl/articles/2019/02/12/rola-nato-w-cyberprzestrzeni/index.html, dostęp: 15.12.2022.

i bezpieczeństwa państwa. Nie oznacza to, że administracja publiczna ma sterować i nadużywać swoich wpływów, aby publikowane treści były zgodne z konkretną linią polityczną. Wręcz przeciwnie, NGOsy mają mieć niezależność w temacie publikacji, z zastrzeżeniem, że nie działają na szkodę państwa lub nie nakłaniają lub insynuują działań oraz zachowań, które mogłyby do takowej szkody doprowadzić. To wiąże się z tym, że organizacje pozarządowe istnieją wiele lat, a władza polityczna może się zmieniać co kadencję. Dlatego rola NGOsów jest tak ważna, gdyż jest stała, ale jednocześnie elastyczna do zmieniającego się dynamicznie środowiska. Co więcej, ta rola jest kluczowa dla podmiotów zajmujących się kwestiami dezinformacji oraz informowania społeczeństwa.

W pierwszej połowie 2022 roku jedenaście organizacji pozarządowych i instytutów badawczych wspólnie opracowało „Kodeks dobrych praktyk – wspólnie przeciw dezinformacji". Kodeks ten podejmuje próbę ujednolicenia standardów walki z dezinformacją. Eksperci współtworzący raport zawarli w nim kluczowe zagadnienia w tym obszarze bezpieczeństwa informacyjnego. Przedstawili również rekomendowane działania i zmiany, które powinny pojawić się wśród podmiotów odpowiedzialnych za przekazywanie treści w sferze informacyjnej, jak również i wśród zwykłych obywateli[17].

Podmioty rządowe współpracują z sektorem NGOsów (oraz uczelniami i jednostkami badawczymi) w zakresie budowania bezpieczeństwa informacyjnego Polski oraz zwalczania operacji o charakterze dezinformacyjnym i propagandowym jedynie w ograniczonym stopniu. Wspomnieć tu można choćby o dwóch podmiotach – Stowarzyszeniu Demagog, oraz o Naukowej i Akademickiej Sieci Komputerowej. Po rosyjskiej inwazji na Ukrainę 24 lutego 2022 r. przeciwdziałanie dezinformacji zostało uznane przez Ministerstwo Spraw Zagranicznych za jeden z trzech kluczowych elementów dyplomacji publicznej. Nawiązano więcej stałych kontaktów z organizacjami pozarządowymi. Niemniej jednak wciąż istnieje wiele czynników, które prowadzą do ograniczonej współpracy organizacji pozarządowych i administracji publicznej.

Luki prawne i instytucjonalne

Stanem na grudzień 2022 roku w polskim systemie brakuje ram prawnych dotyczących zarówno zaangażowania organizacji pozarządowych w budowaniu bezpieczeństwa

[17] NASK, *Powstał kodeks dobrych praktyk w zakresie dezinformacji,* https://www.nask.pl/pl/aktualnosci/4992,Powstal-Kodeks-Dobrych-Praktyk-w-zakresie-dezinformacji.html, dostęp: 15.12.2022.

informacyjnego Polski, jak również ich współpracy z administracją publiczną (rządową i samorządową). Nie powstał również żaden zinstytucjonalizowany organ, który podejmowałby się koordynacji tejże współpracy. Sprawia to, że współpraca ma wymiar głównie doraźny i mocno ograniczony, a potencjał NGOsów nie jest wykorzystywany. Brak legislacji wywołuje również niepewność wśród organizacji pozarządowych w zakresie ich działalności i funkcjonowania.

Rozwiązania prawne obowiązują w przypadku powoływania NGOsów, a także przyznawania grantów. Istnieje zatem podstawa do dalszego procedowania w ramach tworzenia legislacji na rzecz współpracy z administracją publiczną, aby procesy były transparentne.

Luki w zdolnościach i kompetencjach

Istotną kwestią w zakresie budowania bezpieczeństwa informacyjnego jest dostęp do informacji niejawnych. Organizacje pozarządowe i jej przedstawiciele tegoż dostępu, poza nielicznymi przypadkami, nie posiadają. Utrudnia to NGOsom bycie „na bieżąco" z najnowszymi informacji dotyczącymi operacji o charakterze dezinformacyjnym i propagandowym wymierzonych w Polskę. Co za tym idzie, gdy już po pewnym czasie uzyskują taką świadomość i podejmują pewne działania, ich reakcja może być spóźniona.

Warto odnotować, że to właśnie organizacje pozarządowe – bardzo często – publikują informacje o zdarzeniach, zanim zrobi to administracja publiczna. NGOsy stają się zatem punktem odniesienia dla wielu obywateli oraz swego rodzaju wykładnią w problematyce środowiska bezpieczeństwa. Dotyczy to również informacji związanych z szeroko rozumianym bezpieczeństwem państwa oraz dezinformacją uderzającą w polską rację stanu. Dlatego też należy dążyć do jak najszybszego połączenia kompetencji, aby zarówno obywatele otrzymali wiedzę w zakresie pojawiających się wyzwań, a jednocześnie administracja publiczna mogła zaufać wybranym organizacjom pozarządowym, niejako przekazując im kompetencje do opublikowania zweryfikowanych i prawdziwych danych.

Problemy po stronie NGOsów

Jednym z fundamentalnych problemów organizacji pozarządowych są ograniczone fundusze. To z kolei przekłada się na szereg innych problemów. Wspomnieć tu należy o ograniczonych możliwościach udziału w płatnych szkoleniach, braku skutecznej strategii komunikacyjnej i promocji niezależnej aktywności, a w konsekwencji – ograniczonym gronie własnych odbiorców. NGOsy posiadają także relatywnie słabe rozeznanie, co do aktywności i kontaktów

w poszczególnych ministerstwach i jednostkach administracji publicznej. Oprócz powyższych, w niewielkim stopniu NGOsy współpracują ze sobą w skali krajowej, a zwłaszcza te największe z tymi mniejszymi, mającymi charakter regionalny, np. funkcjonującymi w województwach przy granicach.

Problemy po stronie administracji publicznej

Poszczególne podmioty administracji publicznej, w tym również ministerstwa, co wynika z przeprowadzonych rozmów, posiadają relatywnie słabe rozeznanie, jeśli chodzi o organizacje pozarządowe zajmujące się cyberbezpieczeństwem oraz bezpieczeństwem informacyjnym, w tym fact-checkingiem, zwalczaniem dezinformacji czy prostowaniem fejk newsów. Problemem są również fundusze przeznaczane dla organizacji pozarządowych – są one niewystarczające, a procedury i kryteria ich przyznawania niekoniecznie transparentne i apolityczne.

Zainteresowanie oraz obecność administracji publicznej na wydarzeniach organizowanych przez organizacje pozarządowe jest często niewielka. To właśnie jeden z powodów słabego rozeznania NGOsów, zajmujących się bezpieczeństwem informacyjnym. Co więcej, oddziałuje to na same organizacje pozarządowe – czują się wtedy omijane, a to powoduje, że ich głos i wiedza ekspercka nie chcą być słyszalne. Odwrócenie tego trendu, choć nie wymaga to żadnych zmian prawnych i instytucjonalnych, a jedynie dobrej woli i oddelegowanie pracowników np. z MON i MSZ, pozytywnie wypłynęłoby na współpracę na linii administracja publiczna – organizacje pozarządowe.

Problemy we współpracy

Najważniejszym zagadnieniem podnoszonym w tym zakresie podczas rozmów z przedstawicielami organizacji pozarządowych i administracji publicznej był brak wzajemnego zaufania. Składają się na niego innego czynniki, wymienione powyżej i choć po obu stronach występuje wola współpracy, to ten brak zaufania znacząco wpływa na jej możliwości. Organizacje pozarządowe obawiają się, że współpraca z administracją publiczną nie odbywałaby się na zasadach partnerskich, ich działalność mogłaby być ograniczona i narzucona przez rząd, co tym samym naraziłoby je na zarzut stania się „tubą propagandową".

Publikowanie treści zweryfikowanych oraz przystępnych dla odbiorców to współcześnie jedno z największych wyzwań. Dlatego administracja publiczna powinna dostrzegać zarówno potencjał, jak i zagrożenia, wynikające z funkcjonowania organizacji pozarządowych, które

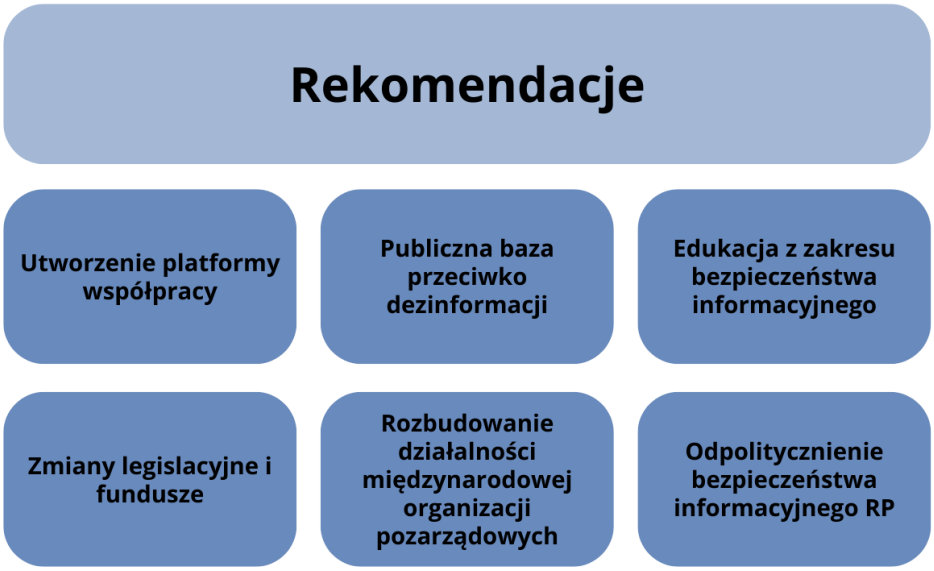
dostarczają na bieżąco treści. W tym aspekcie istnieje kilka wątpliwości, które nie zaburzają współczesnego funkcjonowania NGOsów i kooperacji z administracją publiczną, ale trzeba je mieć na uwadze:

- czy część z organizacji pozarządowych dążąc do tego, aby uzyskać jak najwięcej udostępnień i polubień na portalach społecznościowych, nie zdecyduje się na publikowanie treści kontrowersyjnych i dziennikarskich, niejako odchodząc od swojej statusowej roli?
- czy NGOsy, które chcą publikować materiały aktualne – z dziedziny informacyjnej – mają przeszkolonych (wyedukowanych) specjalistów i ekspertów, którzy sami potrafią dotrzeć do sprawdzonych informacji i nie będą powielać dezinformacji?
- dlaczego tak mała jest współpraca ogólnopolska think-tanków i organizacji pozarządowych, które zajmują się fake-newsami i dezinformacją w kwestii wzajemnego udostępniania treści zweryfikowanych, a jednocześnie można zauważyć niewielkie wspieranie mniejszych organizacji pozarządowych, które mają np. charakter lokalny (przy granicach wschodnich Polski) i mogą dostarczać interesujących informacji bezpośrednio od i dla obywateli?
- jaką rolę chcą pełnić eksperci zaangażowani w NGOsach specjalizujący się w problematyce dezinformacji? Czy kierują się interesem Polski, czy bardziej potrzebują budowania własnej marki?
- gdzie jest „punkt wspólny" dla organizacji pozarządowych i administracji publicznej – w walce z dezinformacją – jeśli chodzi o wzajemną współpracę (gdyż nie może się on kończyć na przekazaniu funduszy)?

W związku z licznymi wątkami, które powinno się brać pod uwagę w bilateralnej współpracy, należy stopniowo realizować kolejne etapy długofalowych projektów; także tych poruszonych w niniejszym raporcie. To oznacza, że wprowadzanie innowacji w dwustronnej kooperacji nie musi mieć charakteru natychmiastowego, a bazować trzeba na dotychczas wypracowanych schematach. Dotyczy to relacji podmiotów administracji państwowej z organizacjami pozarządowymi, które realizowały już projekty z zakresu dezinformacji dla rządu (m.in. Demagog, CyberDefence24, FakeHunter), a zatem znają specyfikę funkcjonowania tej współpracy. Ponadto na znaczeniu musi zyskiwać poszerzanie grupy NGOsów, ponieważ wciąż pojawiają się nowi specjaliści (co wiąże się także z postępującą globalizacją), którzy mają wiedzę ekspercką z zakresu problematyki mniej popularnej (np. Azji, Ameryki

Południowej, czy krajów nordyckich[18]). Oprócz tego, priorytetem powinien być ten sam efekt, który obie strony chcą osiągnąć. Zarówno dla administracji publicznej, jak i organizacji pozarządowych ideą funkcjonowania powinno być wsparcie społeczeństwa obywatelskiego i zneutralizowanie szkodliwych wpływów obcych państw. Jeśli będzie istniał konsensus w tej kwestii, to bilateralna relacja i budowanie sieci zainteresowanych NGOsów będzie efektywnie oraz efektownie prosperować. Filarem musi być wciąż dwustronna wola do nawiązywania współpracy, gdyż tylko takie działanie pozwala na zwiększanie odporności na dezinformacje.

3. Rekomendacje dotyczące współpracy oraz eliminacji luk

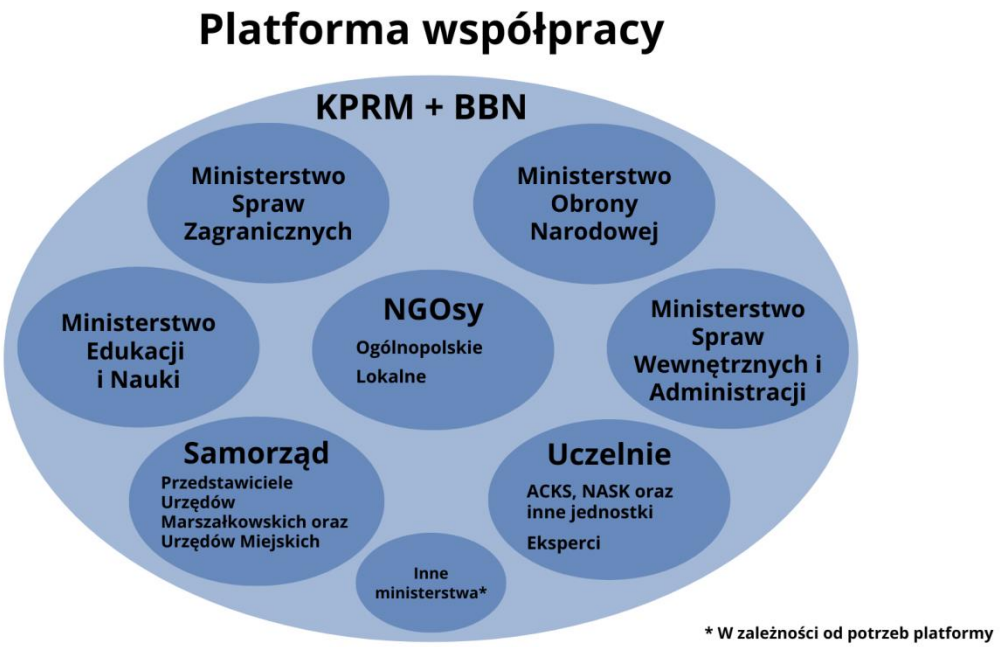


<u>Utworzenie platformy współpracy</u>

Po dokonaniu analizy stanu obecnego współpracy pomiędzy administracją publiczną a organizacjami pozarządowymi, a także po rozmowach z przedstawicielami obu środowisk, główną rekomendacją i postulatem jest stworzenie stałej platformy współpracy. Istotne jest zbudowanie, utrzymywanie i systematyczne udoskonalanie zintegrowanego i koordynowanego na bieżąco systemu wymiany informacji, opinii i współpracy dla administracji publicznej,

[18] M. Gibała, A. Olech, *#CyberMagazyn: Dezinformacja rosyjska i chińska w regionie nordycko-bałtyckim,* https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-dezinformacja-rosyjska-i-chinska-w-regionie-nordycko-baltyckim, dostęp: 15.12.2022.

organizacji pozarządowych, a także uczelni. Co istotne, postuluje się, by w działania po stronie administracji publicznej włączyć nie tylko podmioty rządowe, ale także i samorządowe.



Rolę koordynatora platformy objęłaby Kancelaria Prezesa Rady Ministrów przy wsparciu oraz istotnym zaangażowaniu Biura Bezpieczeństwa Narodowego[19]. Współpraca pomiędzy KRPM i BBN byłaby w tym przypadku pożądana. Wyszczególnione zostały cztery ministerstwa: Ministerstwo Spraw Zagranicznych, Ministerstwo Obrony Narodowej, Ministerstwo Edukacji i Nauki, Ministerstwo Spraw Wewnętrznych i Administracji, które pełnią istotną rolę w zakresie budowania bezpieczeństwa informacyjnego. Niemniej jednak nie jest to zbiór zamknięty. W razie potrzeb wskazane jest, by w prace platformy włączane były także inne ministerstwa. Przykładowo – Ministerstwo Zdrowia w momencie tworzenia działań przeciwko operacjom dezinformacyjnym w zakresie kwestii zdrowotnych (np. związanych z pandemiami). Rządowe Centrum Bezpieczeństwa, podlegające Prezesowi Rady Ministrów, choć nie zostało wyszczególnione na grafice, również powinno, jeśli zostanie uznane tak przez Premiera, być zaangażowane w działania platformy współpracy.

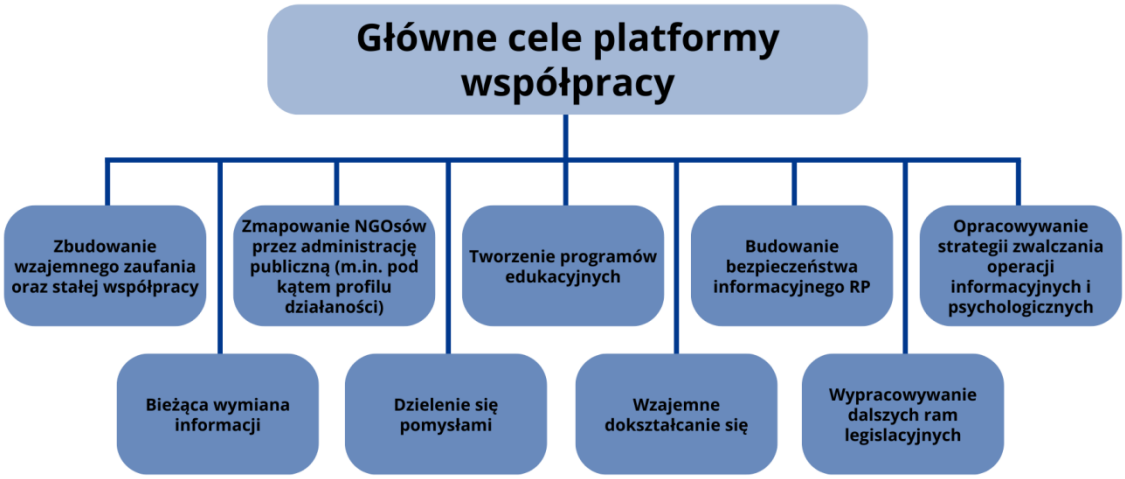
Istotne jest także zaangażowanie samorządów. One również ze względu na swoje kompetencje powinny brać aktywny udział w budowaniu bezpieczeństwa informacyjnego Polski. Dzięki temu możliwe byłoby choćby bardziej skoordynowane prowadzenie kampanii społecznych

[19] BBN z racji swojego charakteru nie może podlegać pod KPRM, stąd też oba podmioty powinny działać na zasadach partnerskich.

w zakresie wykrywania i zwalczania dezinformacji. Co więcej, samorządy mogą stać się obiektem wrogiej operacji o charakterze dezinformacyjnym lub propagandowym (np. obszary przygraniczne). Wtedy też w celu skutecznego zwalczania szkodliwej narracji niezbędne jest działanie nie tylko na poziomie ogólnokrajowym, ale przede wszystkim regionalnym. Stąd też postuluje się, by w działaniach platformy współpracy uczestniczyły nie tylko organizacje pozarządowe o charakterze ogólnopolskim, ale również te o zasięgach regionalnych. Dzięki temu przy wsparciu KPRM możliwe byłoby zbudowanie sieci powiązań między przedstawicielami samorządów a regionalnymi NGOsami. Wybór poszczególnych organizacji pozarządowych mających uczestniczyć w platformie współpracy może zostać dokonany na drodze otwartego konkursu.

Ważną częścią platformy współpracy powinny zostać też uczelnie i jednostki badawcze, a także eksperci z dziedziny cyberbezpieczeństwa i bezpieczeństwa informacyjnego. W spotkaniach i pracach platformy powinni brać udział przedstawiciele Akademickiego Centrum Komunikacji Strategicznej (ACKS), powołanego w 2021 roku przy Akademii Sztuki Wojennej, jak również Naukowej i Akademickiej Sieci Komputerowej (NASK). Warto jednak zaprosić do współpracy także inne think-tanki i jednostki badawcze. W prace platformy poza wszystkimi wymienionymi i przedstawionymi na powyżej granice podmiotami, w razie potrzeby należy zapraszać także inne.

Ważne jest, by spotkania platformy odbywały się regularnie. Nie muszą mieć one jednak regularnego i permanentnego składu. Dotyczy to zarówno organizacji pozarządowych, uczelni, samorządów, jak i ministerstw. Jeśli dane spotkanie miałoby być poświęcone zagadnieniu stricte odporności polskiej polityki zagranicznej czy dyplomacji publicznej na operacje dezinformacyjne lub budowania wizerunku państwa za granicą, to udział np. MSWiA czy lokalnych organizacji pozarządowych nie jest konieczny. Tak samo jeśli spotkanie dotyczyłoby potencjalnych operacji dezinformacyjnych wobec samorządów, to MSZ może, ale nie musi w nim uczestniczyć. Co więcej, jeśli zajdzie taka potrzeba można i powinno się zwoływać doraźne, nadzwyczajne spotkania platformy.



Można również rozważyć powołanie w każdym ministerstwie dedykowanej niewielkiej komórki do zwalczania dezinformacji. Ich funkcjonowanie byłoby koordynowane przez KPRM. Dzięki temu możliwy byłby bieżący i stały przepływ informacji między wszystkimi ministerstwami, a prowadzenie działań przeciwko operacjom dezinformacyjnym i psychologicznym wymierzonym w Polskę byłoby bardziej spójne, a także i szybsze.

W kwestii dostępu do informacji niejawnych rozwiązaniem może być oddelegowanie przez zaangażowane w platformę organizacje pozarządowe oraz uczelnie i instytuty przedstawicieli, którzy zostaliby poddani kontroli Agencji Bezpieczeństwa Wewnętrznego i/lub Służby Kontrwywiadu Wojskowego. Przeprowadzono by wobec nich postępowanie sprawdzające oraz przeszkolono w zakresie ochrony informacji niejawnych. Po pozytywnej weryfikacji swobodnie uczestniczyli w działaniach platformy.

Warto odnotować, że nie każda organizacja pozarządowa, zajmująca się kwestiami bezpieczeństwa i dezinformacji, musi być na początku wzięta pod uwagę w procesie współpracy na linii NGO – administracja publiczna. Pierwotnie należy ograniczyć liczbę organizacji pozarządowych, dbając o stopniowy rozwój kooperacji. Z czasem powinno się – na drodze konsultacji, spotkań i listów intencyjnych – włączać kolejne fundacje i instytucje. Jest to kluczowe dla innowacyjności rozwijanych projektów oraz pozwoli administracji publicznej na otrzymanie szerszej perspektywy, zwłaszcza, że wiele organizacji pozarządowych zrzesza ekspertów z doświadczeniem międzynarodowym, a z drugiej strony, koncentruje się na sprawach lokalnych.

Działania na rzecz obywateli mogą zaczynać się lokalnie, ale będą mieć efekt globalny, dlatego powinno się dążyć do porozumienia na kilku płaszczyznach. Nie tylko włączać znakomite organizacje specjalizujące się w dezinformacji, choć one na początku są pierwszorzędne, ale w przyszłości również mniejsze fundacje. Ostatecznie NGOsy koncentrujące się na propagandzie i rosyjskich działaniach informacyjnych w ramach swojego funkcjonowania będą tworzyć krajowy system współpracy administracji publicznej z organizacjami pozarządowymi. Jednakże wymaga to czasu oraz wyselekcjonowania podmiotów, które będą skutecznie i wytrwale realizować działania w sferze informacyjnej. Zatem rolą obu stron będzie stała kontrola NGOsów, które zajmują się cyberbezpieczeństwem i bezpieczeństwem informacyjnym. Co więcej, choć głównym obszarem działań platformy współpracy byłoby zwalczanie rosyjskich operacji dezinformacyjnych i propagandowych wymierzonych w Polskę, to powinna ona również, gdy tylko zajdzie taka potrzeba, podejmować aktywności w zakresie zwalczania dezinformacji z innych źródeł.

Publiczna baza przeciwko dezinformacji

Należy rozważyć stworzenie ogólnopolskiej i publicznej bazy danych, tworzonej wspólnie przez administrację publiczną i organizacje pozarządowe. Byłoby to miejsce, gdzie będą mogły być dodawane oraz weryfikowane poszczególne informacje, doniesienia, artykuły, narracje i kampanie przez poszczególne – zaangażowane w działania platformy współpracy – organizacje pozarządowe. Byłby to fundament do nadzoru publikowanych treści, które mają szczególnie ważny charakter dla państwa. Tym samym, nie wszystkie treści byłyby przedmiotem zainteresowania, ale tylko te najważniejsze. Treści mogliby dodawać zarówno przedstawiciele administracji publicznej lub współpracujących NGOsów.

Jednocześnie byłby to portal dla obywateli Polski, którzy mieliby do dyspozycji bezpieczną stronę internetową ze zweryfikowanymi i prawdziwymi informacjami, a także danymi na temat bieżących zagrożeń dla polskiej przestrzeni informacyjnej. Dzięki temu realnie możliwe będzie poprawienie jakości bezpieczeństwa informacyjnego, a tym samym odporności Polaków na wymierzone w nich operacje o charakterze dezinformacyjnym bądź psychologicznym, budując umiejętność przeciwstawiania się zagranicznym wpływom (głównie rosyjskim, ale nie tylko). Jeśli udałoby się zrzeszyć kilkanaście podmiotów z całej Polski, także te, które publikują w różnych językach, to treści mogłyby być bardzo sprawnie kolportowane nie tylko w skali całego państwa, ale także na poziomie międzynarodowym. Dlatego też istotne jest, by w razie

utworzenia takiej dedykowanej strony internetowej, posiadała ona także inne wersje językowe (w tym przede wszystkim wersję anglo- i ukraińskojęzyczną).

Edukacja z zakresu bezpieczeństwa informacyjnego

Kolejnym postulatem, który wysuwa się po spotkaniach z przedstawicielami administracji publicznej oraz organizacji pozarządowych, jest stworzenie w podstawie programowej dla szkół podstawowych i szkół średnich zajęć dedykowanych bezpieczeństwu informacyjnemu, a następnie ich realizowanie. Co więcej, zajęcia z zakresu *media literacy* oraz *digital literacy* można również wprowadzić na poziomie edukacji przedszkolnej. Budowanie *societal resilience,* zwłaszcza w zakresie zwiększenia świadomości społecznej o zagrożeniach związanych z przestrzenią informacyjną jest kluczowe dla budowania odporności społeczeństwa na różnego rodzaju zagrożenia zewnętrzne, nie tylko dezinformacyjne i propagandowe bądź psychologiczne. Stąd też konieczne jest zaangażowanie w funkcjonowanie platformy współpracy Ministerstwa Edukacji i Nauki. Programy zajęć z edukacji medialnej/informacyjnej, mogłyby odbywać się na platformie, gdzie można stworzyć szczegółowe plany zajęć. Dlatego tak istotne jest zaangażowanie w nią organizacji pozarządowych, uczelni, ekspertów. Szkoły podlegają pod władze samorządowe (gminne i powiatowe), a przez to również przedstawiciele samorządów muszą być włączeni w tworzenie ram zajęć, a następnie ich wdrażanie. Oprócz tego, eksperci posiadający wsparcie administracji publicznej będą mogli znacznie powiększyć swoje zasięgi, aby dotrzeć do obywateli. Wydaje się, że eksperci są dużo lepiej postrzegani przez społeczeństwo, niż konkretni politycy, ponieważ są – teoretycznie – niezależni.

Skuteczny system przeciwdziałania dezinformacji w Polsce powinien opierać się na mechanizmach zmierzających do zbudowania odporności jednostki, stojącej u jego podstaw. Następnie obejmie zasięgiem grupy lokalne, całe państwo, a na koniec strony zrzeszone i ich partnerów. Podstawowymi zadaniami w obszarze edukacyjnym powinny być: nauka krytycznego myślenia, wypracowanie praktycznych umiejętności badania informacji pozyskanych z mediów oraz zdolności do zweryfikowania czy podana przez media informacja ma potwierdzenie w faktach.

Samo prowadzenie zajęć to z kolei zadanie głównie dla organizacji pozarządowych – tych ogólnopolskich, jak i lokalnych. Mogą one zarówno szkolić nauczycieli, jak również samemu

prowadzić zajęcia. Pewnym relatywnie tanim, a jednocześnie dobrym rozwiązaniem w początkowej fazie wdrażania zajęć o bezpieczeństwie informacyjnym byłoby przygotowanie wideoprezentacji poświęconych manipulacjom, dezinformacji, fejk newsom, toksyczności mediów społecznościowych etc. dostosowanych pod poziom i wiek odbiorców. Prezentacje te następnie mogłyby zostać rozesłane wśród szkół i wyświetlane na zajęciach w ramach godzin wychowawczych lub edukacji dla bezpieczeństwa.

Szkolenia powinny być również skierowane do mediów, zarówno ogólnopolskich, jak i lokalnych. Tutaj również to najpierw platforma współpracy odpowiadałaby za stworzenie cyklów szkoleń i ich ram, a następnie organizacje pozarządowe – te ogólnopolskie i regionalne – prowadziłyby szkolenia z zakresu weryfikacji informacji, wykrywania działań dezinformacyjnych i fejk newsów, oraz odpowiedzialności mediów w budowaniu bezpieczeństwa informacyjnego Polski.

Zmiany legislacyjne i fundusze

Niezbędne są również zmiany i nowe ramy legislacyjne, które umożliwiłyby większe zaangażowanie się organizacji pozarządowych w budowanie bezpieczeństwa informacyjnego Polski, w tym we współpracę z administracją publiczną. Dotyczy to zarówno ram prawnych określających działalność i kompetencje, jak również i funduszy dla organizacji pozarządowych. Przepisy odnoszące się do gratyfikowania i dzielenia, co wskazywali przedstawiciele NGOsów, choć są konieczne, to muszą dawać elastyczność i swobodę działań, a nie ją ograniczać. Ponadto powinny ułatwiać działalność, a nie stawiać przed nią bariery.

Z rozmów z przedstawicielami organizacji pozarządowych wynika, że otrzymywane granty nie zawsze pozwalają w pełni na realizację projektów w zakresie budowania bezpieczeństwa informacyjnego. Postulowane byłoby zatem zwiększenie środków na ten cel oraz utworzenie dedykowanego funduszu rządowego na granty dla organizacji pozarządowych zajmujących się bezpieczeństwem informacyjnym, zwalczaniem dezinformacji oraz fact-checkingiem. Co więcej, powinno się zapewnić pewne ramy dopuszczalności modyfikacji pierwotnych planów wydatków w trakcie realizacji grantów po konsultacjach z grantodawcą. Obecnie jest to w praktyce niemal niemożliwe. Pewnym wzorem do modyfikacji przepisów prawnych w tym zakresie mogłoby być amerykańskie National Endowment for Democracy (NED), gdzie po konsultacjach możliwe są zmiany nawet całych komponentów działań w trakcie projektu.

Co istotne fundusz oraz konkursy grantowe muszą być w pełni otwarte i transparentne, opierać się wyłącznie na ocenie merytorycznej NGOsów. Stąd też rozwiązaniem mogłoby być stworzenie sprecyzowanych ram prawnych oraz powołanie rad konkursowych, złożonych z niezależnych ekspertów, którzy będą opiniować wnioski grantowe. Co więcej, można rozważyć relatywnie precyzyjny podział środków tego dedykowanego funduszu na poszczególne aspekty budowania bezpieczeństwa informacyjnego (tj. określić pulę na bardziej skonkretyzowane działania np. „prowadzenie kampanii społecznych", „zwalczanie rosyjskiej dezinformacji", „działania fact-checkingowe").

Oprócz tego bardzo ważny jest wątek ponadnarodowy. Każda z organizacji pozarządowych, która zajmuje się kwestiami bezpieczeństwa, a przez to bardzo często dezinformacją (choćby weryfikując i publikując treści), ma własną grupę odbiorców oraz plany długoterminowe. Jednakże jest jeden kluczowy element, na który należy zwracać uwagę. Są to podmioty funkcjonujące w Polsce, a zatem również w ramach tych działań jednym ze strategicznych celów powinno być wsparcie, jeśli nie samych interesów Polski, to np. współpracy w ramach organizacji międzynarodowych lub relacji bilateralnych na linii Polska – USA Polska – Niemcy, Polska – Czechy, czy Polska – Japonia. Niektóre z organizacji pozarządowych posiadają zewnętrze (tj. zagraniczne) finansowanie. Zagraniczne finansowanie oczywiście w żaden sposób nie wyklucza z pracy na rzecz interesu Polski. Niemniej, w przypadku zaangażowania organizacji pozarządowych w stałą współpracę z administracją publiczną w zakresie budowania bezpieczeństwa informacyjnego Polski, niezbędna jest dokładniejsza weryfikacja skąd pochodzą środki NGOsów – dotyczy to jednak tych organizacji, które miałyby stać się częścią przedstawionej w raporcie platformy współpracy, a tym samym miałyby uzyskać dostęp do części informacji niejawnych. Pozwoliłoby to na transparentną kooperację, a przez to dość spójną politykę przeciwdziałania szkodliwym wpływom, w tym głównie Federacji Rosyjskiej (ale nie tylko). Zaburzanie dwustronnych relacji i sianie propagandy są jednymi z głównych celów Kremla[20].

[20] S. Gliwa, A. Olech, *Relacje polsko-czeskie i próby ich zakłócenia podejmowane w ramach rosyjskiej kampanii dezinformacyjnej – polska perspektywa*, https://ine.org.pl/relacje-polsko-czeskie-i-proby-ich-zaklocenia-podejmowane-w-ramach-rosyjskiej-kampanii-dezinformacyjnej-polska-perspektywa, dostęp: 13.12.2022.

Rozbudowanie działalności międzynarodowej organizacji pozarządowych

Z perspektywy organizacji pozarządowych ważną kwestią jest również budowanie sieci kontaktów na arenie międzynarodowej z organizacjami z innych państw. Pomóc w tym mogliby przedstawiciele administracji rządowej. Pomoc ta powinna obejmować co najmniej dwa aspekty. Pierwszym z nich są szkolenia o skutecznym składaniu dobrych wniosków o granty międzynarodowe (np. z Sojuszu Północnoatlantyckiego lub Unii Europejskiej). Drugim zaangażowanie i partycypacja organizacji pozarządowych w międzynarodowych konferencjach i szczytach, na których obecni będą również przedstawiciele zagranicznych NGOsów. Innymi słowy – ministerstwa powinny zabierać ze sobą na takie wydarzenia wybranych przedstawicieli polskich organizacji pozarządowych zajmujących się bezpieczeństwem informacyjnym.

Organizacje pozarządowe skoncentrowane na zjawisku dezinformacji na bieżąco mogą weryfikować i punktować publicznie zagrożenia, nawet zanim zrobi to administracja publiczna[21]. Co więcej, ukierunkowując się także na kooperację międzynarodową NGOsów, współpracując z podmiotami zza granicy, będą funkcjonować wspólnie na rzecz przeciwdziałania dezinformacji wymierzonej w organizacje międzynarodowe, których członkiem jest m.in. Polska, a także wymierzonej w dwustronne relacje RP z poszczególnymi państwami (np. z Ukrainą).

Niektóre organizacje pozarządowe i działający w nich eksperci mają już zbudowaną siatkę międzynarodowych kontaktów i współpracy, zaangażowane były również w ponadnarodowe projekty poświęcone bezpieczeństwu informacyjnemu. Ich doświadczenie może przysłużyć się zarówno współpracy z administracją publiczną (rządową, jak i samorządową), jak i działalności platformy współpracy. Co więcej, mogłyby się one dzielić z mniej doświadczonymi na arenie międzynarodowej organizacjami dobrymi praktykami i rozwiązaniami, czy też pomagać w nawiązywaniu pierwszych zagranicznych kontaktów. To również budowanie odporności na dezinformacje dla całego regionu.

[21] J. Dobrowolska, A. Olech, *Polsko-ukraińskie relacje a rosyjskie działania dezinformacyjne,* https://trimarium.pl/projekt/polsko-ukrainskie-relacje-a-rosyjskie-dzialania-dezinformacyjne, dostęp: 13.12.2022.

Odpolitycznienie bezpieczeństwa informacyjnego RP

Ostatnią, choć równie ważną co poprzednie, rekomendacją jest odpolitycznienie sfery bezpieczeństwa informacyjnego Polski. Dotyczy to zarówno poziomu rządowego, jak i relacji rząd – samorządy. Niezbędne jest wypracowywanie ponadpartyjnych inicjatyw, których ramy wybiegają poza okres jednej kadencji. Odnosi się to również do funduszu dla organizacji pozarządowych – proces wyboru zwycięzców konkursów nie powinien być w żadnym stopniu motywowany politycznie.

4. Zakończenie

Jednym z głównych celów niniejszego raportu było przedstawienie idei platformy współpracy organizacji pozarządowych z administracją publiczną w zakresie budowania bezpieczeństwa informacyjnego Polski, ze szczególnym uwzględnieniem realizowania działań na rzecz walki z dezinformacją. Należy zaznaczyć, że jest to innowacyjna koncepcja, która wcześniej nie była przedmiotem badań i opracowań. Pomimo wielu wspólnych elementów w realizowaniu zadań na rzecz przeciwdziałania dezinformacji w Polsce, wciąż nie sformalizowano struktur do obustronnej wymiany dobrych praktyk. Zarówno NGOsy, jak i administracja publiczna, dążą do wyeliminowania z przestrzeni publicznej danych, które są szkodliwe dla społeczeństwa. W związku z tym, posiadając tożsamą misję w walce z dezinformacją, obie strony powinny się wzajemnie uzupełniać i wspierać, ponieważ produktem finalnym jest utrzymujące się bezpieczeństwo Polski.

Co jednak ważne, z perspektywy organizacji pozarządowych kluczowe jest, aby administracja była otwarta na dialog i dążyła do pogłębiania relacji w ramach regularnych inicjatyw i projektów. Dlatego – na podstawie przeprowadzonych licznych konsultacji z partnerami projektu – wskazuje się, że budowanie odporności na zewnętrzne zagrożenia dla przestrzeni informacyjnej (w tym głównie rosyjską propagandę) przy wsparciu NGOsów powinno być realizowane z inicjatywy administracji publicznej, która jest otwarta na współdziałanie z podmiotami pozarządowymi skoncentrowanymi na kwestiach dezinformacji.

W przyszłości, gdy platforma współpracy pomiędzy administracją publiczną a organizacjami pozarządowymi się rozwinie, należy rozważyć rozszerzenie jej działalności również w charakterze międzynarodowym. To pozwoliłoby na skuteczniejszą kooperację na rzecz

zwalczania rosyjskiej dezinformacji zarówno w ramach dwustronnej współpracy np. z sojusznikami ze Stanów Zjednoczonych, krajów bałtyckich lub Ukrainy, na forum organizacji takich jak NATO czy Unia Europejska, lub też w mniej sformalizowanym międzynarodowym gronie państw – Trójkąta Lubelskiego, Trójmorza czy Grupy Wyszehradzkiej.

Autorzy sugerują, aby to administracja publiczna była inicjującym kooperację z organizacjami pozarządowymi. To przede wszystkim przedstawicielom rządu powinno zależeć, aby szkodliwa narracja nie zaburzała funkcjonowania aparatu państwa. Dlatego też, wychodząc naprzeciw organizacjom pozarządowym, działając na rzecz społeczeństwa obywatelskiego, należy zorganizować sieć połączeń między NGOs a administracją publiczną, przy zaangażowaniu innych podmiotów jak instytuty badawcze. Byłoby to możliwe – choć tych opcji jest bardzo wiele – na przykład dzięki platformie współpracy, a także w ramach spotkań podczas wydarzeń i sympozjów, jak i w ramach konferencji internetowych.

Znając specyfikę realizowanych operacji dezinformacyjnych, które mają często zindywidualizowaną grupę odbiorców, na znaczeniu zyskuje stała kooperacja między administracją publiczną i organizacjami pozarządowymi. Celem jest zdemaskowanie szkodliwych działań, które będą uderzać w różne kwestie, od projektów gospodarczych i transportowych, przez kwestie społeczne do konfliktów i wojen. Retoryka dezinformujących najczęściej przybiera podobny charakter działań, czyli: przeciwdziałać poszczególnym rządom, negować współpracę w ramach organizacji międzynarodowych i powstrzymywać udzielanie wsparcia sojusznikom, zwłaszcza przeciw Rosji. Dlatego mając – już teraz – świadomość tej powtarzalności w działaniach Kremla, należy wszechstronnie i wieloaspektowo reagować, wykorzystują różnego rodzaju narzędzia. Jednym z takich narzędzi jest właśnie społeczeństwo obywatelskie i jego silne przedstawicielstwo, czyli organizacje pozarządowe. Dlatego też muszą one być aktywnie zaangażowane w budowanie bezpieczeństwa Polski, w tym bezpieczeństwa informacyjnego i cyberbezpieczeństwa.

Stała aktywność administracji państwowej, organizacji pozarządowych, think-tanków, ciał unijnych, grup roboczych i uczestników programów naukowo-eksperckich, które są ukierunkowane na walkę z dezinformacją, jest kluczowa w procesie budowania niezachwianych relacji między państwami i organizacjami. Nowe projekty, stypendia

i konferencje[22] w ramach wspierania organizacji pozarządowych powinny obejmować również problematykę zwalczania dezinformacji.

Współpraca z organizacjami pozarządowymi, choć przedstawiona w niniejszym opracowaniu jedynie w zakresie zwalczania dezinformacji, posiada potencjał rozszerzania na inne wymiary, w tym energetyczny, technologiczny i militarny. Omawiana w raporcie problematyka musi być przedmiotem dalszych analiz i rozważań, gdyż współcześnie – przy tak agresywnej polityce Federacji Rosyjskiej – niezbędne jest rozwijanie zdolności do przeciwdziałania dezinformacji w państwach Europy Środkowej i Wschodniej. Jest to jeden z kluczowych elementów dla budowania odporności, w tym zaangażowania społeczeństw do popierania współpracy w ramach NATO i UE. To oznacza, że państwa członkowskie muszą cały czas reagować na zagrożenia i wspierać NGOSy, aby nie dopuścić do rozpadu, deterioracji, albo upadku organizacji. Społeczeństwo obywatelskie w Polsce wciąż się rozwija, a uderzająca w nią rosyjska dezinformacja, to kolejne z wielkich wyzwań, które stoi przed Polską i jej sojusznikami. Należy mieć na uwadze, że najbardziej podatni, ale też najbardziej odczuwający efekty dezinformacji, są obywatele. Przeciwdziałanie dezinformacji to niekończący się proces, dlatego wciąż trzeba ulepszać narzędzia, aby efektywniej reagować.

Raport powstał w wyniku konsultacji i spotkań z ekspertami administracji publicznej oraz organizacji pozarządowych. Wysiłek podmiotów, które wzięły udział w pracach analitycznych był dużym wyzwaniem, szczególnie, że dyskutowano o zjawiskach mających wpływ na bezpieczeństwo państwa i jego obywateli. Dlatego też serdecznie dziękujemy za udział i wsparcie merytoryczne przedstawicielom: BBN, MSZ, NASK, ACKS, PISM, Baltic Defence College, uczelni wyższych, Disinfo Digest, Instytutu Zamenhofa, CyberDefence24 oraz Stowarzyszenia Pravda.

[22] A. Adamkiewicz, *Wspólna konferencja RCB i MON nt. dezinformacji,* https://archiwum.rcb.gov.pl/wspolna-konferencja-rcb-i-mon-nt-dezinformacji, dostęp: 10.12.2022.