EUROPA WOBEC DEZINFORMACJI

– BUDOWA ODPORNOŚCI SYSTEMOWEJ W WYBRANYCH KRAJACH

IZABELA ALBRYCHT, FAUSTINE FELICI, MICHAŁ KRAWCZYK, KAMIL MIKULSKI,
TOMASZ PIEKARZ, JAKUB TUSZYŃSKI, ANASTAZJA WIŚNIEWSKA

20 LAT INSTYTUT KOŚCIUSZKI

OPEN INFORMATION PARTNERSHIP

EUROPA WOBEC DEZINFORMACJI – BUDOWA ODPORNOŚCI SYSTEMOWEJ W WYBRANYCH KRAJACH

AUTORZY: IZABELA ALBRYCHT, FAUSTINE FELICI,
MICHAŁ KRAWCZYK, KAMIL MIKULSKI, TOMASZ PIEKARZ,
JAKUB TUSZYŃSKI, ANASTAZJA WIŚNIEWSKA

AUTORZY:

Izabela Albrycht
Wprowadzenie, Rekomendacje

Kamil Mikulski
Unia Europejska

Tomasz Piekarz
Polska

Anastazja Wiśniewska
Niemcy

Faustine Felici
Francja

Michał Krawczyk
Zjednoczone Królestwo

Jakub Tuszyński
Państwa Trójmorza

EDYCJA: Izabela Albrycht, Michał Krawczyk, Kamil Mikulski
PROJEKT GRAFICZNY I SKŁAD: Joanna Świerad-Solińska
TŁUMACZENIE I KOREKTA: Adam Ladziński

Raport został sfinansowany z pomocą Open Information Partnership.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki
ul. Feldmana 4/9-10
31-130 Kraków, Polska
+48 12 632 97 24
www.ik.org.pl
instytut@ik.org.pl

SPIS TREŚCI

Izabela Albrycht

Wprowadzenie

„Odporność systemowa musi znajdować się w społeczeństwach tak samo jak w państwie"

Pomimo wielu przykładów wykorzystania propagandy, dezinformacji czy wojny informacyjnej w działaniach militarnych i cywilnych w przeszłości dopiero epoka cyfrowa umożliwiła działanie na niespotykaną dotąd skalę przy niskim finansowym i organizacyjnym progu wejścia. Co więcej, już dziś widać, że zjawisko to stanowić będzie coraz większe wyzwanie dla bezpieczeństwa krajów demokratycznych i będzie miało wpływ na wynik geopolitycznej rywalizacji, która przybrała na sile pod koniec drugiej dekady XXI w. Niechlubne nasilanie się zaawansowanych zagrożeń informacyjnych związane jest przede wszystkim z postępem technologicznym. Pozyskiwanie większej ilości danych o każdym z nas i naszych preferencjach umożliwia tworzenie bardziej dopasowanych do odbiorcy treści, z kolei rozwój technologii sztucznej inteligencji oraz uczenia maszynowego powoduje proliferację tzw. *deepfake*, które uzupełniają arsenał narzędzi tworzenia *fake news*. Ten ostatni proces stanowi przykład zaburzenia środowiska informacyjnego, a lawina zmanipulowanych lub nieprawdziwych, ale łudząco przypominających prawdziwe multimediów przybiera na sile. W odpowiedzi na to zagrożenie kraje demokratyczne będą musiały balansować między zasadą wolności słowa a potrzebą regulacji przestrzeni informacyjnej. Będą także musiały przyjrzeć się stopniowi odpowiedzialności, z jakim do tego problemu podchodzą platformy internetowe – czyli przestrzenie, które dzięki cyfrowej infrastrukturze i zaaplikowanym algorytmom są głównymi nośnikami informacji we współczesnym świecie. Niezwykle ważne będzie także zharmonizowanie działań w ramach współpracy międzynarodowej, zarówno bilateralnej, jak i multilateralnej, wliczając formaty regionalne[1].

Operacje informacyjne i propaganda są metodami wpływu i projekcji siły regularnie stosowanymi przez Rosję (ale również przez Chiny i Iran) *de facto* na całym świecie: od tych, które zwróciły oczy badaczy tematu, służb i polityków w 2016 r.[2], czyli działań przeprowadzonych w związku z wyborami prezydenckimi w Stanach Zjednoczonych[3], po ostatnio zidentyfikowane aktywności w Gruzji i Mołdawii[4]. Propaganda i dezinformacja w rękach Rosji to także narzędzie w ramach działań hybrydowych, czego przykładem między innymi wojna na Ukrainie. W tym przypadku dezinformacja stała się częścią działań wojennych (ang. *information warfare*), co jako zjawisko ma swoje źródła w rosyjskiej koncepcji „wojny nowej generacji". Zaprezentowana już w 2013 r. przez gen. Walerija Gierasimowa, szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, koncepcja prezentowała operacje informacyjne w cyberprzestrzeni jako stały element działań wojennych, prowadzonych zarówno w czasie konfliktu, jak i pokoju – zaktualizowano ją w 2019 r., podkreślając jednoznacznie istotność działań hybrydowych[5]. Generał Gierasimow stwierdził: „połączenie niewielkiej siły ekspedycyjnej z operacjami informacyjnymi pokazało, że można je rozszerzyć na obronę i rozwój interesów narodowych poza granicami Rosji"[6]. W Europie operacje informacyjne w cyberprzestrzeni pochodzące z terytorium Rosji stały się w ostatnich latach ważnym elementem polityki zagranicznej, często mającej na celu nie tylko realizację interesów ekonomicznych i politycznych, ale także polaryzację społeczeństw. Fala rosyjskiej dezinformacji będąca następstwem zestrzelenia malezyjskiego samolotu MH17 nad terytorium Ukrainy oraz towarzysząca zamachowi na Siergieja Skripala w Wielkiej Brytanii uwydatniły fakt, iż celem podobnych działań informacyjnych może zostać każdy kraj europejski.

Służby alarmują, że coraz częściej kraje demokratyczne stają się celem operacji informacyjnych ze strony Chin. Pekin wykorzystuje prochińskie narracje lub manipulacje, aby realizować swoją polityczną i gospodarczą agendę, mającą na celu dominację technologiczną i ekonomiczną. Wielu

ekspertów zwraca także uwagę, że ta strategia ma swoją drugą, mniej agresywną retorycznie odsłonę, polegającą na próbach uciszania otwartej debaty publicznej, jak ma to miejsce np. obecnie w Estonii, gdzie chińska ambasada wyraziła niezadowolenie z ustaleń estońskiej służby wywiadu zagranicznego, zarzucając im „brak profesjonalizmu" i „ideologiczne uprzedzenie"[7]. Działania Państwa Środka zmierzają zatem także do tego, aby w przestrzeni informacyjnej przemilczane zostały kwestie niewygodne dla Pekinu[8], w tym dotyczące pandemii COVID-19 czy politycznego wpływu Komunistycznej Partii Chin na firmy technologiczne, np. Huawei, zaangażowane w cyfrową transformację świata[9].

Należy zauważyć, że zarówno Chiny, jak i Rosja postrzegają operacje wywierania wpływu (ang. *information operations*, *InfoOps*), w tym dezinformację, jako normalną działalność w czasach pokoju. I choć oba kraje używają do tego innych metod i narzędzi, to wykorzystują te operacje, aby tłumić wewnątrz kraju społeczne protesty lub niezadowolenie, a także na dłuższą metę kontrolować to, co myślą obywatele. Z punktu widzenia bezpieczeństwa Europy istotne jest jednak przede wszystkim, że modele „cyfrowego autorytaryzmu" są przez Chiny i Rosję eksportowane i używane do prowadzenia polityki poza granicami kraju – co znacząco odróżnia te kraje od zachodnich demokracji, które mają tendencję do ograniczania tego typu działalności wyłącznie do działań wojennych[10].

Problem dezinformacji wykracza jednak także poza ramy rywalizacji i konfliktów międzynarodowych czy operacji wpływu. Oddziałuje on bowiem także na życie zwykłych ludzi, co uwypukliła pandemia COVID-19, wraz z którą obserwuje się na niespotykaną dotąd skalę epidemię dezinformacji, określaną przez wielu terminem *infodemia*[11]. W tym przypadku nieprawdziwe informacje mogą wpływać na zdrowie ludzi, a w skrajnych sytuacjach na ich życie, a także skalę rozwoju pandemii w poszczególnych krajach oraz na napięcia polityczne, których osią są różne podejścia do zwalczania epidemii, pogłębiając nie tylko kryzys zdrowia publicznego, ale również erozję zaufania oraz polaryzację społeczeństwa wokół budzących emocje decyzji i wydarzeń. Jednak i w tym z pozoru „niepolitycznym" przypadku konieczna jest interwencja instytucji publicznych, które przede wszystkim powinny zrozumieć naturę i skalę problemu, a następnie podjąć skuteczne działania informacyjne oraz takie, które systemowo wspierać będą budowanie odporności społeczeństwa na dezinformację. W ostatnim roku z wyzwaniem tym próbowała się zmierzyć zarówno Komisja Europejska[12], NATO[13], jak i poszczególni członkowie obu tych organizacji. Wydaje się, że COVID-19 dobitnie uświadomił problem, ale nie została jeszcze nań sformułowana skuteczna odpowiedź systemowa. Możemy jednak oczekiwać, że wyzwanie to pozostanie wysoko na agendzie politycznej krajów demokratycznych. W tzw. „raporcie mędrców" NATO czytamy, że „obywatele państw NATO oczekują ochrony przed nowymi zagrożeniami, w tym cyfrowymi i dezinformacyjnymi, oraz spodziewają się, że ich rządy przy wsparciu Sojuszu rozwiną narzędzia atrybucji i odstraszania. Odporność systemowa musi być elementem i państw, i społeczeństw"[14].

Możliwość rozprzestrzeniania nieprawdziwych informacji bez ograniczeń geograficznych czy technicznych oraz bardzo małym kosztem pojawiła się wraz z rozwojem Internetu oraz platform społecznościowych. Te ostatnie odgrywają kluczową rolę jako narzędzie dotarcia do milionów odbiorców, czerpania zysków z prezentowanych treści czy prowadzenia operacji informacyjnych. Ich nieuregulowany charakter oraz brak przejrzystego prawodawstwa związanego z dezinformacją sprawiają, że kontrola treści w tych serwisach jest bardzo utrudniona. Globalny charakter platform, dla których nie stanowią przeszkody granice, a które przepisy kontrolują w niewystarczającym stopniu, sprawiają, że starają się one wciąż prowadzić „uniwersalną" politykę względem użytkowników na całym świecie, co coraz częściej okazuje się niemożliwe. Wiele krajów podejmuje obecnie próby uregulowania działalności firm technologicznych oraz platform społecznościowych, a także przedstawia legislację bezpośrednio traktującą o dezinformacji.

Globalny charakter platform wiąże się z globalnymi wyzwaniami w zwalczaniu dezinformacji i wymaga współpracy wszystkich interesariuszy. Przykładem może być współpraca wszystkich z wymienionych platform i krajów unijnych w zakresie zwalczania dezinformacji o szczepionce przeciw COVID-19. Wydaje się, i niniejszy raport także przedstawia taką rekomendację, że współpraca krajów demokratycznych oraz sektora prywatnego w tym zakresie jest szczególnie ważna, aby szanse na jej powodzenie rosły.

Dezinformacja? Zagrożenia hybrydowe? *Fake news*?

Określenie „zaburzenia informacji" (ang. *information disorder*) stosowane jest wobec skomplikowanej siatki pojęciowej, która obejmuje popularne terminy takie jak *fake news*, dezinformacja czy też zagrożenia hybrydowe (przynajmniej częściowo). Nie ulega przy tym wątpliwości, że chociaż wspomniane terminy mogą dotyczyć podobnych zjawisk, nie są jednocześnie synonimiczne. *Fake news*, dezinformacja oraz zagrożenia hybrydowe wymykają się próbom ujęcia w ramy niebudzących zastrzeżeń definicji i bywają różnie rozumiane przez stosujące je osoby. Niedookreśloność nie stanęła jednak na przeszkodzie tego, by *fake news* stało się słowem roku brytyjskich wydawców słownika Collins w 2017 r., a dezinformacja i zagrożenia hybrydowe przeniknęły do głębi europejskiej polityki publicznej.

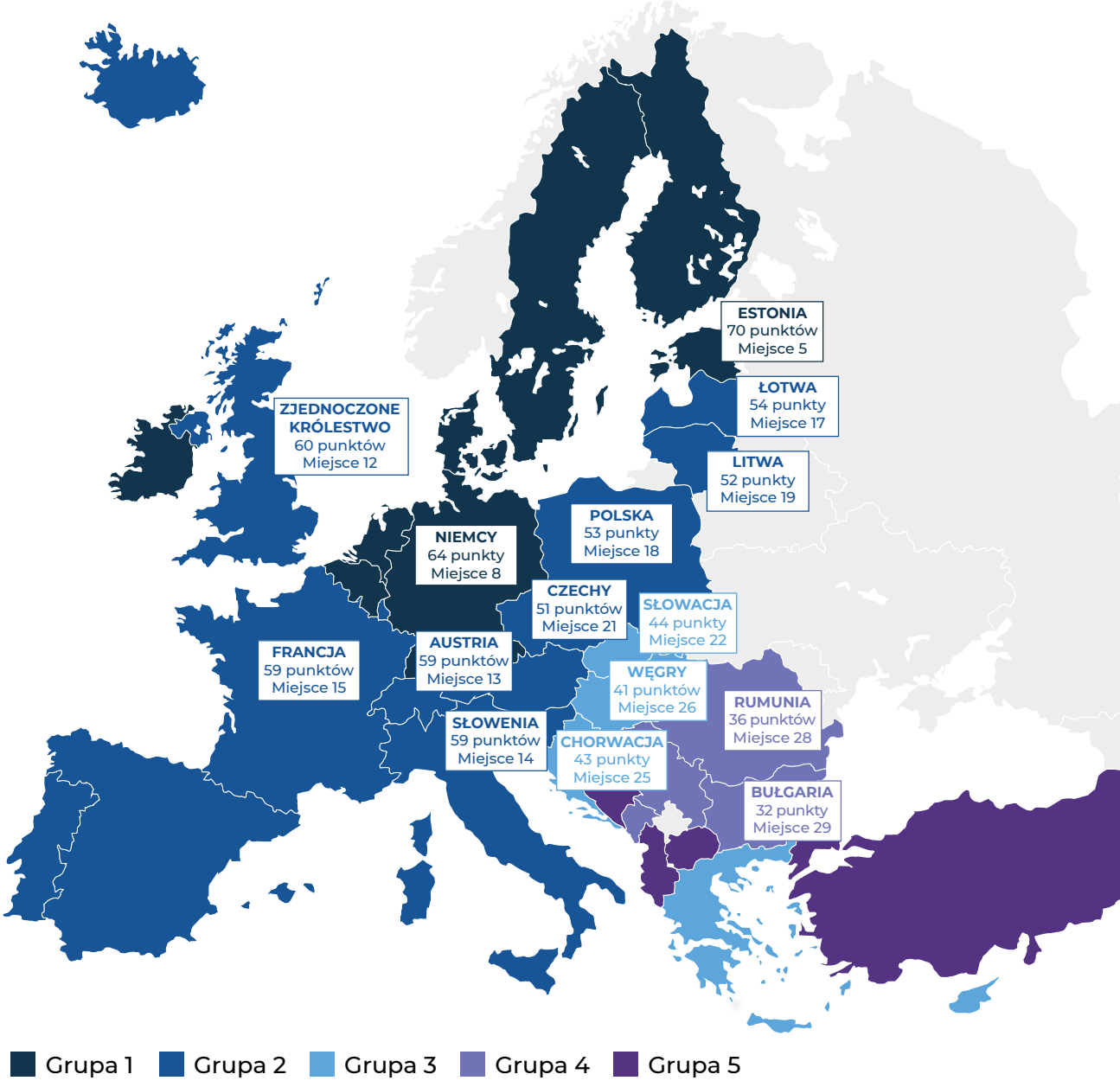
Komunikat Komisji do PE i Rady pt. *Zwalczanie dezinformacji w Internecie: podejście europejskie*[15] wyjaśnia, że „dezinformację należy rozumieć jako możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub zamierzonego wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną". Tę samą definicję przywołują *Plan działania na rzecz zwalczania dezinformacji* oraz *Unijny kodeks postępowania w zakresie zwalczania dezinformacji*, który doprecyzowuje ją jednocześnie w drodze ograniczonej wykładni autentycznej. Warto przy tym zauważyć, że *Unijny kodeks postępowania w zakresie zwalczania dezinformacji* opracowała Grupa ekspercka wysokiego szczebla ds. nieprawdziwych informacji (przyp. autora – w oryg. *fake news*[16]).

Zarówno instytucje Unii Europejskiej, jak i władze państw członkowskich poświęciły wiele uwagi kwestii odpowiedzi na zaburzenia informacji i budowania odporności systemowej (ang. *resilience*) na szczeblach regionalnym oraz narodowym. Do przeciwdziałania owym negatywnym zjawiskom włączyły się również europejskie organizacje społeczeństwa obywatelskiego oraz platformy z sektora mediów społecznościowych. Utworzyły w ten sposób skomplikowany system o dwu strukturach: wertykalnej (od koordynujących współpracę instytucji europejskich, przez państwa członkowskie, do sektorów prywatnego i trzeciego) i horyzontalnej (obejmującą wspólne inicjatywy różnych podmiotów na szczeblach krajowym i międzynarodowym).

Celem niniejszego raportu jest próba holistycznego opisania systemu odporności europejskiej w taki sposób, by zarówno ująć subiektywnie określone najważniejsze inicjatywy, jak i dostarczyć interesujących informacji w kontekście rzadziej pojawiających się w podobnych opracowaniach reakcji na zaburzenia informacyjne występujące w krajach Europy Środkowo-Wschodniej. Dlatego też raport zaczyna się od inicjatyw podejmowanych na poziomie ogólnoeuropejskim przez instytucje unijne, by następnie opisać działania Francji, Niemiec, Wielkiej Brytanii[17] i Polski, a wreszcie opisać najważniejsze działania państw Inicjatywy Trójmorza. Instytut Kościuszki będzie kontynuował temat zaburzeń informacyjnych w ramach działalności Disinfo Lab oraz realizacji podcastu General Talks. Zapraszamy Państwa do lektury i śledzenia naszych publikacji.

Poziom kompetencji medialnych w Europie

European Policies Initiative opublikowała w 2019 r. ranking poziomu kompetencji medialnych w 35 krajach Europy. Poniżej znajdują się uwzględnione w raporcie państwa ze wskazaniem miejsca w rankingu oraz uzyskanej punktacji.



Źródło: European Policies Initiative, Open Society Institute – Sofia.

PRZYPISY

1 W przypadku Europy Środkowo-Wschodniej funkcjonują dwie platformy dla takiej współpracy. Pierwsza to Grupa Wyszehradzka, która w ostatniej wspólnej Deklaracji Cyfrowej z Krakowa podpisanej 17 lutego 2021 r. podkreśla potrzebę współpracy w zakresie dezinformacji; druga to Inicjatywa Trójmorza.

2 Należy zauważyć, że intensyfikacja dezinformacji inspirowanej z zewnątrz w Polsce nasiliła się od roku 2014 – po wybuchu „rewolucji godności" na kijowskim Majdanie, a następnie konfliktu rosyjsko-ukraińskiego.

3 W tym wypadku dezinformacja rozsiewana była przez rosyjskich trolli z Agencji Badań Internetowych (ang. *Internet Research Agency*) wraz z szeregiem innych działań operacyjnych rosyjskich służb jak np. włamanie do skrzynki mailowej Hillary Clinton, stanowiły operację mającą na celu wpływ na wyniki tych wyborów.

4 Estonian Foreign Intelligence Service, *International Security and Estonia 2020*, [online]: https://www.valisluureamet.ee/pdf/raport-2020-en.pdf.

5 A. Krzak, *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, [online]: http://www.abw.gov.pl/download/1/2420/1PBW18AKrzak.pdf.

6 red. H. Chałupczak, K. Marzęda-Młynarska, M. Pietraś, R. Suduł, *Zagrożenia bezpieczeństwa w procesach globalizacji*, 2020, s. 40.

7 *Embassy protests foreign intelligence service report China coverage*, [online]: https://news.err.ee/1608114640/embassy-protests-foreign-intelligence-service-report-china-coverage.

8 B. Allen-Ebrahimian, *Estonia warns of "silenced world dominated by Beijing"*, Axios 2021, [online]: https://www.axios.com/estonia-warns-of-silenced-world-dominated-by-beijing-09e54843-6b45-491a-9bfd-e880f6f14795.html.

9 A. Satariano, *Inside a Pro-Huawei Influence Campaign*, [online]: https://www.nytimes.com/2021/01/29/technology/commercial-disinformation-huawei-belgium.html.

10 Jean-Baptiste Jeangène Vilmer, Paul Charon, *Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare*, [online]: https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.

11 The Lancet Infectious Diseases, *The COVID-19 infodemic*, 2020, [online]: https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30565-X/fulltext.

12 Speech of Vice President Věra Jourová on countering disinformation amid COVID-19, *From pandemic to infodemic*, [online]: https://ec.europa.eu/commission/presscorner/detail/en/speech_20_1000.

13 NATO's approach to countering disinformation: a focus on COVID-19, [online]: https://www.nato.int/cps/en/natohq/177273.htm.

14 *NATO 2030, United for a new era*, 2021, s. 19, [online]: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

15 Komisja, *Tackling online disinformation: a European Approach*, 26 kwietnia 2018, [online]: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=PL.

16 Sposób, w jaki Unia odwołuje się do zagadnień dezinformacji i *fake news*, wydaje się niekonsekwentny. O ile w opisanym przypadku Unia utożsamia dezinformację z *fake news*, to raport Wspólnego Centrum Badawczego UE z 2018 r. *The digital transformation of news media and the rise of disinformation and fake news* postrzega je jako oddzielne zjawiska i odmiennie definiuje.

17 Choć Wielka Brytania nie jest już krajem członkowskim UE, to pozostaje jednym z państw najaktywniej przeciwdziałających dezinformacji i zagrożeniom hybrydowym.

Kamil Mikulski

Dezinformacja i zagrożenia hybrydowe z perspektywy prawa i polityki Unii Europejskiej

Wstęp

Unia Europejska jest organizacją międzynarodową z elementami ponadnarodowymi, która działa w ramach złożonego systemu instytucjonalno-prawnego. W poszczególnych obszarach (sektorach) została wyposażona, zależnie od poziomu ich uwspólnotowienia, w określone kompetencje przez państwa członkowskie: wyłączne, dzielone, uzupełniające oraz szczególne (koordynujące)[1]. Od połowy drugiej dekady XXI w. Unia podejmuje szereg działań mających na celu przeciwstawienie się negatywnym zjawiskom dezinformacji i zagrożeń hybrydowych w oparciu o zróżnicowane instrumenty – najczęściej w drodze tzw. „aktów prawa miękkiego"[2] i dokumentów roboczych służb Komisji (np. roczna ewaluacja wdrożenia Unijnego kodeksu postępowania w zakresie zwalczania dezinformacji), ale również poprzez powszechnie obowiązujące akty prawa UE (np. Rozporządzenie o Ochronie Danych Osobowych – RODO). Przedmiotem niniejszego rozdziału jest przekrojowy opis działań różnych instytucji UE – głównie Komisji, Rady Europejskiej oraz Parlamentu – skierowanych do państw członkowskich, sektorów prywatnego i trzeciego, a także obywateli UE. Ze względu na ograniczony rozmiar rozdziału pominięte zostaną działania UE podejmowane w kooperacji z Radą Europy, OBWE i NATO, instrumenty Wspólnej Polityki Sąsiedztwa oraz zagadnienia tylko pośrednio powiązane z dezinformacją/zagrożeniami hybrydowymi, np. ochrona danych osobowych.

Dezinformacja, *fake news* i zagrożenia hybrydowe – charakterystyka zjawiska i komentarz definicyjny

Komisja Europejska we wspólnym komunikacie do Parlamentu Europejskiego i Rady z 6 kwietnia 2016 r. pt. *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*[3] ustanawia bardzo szeroką definicję zagrożeń hybrydowych. Są to mianowicie zagrożenia, które cechują się „kombinacj[ą] represyjnych i wywrotowych działań, konwencjonalnych i niekonwencjonalnych metod (tj. dyplomatycznych, militarnych, ekonomicznych i technologicznych), które mogą być stosowane w sposób skoordynowany przez podmioty państwowe i niepaństwowe, by osiągnąć określone cele, przy czym działania te są poniżej progu oficjalnie wypowiedzianej wojny". W dalszej części dokumentu deskryptywna definicja Komisji stwierdza wprost, że w przypadku zagrożeń hybrydowych „[z]azwyczaj nacisk kładzie się na wykorzystanie podatności danego celu na zagrożenia i kreowanie dwuznaczności, by utrudnić procesy decyzyjne. Kampanie dezinformacyjne prowadzone na masową skalę przy wykorzystaniu mediów społecznościowych w celu kontrolowania dyskursu politycznego lub radykalizowania postaw, rekrutacji »grup-przykrywek« i kierowania nimi mogą być nośnikiem zagrożeń hybrydowych". Nie ulega zatem wątpliwości, że szczególnym i głównym przykładem zagrożenia hybrydowego jest właśnie dezinformacja.

Inny dokument, komunikat Komisji do PE i Rady pt. *Zwalczanie dezinformacji w Internecie: podejście europejskie*[4], wyjaśnia z kolei, że dezinformację „należy rozumieć jako możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną". Jednocześnie warto zauważyć, że *Unijny kodeks postępowania w zakresie zwalczania dezinformacji* (zwany dalej *Unijnym kodeksem postępowania*) opracowany został przez Grupę ekspercką wysokiego szczebla ds. nieprawdziwych informacji (której nazwa w innych językach zawiera wyrażenia *fausses nouvelles* i *fake news*[5]). Tę samą definicję przywołują *Plan działania na rzecz zwalczania dezinformacji* oraz *Unijny kodeks postępowania w zakresie zwalczania dezinformacji*, który doprecyzowuje ją jednocześnie w drodze ograniczonej wykładni autentycznej.

Zagrożenia hybrydowe/ dezinformacja a kompetencje UE i jej architektura instytucjonalna

Mając na względzie zarówno same niedookreślone definicje zjawisk, jak i przedstawione we *Wspólnych ramach* sektorowe ryzyka, jakie niosą ze sobą dezinformacja i zagrożenia hybrydowe, można zauważyć, że te ostatnie nie mają charakteru, który w sposób rozstrzygający kwalifikowałby je do pojedynczego obszaru polityki UE. Zależnie od obszaru, a zatem i rodzaju kompetencji, UE wyposażona jest w zróżnicowane instrumenty prawne, w których może regulować zagrożenia hybrydowe/dezinformację. Przykładowo, w odniesieniu do ochrony danych osobowych wyposażona jest w kompetencję wyłączną i mogła wydać RODO; na gruncie bardziej „typowej" dezinformacji, w sektorach, gdzie Unia ma kompetencje szczególne, będzie musiała poprzestać na aktach prawa miękkiego i koordynacji działań państw członkowskich. W odniesieniu do partnerstwa publiczno-prywatnego Unia pierwotnie preferowała współpracę międzysektorową oraz samoregulację, licząc na efektywne włączenie się w budowanie europejskiego systemu odporności m.in. przez platformy z sektora mediów społecznościowych. Stan ten najprawdopodobniej zmieni się po wejściu w życie rozporządzenia regulującego usługi cyfrowe (więcej w dalszej części rozdziału).

Zróżnicowany charakter zagrożeń oraz złożony system unijnych kompetencji regulacyjnych znajdują swoje odbicie w przestrzeni instytucjonalnej. Uogólniając, można wskazać, że najaktywniejszymi instytucjami UE w podejmowaniu działań są Komisja, Rada Europejska, Parlament oraz Rada

Unii Europejskiej (zwana dalej Radą). Do innych aktywnych organów i agencji UE należą Wysoki Przedstawiciel ds. Polityki Zagranicznej i Polityki Bezpieczeństwa, podlegająca mu Europejska Służba Działań Zewnętrznych, w tym szczególnie Centrum Analiz Wywiadowczych UE (ang. *EU Intelligence and Situation Centre*, INTCEN) oraz jego komórki utworzone na mocy Wspólnych ram z 2015 r.: odpowiadająca za komunikację strategiczną – szczególnie w odniesieniu do krajów Partnerstwa Wschodniego – grupa zadaniowa East StratCom oraz komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (ang. *Hybrid Fusion Cell*). Istotne znaczenie w kontekście badań i szkoleń ma Centrum Doskonalenia ds. przeciwdziałania zagrożeniom hybrydowym (ang. *Hybrid Center of Excellence*). W zakresie swoich specjalności aktywność w przedmiocie zwalczania dezinformacji wykazują również agencje UE CERT-EU, FRONTEX oraz EUROPOL. Komisja ściśle współpracuje z pozostałymi instytucjami, organami i agencjami UE zarówno samodzielnie, jak i poprzez instytucjonalne ramy, w których funkcjonuje Wysoki przedstawiciel, który jednocześnie odpowiada za prowadzenie WPZiB (oraz WPBiO), wiceprzewodniczy Komisji oraz przewodniczy Radzie Spraw Zagranicznych (ang. *Foreign Affairs Council*, FAC) w ramach Rady. O ile FAC jest jedną z konfiguracji stałych przedstawicieli w ramach Rady, należy zauważyć, że w agendzie Rady zagadnienie przeciwdziałania dezinformacji pojawia się w pracach zarówno komitetu COREPER II (nie tylko FAC), jak i COREPER I.

Regulacje i rozwój polityki UE w zakresie przeciwdziałania zagrożeniom hybrydowym i dezinformacji

W latach 2015–2020 nastąpił gwałtowny rozwój polityki i instrumentów regulacyjnych UE w odniesieniu do zagrożeń hybrydowych i dezinformacji, który przyjął formę strategicznych decyzji, raportów oraz aktów prawa miękkiego. Co prawda przed konkluzjami Rady Europejskiej z 2015 r. Unia podejmowała różnego rodzaju działania w celu zwalczania zagrożeń hybrydowych i dezinformacji, jednak miały one charakter incydentalny. Przykładem jest wspominające o sponsorowanej przez państwo nacjonalistycznej propagandzie rosyjskiej oświadczenie przewodniczącego Rady Europejskiej, Hermana Van Rompuya, i przewodniczącego Komisji Europejskiej[6], które dotyczy dodatkowych środków ograniczających (ang. *restrictive measures*, popularnie – sankcji) nałożonych na Rosję w związku z bezprawnym naruszaniem integralności terytorialnej Ukrainy. Aneksja Krymu i Sewastopola przez Rosję stała się przyczyną przyjęcia przez Radę Europejską pierwszych konkluzji, które uruchomiły budowę instytucjonalno-politycznej architektury odpornościowej UE.

Konkluzje Rady Europejskiej z 20 marca 2015 r. i 26 czerwca 2015 r.

Pierwszym z głównych dokumentów UE dotyczącym zagadnienia rosyjskiej dezinformacji były konkluzje Rady Europejskiej z 20 marca 2015 r. W części dotyczącej Europejskiej Polityki Sąsiedztwa (sekcja 13) Rada Europejska podkreśliła, że dostrzega „(...) potrzebę przeciwstawienia się trwającym kampaniom dezinformacyjnym prowadzonym przez Rosję i wezwała wysoką przedstawiciel, by we współpracy z państwami członkowskimi i instytucjami UE przygotowała do czerwca plan działania dotyczący strategicznej komunikacji. Utworzenie zespołu ds. komunikacji jest pierwszym krokiem w tym zakresie”[7]. Rada Europejska nawiązała zatem do trzech istotnych kwestii: 1) dostrzegła potrzebę sformułowania odpowiedzi UE na dezinformację, 2) określiła Wysoką Przedstawiciel jako organ kompetentny do utworzenia w kooperacji z państwami członkowskimi i instytucjami UE planu działania dotyczącego strategicznej komunikacji oraz 3) wyznaczyła pierwszy krok i termin jego realizacji. Opublikowany 22 czerwca 2015 r. *Plan działań na rzecz komunikacji strategicznej*[8] informuje o utworzeniu opartego na Europejskiej Polityce Sąsiedztwa Partnerstwa Wschodniego i stanowiącego część Europejskiej Służby Działań Zewnętrznych (ESDZ) zespołu East StratCom.

Fakt, że Unia Europejska jako pierwszy krok zaleciła utworzenie specjalistycznej komórki ds. komunikacji strategicznej i dyplomacji publicznej ma znaczenie z czterech powodów. Po pierwsze, można było ją utworzyć stosunkowo szybko i z minimalnymi zmianami w obrębie instytucji, po drugie podkreślono znaczenie (cyber)przestrzeni informacyjnej (z perspektywy Rady Europejskiej priorytetowe), po trzecie zespół East StratCom powstał w ramach struktury instytucjonalnej ESDZ – podległej bezpośrednio Wysokiej Przedstawiciel agencji koordynującej działania państw członkowskich – i po czwarte stanowił przyczynek do bardziej kompleksowego oszacowania znaczenia zagrożeń hybrydowych i dezinformacji dla europejskiego systemu bezpieczeństwa i architektury instytucjonalnej. W czerwcu 2015 r. Rada Europejska przyjęła konkluzje[9], w których ponownie wezwała[10] do mobilizacji instrumentów finansowych koniecznych dla przeciwdziałania zagrożeniom hybrydowym. Rezultaty obu konkluzji zostały opublikowane niespełna rok później.

Wspólny Komunikat do Parlamentu Europejskiego i Rady z 6 kwietnia 2016 r. pt. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym oraz Sprawozdanie Anny Fotygi z 14 października 2016 r.

Niezwykle trudno oszacować, który z dokumentów UE miał najważniejsze znaczenie dla budowania odporności (ang. *resilience*) unijnego systemu instytucjonalnego, jednak to właśnie komunikat z 6 kwietnia 2016 r.[11] w kompleksowy sposób scharakteryzował zjawisko dezinformacji w szerszym kontekście zagrożeń hybrydowych (dezinformacja jest szczególnym rodzajem zagrożenia hybrydowego) oraz przedstawił je z perspektywy ryzyka politycznego dla poszczególnych sektorów. We *Wspólnych ramach* z kolei po raz pierwszy w kontekście zagrożeń hybrydowych pojawiła się konceptualizacja odporności systemowej, która obejmuje m.in. zapobieganie kryzysom, reagowanie na nie i przezwyciężanie ich skutków. Wysoka Przedstawiciel i Komisja włączają do budowania odporności systemowej Parlament i Radę, dzieląc konieczne do wykonania zadania między różne instytucje, organy i ciała, w tym Komisję, Wysoką Przedstawiciel, ENISA oraz CERT-EU wraz z 28 narodowymi CSIRT-ami. Ramy wprowadzają istotne i daleko idące zmiany instytucjonalne, rozwijając istniejący zespół komunikacji strategicznej (ang. *East and Arab StratCom Task Forces*), ustanawiając Hybrid Fusion Cell oraz tworząc w Helsinkach Centrum doskonałości „przeciwdziałające zagrożeniom hybrydowym" (ww. *Hybrid CoE*)[12].

W odniesieniu sektorowym *Wspólne ramy* zidentyfikowały zagrożenia i określiły działania konieczne do skutecznego im przeciwdziałania. Wyróżnione obszary i sektory obejmowały: ochronę infrastruktury krytycznej, w tym łańcuchów dostaw, sieci energetyczne i transport energii, przestrzeń kosmiczną, zdolności obronne, ochronę zdrowia publicznego i bezpieczeństwo żywnościowe, cyberbezpieczeństwo, przemysł, energia, systemy finansowe oraz transport. Wyróżniły również działania wymierzone w finansowanie zagrożeń, rozpoznały radykalizację i ekstremizm jako należące do źródeł zagrożeń oraz wskazały konieczność zacieśniania współpracy z państwami trzecimi (gł. z państwami należącymi do Partnerstwa Wschodniego oraz objętymi Europejską Polityką Sąsiedztwa krajami Maghrebu i Maszreku) oraz z NATO, ONZ i OBWE. Działania Rady Europejskiej, Wysokiej Przedstawiciel i Komisji spotkały się ze zrozumieniem i poparciem Parlamentu, którego Komisja Spraw Zagranicznych wezwała do przeciwdziałania dezinformacji, propagandzie i innym zagrożeniom hybrydowym, rozpoznając na poziomie politycznym negatywną rolę Rosji oraz ISIS/Daesz. Sprawozdanie Komisji Spraw Zagranicznych z 14 października 2016 r.[13] przeszło do historii jako tzw. Sprawozdanie Anny Fotygi.

Konkluzje Rady Europejskiej z marca 2018

Marzec 2018 r. jest istotną cezurą dla budowy potencjału UE w zakresie przeciwdziałania zagrożeniom hybrydowym. Otrucie Siergieja Skripala w Londynie stanowiło asumpt polityczny dla Rady Europejskiej, która zgodnie z prawem UE nadaje

Unii impulsy niezbędne do jej rozwoju i określa ogólne kierunki i priorytety polityczne (art. 15 ust. 1 TUE). 22 marca Rada Europejska przyjęła konkluzje[14], w drodze których wezwała Unię Europejską oraz państwa członkowskie do wzmocnienia zdolności odpowiadania na zagrożenia hybrydowe, włączając w to obszary cyberbezpieczeństwa, komunikacji strategicznej i kontrwywiadu[15]. Rada Europejska wyznaczyła Komisję Europejską i Wysoką Przedstawiciel do realizacji tego zadania i raportowania Radzie Europejskiej postępów we wdrożeniu.

Komunikat z 26 kwietnia 2018 r. – *Zwalczanie dezinformacji w Internecie: podejście europejskie*

W następstwie konkluzji Rady Europejskiej, Komisja opublikowała 26 kwietnia 2018 r. komunikat pt. *Zwalczanie dezinformacji w Internecie: podejście europejskie*, w którym zdefiniowała dezinformację jako zagrożenie wyodrębnione z używanego wcześniej pojęcia zagrożenia hybrydowego. Ponadto Komisja po raz pierwszy określiła nadrzędne zasady i cele związane z przeciwdziałaniem dezinformacji. Warto tu zaznaczyć, że wprawdzie Komisja nieco wcześniej – w marcu 2018 r. – opublikowała także *Rekomendacje dotyczące środków skutecznego przeciwdziałania nielegalnym treściom online*[16], jednak nie odniosła się w nich wprost do dezinformacji lub zagrożeń hybrydowych.

Ponadto w punkcie 3.1.1 komunikatu pt. *Szybkie i skuteczne działanie platform internetowych w celu ochrony użytkowników przed dezinformacją* Komisja zawiera negatywną ocenę działań platform z sektora mediów społecznościowych w kontekście zapewnienia wystarczającej przejrzystości reklamy politycznej i treści sponsorowanych, jak również marketingu informacyjnego prowadzonego przez *influencerów* lub przez boty. Jako remedium proponuje wzmożenie wysiłków przez platformy oraz skutecznie wdrażaną i monitorowaną samoregulację w postaci ambitnego kodeksu postępowania opartego na kluczowych zasadach zaproponowanych przez grupę ekspertów wysokiego szczebla oraz zobowiązującego platformy internetowe i branżę reklamową do osiągnięcia wymienionych w komunikacie celów.

Plan działania na rzecz zwalczania dezinformacji z 2018 r.

Sygnały od Rady Europejskiej oraz przygotowanie ram instytucjonalnych i oszacowanie ryzyka politycznego przez Komisję i Wysoką Przedstawiciel otworzyły drogę do opracowania kompleksowego planu budowy systemowej odporności. 5 grudnia 2018 r. opublikowany został *Plan działania na rzecz zwalczania dezinformacji*[17] (ang. *Action Plan Against Disinformation*, dalej: *Plan działania*). *Plan działania* określa cztery filary walki z dezinformacją oraz dziesięć zadań, przed którymi stoi Unia Europejska. Podkreślono w nich konieczność wzmocnienia potencjału i finansowania komunikacji strategicznej oraz delegatur unijnych (warto tu zauważyć – delegatury mimo chronicznego niedoboru personelu prowadzą niekiedy analizę wywiadowczą, szczególnie cenną przy zagrożeniach hybrydowych i dezinformacji) oraz nałożono na Wysoką Przedstawiciel obowiązek oceny, czy konieczne jest utworzenie specjalnych grup zadaniowych dla południowego sąsiedztwa UE oraz dla Zachodnich Bałkanów. Co więcej, ustanowiono System Szybkiego Ostrzegania (ang. *Rapid Alert System*, RAS) wspólny dla państw członkowskich, innych podobnych sieci monitorujących, Parlamentu Europejskiego, NATO i Mechanizmu Szybkiego Reagowania (ang. *Rapid Response Mechanism*) grupy G7.

Komisja wezwała również do wzmocnienia współpracy z Parlamentem, szczególnie w wymiarze komunikacji oraz wspierania wartości europejskich i polityk publicznych. Aspekt współpracy i komunikacji strategicznej poruszony został również w odniesieniu do sąsiadów UE, natomiast w stosunku do społeczeństwa obywatelskiego Unia stwierdziła konieczność wspierania edukacji, umiejętności korzystania z mediów i wzmacniania świadomości w zakresie powstających zagrożeń.

Unia Europejska a współpraca z innymi sektorami

Współpraca UE z gigantami z sektora mediów społecznościowych

Równolegle przebiegały prace powołanej w styczniu 2018 r. i składającej się z 39 członków Grupy Wysokiego Szczebla (HLEG), które zaowocowały publikacją raportu pod angielskim tytułem *A multi-dimensional approach to disinformation*. W skład HLEG wchodzili przedstawiciele sektora prywatnego (w tym platform społecznościowych), publicznego (np. uczelnie publiczne), trzeciego sektora, a także niezależni eksperci oraz dziennikarze. Na podstawie raportu Komisja zrealizowała założenia komunikatu z kwietnia 2018 r. i opracowała Unijny kodeks postępowania. Unijny kodeks postępowania nakłada na sygnatariuszy szereg obowiązków, przede wszystkim w odniesieniu do transparentności reklamy politycznej, przeciwdziałania wprowadzającym w błąd informacjom, zamykania fałszywych kont, właściwego wyróżnienia działalności botów oraz zapewnienia integralności usług. Kodeks usiłuje znaleźć właściwy balans między ograniczeniem dezinformacji i jej negatywnych skutków w cyberprzestrzeni oraz zagwarantowaniem dostępu do rzetelnej informacji i zapewnieniem pluralizmu światopoglądowego. Podkreśla ponadto konieczność wzmocnienia pozycji konsumenta oraz społeczności naukowej i nakłada na sygnatariuszy obowiązek inwestowania w środki technologiczne w celu priorytetowego traktowania istotnych, autentycznych, dokładnych i wiarygodnych informacji.

Kompromisowy charakter podejścia Komisji polega zatem na uregulowaniu współpracy publiczno-prywatnej[18] w drodze stworzonego przy współudziale biznesu w ramach HLEG aktu samoregulacyjnego. W ramach Akcji nr 6 *Planu działania* Komisja nałożyła na siebie obowiązek bliskiego i stałego monitorowania implementacji Unijnego kodeksu postępowania, zastrzegając wprost, że jeżeli implementacja i efekty Unijnego kodeksu postępowania okażą się niezadowalające, Komisja zaproponuje inne działania, w tym regulacyjne. Tak bezpośrednie sformułowanie ze strony instytucji unijnej oznaczało, że wprawdzie Unia postrzegała skuteczną współpracę z gigantami z sektora mediów społecznościowych jako optymalną, jednak wprost komunikowała swoim partnerom, jakie są potencjalne konsekwencje niesatysfakcjonującego poziomu współpracy. W momencie pisania niniejszego artykułu Unijny kodeks postępowania jako akt samoregulacyjny podpisany został po stronie sektora mediów społecznościowych przez firmy Facebook, Twitter, Google, Mozilla i TikTok, a także przez kilka stowarzyszeń branżowych (ang. *trade associations*)[19]. Sygnatariusze zostali zobligowani do raportowania wdrożenia postanowień Unijnego kodeksu postępowania.

W grudniu 2020 r. Komisja opublikowała projekt rozporządzenia regulującego usługi cyfrowe (ang. *Digital Services Act*, DSA[20]), w którym – w uzasadnieniu – przywołała problem dezinformacji na platformach internetowych. Dezinformacja w DSA pojawia się głównie w kontekście grupy platform „bardzo dużych" („*very large*", tj. o średniej liczbie faktycznych użytkowników obejmującej ponad 10% populacji UE, o doniosłej roli i znacznym wpływie na jej obywateli) oraz w odniesieniu do ograniczania ryzyka systemowego i zarządzania kryzysowego. DSA przywołuje inne właściwe przedmiotowo dokumenty UE, takie jak np. Unijny kodeks postępowania, oraz egzemplifikuje szczególne formy rozpowszechniania dezinformacji na platformach online – m.in. przez boty i trolle.

Współpraca UE z państwami członkowskimi oraz organizacjami pozarządowymi

Współpraca na linii UE – państwa członkowskie odbywa się na kilku płaszczyznach, ale rola krajów UE zaznacza się przede wszystkim wszędzie tam, gdzie przeważa międzyrządowy proces podejmowania decyzji, czyli głównie w Radzie oraz Radzie Europejskiej. Ponieważ zagadnienie wkładu Rady oraz roli Wysokiego Przedstawiciela zostało już poruszone wcześniej, należy zwrócić uwagę również na pozapolityczne obszary, gdzie

efektywna współpraca jest absolutnie niezbędna. Kompetencja szczególna (koordynująca) w zakresie WPZiB oraz WPBiO oznacza, że państwa członkowskie nie ograniczyły swojej suwerenności w tym obszarze i nie przekazały UE narzędzi do realizacji tych polityk. W konsekwencji poziom wiedzy i możliwości UE zależy w tym zakresie od charakteru (w tym jakości) informacji przekazanych przez państwa członkowskie.

Personel Centrum Analizy Wywiadowczej UE (INTCEN) liczył w 2019 r. ok. 100 osób, co nie jest adekwatną liczbą do prowadzenia pracochłonnych zadań na poziomie operacyjnym (np. zbierania danych). Warto tu również zwrócić uwagę, że przeszkodą bywa niedostateczne przeszkolenie pracowników INTCEN, którzy często nie należą do personelu międzynarodowego, tylko do kategorii tzw. oddelegowanych ekspertów krajowych (ang. *seconded national experts*). Rzecz jasna, personel East StratCom oraz Hybrid Fusion Cell (przynależącej do INTCEN), a zatem podmiotów, które bezpośrednio zajmują się kwestią monitorowania i odpowiedzi UE na zagrożenia hybrydowe i dezinformację, jest znacznie mniej liczny. Poza czynnikiem ludzkim występuje również niepożądane zjawisko rezerwy państw członkowskich w dzieleniu się informacjami wywiadowczymi, które bywają postrzegane jako element przewagi informacyjnej nad innymi państwami. Przykładowo, kluczowy dla *Planu działań* i uruchomiony w marcu 2019 r. System Szybkiego Ostrzegania nie został do października użyty ani razu[21]. Być może fakt sporadycznego wykorzystania RAS w czasie *infodemii* związanej z pandemią COVID-19 jest zapowiedzią przełomu i intensyfikacji współpracy.

Unia Europejska działa w relacjach z innymi podmiotami i wspiera sektor pozarządowy za pomocą instrumentów finansowych. Już w komunikacie kwietniowym *Zwalczanie dezinformacji w Internecie: podejście europejskie*, oprócz opracowania Unijnego kodeksu postępowania, Unia zobowiązała się do działania na rzecz niezależnej paneuropejskiej sieci fact-checkingowej, umiejętności korzystania z mediów (ang. *media literacy*), a także jakościowego dziennikarstwa. Dzięki funduszom z programu Horyzont 2020 (grant nr 825469) w listopadzie 2018 r. powstało międzynarodowe obserwatorium dezinformacji i analizy platform społecznościowych SOMA[22]. SOMA stanowi kompleksową platformę rozwijającą świadomość społeczną w sprawach związanych z dezinformacją i zagrożeniami hybrydowymi w drodze raportów zawierających rezultaty transgranicznej i wielojęzycznej analizy dezinformacji oraz poprzez darmowe webinary i szkolenia. SOMA utworzyła ponadto trzy narodowe centra badawcze i nawiązała kontakt z ok. 70 podmiotami trudniącymi się analizą mediów społecznościowych. Wśród innych szczególnie cennych projektów rozwijanych przez sieć można wymienić DisInfoNet, czyli darmowy program *open source*[23] umożliwiający badanie dezinformacji w makroskali przy wykorzystaniu analizy sentymentu.

Innym przykładem współpracy UE (głównie) z trzecim sektorem jest powstająca aktualnie sieć – Europejskie Obserwatorium Mediów Cyfrowych (ang. *European Digital Media Observatory*, EDMO). Ma ono na celu stworzenie – w oparciu o struktury Europejskiego Instytutu Uniwersyteckiego (ang. *European University Institute*, EUI) we Florencji – ogólnoeuropejskiego centrum, któremu podlegałyby organizacyjnie i funkcjonalnie jedno- i wielonarodowe, tworzone oddolnie ośrodki. Unia finansuje EDMO za pośrednictwem instrumentu Łącząc Europę (ang. *Connecting Europe Facility*, CEF) i przeznaczy łącznie ok. 11,5 mln euro. Poza EDMO Unia współpracuje również bezpośrednio z przedstawicielami społeczeństwa obywatelskiego m.in. poprzez zaangażowanie w wydarzenia i korzystanie z działalności eksperckiej i konsultingowej. Nie licząc wspomnianej wcześniej grupy HLEG, Unia kontaktuje się sporadycznie z organizacjami pozarządowymi. Przykładem może być współpraca Parlamentu Europejskiego z Open Information Partnership (poprzez utworzenie Specjalnego Komitetu ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne[24] w Unii Europejskiej, w tym Dezinformacji – oficjalna nazwa ang. *Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation*, INGE) oraz uczestnictwo

przedstawicieli Komisji w corocznej konferencji think-tanku EU Disinfo Lab. Ponadto Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii (DG CONNECT) w ramach zapewnienia obywatelom UE możliwości partycypacji w rozwoju polityk publicznych i rozwoju kontaktu z przedstawicielami społeczeństwa obywatelskiego uruchomiła w 2015 r. Uniwersytet DG Connect, w którym mierzy się z nowymi zagrożeniami, w tym z dezinformacją. Dodatkowo, w ramach wszechnicy Futurium, Komisja pełni rolę edukacyjną – od 2018 r. zorganizowała blisko 40 warsztatów dotyczących umiejętności korzystania z mediów.

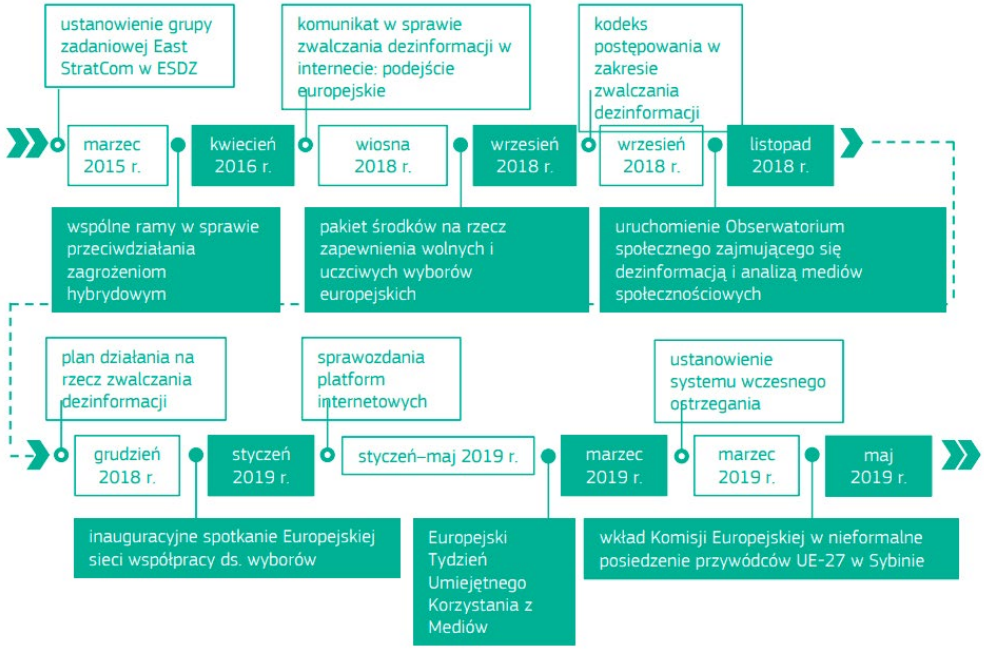
Ocena jakościowa współpracy UE z sektorem prywatnym, publicznym i organizacjami pozarządowymi

Komisja Europejska opublikowała dwa istotne raporty pozwalające na ewaluację skuteczności działań Unii Europejskiej i jakości współpracy między UE a innymi podmiotami (instytucjami, agencjami, państwami członkowskimi) oraz sektorem prywatnym (platformami z sektora mediów społecznościowych oraz organizacjami branżowymi). Pierwszym z dokumentów jest *Sprawozdanie z realizacji planu działania przeciwko dezinformacji*[25] (ang. *Report on the implementation of the Action Plan Against Disinformation*) z 14 czerwca 2019 r.

Komisja i Wysoki przedstawiciel koncentrują się na podkreśleniu sukcesów i potencjału wypracowanych rozwiązań. Przykładowo, podkreślają znaczenie współpracy międzynarodowej i znaczenie Systemu Szybkiego Ostrzegania dla wzajemnego ostrzegania. Raport mimo ogólnej pozytywnej oceny wzywa do dalszego rozwoju współpracy i budowy zdolności do przeciwdziałania dezinformacji i zagrożeniom hybrydowym. Zawiera również cząstkową ewaluację postępów w implementacji Unijnego kodeksu postępowania.

Ma to minimalne znaczenie z uwagi na to, że na podstawie samoocen oraz kilku innych raportów

Ilustracja 1. Przegląd wspólnych i skoordynowanych działań UE przeciwko dezinformacji.



Źródło: *Sprawozdanie z realizacji planu działania przeciwko dezinformacji*, s. 3.

(Komisji, ERGA, VVA) Komisja opublikowała we wrześniu 2020 r. nowy i aktualniejszy dokument roboczy[26] zawierający ewaluacje implementacji Unijnego kodeksu postępowania. Do problemów implementacyjnych dokument roboczy zaliczył niekompletne i niespójne stosowanie Unijnego kodeksu postępowania wśród platform z sektora mediów społecznościowych oraz w państwach członkowskich, szczególnie w zakresie:

- nadzoru nad miejscem publikacji reklam,
- przejrzystości finansowania reklam politycznych i tematycznych,
- integralności świadczonych usług,
- wzmacniania konsumentów i badań.

Ponadto Komisja zarzuciła sygnatariuszom brak wypracowania jednolitych definicji dotyczących wspomnianych wyżej kwestii. Dokument roboczy zidentyfikował również powiązane problemy, które wprawdzie nie zostały bezpośrednio ujęte w tym kodeksie, ale wskazują na zbyt wąski zakres jego regulacji i powodują niewłaściwe funkcjonowanie systemu – przypomnieć tu należy, że Komisja uzależniła poprzestanie na kodeksie od właściwego wdrożenia, ale także i efektywności.

Do innych problemów zaliczone zostały:

- manipulacja zachowaniem w cyberprzestrzeni (nieujęta w Unijnym kodeksie postępowania),
- mikro-celowanie (ang. *micro-targeting*) reklam politycznych,
- brak oparcia na kryterium uczciwości (ang. *fairness*) w odniesieniu do reklam politycznych,
- brak Kluczowych Wskaźników Wydajności (ang. *Key Performance Indicators*, KPIs) dla monitorowania i nadzoru nad implementacją Unijnego kodeksu postępowania.

Warto zauważyć, że dokument roboczy poświęca trzy strony na docenienie osiągnięć wdrożenia kodeksu i czterokrotnie więcej na krytykę i niedociągnięcia w implementacji. Nie ulega wątpliwości, że po roku od wejścia w życie kodeksu postępowania jakość współpracy publiczno-prywatnej pozostawia wiele do życzenia, jednak kwestią kluczową jest to, czy odpowiednim remedium byłyby inne działania po stronie instytucji UE, dla przykładu droga legislacyjna.

Opublikowany 3 grudnia 2020 r. przez Komisję *Komunikat w sprawie europejskiego planu działania na rzecz demokracji*[27] zawiera szereg kierunków przyszłego rozwoju instytucjonalnego i materialnego w zakresie przeciwdziałania zagrożeniom hybrydowym i dezinformacji. Na pierwszy plan wysuwa się zagadnienie ingerencji w procesy demokratyczne (wybory) oraz kwestie związane z jakością życia publicznego i prasą. Przykładowo zakłada on lepszą ochronę dziennikarzy oraz osób publicznych przed bezprawnymi i złośliwymi pozwami (ang. *abusive lawsuits*) oraz polepszenia jakości demokracji uczestniczącej i partycypacyjnej (ang. *participatory and deliberative*). W kontekście dezinformacji zawiera kilka niezwykle istotnych ocen i wskazuje przyszłe kierunki działań Unii. Mianowicie, Komisja w 2021 r. zaprezentuje projekt ustawodawczy dotyczący jawności sponsorowanych treści politycznych, uzupełniający kwestie uregulowane w *DSA*. Dodatkowo do (rozbudowanego już wcześniej) rozróżnienia na zagrożenia hybrydowe, dezinformację, *fake news*, ingerencje wyborcze itp. dodaje nowy katalog i zapowiada utworzenie zindywidualizowanych polityk i instrumentów do przeciwdziałania wymienionym zjawiskom.

Komisja wyróżnia: a) *misinformation* (brak polskiego odpowiednika, zazwyczaj: nieprawdziwe, wprowadzające w błąd informacje) jako fałszywe lub wprowadzające w błąd treści bez złośliwych intencji, b) dezinformację (ang. *disinformation*) jako fałszywe lub wprowadzające w błąd treści rozpowszechniane w celu oszustwa lub osiągnięcia gospodarczych lub politycznych korzyści i zdolne spowodować szkodę publiczną, c) operacje wpływu informacyjnego (ang. *information influence operations*), czyli skoordynowane wysiłki wewnętrznych lub zewnętrznych podmiotów usiłujące wpłynąć na pewną grupę docelową poprzez szereg zwodniczych (ang. *deceptive*)

środków, wliczając tłumienie niezależnych źródeł informacji w połączeniu z dezinformacją oraz d) zewnętrzną (zagraniczną) ingerencję w przestrzeń informacyjną (ang. *foreign interference in the information space*), często przeprowadzaną jako część szerszej operacji hybrydowej, która może być rozumiana jako zwodnicze wysiłki mające na celu zakłócenie swobodnego formowania się i wyrażania woli politycznej jednostek przez zagraniczny podmiot państwowy lub jego przedstawicieli. Jest to niezaprzeczalnie rewolucja w postrzeganiu zjawiska.

Podsumowanie

Unia Europejska od 2015 r. poczyniła znaczne postępy w zakresie zwiększania odporności systemowej na zagrożenia hybrydowe oraz dezinformację.

W krótkim czasie UE:

- zbadała, zdefiniowała i skonceptualizowała zjawiska tak, by stworzona siatka pojęciowa odpowiadała zróżnicowanym zadaniom systemu instytucjonalnego UE;
- przeprowadziła kompleksową analizę strategicznego ryzyka i potencjalnych konsekwencji zagrożeń hybrydowych / dezinformacji dla różnych sektorów;
- opracowała konsekwentnie realizowany *Plan działania* oraz plan z grudnia 2020 r.;
- wyznaczyła organy właściwe do rozwoju architektury bezpieczeństwa w postaci Komisji i Wysokiego Przedstawiciela oraz włączyła Parlament – głównie w zakresie obcych ingerencji w procesy demokratyczne;
- rozwinęła własne możliwości koordynacyjne w ramach INTCEN oraz utworzyła Grupę Zadaniową East StratCom (a następnie dwie kolejne, ukierunkowane na Afrykę i Bliski Wschód oraz Bałkany Zachodnie);
- utworzyła Komórkę UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych oraz Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym;
- opracowała Unijny kodeks postępowania, intensyfikując współpracę z firmami z sektora mediów społecznościowych oraz stowarzyszeniami branżowymi;
- uruchomiła znaczne środki na budowę infrastruktury odpornościowej, współtworząc i wspierając powstanie paneuropejskich sieci monitorujących, weryfikujących i badawczych dla zagrożeń hybrydowych i dezinformacji;
- ułatwiła współudział społeczeństwa obywatelskiego w tworzeniu polityk publicznych;
- zaangażowała się na rzecz edukacji obywatelskiej i podnoszenia świadomości co do ryzyka niesionego przez zagrożenia hybrydowe i dezinformację.

Mając na względzie fakt, że zarówno zagrożenia hybrydowe, jak i dezinformacja rozwijają się niezwykle dynamicznie, a zmiany polityczne, instytucjonalne oraz prawne są reaktywne i wtórne wobec zagrożeń, powyższe dokonania są imponujące. Z całą pewnością nie można jednak stwierdzić, że udało się osiągnąć cel, czyli stworzyć demokratyczny i funkcjonujący system odporności na wspomniane zagrożenia. Wiele do życzenia pozostawia jakość współpracy z sektorem publicznym (zwłaszcza z państwami członkowskimi) oraz prywatnym. Jakość wdrożenia Unijnego Kodeksu Postępowania stawia pod znakiem zapytania przyszły samoregulacyjny kształt partnerstwa publiczno-prywatnego między Unią a gigantami sektora mediów społecznościowych. Dostęp do rzetelnej informacji, jakościowe dziennikarstwo oraz wiarygodne instytucje są podstawą działania społeczeństwa informacyjnego i funkcjonującej demokracji. Pozostaje mieć nadzieję, że Unia, która – jak wynika z opublikowanych dokumentów – rozumie powagę zagrożenia i niedociągnięcia własnych działań, będzie w stanie jeszcze skuteczniej chronić swoich obywateli.

PRZYPISY

1 Koordynujące – w zakresie Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB, ang. CFSP) oraz stanowiącej jej integralną część Wspólnej Polityki Bezpieczeństwa i Obrony (WPBiO, ang. CSDP).

2 Miękkie prawo (ang. *Soft law*) to wywodzące się z prawa międzynarodowego publicznego i często spotykane w prawie UE niewiążące akty prawne, które mimo to mają znaczenie regulacyjne. Do przykładów należą zalecenia i opinie (ujęte w art. 288 TFUE), a także zielone i białe księgi, komunikaty, komunikaty wyjaśniające (interpretacyjne), kodeksy dobrej praktyki, programy działania, sprawozdania oraz wytyczne. Więcej: Ziemowit Cieślik, *VI. Rola Sejmu w Unii Europejskiej*, s. 155, [online]: http://orka.sejm.gov.pl/wydbas.nsf/0/F873B8E7897A0892C1257F03002E76DC/$File/Strony%20odPrzewodnik-7.pdf.

3 Komisja Europejska, *Wspólne ramy dotyczą[c]e przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*, JOIN(2016) 18 final, 6 kwietnia 2016, [online]: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52016JC0018.

4 Komisja Europejska, *Zwalczanie dezinformacji w Internecie: podejście europejskie*, 26 kwietnia 2018, [online]: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018DC0236.

5 Sposób, w jaki Unia odwołuje się do zagadnień dezinformacji i *fake news*, wydaje się niekonsekwentny. O ile w opisanym przypadku Unia utożsamia dezinformację z *fake news*, raport Wspólnego Centrum Badawczego UE z 2018 r. *The digital transformation of news media and the rise of disinformation and fake news* postrzega je jako oddzielne zjawiska i odmiennie definiuje.

6 Rada Europejska, *Oświadczenie*, EUCO 158/14, 29 lipca 2014, [online]: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/144158.pdf.

7 Rada Europejska, *Konkluzje z 19-20 marca 2015*, EUCO 11/15, 20 marca 2015, [online]: https://www.consilium.europa.eu/media/21878/st00011pl15.pdf.

8 Komisja Europejska, *Plan działań na rzecz komunikacji strategicznej*, Ares(2015)2608242, 22 czerwca 2015, [online]: https://archive.vn/iaGkd.

9 Rada Europejska, Konkluzje z 25-26 czerwca 2015, EUCO 22/15, 26 czerwca 2015, [online]: https://data.consilium.europa.eu/doc/document/ST-22-2015-INIT/en/pdf.

10 Ciekawostką jest błąd w tłumaczeniu oficjalnej wersji polskiej kolejnego z opisywanych dokumentów - Wspólnych ram, w którym powołując się na Konkluzje z czerwca 2015 polska wersja tłumaczy *recall* jako odwołać, a nie ponownie wezwać. Autor niniejszego artykułu dementuje – Unia nie odwołała wówczas mobilizacji instrumentów finansowych do przeciwdziałania zagrożeniom hybrydowym.

11Komisja Europejska, *Wspólne ramy*..., op. cit., JOIN(2016) 18 final, 6 kwietnia 2016, [online]: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52016JC0018.

12 Zadania i kompetencje Hybrid Fusion Cell i Hybrid CoE zostały rozszerzone w drodze postanowień Wspólnego komunikatu z 13 czerwca 2018 r. *Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe*.

13 Parlament Europejski, *Sprawozdanie w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich*, 2016/2030(INI), 14 października 2016, [online]: https://www.consilium.europa.eu/media/33471/22-euco-final-conclusions-pl.pdf.

14 Rada Europejska, *Posiedzenie Rady Europejskiej (22 marca 2018 r.) – Konkluzje*, EUCO 1/18, 22 marca 2018, [online]: https://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf.

15 Ibidem, s. 5.

16 Komisja Europejska, *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final)*, 1 marca 2018, [online]: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50095.

17 Komisja Europejska, *Plan działania na rzecz zwalczania dezinformacji*, 5 grudnia 2018, [online]: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018JC0036.

18 Poza Unijnym kodeksem postępowania 1 marca 2018 r. powstały jeszcze *Zalecenia Komisji (2018/334) w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie*, które odnosiły się jednak bardziej do treści nielegalnych i terroryzmu niż dezinformacji.

19 Między innymi AACC, EACA, EDIMA, IAB, SAR, UBA, WFA, AKA oraz Kreativitet & Kommunikation.

20 Komisja Europejska, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, COM(2020) 825 final, 15 grudnia 2020, [online]: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&from=EN.

21 Samuel Stolton, *EU Rapid Alert System used amid coronavirus disinformation campaign*, Euractiv, 4 marca 2020, [online]: https://www.euractiv.com/section/digital/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/.

22 CORDIS, *Social Observatory for Disinformation and Social Media Analysis*, grant no. 825469, [online]: https://cordis.europa.eu/project/id/825469.

23 Funkcjonalna wersja nie została jeszcze opublikowana jednak wersję demo można zobaczyć pod następującym adresem: http://193.204.157.124/.

24 W 2019 r. Parlament Europejski wydał również krótki dokument pt. *Online disinformation and the EU's response*, w którym rozpoznaje zagrożenia oraz podkreśla potencjalne konsekwencje dezinformacji dla wyborów europejskich.

25 Komisja Europejska, *Sprawozdanie z realizacji planu działania przeciwko dezinformacji*, JOIN(2019) 12 final, 14 czerwca 2019, [online]: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52019JC0012.

26 Komisja Europejska, *Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement*, SWD(2020) 180 final, 10 września 2020, [online]: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212.

27 Komisja Europejska, *Komunikat Komisji w sprawie europejskiego planu działania na rzecz demokracji*, COM(2020) 790 final, 3 grudnia 2020, [online]: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0790.

Tomasz Piekarz

Legislacja i polityka Polski wobec zjawiska dezinformacji

Zwalczanie dezinformacji leży w sferze zainteresowania organów i instytucji zajmujących się bezpieczeństwem narodowym. ***Koncepcja obronna Rzeczypospolitej Polskiej*** opublikowana w 2017 r. przez Ministerstwo Obrony Narodowej (MON) wspomina o wykorzystaniu dezinformacji przez Federację Rosyjską jako aktywnego środka realizowania polityki[1]. Do zagrożenia ze strony Rosji odnosi się również przyjęta w 2020 r. ***Strategia Bezpieczeństwa Narodowego RP***, która wymienia dezinformację jako jeden z pozamilitarnych elementów działań poniżej progu wojny w celu „destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych"[2]. Opisując środowisko bezpieczeństwa RP, Strategia zwraca również uwagę na szczególną rolę cyberprzestrzeni, która w kontekście rewolucji cyfrowej stwarza coraz większe pole do manipulacji informacją. Ponadto pośród celów strategicznych wyróżniono „zapewnienie bezpiecznego funkcjonowania państwa i obywateli w przestrzeni informacyjnej"[3] oraz wynikające z niego cztery działania do zrealizowania:

1. Budowa zdolności do ochrony przestrzeni informacyjnej (włączając systemowe zwalczanie dezinformacji) definiowanej jako przenikające się warstwy przestrzeni wirtualnej, fizycznej i poznawczej.
2. Stworzenie jednolitego systemu komunikacji strategicznej państwa.
3. Aktywne przeciwdziałanie dezinformacji poprzez budowę zdolności i procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych.

4. Dążenie do zwiększania świadomości społecznej o zagrożeniach związanych z manipulacją informacją poprzez edukację w zakresie bezpieczeństwa informacyjnego[4].

Strategia zawiera rekomendacje przygotowane przez **Biuro Bezpieczeństwa Narodowego (BBN)**, które opracowało również koncepcję systemu komunikacji strategicznej i zwalczania dezinformacji składającego się z pięciu obszarów:

1. Utworzenie na najwyższym szczeblu zarządzania państwem komórki ds. komunikacji strategicznej. Powstanie komórki miałoby być odpowiedzią na potrzebę dostępu instytucji państwa do szerokiej gamy kanałów komunikacji i mediów. Komórka miałaby także wyposażać instytucje w „narzędzia rozpoznawania oraz oddziaływania na sytuację w różnych obszarach bezpieczeństwa narodowego"[5]. Do spektrum jej działalności BBN zalicza również: prognozowanie i planowanie działań komunikacyjnych biorących pod uwagę aktualne wydarzenia i długoterminowe prognozy, a także formułowanie strategii komunikacji, tworzenie kluczowych przekazów dla podmiotów podległych Radzie Ministrów, opracowywanie scenariuszy reakcji na kampanie dezinformacyjne oraz gromadzenie przekazów medialnych o potencjalnie wrażliwych sytuacjach.
2. Aktywne przeciwstawianie się dezinformacji poprzez ciągłe monitorowanie, analizowanie i kształtowanie polskiej przestrzeni informacyjnej. Korzystając z doświadczeń własnych oraz zagranicznych partnerów, należy dążyć do budowy zdolności i procedur w celu osiągnięcia gotowości do zwalczania dezinformacji, utrzymując jednocześnie inkluzywność systemu polegającą na włączeniu organizacji pozarządowych, platform internetowych, przedstawicieli mediów i obywateli do pozyskiwania i analizowania informacji ukazujących się w przestrzeni informacyjnej.
3. Budowa świadomości społecznej i edukacji o bezpieczeństwie informacyjnym, która powinna być zaimplementowana jako obowiązkowy element kształcenia. Jego celem powinna być m.in. nauka krytycznego myślenia wśród uczniów, rozpoznawania dezinformacji i jej rodzajów.
4. Aktywna obrona cyberprzestrzeni, której struktury powinny być zarówno ofensywne, jak i defensywne. Powinna ona m.in. monitorować i reagować na zagrożenia nie tylko na terytorium Polski, ale również podczas działań polskich placówek dyplomatycznych oraz sił zbrojnych poza granicami kraju. Według BBN znaczna część tych zadań jest realizowana przez Krajowy System Cyberbezpieczeństwa.
5. Tworzenie polskiego *soft power* przy udziale sektora rządowego, pozarządowego i prywatnego działających autonomicznie, ale posiadających precyzyjne priorytety i cele. Konieczna jest również budowa kanałów komunikacji wykorzystujących m.in. kulturę masową. Kreacja *soft power* powinna być koordynowana przez wyznaczone do tego podmioty uwzględniające cele polityki historycznej oraz narzędzia współpracy międzynarodowej i dyplomacji.

Według BBN utworzenie systemu wymaga od administracji państwa ponadresortowej współpracy na wielu płaszczyznach. Ponadto całościowa ochrona sfery informacyjnej państwa wymaga aktywizacji środowisk pozarządowych i akademickich, sektora prywatnego, a także samych obywateli, gdyż skuteczna walka z dezinformacją powinna opierać się na pozytywnym wsparciu oddolnych inicjatyw[6]. BBN opracowało również projekt *Doktryny bezpieczeństwa informacyjnego RP*, który jednakże od publikacji w 2015 r. pozostaje wciąż w fazie planowania. Doktryna wyróżnia m.in. dezinformację jako jedno z najpoważniejszych zagrożeń wynikających z niedoskonałego funkcjonowania społeczeństwa obywatelskiego, a także funkcjonowania w cyberprzestrzeni[7].

Na poziomie ministerialnym w temat dezinformacji angażuje się **Ministerstwo Sprawiedliwości** poprzez projekt ustawy z 15 stycznia 2021 r.

o ochronie wolności słowa w internetowych serwisach społecznościowych, który wymierzony jest w *fake news* i arbitralne blokowanie kont użytkowników przez największe platformy społecznościowe (posiadające ponad milion użytkowników). Projekt nakłada szereg obowiązków na serwisy, które m.in. „nie będą mogły według własnego uznania usuwać wpisów ani blokować kont użytkowników, jeśli treści na nich zamieszczone nie naruszają polskiego prawa”[8]. Projekt dodatkowo nakłada na serwis obowiązek sporządzania sprawozdania o sposobie rozstrzygania reklamacji, gdy ich liczba przekroczy 100 w roku kalendarzowym, które następnie będzie dostępne publicznie w Dzienniku Urzędowym Urzędu Komunikacji Elektronicznej (UKE) niezwłocznie po wystąpieniu przez platformę z wnioskiem o jego opublikowanie. Projekt przewiduje również powołanie od jednego do trzech przedstawicieli platformy, którzy będą reprezentowali ją w czynnościach sądowych oraz odpowiadali za rozpatrywanie reklamacji i kontakty z Radą Wolności Słowa. Wszyscy reprezentanci muszą znać język polski. Platformy zobowiązane będą także do ustanowienia wewnętrznych postępowań kontrolnych w zakresie reklamacji użytkowników na dezaktywacje kont oraz ograniczanie do nich dostępu przez zmniejszanie widoczności, a także skarg na rozpowszechnianie treści o charakterze bezprawnym – przy czym platforma ma 48 godzin na ich rozpatrzenie. Projekt zakłada powołanie Rady Wolności Słowa, w skład której wchodzi pięciu członków wybieranych przez sejm większością 3/5 na sześcioletnią kadencję. Ponadto członkiem Rady może zostać jedynie osoba posiadająca wyższe wykształcenie prawnicze lub wiedzę w zakresie nowych technologii lub językoznawstwa. Instytucja ta kontroluje przestrzeganie przez portale nowych obowiązków i stanowi drugą instancję postępowania, do której użytkownicy mogą zgłaszać się z odwołaniem od niepożądanej decyzji właściciela platformy. W tym zakresie projekt jest rozszerzeniem opisanego w podrozdziale o mediach społecznościowych tzw. punktu kontaktowego. W przypadku niewywiązywania się przez serwisy z obowiązków nałożonych ustawą Rada może w drodze decyzji nałożyć karę od 50 tysięcy do 50 milionów złotych. Projekt zakłada mocne związanie nowego organu z UKE, który zapewni obsługę merytoryczną, administracyjną i biurową, a także będzie finansować działalność Rady. Projekt wprowadza również możliwość skargi na bezprawne treści (w tym naruszające dobra osobiste), którą platformy muszą rozpatrzeć także w ciągu 48 godzin. Brak terminowej reakcji ma skutkować przekazaniem sprawy do Rady, która będzie prowadziła postępowania wyłącznie w trybie elektronicznym. Projekt ustawy przewiduje również powołanie nowej instytucji – tzw. ślepego pozwu, który pozwoli poszkodowanym przez nieznaną osobę (np. konto nieprawdziwej osoby na platformie społecznościowej) złożyć pozew o ochronę dóbr osobistych, wskazując jedynie adres URL, pod którym zostały opublikowane treści, datę i godzinę publikacji oraz nazwę profilu[9]. Projekt legislacyjny będzie poddany dalszym pracom na poziomie rządu, służącym jego przyjęciu do porządku prawnego RP.

W walkę z dezinformacją angażuje się również **Ministerstwo Spraw Zagranicznych** (MSZ). MSZ koncentruje się na: podnoszeniu świadomości urzędników, budowaniu własnych zdolności instytucjonalnych, współpracy z komórkami komunikacji strategicznej partnerów z UE i NATO, projektowaniu i prowadzeniu kampanii informacyjnych, a także wsparciu polskich organizacji pozarządowych. MSZ utworzyło w 2019 r. w swoich strukturach komórkę odpowiedzialną za identyfikację, przeciwdziałanie i reagowanie na dezinformację dotyczącą priorytetów polskiej polityki zagranicznej. MSZ organizuje również szkolenia i warsztaty w zakresie przeciwdziałania dezinformacji, które kieruje m.in. do dziennikarzy, administracji państwowej i uczniów Krajowej Szkoły Administracji Publicznej oraz Akademii Dyplomatycznej. Ponadto MSZ aktywnie wspiera organizacje pozarządowe działające w obszarze zwalczania dezinformacji w kraju i zagranicą, a także współpracuje z partnerami z UE i NATO, angażując się finansowo i kadrowo w unijną komórkę ds. przeciwdziałania dezinformacji StratCom w strukturach Europejskiej Służby Działań Zewnętrznych.

Polska jest także członkiem *The European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE) oraz uczestniczy w projektach *NATO Strategic Communications Centre of Excellence* (której szefem sztabu w latach 2018–2021 jest komandor porucznik Grzegorz Łyko[10]). MSZ jest także resortem koordynującym współpracę unijną w ramach unijnego *Rapid Alert System*[11].

MSZ miało także wkład w powołanie w 2018 r. Zespołu Roboczego ds. Zagrożeń Hybrydowych afiliowanego przy Zespole Zarządzania Kryzysowego **Rządowego Centrum Bezpieczeństwa** (RCB)[12], który jest istotnym ogniwem zapobiegania, przeciwdziałania i reagowania na zagrożenia hybrydowe, do których zalicza się dezinformację. Rolą Zespołu jest również analiza sytuacyjna i koordynacja działań w zakresie przygotowania struktur, narzędzi identyfikacji i obrony przed działaniami hybrydowymi. Prowadzi on również monitoring zagrożeń, ocenia ryzyko wystąpienia sytuacji kryzysowych wywołanych działaniami hybrydowymi, a także odpowiada za przygotowanie planu reagowania i koordynację jego wykonania przez organy administracji rządowej, instytucji i służb[13]. Zespół powstał w odpowiedzi na wnioski z ćwiczeń Systemu Reagowania Kryzysowego NATO CMX16 i CMX17, które wskazywały na konieczność powołania odpowiedniej komórki na szczeblu rządowym. Działalność RCB koncentruje się również na publikacjach kierowanych do ministrów i innych decydentów państwowych oraz szefów służb. Jedną z publikacji jest tworzony m.in. przez RCB *Monitor bezpieczeństwa granicy wschodniej RP – zewnętrznej granicy UE*, który zawiera rozdział *Bezpieczeństwo informacyjne* analizujący „najważniejsze działania dezinformacyjne dotyczące Polski, mające budować negatywny obraz RP na zewnątrz, a także oddziaływać na opinię publiczną i procesy społeczno-polityczne w kraju"[14]. RCB zaangażowane jest również w szereg działań eksperckich o mniejszej skali, omawiając zagrożenia dezinformacji i wojny informacyjnej na łamach „Biuletynu Analitycznego" RCB, a także poruszając je podczas konferencji. Niemniej jednak są to jednostkowe i jednorazowe działania[15].

Jako podmiot zaangażowany w zwalczanie dezinformacji należy wyróżnić również **państwowy instytut badawczy NASK** (Naukowa i Akademicka Sieć Komputerowa). Podstawowym obszarem działalności NASK są działania związane z zapewnianiem bezpieczeństwa Internetu, w ramach których instytut zajmuje się dezinformacją. W tym zakresie NASK wydaje zarówno cykliczne eksperckie raporty uwzględniające zagrożenia dezinformacją (raporty *Cyberbezpieczeństwo A.D. 2018* oraz *2019*), prowadzi kampanie informacyjne (#OznaczDezinfo – przeciw infodemii o koronawirusie) i badania społeczne[16], a także warsztaty i szkolenia (np. dla komitetów wyborczych i przedstawicieli mediów przed wyborami do europarlamentu w 2019 r.)[17]. NASK jest również podmiotem, który stworzył portal BezpieczneWybory.pl wraz z ówczesnym Ministerstwem Cyfryzacji oraz zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) z MON i Agencji Bezpieczeństwa Wewnętrznego (ABW), który został powołany do pełnienia roli informacyjnej i edukacyjnej[18].

W zwalczanie dezinformacji włączyła się również Polska Agencja Prasowa (PAP) oraz agencja rządowa GovTech Polska. Wspólnie uruchomiły projekt #FakeHunter, który ma na celu „demaskowanie nieprawdziwych wiadomości dotyczących wirusa SARS-CoV-2"[19]. Dostrzegając sukces projektu, postanowiono rozszerzyć go również o rynek finansowy, co uczyniono przy udziale Komisji Nadzoru Finansowego (KNF)[20].

Studium przypadku współpracy organów państwowych w instytucjach UE może stanowić powołana na mocy obowiązującej w Polsce konstytucji z 1997 r. **Krajowa Rada Radiofonii i Telewizji** (KRRiT), która zgodnie z ustawą o radiofonii i telewizji „stoi na straży wolności słowa w radiu i telewizji, samodzielności nadawców i interesów odbiorców oraz zapewnia otwarty i pluralistyczny charakter radiofonii i telewizji"[21]. KRRiT jest członkiem powstałej w 2014 r. Europejskiej Grupy Regulatorów ds. Audiowizualnych Usług Medialnych (ERGA), która wspiera KE w monitorowaniu

zobowiązań zawartych w *Kodeksie postępowania w zakresie zwalczania dezinformacji*, będąc jednocześnie platformą zrzeszającą wysokich przedstawicieli niezależnych krajowych regulatorów rynków mediów audiowizualnych. ERGA prowadzi monitoring zobowiązań poprzez dedykowane eksperckie grupy i podgrupy zadaniowe, w których skład wchodzą przedstawiciele organów regulacyjnych państw członkowskich UE. Reprezentanci KRRiT należą do Grupy Zadaniowej nr 1, Podgrupy Roboczej ERGA ds. pluralizmu mediów, której zadaniem było monitorowanie realizacji zobowiązań zawartych w ww. Kodeksie przez Google, Facebook i Twitter. Monitorowanie odbyło się w dwóch fazach:

1. Pierwsza miała miejsce przed rozpoczęciem kampanii wyborczej do PE, a jej celem była weryfikacja wykonania przez sygnatariuszy obowiązków zapewniających wdrożenie mechanizmów zwiększających ochronę procesów wyborczych przed dezinformacją.
2. Druga stanowiła kompleksową ocenę realizacji wszystkich zobowiązań przyjętych w Kodeksie.

KRRiT w celu realizacji pierwszej fazy powołała tymczasowy zespół składający się z jej ekspertów, który analizował w ramach Podgrupy Roboczej reklamy polityczne pod kątem „zapewnienia przez ww. sygnatariuszy kodeksu transparentnych zasad i procedur rozpowszechniania tego rodzaju przekazów reklamowych, stopnia odróżnialności i rozpoznawalności reklam politycznych, ich cen, tożsamości podmiotów zlecających reklamy, zasięgu oddziaływania reklam, jej grup docelowych, efektywności wprowadzonych procedur rejestracyjnych oraz identyfikacji i usuwania reklam niespełniających wymogów rejestracyjnych, a także dostępności dla użytkowników danych przechowywanych w archiwach/bibliotekach poszczególnych platform i serwisów”[22]. Bazę analizy prowadzonej od 13 do 17 maja 2019 r. stanowiło kilkadziesiąt reklam politycznych polskich komitetów wyborczych – choć początkowo zakres badań ERGA miał być szerszy, został ograniczony ze względu na zbliżający się termin wyborów do Parlamentu Europejskiego oraz limitowany dostęp regulatorów do danych. Należy podkreślić, że nie wszystkie państwa będące członkami ERGA „wyraziły gotowość do przeprowadzenia tego monitoringu, powołując się m.in. na brak skutecznych narzędzi do weryfikacji, odpowiednio przeszkolonych specjalistów oraz zbyt ograniczony czas na zebranie i analizę danych”[23]. Ostatecznie 13 spośród 16 organów regulacyjnych, które zadeklarowały udział w badaniu, dokonało kompletnego monitoringu. Analiza KRRiT wykazała częściowe wdrożenie postanowień Kodeksu przez monitorowane podmioty[24]. W ramach drugiej fazy monitoringu KRRiT analizowała około 80 reklam politycznych na platformach Facebook i Google przed wyborami parlamentarnymi w Polsce (13 października 2019 r.). Badania zostały przeprowadzone przez tę samą grupę ekspertów stosujących ponownie metodologię wykorzystaną przy fazie pierwszej. Zespół powołany przez KRRiT nie zidentyfikował znacznych usprawnień w działaniu i procedurach platform odnoszących się do przejrzystości reklam politycznych od czasu badań z maja[25]. Biorąc pod uwagę ustawowe cele stojące przed KRRiT, jak i doświadczenie w monitoringu zobowiązań unijnego Kodeksu, regulator w obliczu nowych wyzwań związanych z rozwojem form dezinformacji (także w mediach tradycyjnych) jest wskazywany jako ten, który powinien przyjąć część odpowiedzialności za jej zwalczanie w Polsce. Jak wynika z odpowiedzi Przewodniczącego KRRiT na pytania zadane przez Rzecznika Praw Obywatelskich dotyczące mowy nienawiści w telewizji, Rada pracuje „nad przygotowaniem dokumentu poświęconego przeciwdziałaniu zjawiskom tzw. *fake news*, dezinformacji oraz mowy nienawiści w przestrzeni medialnej”[26]. Raport, datowany na grudzień 2020 r., przedstawił działania podejmowane przez instytucje europejskie i wybrane kraje członkowskie w dziedzinie walki z dezinformacją, a także ograniczania zjawiska w Polsce, omawiając szczególne w tym kontekście znaczenie edukacji medialnej rozumianej jako kształtowanie umiejętności korzystania z mediów[27].

Działania organizacji pozarządowych w Polsce

Działania organizacji pozarządowych w Polsce ogniskują się na kilku obszarach:

- pracy eksperckiej skierowanej do decydentów w administracji państwowej oraz zainteresowanych grup,
- edukacji medialnej społeczności (ang. *media literacy*),
- promowaniu jakościowego dziennikarstwa,
- fact-checkingu.

Działalność ekspercką prowadzi **Fundacja Centrum Analiz Propagandy i Dezinformacji**. Wśród jej celów znajduje się m.in. zwiększanie wiedzy społecznej na temat weryfikacji informacji oraz podejmowanie inicjatyw edukacyjnych i badawczych w zakresie propagandy i dezinformacji[28]. Centrum w ramach pracy eksperckiej wydaje publikacje i rekomendacje dla administracji państwowej np. w ramach komunikacji strategicznej Polski, w publikacji *StratCom: perspektywa polska. Struktura systemu komunikacji i analiza kampanii na temat 20. rocznicy przystąpienia polski do NATO*[29]. Zagadnieniami dezinformacji i bezpieczeństwem środowiska informacyjnego zajmuje się również **Fundacja INFO OPS Polska**. Fundacja prowadzi szereg projektów związanych z publikacjami eksperckimi i warsztatami. Jednym z nich jest INFO OPS EXE organizowany we współpracy ze wspomnianą już rządową agencją GovTech Polska podczas wydarzenia GovTech Festival. Jego celem jest rozwój kompetencji w zakresie rozpoznawania dezinformacji w środowisku wirtualnym[30]. Ponadto Fundacja sprawuje patronat merytoryczny nad projektem Disinfo Digest (badania i przeciwdziałanie manipulacji środowiskiem informacyjnym) oraz przeprowadza analizy rozpoznania operacji informacyjnych i bezpieczeństwa środowiska informacyjnego[31]. W ramach działalności eksperckiej należy nieskromnie wymienić także **Instytut Kościuszki**, w którym od 2019 r. funkcjonuje zespół CYBERSEC Disinfo Lab. Zespół zaangażowany jest w projekt Prozodia, który rozwija w konsorcjum z Akademią Górniczo-Hutniczą w ramach grantu przyznanego przez Narodowe Centrum Badań i Rozwoju. Celem projektu jest „stworzenie metodologii oraz rozwiązań informatycznych wspierających analityka badającego zjawisko dezinformacji w cyberprzestrzeni"[32]. Działania prowadzone przez Instytut Kościuszki służą wypracowaniu metodologii pracy analityka – w tym celu zespół monitoruje powstawanie i rozprzestrzenianie się narracji dezinformacyjnych, a także prowadzi cykliczną analizę polskiej przestrzeni informacyjnej[33]. CYBERSEC Disinfo Lab współpracuje również z Open Information Partnership (zrzeszenie europejskich organizacji pozarządowych, portali informacyjnych i podmiotów rynku medialnego mające na celu wspomaganie kooperacji i przeciwdziałania dezinformacji i propagandzie, a także promowania rzetelnego dziennikarstwa), wydając raporty eksperckie m.in. o dezinformacji w polskiej cyberprzestrzeni związanej z pandemią COVID-19[34]. Instytut jest również członkiem organizacji stworzonej przez KE – Social Observatory for Disinformation and Media Analysis (SOMA), która ma na celu „wspomaganie i rozwijanie europejskiej społeczności podmiotów zwalczających dezinformację"[35].

Według istniejących badań „podejmowane dotychczas działania edukacyjne, zmierzające do nauczenia młodych użytkowników krytycznego odbioru mediów, mają pozytywny efekt na ochronę przed skutkami dezinformacji"[36]. W opinii NASK działania te zarówno w Polsce, jak i wielu innych państwach członkowskich zostały w dominującej części zagospodarowane przez sektor pozarządowy[37]. Aktywność w tym obszarze prowadzi **Stowarzyszenie Demagog** poprzez projekt Akademia Fact-Checkingu, który kieruje nie tylko do uczniów, studentów i nauczycieli, ale także do biznesu i seniorów. Dotychczas Stowarzyszenie przeprowadziło 150 warsztatów i szkoleń dla 3800 uczestników, współpracując w ich realizacji m.in. z Instytutem Kościuszki (podczas CYBERSEC for YOUTH) czy też Konsulatem Generalnym USA w Krakowie[38]. Stowarzyszenie stworzyło również

przeglądarkową grę edukacyjną *Fajnie, że wiesz*, która ma na celu naukę rozpoznawania fałszywych informacji[39]. W tym zakresie wyróżnić należy również projekt Edukacja Medialna mający na celu wykształcenie umiejętności krytycznego odbioru mediów, który prowadzi **Fundacja Nowoczesna Polska**. Jest to kompleksowy program nauczania udostępniony za darmo i dostosowany do wszystkich etapów kształcenia. Serwis Edukacja Medialna działa pod honorowym patronatem Ministerstwa Kultury i Dziedzictwa Narodowego oraz Ministerstwa Edukacji i Nauki[40]. Własny program edukacyjny dla szkół rozwinął również **Ośrodek Analiz Cegielskiego**. Projekt Sposób na Dezinformację zakłada przeprowadzenie 50 lekcji na terenie Polski we współpracy z lokalnymi organizacjami, które zakwalifikują się do programu, a następnie ich przedstawiciele po przejściu programu przygotowującego będą mogli kształcić uczniów szkół ponadpodstawowych[41].

Działania trzeciego sektora skupiają się również na wsparciu dziennikarzy, którym często nieintencjonalnie zdarza się powielać nieprawdziwe lub mylące informacje ze względu na ich przytłaczającą ilość i trudność w weryfikacji. W celu ograniczenia błędów dziennikarskich **Fundacja Panoptykon** oraz **Fundacja Reporterów** stworzyły publikację będącą podręcznikiem pt. *Stop dezinformacji. Przewodnik dla dziennikarzy i redakcji*. Dokument wydany we wrześniu 2019 r. (przed wyborami parlamentarnymi w Polsce) skupia się na rozwoju umiejętności: weryfikacji informacji i jej źródeł, relacjonowania wyborów parlamentarnych i ograniczania wpływu dezinformacji na proces wyborczy oraz długoterminowej budowy wizerunku i pozycji redakcji jako rzetelnej i godnej zaufania[42]. Odrębne aktywności związane ze szkoleniem dziennikarzy w sferze przeciwdziałania i zwalczania dezinformacji prowadzi Fundacja Reporterów (skupiona na dziennikarstwie śledczym). W zakresie oferowanych warsztatów Fundacja naucza „dziennikarstwa śledczego, pozyskiwania i weryfikacji informacji, nowoczesnych metod i narzędzi dziennikarskich, pracy z mediami społecznościowymi i otwartymi źródłami (OSINT), fact-checkingu, bezpieczeństwa w sieci czy prowadzenia portali internetowych i zarządzania zespołami newsowymi"[43]. Fundacja dotychczas prowadziła warsztaty i szkolenia w Polsce i wielu państwach europejskich, na konferencjach, w redakcjach oraz na uczelniach wyższych[44].

Dużą aktywność polskich organizacji pozarządowych w obszarze przeciwdziałania i zwalczania dezinformacji można zaobserwować w *fact-checkingu*. Wspomniane już Stowarzyszenie Demagog poza Akademią Fact-Checkingu zajmuje się głównie weryfikacją obietnic i wypowiedzi polityków. Stowarzyszenie jest pierwszą i jak dotychczas (styczeń 2021 r.) jedyną organizacją tego typu w Polsce, która należy do Międzynarodowej Sieci Fact-Checkingowej (IFCN) zrzeszającej ponad 70 organizacji z całego świata, które przyjęły wspólne zasady sprawdzania faktów. Demagog, dołączając do IFCN, zyskał możliwość udziału w programie niezależnej weryfikacji informacji Facebooka[45]. W ramach weryfikacji informacji (także zgłaszanych przez obywateli) i zwalczaniu *fake news* Stowarzyszenie tworzy analizy i raporty, a także prowadzi comiesięczny, ekspercki newsletter Demagog INFOSKAN zawierający analizy dezinformacji[46]. Najbardziej rozpoznawalny polski portal zajmujący się m.in. *fact-checkingiem*, a jednocześnie drugi obok Demagoga uwzględniony na liście Reporters' Lab stworzonej przez Duke University, to OKO.press prowadzony przez **Fundację Ośrodek Kontroli Obywatelskiej OKO**[47]. Portal koncentruje się na weryfikacji faktów i wypowiedzi polityków, a także na dziennikarstwie śledczym[48] i cieszy się dużą popularnością – nr 7 wśród najbardziej opiniotwórczych portali internetowych w Polsce i nr 1 pośród nowych marek mediów internetowych (badania Digital News Report 2020)[49]. Jednocześnie portal wyróżnia się spośród analogicznych organizacji zaangażowaniem w komentowanie wydarzeń polskiej sceny politycznej, a jego powstanie w 2016 r. zostało wsparte finansowo m.in. przez Polityka Sp. z o.o. S.K.A. i Agora Holding Sp. z o.o. (wydawcy czołowych mediów liberalnych w Polsce) i było odpowiedzią na „losy demokracji i mediów w Polsce rządzonej przez

PiS”[50]. Własny projekt z tego zakresu prowadzi również wspomniany Ośrodek Analiz Cegielskiego, który założył portal odfejkuj.info zajmujący się weryfikacją zgłoszonych informacji, a także tworzeniem własnych analiz i artykułów. Powstanie portalu zostało wsparte przez Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018–2030[51]. Należy zaznaczyć, że poza organizacjami pozarządowymi w zwalczanie dezinformacji i *fake news* angażują się również przedsiębiorstwa medialne, tworząc własne portale: konkret24.pl (Grupa TVN), Demaskator24.pl (Agencja Informacyjna AIP 24 – Polska Press Grupa) i Antyfake (HGA Media). Jak podkreśla NASK, żaden z powyższych projektów nie angażuje się we współpracę międzynarodową w ramach europejskich inicjatyw. Organizacje nie mają również wspólnej linii zwalczania dezinformacji i działają niezależnie od siebie[52].

Działania mediów społecznościowych w Polsce

Polski rynek mediów społecznościowych ma strukturę oligopolu, na którym dominuje kilka platform ze Stanów Zjednoczonych. Do najpopularniejszych można zaliczyć cztery z nich: YouTube, Facebook, Instagram oraz Twitter[53], które skupiają się w trzech grupach kapitałowych (Alphabet, Facebook i Twitter), będących jednocześnie sygnatariuszami *Kodeksu postępowania w zakresie zwalczania dezinformacji*, opublikowanego przez KE w 2018 r. Należy podkreślić, że Kodeks „był formą samoregulacji sektora biznesowego i został opracowany przez przedstawicieli platform internetowych, branży reklamowej i mediów, przy wsparciu środowisk akademickich i społeczeństwa obywatelskiego”[54]. Z oceny efektywności Kodeksu zakończonej we wrześniu 2020 r. wynika, że platformy wdrożyły jego postanowienia w stopniu zadowalającym, jednak niecałkowitym[55]. Należy zauważyć, że chociaż powyższe platformy klasyfikowane są jako media społecznościowe, mają znacząco odmienne formy. Podczas gdy firmy Facebook i Twitter moderują głównie treści tekstowe, Google (YouTube) moderuje treści wideo, a Instagram treści graficzne, co przekłada się na inną charakterystykę problemów dezinformacji na różnych platformach.

Najpopularniejsza platforma (odsetek odwiedzających ją co najmniej raz w miesiącu internautów przekracza 90%[56]) to YouTube. Mimo że współpraca z organami państwowymi nie wydaje się jej priorytetem (choć od lipca 2020 r. została objęta podatkiem od VoD[57]) to jednak po wpisaniu w wyszukiwarkę słów związanych z pandemią COVID-19 platforma odsyła do sprawdzenia informacji z oficjalnej strony Ministerstwa Zdrowia oraz promuje materiały z rzetelnych kanałów. YouTube nie współpracuje również z sektorem pozarządowym w Polsce w ramach moderacji treści, aczkolwiek może to w przyszłości ulec zmianie, gdyż platforma rozszerzyła kooperację *fact-checkingową* z siecią IFCN, której członkiem jest wspomniane Stowarzyszenie Demagog, o kolejne kraje – Wielką Brytanię i Niemcy[58]. Tym samym działalność YouTube w Polsce obejmuje dezaktywację lub usuwanie kont użytkowników naruszających reguły portalu, przy czym należy zaznaczyć, że platforma posiada rozbudowany system zwalczania dezinformacji oraz oznaczania kanałów sponsorowanych przez rządy (np. Sputnik)[59]. Prowadzeniem działalności w ramach spraw publicznych (ang. *public affairs*) zajmuje się właściciel platformy, Google, i jego polski oddział, który aktywnie działa m.in. w obszarze kształcenia kompetencji cyfrowych i medialnych (*media literacy*) czy też szkolenia dziennikarzy. Jednym z flagowych projektów Google skierowanych do dzieci i młodzieży są Asy Internetu. Z informacji uzyskanych od organizatora wynika, że w programie uczestniczyła 1/3 polskich szkół i 65 tysięcy uczniów. Ma on na celu podniesienie umiejętności cyfrowych i medialnych[60]. Ponadto Google prowadzi szereg międzynarodowych programów szkoleniowych i grantowych np. dla projektów zwalczających dezinformacje nt. szczepionek przeciw COVID-19[61], szkoli dziennikarzy rozwijających kompetencje cyfrowe (w tym *fact-checking* i wykrywanie dezinformacji)[62], czy też udostępnia narzędzie do *fact-checkingu*[63].

Z kolei **Facebook** (właściciel Instagrama) prowadzi w Polsce aktywną działalność w wielu obszarach, współpracując zarówno z sektorem rządowym, jak i pozarządowym pod marką swojej platformy. W zakresie *fact-checkingu* amerykańskiego giganta wspiera wspomniane już Stowarzyszenie Demagog będące jednym z niezależnych weryfikatorów, którzy mogą oceniać wiarygodność informacji zamieszczanych na platformie (weryfikatorzy działają także na Instagramie[64]). Mniejszy, niesformalizowany udział w zwalczaniu dezinformacji i *fake newsów* zamieszczonych na portalu ma również OKO.press. W maju 2019 r. śledztwo portalu i przekazanie informacji Facebookowi doprowadziło do zamknięcia siatki 13 polskojęzycznych stron mających ponad milion polubień – choć według OKO.press kompletna siatka to co najmniej 80 stron i niemal 5 milionów polubień[65]. Platforma społecznościowa współpracuje również z organizacjami pozarządowymi w ramach edukacji medialnej społeczeństwa. Wspólnie z Polityką Insight (organizacja pozarządowa o charakterze eksperckim) w 2018 r. opublikowała raport *Jak czytać w erze fake news*. Dokument jest podsumowaniem cyklu warsztatów realizowanych na wiodących polskich uniwersytetach, dzięki którym platformie udało się zebrać 118 zaleceń dotyczących walki z dezinformacją. Facebook prowadził również działania edukacyjne, które rozpowszechniał we współpracy z PAP. Platforma stworzyła narzędzie edukacyjne w postaci infografik na temat rozpoznawania fałszywych informacji w sieci, które dzięki rozpowszechnieniu na kanałach PAP dotarło do ponad 10 milionów użytkowników w Polsce[66]. Ponadto ogłosiła w 2018 r. uruchomienie programu skierowanego do polskich startupów i mikroprzedsiębiorstw, który ma na celu m.in. kształcenie kompetencji w zakresie edukacji medialnej[67].

Facebook utrzymuje również bezpośrednie relacje z rządem. W listopadzie 2018 r. Ministerstwo Cyfryzacji (MC) podpisało porozumienie z platformą, wprowadzające rozbudowane możliwości odwołania się użytkowników, których konta zostały zablokowane – pierwsze takie porozumienie na świecie. Platforma zgodziła się na utworzenie tzw. punktu kontaktowego, do którego właściciele zablokowanych lub usuniętych kont będą „mogli składać wnioski o przeprowadzenie dodatkowej kontroli [sprawdzającej,] czy blokada nastąpiła słusznie"[68]. Korzystanie z punktu kontrolnego zostało obwarowane dwoma warunkami:

1. Usunięte strony, profile lub treści muszą należeć do kategorii wymienionych w formularzu opracowanym przez Ministerstwo Cyfryzacji.

2. Użytkownik podjął wcześniej nieudaną próbę odwołania się od decyzji, a Facebook odrzucił odwołanie lub nie odpowiedział na nie w ciągu 72 godzin.

Sygnatariuszem porozumienia jest również NASK, który odpowiadał za wdrożenie projektu oraz jego ciągłą obsługę informatyczną. NASK pełni także rolę pośrednika, który przekazuje zablokowane treści lub konta do ponownego rozpatrzenia przez platformę[69]. Do formularza kontaktowego od grudnia 2018 r. do 26 maja 2020 r. wpłynęło 2168 wniosków, z czego 605 rozpatrzono pozytywnie, przywracając tym samym zablokowane treści lub profile[70]. Należy podkreślić, że MC zaprosiło pozostałe platformy społecznościowe do partycypacji w tym unikatowym w skali globu rozwiązaniu. Jak wynika z wypowiedzi byłego wiceministra cyfryzacji Karola Okońskiego z 28 listopada 2019 r., rząd prowadzi rozmowy o możliwości rozszerzenia punktu kontaktowego z platformami YouTube oraz Twitter. Wiceminister w rozmowie przewidywał, że „w ciągu kilku nadchodzących miesięcy uda się osiągnąć porozumienie"[71]. Niestety od tego czasu MC (zlikwidowane 7 października 2020 r.) nie informowało o stanie rozmów z platformami, a do grudnia 2020 r. nie uruchomiono punktów kontaktowych YouTube i Twitter. Niemniej na portalu rządowym umożliwiającym odwołanie od decyzji widnieje komunikat o specjalnie utworzonej przez Twitter informacji dla polskich użytkowników oraz metodzie postępowania w przypadku odwołania od decyzji platformy, dostępnej na jej witrynie[72]. Fakt ten sugeruje, że Twitter nie zdecydował się dołączyć do inicjatywy MC.

Niemniej jednak, rząd współpracuje z **Twitterem** w innym obszarze. Jak informuje Ministerstwo Zdrowia (MZ), od marca 2020 r. po wpisaniu w wyszukiwarkę platformy słów koronawirus, COVID-19 i ich różnych konfiguracji, użytkownikowi wyświetla się jako pierwszy komunikat przekierowujący do strony MZ po rzetelne informacje. Według byłego Ministra Cyfryzacji pełniącego obecnie rolę Sekretarza Stanu w Kancelarii Prezesa Rady Ministrów Marka Zagórskiego, działanie to jest nakierowane na walkę z dezinformacją dotyczącą zagrożenia koronawirusem[73]. Niestety Twitter nie podejmuje szerszej współpracy zarówno z rządem, jak i sektorem pozarządowym oraz nie posiada biura zlokalizowanego w Polsce.

Podsumowanie

Świadomość polskiej administracji rządowej i wojskowej wobec zagrożeń wynikających z dezinformacji należy ocenić wysoko, co w znacznej mierze jest pochodną wrogich działań Federacji Rosyjskiej w przestrzeni informacyjnej. Z jednej strony Polska jako główne zagrożenie dla swojego bezpieczeństwa traktuje Rosję i możliwie szczegółowo stara się śledzić jej wszelkie wrogie działania (w tym z zakresu wojny informacyjnej), z drugiej Rosja na przestrzeni ostatniej dekady do osiągania własnych celów politycznych wielokrotnie wykorzystywała akcje dezinformacyjne w państwach NATO i UE, spośród których najgłośniejsze to zaangażowanie w kampanię prezydencką w USA w 2016 r. oraz kampanię referendalną dotyczącą brexitu w Wielkiej Brytanii w tym samym roku. Z tego powodu najważniejsze strategiczne dokumenty dotyczące bezpieczeństwa narodowego oraz obronności wymieniają potencjalne działania dezinformujące na dużą skalę jako jedno z pozamilitarnych zagrożeń. Jednocześnie przedstawione są rekomendacje, jak z nimi walczyć, w których powtórzono konieczność budowy międzyinstytucjonalnej komórki zwalczającej dezinformację i koordynującej komunikację państwa. Namiastkę takiej komórki stanowi Zespół Roboczy powołany przy RCB. Niepokojące jest jednak nieprzyjęcie od 2015 r. projektu *Doktryny bezpieczeństwa informacyjnego RP*.

Jednocześnie podmioty z sektora publicznego aktywnie angażują się we współpracę międzynarodową w ramach działań UE i NATO (MSZ). Aktywna rola KRRiT w pracach ERGA i monitorowaniu wywiązywania się ze zobowiązań przyjętych przez media społecznościowe, a także rozwijanie własnych dokumentów poświęconych m.in. zagrożeniom dezinformacji dowodzi zaangażowania krajowego regulatora.

W Polsce działa również wiele organizacji pozarządowych skupiających się na zwalczaniu dezinformacji poprzez zróżnicowane aktywności. W ramach pracy eksperckiej (prowadzonej również przez państwowy instytut badawczy NASK) powstaje wiele publikacji, analiz, szkoleń, a nawet rozwiązań informatycznych. Trzeci sektor angażuje się równie aktywnie w szkolenia z zakresu edukacji medialnej kierowane zarówno do dziennikarzy, jak i młodzieży szkolnej, seniorów czy też zwykłych, zainteresowanych obywateli. Szczególny wymiar ma wsparcie dziennikarzy jako profesji wyjątkowo narażonej na możliwe uleganie dezinformacji i nieintencjonalne zwiększanie jej zasięgów. Organizacje prowadzą również działania w ramach tzw. *fact-checkingu*, weryfikując prawdziwość wypowiedzi polityków i osób publicznych, artykułów i doniesień medialnych bądź treści zgłoszonych przez użytkowników platform społecznościowych lub czytelników mających wątpliwości co do rzetelności informacji. Spośród nich szczególnie wyróżnić należy Stowarzyszenie Demagog, które jako jedyne jest członkiem międzynarodowej sieci IFCN, co pozwala na prowadzenie weryfikacji na platformach należących do Facebooka. Niestety organizacje pozarządowe współpracują ze sobą w ograniczonym stopniu i nie posiadają wspólnych celów strategicznych i taktycznych w zwalczaniu dezinformacji.

Podobnie ograniczona do absolutnego minimum jest współpraca Twittera i YouTube'a z rządem oraz organizacjami pozarządowymi, pomimo że są to platformy, z których korzysta odpowiednio 35% i 92% Polaków. Należy jednak podkreślić, że obie prowadzą szereg działań wymierzonych w zwalczanie dezinformacji na swoich serwisach, a Google

(spółka matka YouTube'a) zaangażowany jest m.in. w wiele programów rozwijających kompetencje cyfrowe i medialne wśród uczniów i dziennikarzy, a także wspiera w programach grantowych projekty zwalczające dezinformację. Odmiennie prezentuje się zaangażowanie Facebooka, który, poza prowadzeniem szeregu aktywności edukacyjnych samodzielnie oraz we współpracy z trzecim sektorem, podpisał bezprecedensowe w skali świata porozumienie z Ministerstwem Cyfryzacji i NASK. Na jego podstawie umożliwiono polskim użytkownikom odwołanie się w drugiej instancji od decyzji Facebooka o zablokowaniu lub usunięciu danych treści lub stron. Mimo prowadzenia dialogu z pozostałymi popularnymi platformami społecznościowymi w Polsce od uruchomienia rozwiązania w 2018 r. nie zdecydowały się one na dołączenie i implementację mechanizmu. Wyróżnić należy także najnowszy projekt przedstawiony przez Ministerstwo Sprawiedliwości, który ma na celu wprowadzenie nadrzędności prawa polskiego nad regulaminami platform społecznościowych oraz mechanizmu tzw. ślepego pozwu umożliwiającego walkę z mową nienawiści w internecie, a także uregulowanie kwestii związanych z wolnością słowa na dużych platformach.

W świetle powyższych działań i aktywności należy stwierdzić, że zagrożenie dezinformacją w Polsce spotyka się z dużą świadomością i szeroką odpowiedzią wielu organizacji pozarządowych oraz podmiotów administracji publicznej. Z kolei zaangażowanie sektora prywatnego w Polsce poza Facebookiem jest ograniczone, co wiąże się również z globalnym spojrzeniem platform i ich różnorodną specyfiką stawiającą w centrum albo treści tekstowe, albo graficzne, albo audiowizualne, a także różnymi mechanizmami działania. Niestety, zwalczanie zagrożeń jest nieskoordynowane. Nie istnieje przyjęty przez państwo we współpracy z sektorem pozarządowym plan odpowiedzi na dezinformację, a działania administracji dotychczas skupiają się głównie na monitoringu. Pomimo tego doświadczenie opisanych podmiotów w wielowarstwowym reagowaniu na problem dezinformacji jest pokaźne, co stanowi duży potencjał do utworzenia i przyjęcia celów, wokół których organizacje rządowe i pozarządowe ogniskować będą swoją działalność.

PRZYPISY

1 Ministerstwo Obrony Narodowej, *Koncepcja Obronna Rzeczypospolitej Polskiej*, 2017, s. 24.

2 Biuro Bezpieczeństwa Narodowego, *Strategia Bezpieczeństwa Narodowego RP*, 2020, s. 6, [online]: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.

3 Ibidem, s. 21.

4 Ibidem, s. 21.

5 Biuro Bezpieczeństwa Narodowego, *System komunikacji strategicznej w zwalczaniu dezinformacji*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, Magdalena Wrzosek (red.), NASK Państwowy Instytut Badawczy, Warszawa 2019, s. 10.

6 Ibidem, s. 9–10.

7 Biuro Bezpieczeństwa Narodowego, *Doktryna Bezpieczeństwa Informacyjnego RP, projekt 2015*, s. 6–7, [online]: https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

8 Ministerstwo Sprawiedliwości, *Przełomowa ustawa o ochronie wolności słowa w internecie*, 2020, [online]: https://www.gov.pl/web/sprawiedliwosc/przelomowa-ustawa-o-ochronie-wolnosci-slowa-w-internecie.

9 Projekt ustawy *o ochronie wolności słowa w internetowych serwisach społecznościowych*, 15 stycznia 2021 r.

10 NATO Strategic Communications Centre of Excellence, *Employees*, [online]: https://www.stratcomcoe.org/employees.

11 Biuro Rzecznika Prasowego MSZ, *Działania Ministerstwa Spraw Zagranicznych RP w obszarze przeciwdziałania obcej dezinformacji*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 11–12.

12 Grzegorz Świszcz, Anna Zasadzińska-Baraniewska, *Działania Rządowego Centrum Bezpieczeństwa w zakresie przeciwdziałania dezinformacji*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 17.

13 Rządowe Centrum Bezpieczeństwa, *KRAJOWY PLAN ZARZĄDZANIA KRYZYSOWEGO Aktualizacja 2020 CZĘŚĆ A*, 2020, s. 48, [online]: https://rcb.gov.pl/wp-content/uploads/KPZK-cz.-A-2020-1-1.pdf.

14 Grzegorz Świszcz, Anna Zasadzińska-Baraniewska, *Działania Rządowego Centrum Bezpieczeństwa w zakresie przeciwdziałania dezinformacji*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 17.

15 Ibidem, s. 17–18.

16 NASK Państwowy Instytut Badawczy, *strona główna*, [online]: https://www.nask.pl

17 Magdalena Wrzosek (red.), *Cyberbezpieczeństwo A.D. 2019*, NASK Państwowy Instytut Badawczy, Warszawa 2020, s. 181–182.

18 NASK Państwowy Instytut Badawczy, *POWIEDZ: „SPRAWDZAM!". NIE DAJ SIĘ MANIPULACJOM W INTERNECIE*, [online]: https://www.nask.pl/pl/aktualnosci/2365,Powiedz-quotSprawdzamquot-Nie-daj-sie-manipulacjom-w-internecie.html.

19 #FakeHunter, *O projekcie*, [online]: https://fakehunter.pap.pl/o-projekcie#collapseOne.

20 Dariusz Dalmanowicz, *Three Polish institutions to fight fake news on financial market*, The First News 2020, [online]: https://www.thefirstnews.com/article/three-polish-institutions-to-fight-fake-news-on-financial-market-13778.

21 Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji, art. 6 ust. 1.

22 Agnieszka Wąsowska, Marek Krawczyk, *Działania monitorujące Krajowej Rady Radiofonii i Telewizji – „Kodeks postępowania w zakresie przeciwdziałania dezinformacji"*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej.Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 19.

23 Ibidem, s. 19.

24 Ibidem, s. 18–20.

25 ERGA, *ERGA Report on disinformation: Assessment of the implementation of the Code of Practice*, 2020, s. 21, [online]: https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf.

26 Rzecznik Praw Obywatelskich, *KRRiT wyda dokument, jak przeciwdziałać fake newsom, dezinformacji i mowie nienawiści w przestrzeni medialnej*, 2020, [online]: https://www.rpo.gov.pl/pl/content/krrit-okresli-jak-przeciwdzia%C5%82ac-fake-new-som-dezinformacji-mowie-nienawisci-w-mediach.

27 KRRiT, *Fake news - dezinformacja online: próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, [online]: http://www.krrit.gov.pl/Data/Files/_public/Portals/0/obserwator/fake-news_obserwator-krrit-1.pdf.

28 Centrum Analiz Propagandy i Dezinformacji, *O Fundacji*, [online]: https://capd.pl/pl/misja-i-cele.

29 Marta Kowalska, Szymon Wigienka, *StratCom: perspektywa polska. Struktura systemu komunikacji i analiza kampanii na temat 20. rocznicy przystąpienia polski do NATO, Centrum Analiz Propagandy i Dezinformacji 2019*, [online]: https://capd.pl/pl/analizy/221-stratcom-perspektywa-polska-struktura-systemu-komunikacji-i-analiza-kampanii-na-temat-20-rocznicy-przystapienia-polski-do-nato.

30 INFO OPS Polska, *INFO OPS EXE*, 2020, [online]: https://infoops.pl/zaproszenia/.

31 INFO OPS Polska, *projekty*, [online]: https://infoops.pl/projekty-2/.

32 Instytut Kościuszki, CYBERSEC DISINFO LAB: PROJEKT PROZODIA, 2020, [online]: https://ik.org.pl/projekty/projekt-infoguardpl-prozodia/.

33 Ibidem.

34 Instytut Kościuszki, RAPORT COVID-19: DEZINFORMACJA W POLSKIEJ CYBERPRZESTRZENI, 2020, [online]: https://ik.org.pl/publikacje/raport-covid-19-dezinformacja-w-polskiej-cyberprzestrzeni/.

35 Instytut Kościuszki, CYBERSEC DISINFO LAB: PROJEKT PROZODIA, op. cit.

36 Anna Borkowska, Zuzanna Polak, *Edukacja medialna jako forma przeciwdziałania dezinformacji. Jak chronić dzieci i młodzież przed manipulacją?*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 39.

37 Ibidem, s. 40.

38 Stowarzyszenie Demagog, *Akademia Fact-Checkingu*, [online]: https://akademia.demagog.org.pl/.

39 Stowarzyszenie Demagog, *Uodpornij się na fake newsy z Fajnie, że wiesz!*, 2020, [online]: https://demagog.org.pl/analizy_i_raporty/fajnie-ze-wiesz/.

40 Edukacja Medialna, *o projekcie, Fundacja Nowoczesna Polska*, [online]: https://edukacjamedialna.edu.pl/info/o-nas/.

41 Ośrodek Analiz Cegielskiego, *Sposób na dezinformację*, [online]: https://snd.osrodekanaliz.pl/.

42 Fundacja Panoptykon, *Stop dezinformacji. Przewodnik dla dziennikarzy i redakcji*, 2019, [online]: https://panoptykon.org/wiadomosc/stop-dezinformacji-przewodnik-dla-dziennikarzy-i-redakcji.

43 Fundacja Reporterów, *Szkolenia*, 2017, [online:] https://fundacjareporterow.org/o-nas/szkolenia/.

44 Ibidem.

45 Stowarzyszenie Demagog, *Demagog dołącza do Programu niezależnej weryfikacji informacji Facebooka, 2019*, [online]: https://demagog.org.pl/analizy_i_raporty/demagog-dolacza-do-programu-niezaleznej-weryfikacji-informacji-facebooka/.

46 Stowarzyszenie *Demagog INFOSKAN – zapisz się do newslettera!*, 2020, [online]: https://demagog.org.pl/analizy_i_raporty/infoskan-zapisz-sie-do-newslettera/.

47 Rafał Babraj, *Czym jest fact-checking? – zarys inicjatyw na świecie i w Polsce*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 43–44.

48 OKO.press, *O nas*, [online]: https://oko.press/o-nas/.

49 Miłada Jędrysik, Piotr Pacewicz, *OKO.press wśród najbardziej opiniotwórczych i czytanych mediów*, 2020, [online]: https://oko.press/oko-press-wsrod-najbardziej-opiniotworczych-i-czytanych-mediow/.

50 OKO.press, *Kto stoi za OKO.press? Szczera do bólu informacja o naszych finansach*, 2017, [online]: https://oko.press/stoi-oko-press-szczera-bolu-informacja-o-naszych-finansach/.

51 Odfejkuj.info, *Kim jesteśmy?*, [online]: https://odfejkuj.info/onas/.

52 Rafał Babraj, *Czym jest fact-checking? – zarys inicjatyw na świecie i w Polsce*, op. cit., s. 43–44.

53 Money.pl, *Media społecznościowe. Które wybierają Polacy?*, 2020, [online]: https://www.money.pl/gospodarka/media-spolecznosciowe-ktore-wybieraja-polacy-6529596997314689a.html.

54 Magdalena Wrzosek (red.), *Wprowadzenie*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 7.

55 Paweł Zegarow, *OCENA UNIJNEGO KODEKSU POSTĘPOWANIA W ZAKRESIE ZWALCZANIA DEZINFORMACJI*, NASK Państwowy Instytut Badawczy 2020, [online]: https://cyberpolicy.nask.pl/ocena-unijnego-kodeksu-postepowania-w-zakresie-zwalczania-dezinformacji/.

56 We Are Social, Hootsuite, *Digital 2020. GlobaL Digital Overview*, 2021, [online]: Digital 2020 - We Are Social.

57 Wirtualnemedia, *4 mln zł w ciągu kwartału z „podatku od VoD", płacą go też Agora i Grupa RMF*, 2020, [online]: https://www.wirtualnemedia.pl/artykul/vod-serwisy-podatek-do-pisf-placa-netflix-i-hbo.

58 John Glenday, *YouTube rolls out conspiracy debunking fact-check feature in the UK*, The Drum 2020, [online]: https://www.thedrum.com/news/2020/09/24/youtube-rolls-out-conspiracy-debunking-fact-check-feature-the-uk.

59 Google, *How Google Fights Disinformation*, luty 2019, [online]: https://kstatic.googleusercontent.com/files/388aa7d18189665e5f5579aef18e181c2d4283fb7b0d4691689dfd1bf92f7ac2ea6816e09c02eb98d5501b8e5705ead65af653cdf94071c47361821e362da55b, s. 17–24.

60 Google, *Asy Internetu*, [online]: https://beinternetawesome.withgoogle.com/pl_all/.

61 Google, *An open fund for projects debunking vaccine misinformation*, 2021, [online]: https://www.blog.google/outreach-initiatives/google-news-initiative/open-fund-projects-debunking-vaccine-misinformation.

62 Google, *Building a stronger future for journalism*, Google News Initiative, [online]: https://newsinitiative.withgoogle.com/intl/pl/.

63 Google, *Google Fact Check Tools*, [online]: https://toolbox.google.com/factcheck/explorer.

64 Wirtualnemedia, *Instagram rozpoczyna aktywną walkę z fake newsami. Korzysta z organizacji fact-checkers pracujących dla Facebooka*, 2019, [online]: https://www.wirtualnemedia.pl/artykul/instagram-rozpoczyna-aktywna-walke-z-fake-newsami-korzysta-z-organizacji-fact-checkers-pracujacych-dla-facebooka-dlaczego.

65 Daniel Flis, *Sukces śledztwa OKO.press! FB usunął strony promujące m.in. fake newsy i Adama Andruszkiewicza*, OKO.press 2019, [online]: https://oko.press/sukces-sledztwa-oko-press-fb-usunal-strony-promujace-m-in-fake-newsy-i-adama-andruszkiewicza/.

66 Jakub Turowski, *Walka, która nigdy się nie kończy – jak Facebook ogranicza rozprzestrzenianie się dezinformacji*, w: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes.*, op. cit., s. 63.

67 Facebook, *Training 1 Million People and Small Businesses in Europe by 2020*, 2018, [online]: https://about.fb.com/news/2018/01/community-boost-europe/.

68 Cyfryzacja KPRM, *Pierwsze tego typu porozumienie. Ministerstwo Cyfryzacji i Facebook*, Serwis Rzeczpospolitej Polskiej 2018, [online]: https://www.gov.pl/web/cyfryzacja/pierwsze-tego-typu-porozumienie-ministerstwo-cyfryzacji-i-facebook.

69 Ibidem.

70 CyberDefence24, *„Punkt kontaktowy" dla użytkowników Facebooka. Czy wyniki pracy są zadowalające?*, 2020, [online]: https://www.cyberdefence24.pl/punkt-kontaktowy-dla-uzytkownikow-facebooka-czy-wyniki-pracy-sa-zadowalajace.

71 Wirtualnemedia, *Wiceminister cyfryzacji: Będzie polski punkt kontaktowy dla YouTube'a i Twittera. Trwają rozmowy z Rosjanami o 5G*, 2019, [online]: https://www.wirtualnemedia.pl/artykul/wiceminister-cyfryzacji-bedzie-polski-punkt-kontaktowy-dla-youtube-a-i-twittera-trwaja-rozmowy-z-rosjanami-o-5g-dlaczego-kiedy-5g-w-polsce-terminy-warunki-ceny.

72 Serwis Rzeczypospolitej Polskiej, *Odwołaj się od decyzji portalu*, [online]: https://www.gov.pl/web/gov/odwolaj-sie-od-decyzji-portalu.

73 Cyfryzacja KPRM, *Koronawirus w internecie – razem przeciw dezinformacji i nieuczciwym praktykom*, Serwis Rzeczpospolitej Polskiej 2020, [online]: https://www.gov.pl/web/cyfryzacja/koronawirus-w-internecie--razem-przeciw-dezinformacji-i-nieuczciwym-praktykom.

Anastazja Wiśniewska

Zjawisko dezinformacji w Niemczech

Legislacja i polityka Niemiec wobec zjawiska dezinformacji

Istotną cezurą w polityce Niemiec wobec zagrożeń hybrydowych i dezinformacji był tzw. *casus* Renate Künast, członkini partii Zieloni, która w 2017 r. rzekomo miała skomentować zbrodnię imigranta, który zamordował młodą kobietę we Fryburgu słowami: „straumatyzowany młody uchodźca może i kogoś zabił, ale i tak musimy mu pomóc”[1]. Stan faktyczny wskazywał jednak na to, że posłanka nie była autorką przypisywanej jej wypowiedzi, a celem *fake news* było wzmożenie nastrojów antyimigracyjnych i wyrządzenie szkody wizerunkowej Zielonym. Po wytoczeniu przez posłankę sprawy cywilnej platformie Facebook nieprawdziwe informacje zostaly usunięte w ciągu trzech dni. *Casus* Renate Künast zwrócił uwagę prawodawcy na zagrożenie, jakie dezinformacja może stanowić dla niemieckiej demokracji, debaty publicznej i nastrojów społecznych.

Obecnie w niemieckim porządku prawnym tworzenie i rozpowszechnianie dezinformacji i *fake news* nie jest regulowane w drodze generalnego aktu prawnego, tylko poprzez wyspecjalizowane akty prawne. Są nimi m.in.:

Ustawa o egzekwowaniu przepisów dotyczących sieci (niem. *Netzwerkdurchsetzungsgesetz*, NetzDG)

Uchwalona w 2017 r., jest przykładem regulacji prawnej koncentrującej się na moderowaniu treści. NetzDG ma na celu poprawę egzekwowania prawa i zwiększenie odpowiedzialności mediów społecznościowych za działania w zakresie wypowiedzi w sieci. Zgodnie z obowiązującym prawem platformy muszą zapewnić użytkownikom mechanizm zgłaszania treści, badania ich oraz usuwania materiałów w ciągu 24 godzin od zgłoszenia naruszenia[2].

Platformy społecznościowe ryzykują karą pieniężną w wysokości do 50 mln euro za nieprzestrzeganie przepisów. Nie są jednak zobowiązane do samodzielnego poszukiwania szkodliwych treści naruszających warunki korzystania z danej platformy bądź uznawanych za niezgodne z prawem[3].

Ustawa ma zastosowanie wyłącznie do sieci mediów społecznościowych, które mają dwa miliony lub więcej zarejestrowanych użytkowników w Niemczech. Sieci mediów społecznościowych są zdefiniowane jako „dostawcy usług telemedialnych, którzy prowadzą platformy internetowe z zamiarem osiągnięcia zysku i na których użytkownicy mogą dzielić się treściami z innymi użytkownikami lub udostępniać je publicznie"[4]. Operatorzy platform społecznościowych są zobowiązani do oferowania swoim użytkownikom łatwego mechanizmu składania skarg, informowania skarżących o ich rezultatach, publikować co sześć miesięcy raport z informacją na temat liczby skarg (dotyczy tylko platform otrzymujących ponad 100 skarg rocznie) oraz wyznaczyć reprezentanta w Niemczech do obsługi potencjalnych kar finansowych i procedur sądowych[5].

Nowelizacja ustawy z 18 czerwca 2020 r., mająca na celu wzmocnienie praw użytkowników i zwiększenie przejrzystości działań platform społecznościowych m.in. poprzez uproszczenie powiadamiania użytkowników i ułatwienie procesu odwoławczego do przywrócenia treści, wywołała niepokój opinii publicznej. Zaostrzenie prawa nakłada obowiązek przekazania zgłoszonych treści przez platformy społecznościowe do Federalnego Urzędu Śledczego (niem. *Bundeskriminalamt*, BKA), zgodnie z którym sieci społecznościowe muszą udostępnić organom państwa niektóre dane użytkowników, w tym adresy IP lub numery portów. Ma to na celu zagwarantowanie skutecznego ścigania autorów szerzących dezinformację i propagujących nieprawdziwe informacje[6]. Dodatkowo ustawa przewiduje wdrożenie procedury roszczenia wzajemnego, która pozwoliłaby osobom zamieszczającym treści i umieszczającym skargi na ponowne opublikowanie treści usuniętych z przyczyn nieuzasadnionych, poddanie ich ponownej ocenie, a także uznanie utworzonych organów arbitrażowych do rozstrzygania sporów między użytkownikami a platformami w postępowaniach pozasądowych.

Umowa międzylandowa w sprawie mediów (niem. *Medienstaatsvertrag*, MStV)

Regulacja mediów weszła w życie 7 listopada 2020 r., decyzją wszystkich krajów związkowych. Odnosi się do wyzwań, jakie stwarzają algorytmy sortowania i rekomendowania treści na portalach wideo, takich jak YouTube i Netflix oraz pośredników medialnych (np. Facebook, Google i Twitter Inc.). Celem nadrzędnym umowy jest zapobieganie rozpowszechnianiu treści niezgodnych z warunkami usług (przez nakładanie ograniczeń ich wyświetlania), promocja treści dziennikarskich (programy broadcastingowe), a także stworzenie łatwych do zrozumienia zaleceń i instrukcji dotyczących sposobu działania algorytmów[7].

Ustawa przeciw ograniczeniom konkurencji (niem. *GWB- Digitalisierungsgesetz*)

Nowelizacja ustawy zaproponowana przez Federalne Ministerstwo Gospodarki i Energetyki (niem. *Bundesministerium für Wirtschaft und Energie*) 9 września 2020 r. skupia się na zwiększeniu równowagi w gospodarce cyfrowej i zbadaniu, w jaki sposób cyfrowe podmioty (takie jak Facebook, Google i Amazon) mogą nadużywać swojej dominującej pozycji rynkowej do ograniczenia konkurencji[8]. Ustawa proponuje ściślejszą kontrolę nadużyć w dużych firmach działających w sektorze cyfrowym, a także większą ochronę prawną oraz ulgi, zwłaszcza dla małych i średnich przedsiębiorstw. Nowelizacja mogłaby być ważnym krokiem w kierunku dalszego dostosowania ram prawnych do modeli biznesowych operatorów platform.

Aktywność federalnego rządu Niemiec w obszarze działań legislacyjnych skierowanych przeciw dezinformacji, obejmuje również:

- współpracę z ministerstwami, instytucjami rządowymi i organizacjami pozarządowymi wspierającymi projekty i działania mediów, edukację cyfrową i kompetencje medialne, m.in. w celu zwalczania mowy nienawiści, cybermobbingu i dezinformacji, w szczególności w odniesieniu do dzieci i młodzieży;
- kooperację z rządami państw członkowskich Unii Europejskiej w poszukiwaniu skutecznych środków przeciwko mowie nienawiści i dezinformacji[9];
- poszerzanie kompetencji w zakresie technologii cyfrowych, mających kluczowe znaczenie dla budowania odporności na cyberzagrożenia i wzmocnienia suwerenności cyfrowej na szczeblu krajowym oraz europejskim[10].

Edukacja medialna w Niemczech

Na szczeblu narodowym federalny rząd Niemiec współpracuje z ministerstwami i instytucjami rządowymi wspierającymi projekty dotyczące edukacji cyfrowej i poszerzania kompetencji medialnych. Do przykładów należą m. in.:

- Federalna Agencja Kształcenia Obywatelskiego (niem. *Die Bundeszentrale für politische Bildung*), która wspiera rozwój kompetencji medialnych poprzez liczne inicjatywy, np. organizację gier symulacyjnych lub publikację przewodników opisujących współczesny krajobraz medialny, a także poprzez dostarczanie informacji o możliwościach włączania mediów cyfrowych do pracy edukacyjnej[11];
- Federalne Ministerstwo ds. Rodziny, Seniorów, Kobiet i Młodzieży (niem. *Bundesministerium für Familie, Senioren, Frauen und Jugend*) wzmacnia kompetencje medialne wśród rodziców i specjalistów w dziedzinie edukacji. Ministerstwo promuje również nawiązywanie kontaktów między profesjonalistami z branży mediów oraz wspiera konkursy skierowane do dzieci i młodzieży. Partnerem w realizacji wyżej wspomnianych konkursów jest Centrum Filmowe dla Dzieci i Młodzieży w Niemczech (niem. *Deutsches Kinder- und Jungendfilmzentrum*[12];
- Federalne Ministerstwo Edukacji oraz Badań naukowych (niem. *Bundesministerium für Bildung und Forschung*) działa na rzecz wspierania i promowania korzystania z mediów cyfrowych w zakresie zawodowym, przez finansowanie programów zwiększających kompetencje medialne[13].

Ponadto, od 2010 r. w Niemczech powstało ponad dwadzieścia inicjatyw, które służą zwalczaniu mowy nienawiści, cybermobbingu i dezinformacji (Tabela 1).

Jako że kraje związkowe są odpowiedzialne za edukację – edukacja cyfrowa jest również częścią ich kompetencji. Urzędy ds. mediów w krajach związkowych (niem. *Landesmedienanstalten*) działają w zakresie ustawodawczym dotyczącym ochrony młodzieży w mediach. W ich kompetencjach leży promowanie ich umiejętności cyfrowych. Komisja ds. ochrony nieletnich w mediach (niem. *Kommission für Jugendmedienschutz*, KJM) bada czy treści rozpowszechniane przez środki masowego przekazu naruszają porozumienie między krajami związkowymi dotyczące ochrony młodzieży w mediach (niem. *Jugendmedienschutz-Staatsvertrag*, JMStV) i podejmuje decyzje o ewentualnych karach[14].

Co więcej, w oparciu o podsumowania raportu European Policies Initiative z 2019 r., Niemcy zajęły ósme miejsce w rankingu państw europejskich [Mapa, strona 8]. Ranking szacuje odporność trzydziestu pięciu państw na dezinformację i *fake news*, korzystając ze wskaźników wolności mediów, edukacji i stosunku społeczeństwa do mediów. Wynik sugeruje bardzo dobrą efektywność inicjatyw zwiększających kompetencje medialne[15].

Tabela 1. Przykładowe inicjatywy zwiększania kompetencji medialnych.

NAZWA	OPIS
Dieter Baacke Preis	Nagroda honoruje medialno-pedagogiczne/medialne projekty i metody edukacyjne. Jest ona przyznawana przez Stowarzyszenie na rzecz edukacji medialnej i kultury komunikacji (niem. *Gesellschaft für Medienpädagogik und Kommunikationskultur*, GMK) oraz Federalne Ministerstwo ds. Rodziny, Seniorów, Kobiet i Młodzieży (niem. *Bundesministerium für Familie, Senioren, Frauen und Jugend*, BMFSFJ). Celem jest zwiększenie świadomości i zdolności krytycznego myślenia w rozumieniu nowych mediów i związanych z nimi zagrożeń.
Seitenstark	Projekt zrzesza ponad 60 stron internetowych dla dzieci. W jego skład wchodzą strony internetowe niezależnych pedagogów, dziennikarzy, ministerstw federalnych, firm, kościołów, stowarzyszeń i klubów dziecięcych. Celem projektu jest tworzenie standardów jakości dla dziecięcych stron internetowych.
Blickwechsel	Zespół Blickwechsel zapewnia seminaria i kursy szkoleniowe z zakresu edukacji medialnej dla wychowawców i nauczycieli, prowadzi wieczory dla rodziców w szkołach i świetlicach o edukacji medialnej, a ponadto inicjuje praktyczne projekty medialne z dziećmi i młodzieżą w celu poprawy ich umiejętności korzystania z mediów.
Schau hin! Was Dein Kind mit Medien macht.	Internetowy przewodnik dla rodziców na temat mediów tradycyjnych, mediów społecznościowych, smartfonów i cyfrowych technologii.
Ein Netz für Kinder	Przewodnik dla rodziców i opiekunów dotyczący poznawania i bezpiecznego użytkowania Internetu przez dzieci.
Demokratielabore	Warsztaty mające na celu informowanie młodzieży m.in. o mowie nienawiści, uczestnictwie w życiu społecznym i zaangażowaniu w nie[16].

Źródło: Opracowanie własne na podstawie danych zebranych przez European Audiovisual Observatory, 2016.

Działania organizacji pozarządowych w walce z dezinformacją

Oprócz działań rządowych i legislacyjnych rolę uzupełniającą w zakresie edukacji medialnej i walki z dezinformacją odgrywa trzeci sektor, reprezentowany przez organizacje pozarządowe, organizacje *fact-checkingowe* czy instytuty, takie jak Instytut Badań nad Mediami i Edukacji Medialnej (niem. *Institut für Medienpädagogik in Forschung und Praxis*, JFF), znajdujące się przy władzach każdego kraju związkowego[17]. Technologie cyfrowe dają możliwość uczestniczenia w tworzeniu i rozpowszechnianiu informacji na niespotykaną dotąd skalę, co pociąga za sobą inwestycje w rozwój świadomości cyfrowej oraz konieczność przeciwdziałania rozpowszechnianiu nieprawdziwych treści. Do obszarów szczególnego działania po stronie niemieckiego sektora pozarządowego należą: zwiększenie kompetencji technologicznych, rozwój umiejętności zarządzania tożsamością cyfrową oraz rozwój świadomości w zakresie cyfrowej nauki i odpowiednich form artykulacji cyfrowej[18].

Organizacje *fact-checkingowe*

Do organizacji *fact-checkingowych*, które są zweryfikowanymi sygnatariuszami kodeksu Międzynarodowej Sieci Fact-Checkingowej (ang. *International Fact-Checking Network*, IFCN), należą ***dpa-Faktencheck*** przy redakcji Deutsche Presse-Agentur oraz ***Correctiv***. W wyniku wybuchu pandemii COVID-19 oraz towarzyszącej jej *infodemii*

powstaje coraz więcej organizacji *fact-checkingowych*. *Duke Reporters' Lab* dodał do swojej listy ***Faktenfinder***, afiliowany przy niemieckim konsorcjum radiofonii i telewizji publicznej **ARD**.

Niemieckie środowisko *fact-checkingowe* współtworzą następujące inicjatywy i strony internetowe:

Wafana – pierwsza organizacja *fact-checkingowa*, powstała w 2016 r. Jej nazwa, Wafana, jest połączeniem słów: prawda (niem. *Wahrheit*), fakty (niem. *Fakten*) i wiadomości (niem. *Nachrichten*). Organizacja ta prowadzi szkolenia online z weryfikacji treści dla dziennikarzy w całym kraju.

Crowdalyzer – narzędzie wykorzystujące algorytmy uczenia maszynowego (ang. *machine learning*), służące do monitorowania mediów społecznościowych, utworzone przez *Wafanę* w 2017 r. Pozwalało ono dziennikarzom nie tylko zauważać nieprawdziwe wiadomości, ale także wskazywać grupy docelowe, do których te informacje są kierowane[19].

CrowdNewsroom – specjalna platforma, zainicjowana przez organizację *fact-checkingową Correctiv*, weryfikująca doniesienia związane z pandemią koronawirusa, służąca do sprawdzania podejrzanych informacji wywołujących zaniepokojenie opinii publicznej. Dane zgromadzone na platformie są weryfikowane przez dziennikarzy z redakcji, zajmujących się oceną ich zgodności z faktami.

AFP Germany – globalna agencja informacyjna. W ramach partnerstwa z Facebookiem niemiecki stał się szesnastym językiem, w którym *AFP* zestawia swoje *fact-checkingowe* artykuły i publikuje je na wielojęzycznej stronie ***AFP Fact Check***[20].

Hoaxmap – strona zajmująca się informacjami dotyczącymi uchodźców i imigrantów. Na cyfrowej mapie Niemiec można zlokalizować fałszywe wiadomości, szukając w kategoriach takich jak kraj związkowy, miejscowość oraz tematyka.

SWR-Fakefinder – narzędzie, które poprzez grę pomaga odróżnić nieprawdziwe wiadomości od prawdziwych. Do każdego zadania zostały dołączone linki do stron poświęconych demaskowaniu fałszywych wiadomości.

First Draft News – organizacja założona w 2015 r., która opracowuje wytyczne jak postępować w przypadku rozpowszechniania dezinformacji w mediach społecznościowych. W Niemczech z inicjatorami First Draft współpracują: dpa, Die Zeit, ARD i Zweites Deutsches Fernsehen (ZDF)[21].

Działania mediów społecznościowych w Niemczech

Obecnie w cyberprzestrzeni mamy do czynienia z fałszywymi stronami, botami i trollami, które usiłują manipulować opinią publiczną. W 2017 r. Angela Merkel, kanclerz Niemiec, odniosła się do zagrożeń związanych z dezinformacją i wyraziła potrzebę regulacji mediów społecznościowych. Niemniej jednak często debatuje się, czy są one wystarczające. W 2018 r. Human Rights Watch odniosła się do ustawy o egzekwowaniu przepisów dotyczących sieci (niem. *Netzwerkdurchsetzungsgesetz*, NetzDG), uznając ją za niejasną regulację, która zamienia prywatne firmy w nadgorliwych cenzorów i pozostawia użytkowników bez odpowiedniej ochrony prawnej. Nick Wallace (analityk Center for Data Innovation) i Alan McQuinn (analityk Information Technology and Innovation Foundation) twierdzą, że próby regulacji dezinformacji w mediach społecznościowych w Niemczech są niepraktyczne ze względu na brak jednoznacznej definicji. Zmiany w tym obszarze mogą także zwiększyć koszty platform. Z tego względu wdrożenie mechanizmów usuwania treści wśród start-upów może być niewykonalne wobec braku zasobów wielkich dostawców do moderowania treści[22].

Współpraca Facebooka z organizacjami *fact-checkingowymi*

W Niemczech ***Correctiv***, ***dpa-Faktencheck*** oraz Facebook współpracują w celu sprawdzaniu faktów. Algorytmy stosowane na platformie mogą wzmacniać rozprzestrzenianie się fałszywych informacji wśród użytkowników. Facebook dostarcza analitykom listę zgłoszonych postów, które są następnie analizowane. Jeśli dojdzie do opublikowania nieprawdziwych wiadomości, użytkownicy zobaczą poprawioną wersję wyświetlaną pod oryginalnym postem, a osoba chcąca podzielić się fałszywą treścią otrzyma ostrzeżenie[23].

Inicjatywy międzynarodowe – Unia Europejska a Niemcy

Biorąc pod uwagę globalny charakter Internetu, przeciwdziałanie dezinformacji nie może się zatrzymać wyłącznie na obszarze Niemiec. Aktywna komunikacja strategiczna w kraju i za granicą jest niezbędna do skuteczniejszego zwalczania dezinformacji. Objęcie przez Niemcy prezydencji w Radzie Unii Europejskiej w lipcu 2020 r. zintensyfikowało działania skierowane ku przyspieszeniu i zrównoważeniu transformacji cyfrowej, a także rozwojowi suwerenności cyfrowej i technologicznej[26]. Zgodnie z programem prezydencji Berlin skupił się na postępie technologicznym w dziedzinie sztucznej inteligencji i technologii kwantowych oraz ochronie suwerenności obywateli w zakresie dostępu i przechowywania danych na wszystkich urządzeniach użytkowników bez ingerencji osób trzecich[27]. Rada Unii Europejskiej, tworząc odpowiednie warunki prawne, dała możliwość bezpiecznego użytkowania sieci w postaci tzw. standardyzowanych elementów zabezpieczających (ang. *Standardised Secure Elements*).

Ponadto do innych inicjatyw podjętych przez decydentów Unii Europejskiej należy powołanie w 2018 r. przez Komisję Europejską Grupy wysokiego szczebla ds. fałszywych wiadomości i dezinformacji online (ang. *High-Level Group on fake news and online disinformation*, HLEG – więcej uwagi zostało jej poświęcone w rozdziale dotyczącym UE)[28]. W ramach prac HLEG brały udział przytoczone niżej niemieckie podmioty.

Tabela 2. Mechanizm fact-checkingowy na platformie Facebook w Niemczech.

TYP 1	TYP 2
Udostępnienie postu zweryfikowanego jako „fake" przez analityków skutkuje pojawieniem się okienka z informacją, że post został zakwestionowany[24].	Pod zakwestionowanym postem pojawia się link do treści skorygowanej przez partnerów fact-checkingowych w zakładce „Więcej na ten temat". Początkowo Facebook używał do tego wyraźniejszego oznaczenia: bezpośrednio pod wiadomością pojawiał się czerwony znak ostrzegawczy i komunikat informujący o wątpliwej treści. Jednakże ten wariant został odrzucony z powodu ryzyka pogłębienia przekonań zamiast ich podważenia[25].

Źródło: Opracowanie własne.

Tabela 3. Niemieccy przedstawiciele HLEG.

PRZEDSTAWICIEL	OPIS
Arbeitsmegeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland (ARD)	Redakcja stacji telewizyjnej ARD stworzyła narzędzie do weryfikacji *fake newsów* o nazwie Faktenfinder. Dziennikarze przedstawiają w nim własne opinie w odniesieniu do publikowanych treści na mediach społecznościowych.
Bertelsmann & Co	Przedstawiciele kilku oddziałów Grupy RTL uczestniczyli w warsztatach weryfikacji treści generowanych przez użytkowników (ang. *User-Generated Content*, UGC). Uczestnicy zostali przeszkoleni w zakresie weryfikacji UGC oraz wymienili poglądy na temat tego, jak ich firmy mogą współpracować w tej dziedzinie i reagować na wyzwania związane z dezinformacją, służąc lokalnym i międzynarodowym potrzebom[29].
Lie Detectors	Działający w Belgii, Austrii i Niemczech projekt skierowany do dzieci i młodzieży w celu zwiększenia ich kompetencji medialnych i nauki krytycznego myślenia względem informacji online. Przez współpracę z dziennikarzami i wybranymi ekspertami dąży do rozwoju umiejętności cyfrowych, tworząc pozytywny kontakt między dziennikarzami, dziećmi oraz nauczycielami. Ponadto organizacja wpływa na kształtowanie polityki, doradzając Komisji Europejskiej, jak radzić sobie z rozprzestrzenianiem się i społeczno-gospodarczym wpływem dezinformacji[30].

Źródło: Opracowanie własne.

Na szczeblu narodowym rola niemieckich przedstawicieli grupy HLEG polega głównie na współpracy z sektorem publicznym oraz organizacjami *fact-checkingowymi* w celu zwiększenia przejrzystości wiadomości online, promowania umiejętności korzystania z mediów, przeciwdziałania dezinformacji i pomocy użytkownikom w poruszaniu się w środowisku mediów cyfrowych. Ponadto koncentrują się oni na opracowaniu narzędzi umożliwiających im i dziennikarzom walkę z dezinformacją oraz wspieraniu pozytywnego zaangażowania w szybko rozwijające się technologie informacyjne[31].

Wraz z wybuchem pandemii COVID-19 władze Niemiec zintensyfikowały współpracę ze Światową Organizacją Zdrowia (ang. *World Health Organization*) oraz operatorami platform społecznościowych na rzecz zwalczania dezinformacji[32]. Do kluczowych zadań należą przede wszystkim: zwiększenie dostępności wiarygodnych informacji oraz wspieranie niezależnych mediów poprzez współpracę z organami ochrony zdrowia publicznego. Pod tym względem prezydencja Niemiec w Radzie UE postawiła sobie za cel wzmocnić cyfrowe uczestnictwo obywateli w kontekście szerzenia umiejętności i kompetencji właściwych dla epoki cyfrowej, uwzględniając aspekt pandemii, którym jest jej wpływ na sektor edukacji.

Podsumowanie

Wyżej wspomniane rozwiązania legislacyjne i dobre praktyki w zakresie działań trzeciego sektora wskazują, że przeciwdziałanie zagrożeniom hybrydowym i dezinformacji wymaga połączenia wysiłków i współpracy wszystkich zainteresowanych stron. Zintegrowane, systemowe podejście na poziomie instytucjonalnym, określone obowiązki przypisane konkretnym organom państwa, dostawcom usług cyfrowych czy analitykom *fact-checkingowym* oraz połączenie ich metod działania wydają się być o wiele bardziej skutecznym sposobem przeciwdziałania tym zagrożeniom w cyfrowym świecie.

Ukierunkowane działania i ścisła kooperacja między federalnym rządem Niemiec a dostawcami usług cyfrowych są kluczowe, szczególnie w zakresie legislacyjnym, w celu stworzenia przejrzystych regulacji, definiujących zjawisko dezinformacji, rolę platform społecznościowych i ich prawną odpowiedzialność. Ponadto dalsze rozwijanie kompetencji medialnych, wsparcie organizacji zajmujących się dezinformacją przez federalny rząd Niemiec, a także wdrażanie rozwiązań Unii Europejskiej to aktywności konieczne do zwiększenia niemieckiej odporności systemowej wobec zagrożeń hybrydowych i dezinformacji.

PRZYPISY

1 Magdalena Gwóźdź, *Fake News – co to takiego i jaki mają zasięg*, 2016, [online]: https://www.dw.com/pl/fake-news-co-to-takiego-i-jaki-maj%C4%85-zasi%C4%99g/a-36742325.

2 Ibidem.

3 Library of Congress, *Initiatives to counter fake news: Germany*, 2020, [online]: https://www.loc.gov/law/help/fake-news/germany.php.

4 Ibidem.

5 Krajowa Rada Radiotelefonii i Telewizji, *Fake news – dezinformacja online*, 2020, [online]: http://www.krrit.gov.pl/Data/Files/_public/Portals/0/analizy/fake-news_obserwator-krrit.pdf.

6 Bundesministerium der Justiz und für Verbraucherschutz, *Weiterentwicklung des Netzwerkdurchsetzungsgesetzes*, 2020, [online]: https://www.bmjv.de/SharedDocs/Artikel/DE/2020/040120_NetzDG.html.

7 Ibidem.

8 Ibidem.

9 Library of Congress, *Initiatives to counter fake news: Germany*, op. cit.

10 Wypowiedź Annegret Kramp-Karrenbauer, Minister Obrony Narodowej Niemiec podczas CYBERSEC Global 2020, [online]: https://youtu.be/my_5laNcsvk.

11 Die Bundeszentrale für politische Bildung, *Medienpädagogik*, 2020, [online]: https://www.bpb.de/lernen/digitale-bildung/medienpaedagogik/.

12 Bundesministerium für Familie, Senioren, Frauen und Jugend, *Medienkompetenz stärken*, 2018, [online]: https://www.bmfsfj.de/bmfsfj/themen/kinder-und-jugend/medienkompetenz/medienkompetenz-staerken/75350.

13 Bundesministerium für Bildung und Forschung, *Bekanntmachung*, 2016, [online]: https://www.bmbf.de/foerderungen/bekanntmachung-1137.html.

14 EACEA National Policy Platforms, *National strategy*, 2017, [online]: https://eacea.ec.europa.eu/national-policies/.

15 Ibidem.

16 Library of Congress, *Initiatives to counter fake news: Germany*, op. cit.

17 EACEA National Policy Platforms, *National strategy*, 2017, [online]: https://eacea.ec.europa.eu/national-policies/.

18 Landesmedienzentrum Baden-Württemberg, *Medienbildung und gesellschaft*, 2020, [online]: https://www.lmz-bw.de/medien-und-bildung/medienwissen/medienbildung/grundlagen-der-medienbildung-und-mediendidaktik/medienbildung-und-gesellschaft/.

19 Clothilde Goujard, *Fact-checking around the world: Inside Germany's Wafana*, 2018, [online]: https://ijnet.org/en/story/fact-checking-around-world-inside-germany%E2%80%99s-wafana.

20 AFP, *AFP consolidates its place as global fact check leader with new German service*, 2020, [online]: https://www.afp.com/en/agency/press-releases-newsletter/afp-consolidates-its-place-global-fact-check-leader-new-german-service.

21 First Draft, *Disinformation is damaging communities around the world*, 2020, [online]: https://firstdraftnews.org/.

22 The Local, *Opinion: Germany shouldn't force social media firms to be arbiters of truth*, 2017, [online]: https://www.thelocal.de/20170201/why-germany-shouldnt-force-social-media-companies-to-be-the-arbiters-of-truth.

23 Natasha Lomas, *Germany tightens online hate speech rules to make platforms send reports straight to the feds*, 2020, [online]: https://techcrunch.com/2020/06/19/germany-tightens-online-hate-speech-rules-to-make-platforms-send-reports-straight-to-the-feds/.

24 Philipp Müller, *Warnen oder Löschen: Wie sollen Plattformen mit Falschmeldungen verfahren?*, 2019, [online]: https://www.bpb.de/gesellschaft/digitales/digitale-desinformation/290481/wie-sollen-plattformen-mit-falschmeldungen-verfahren.

25 Christina Iglhaut, *Facts for democracy*, 2020, [online], https://www.deutschland.de/en/topic/culture/combatting-fake-news-about-coronavirus-how-germany-is-tackling-the-problem.

26 Rada Unii Europejskiej, *Razem wzmocnijmy Europę. Program prezydencji Niemiec w Radzie Unii Europejskiej*, 2020, [online]: https://www.eu2020.de/blob/2363548/a70fe31786bb2506b3a51d9b2e26c76f/07-03-pdf-programm-pl-data.pdf.

27 Ibidem.

28 Komisja Europejska, *Zwalczanie dezinformacji w internecie: Podejście europejskie*, 2018, [online]: https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-236-F1-PL-MAIN-PART-1.PDF.

29 Bertelsmann, *Alliance against fake news*, 2017, [online]: https://www.bertelsmann.com/corporate-responsibility/projects-worldwide/project/alliance-against-fake-news.jsp.

30 Lie Detectors, *Critical Thinking*, 2021, [online]: https://lie-detectors.org/.

31 European Audiovisual Observatory, *Mapping of media literacy practices and actions in EU-28*, 2016, [online]: https://rm.coe.int/1680783500.

32 Susan Bergner, Remco van de Pas, Louise van Schaik, Maike Voss, *Upholding the World Health Organization*, Stiftung Wissenschaft und Politik 2020, [online]: https://www.swp-berlin.org/10.18449/2020C47/.

Faustine Felici

Francja

Wstęp

W maju 2017 roku, kilka dni przed drugą turą wyborów prezydenckich, Francja stanęła w obliczu zjawiska bezprecedensowego – szybko ochrzczonego przez prasę mianem „MacronLeaks". Ujawniono w sieci 15 GB danych – około 150000 e-maili i dokumentów – pochodzących ze skrzynek pocztowych działaczy partii ówczesnego kandydata Emmanuela Macrona, co sprowokowało ożywione debaty w fali postów w mediach społecznościowych i jakoby dostarczyło ogromu informacji niezdecydowanym wyborcom. Zmieszanie oryginalnych dokumentów z podrobionymi e-mailami i sfałszowanymi folderami sugeruje jednak, że zamiarem było oszukanie Francuzów, zmanipulowanie ich, a przede wszystkim wpłynięcie na ich głosy. Zasięg dokumentów oraz towarzyszących im komentarzy i wprowadzających w błąd analiz[1] bez wątpienia poszerzyła cyfrowa i sieciowa natura całego zajścia. Mimo że operacje wpływu są od dawna powszechnie stosowane, szybka digitalizacja sfery publicznej i informacyjnej otwiera podmiotom działającym w złej wierze nowe ścieżki osiągania swoich celów. W coraz bardziej połączonym społeczeństwie, dla którego członków sieci społecznościowe stanowią drugie ulubione[2] źródło informacji – a nawet, w przypadku młodych obywateli Francji, liczących 18–34 lat, pierwsze[3] – kampanie wyborcze wypaczane przez fałszywe informacje lub internetowe akcje dezinformacyjne sprzyjające podziałom społecznym są faktycznym zagrożeniem dla demokracji. François Hollande – Prezydent Republiki Francuskiej w okresie afery MacronLeaks – obiecał, że nic w tej kwestii nie pozostanie „bez odpowiedzi"[4]. Prokuratura w Paryżu wszczęła śledztwo, a Narodową Agencję Cyberbezpieczeństwa (fr. *Agence Nationale de la Sécurité des Systèmes d'Information*, ANSSI) poproszono o udzielenie w sprawie technicznego wsparcia.

Jak w kraju, który wysoko ceni wolność wypowiedzi, a „swobodne wypowiadanie myśli i poglądów jest jednym z najcenniejszych praw człowieka”[5], władze francuskie radzą sobie ze stawianiem tamy kampaniom dezinformacyjnych i przeciwdziałaniem tzw. *fake news*? Rozdział przyjrzy się tej drażliwej kwestii, badając francuskie ustawodawstwo i politykę wymierzone w publikowanie dezinformacji oraz prezentując inicjatywy pozarządowe odnoszące się do tego tematu. Na koniec relacje firm stojących za mediami społecznościowymi z rządem zostaną zanalizowane przez pryzmat bezprecedensowego eksperymentu wykonanego w ramach Facebooka.

Prawodawstwo i polityka Francji w walce z dezinformacją

Choć obawy związane z dezinformacją dały o sobie znać wraz z rozwojem mediów internetowych i społecznościowych w XXI w., sam temat nie jest przecież *terra incognita*. Próby manipulacji i dzielenia opinii publicznej liczą sobie przynajmniej tyle lat, ile wynalazek mediów masowych. Nie dziwi zatem informacja, że pierwsze przepisy mierzące się z tą kwestią we Francji wywodzą się z XIX w. Ustawie, uznanej za przestarzałą i niezdolną odnieść się do problemu dezinformacji w internecie, towarzyszą od 2018 r. nowe regulacje.

Ustawa z 29 lipca 1881 r. o wolności prasy

Wielokrotnie nowelizowana od czasu przyjęcia, ustawa z 29 lipca 1881 r. o wolności prasy nadal obowiązuje we Francji. Jest skierowana nie przeciw tworzeniu fałszywych wiadomości, a ich rozpowszechnianiu, a zatem manipulacjom medialnym. Ustawa definiuje m.in. co uważa się za fałszywe wiadomości oraz uznaje ich szerzenie za przestępstwo w sensie prawa karnego: „Publikacja, rozpowszechnianie i reprodukcja w złej wierze za pośrednictwem dowolnych środków wiadomości fałszywych, sfabrykowanych, sfałszowanych bądź kłamliwych przypisywanych osobom trzecim, która zakłóca porządek publiczny lub jest zdolna go zakłócić, podlega karze 45000 euro”[6]. Tak samo karane jest zniesławienie i znieważenie. Wymiar sprawiedliwości określił stopniowo rodzaj informacji zdolnych zakłócić porządek publiczny. Należą do nich m.in. te, które mogą naruszyć stosunki międzynarodowe, wywołać reglamentację żywności, masową emigrację lub grożące wywołaniem rewolty[7]. Nie wszystkie *fake newsy* stanowią więc zakłócenie porządku publicznego.

Choć wolność wyrażania poglądów uważa się za fundamentalną i postrzega jako filar demokratycznego ładu we Francji, nie jest ona bynajmniej bezgraniczna, a fałszywe informacje to jeden z obszarów, w których od dawna podlega regulacjom. Nadejście internetu oraz szybki rozwój mnożących się mediów społecznościowych zadziałały jak katalizator nowych naruszeń i wyzwań – wśród nich anonimowość podmiotów w sieci – zaburzających kruchą równowagę znalezioną w ustawie z 1881 r. Do jej zalet należał nakaz wyznaczenia i podania osoby odpowiedzialnej za publikację, która ponosi odpowiedzialność w razie szerzenia *fake newsów*. Internetowa anonimowość nie pozwala na analogiczny jak w przypadku prasy poziom odpowiedzialności, którą ponosiliby piszący w sieci. Wybory prezydenckie z 2017 r. utorowały drogę do przemyślenia tego tematu, co poskutkowało uzupełnieniem legislacyjnego arsenału do walki z dezinformacją o nowe przepisy.

Ustawa z 22 grudnia 2018 r. o zwalczaniu manipulacji informacjami

Wspomniane wybory wraz ze sprawą MacronLeaks stanowiły punkt zwrotny w ocenie potencjalnej szkodliwości dezinformacji dla demokratycznego ładu w oczach francuskich elit politycznych. 29 maja 2017 r., zaledwie kilka dni po wygranych wyborach, Emmanuel Macron wspomniał o tej kwestii na konferencji prasowej kończącej oficjalną wizytę prezydenta Rosji Władimira Putina. Potępił praktyki stacji Russia Today i agencji Sputnik, które „nie zachowały się jak środki przekazu i jak dziennikarze, ale jak ośrodki wpływu i propagandy,

kłamliwej propagandy – ni mniej, ni więcej”[8], a w styczniu 2018 ogłosił zamiar doprowadzenia do zmian we francuskim systemie prawnym, aby chronić demokratyczny ład państwa przed fałszywymi informacjami. Jako pierwszoplanowe przy manipulacji informacjami wskazano dwie kwestie: media kontrolowane przez obce państwa – jako środki wpływu – oraz status platform cyfrowych, który nie pozwala obarczać ich należytą odpowiedzialnością za treści przez nie rozpowszechniane.

Tych problemów dotyczy ustawa z 22 grudnia 2018 r. Skupia się głównie na okresach wyborczych – rozpoczynających się trzy miesiące przed dniem wyborów ogólnokrajowych – i wprowadza nowe możliwości szybkiego działania. I tak, na żądanie prokuratora, kandydata, partii politycznej lub koalicji czy też dowolnej osoby mającej uzasadniony interes, sędzia orzekający może nakazać podjęcie „wszelkich proporcjonalnych i niezbędnych środków”, aby uniemożliwić szerzenie „celowych, sztucznych lub zautomatyzowanych oraz na masową skalę [...] nieścisłych lub mylących twierdzeń lub posądzeń potencjalnie wpływających na uczciwość wyborów”[9]. Postanowienie musi być wydane w ciągu 48 godzin. Tak krótki termin dobrano celowo, wyraźnie wychodząc naprzeciw kampaniom internetowym, które potrafią rozprzestrzeniać się szybciej niż w jakimkolwiek innym medium.

W rezultacie ustawy z 22 grudnia 2018 r. – określanej też jako ustawa przeciw *fake newsom* – platformy cyfrowe i media społecznościowe przyjęły na siebie nowe obowiązki. Te koncentrują się głównie na poprawie przejrzystości związanych z polityką materiałów reklamowych w sieci. W okresach wyborczych platformy internetowe z ponad pięcioma milionami unikalnych użytkowników miesięcznie muszą zatem[10]:

- dostarczać użytkownikom wiernych, jasnych i przejrzystych informacji o tożsamości osoby lub organizacji, która kupiła płatną treść powiązaną z debatą o znaczeniu krajowym,
- dostarczać użytkownikom wiernych, jasnych i przejrzystych informacji o użyciu ich danych osobowych w kontekście promowania treści informacyjnych powiązanych z debatą o znaczeniu krajowym,
- upubliczniać wysokość wynagrodzenia otrzymanego w zamian za promowanie takich treści informacyjnych, w razie gdy przekracza ono 100 euro.

Wreszcie w celu zajęcia się kwestią ingerencji mediów sterowanych z zagranicy w wyborach krajowych ustawa 22 grudnia 2018 r. poszerzyła uprawnienia głównej agencji regulacyjnej nadawców radiowych i telewizyjnych (*Conseil supérieur de l'audiovisuel*, CSA). Może ona zawiesić[11] do końca głosowania lub wycofać[12] koncesję na nadawanie każdemu operatorowi radia bądź telewizji kontrolowanemu przez obce państwo albo znajdującemu się pod jego wpływem w razie emisji czy to fałszywych informacji, które mogłyby wpłynąć na wynik wyborów, czy treści, które mogłyby szkodzić „fundamentalnym interesom Narodu” – co wprost obejmuje szerzenie fałszywych informacji, aby zakłócić sprawne funkcjonowanie instytucji. Decyzja o wycofaniu koncesji nadawczej operatora może być motywowana treściami rozpowszechnianymi za pomocą środków elektronicznych, w tym w internecie, nie może jednak opierać się wyłącznie na tym czynniku.

Zarazem niektóre postanowienia nowych przepisów nakładają na platformy internetowe obowiązek współpracy, by nakłonić je do wprowadzenia i upublicznienia nowych kroków na rzecz usuwania *fake newsów*. Po pierwsze operatorzy platform internetowych muszą wyznaczyć we Francji przedstawiciela prawnego, który posłuży jako osoba kontaktowa przy stosowaniu nowych regulacji. Platformy pośród innych działań powinny zapewnić użytkownikom możliwość oznaczania fałszywych informacji w sposób „łatwo dostępny i widoczny”[13]. Dodatkowe wysiłki mogą objąć następujące pola:

- przejrzystość algorytmów platformy,
- promowanie treści z prasy, agencji informacyjnych i serwisów komunikacji audiowizualnej,
- walka z kontami rozsiewających fałszywe informacje na masową skalę,
- informowanie użytkowników o naturze, pochodzeniu i trybach rozpowszechniania treści,
- informowanie użytkowników o tożsamości osób przekazujących wynagrodzenie w zamian za promowanie treści informacyjnych,
- propagowanie umiejętności korzystania z mediów i informacji[14].

Wszystkie działania podejmowane pod tym względem oraz przekazane na nie środki mają być spisywane w corocznym dokumencie przekazywanym do CSA, która później publikuje raport o stosowanych przez platformy internetowe środkach walki z fałszywymi informacjami oraz ocenę ich skuteczności. Ta sama agencja regulacyjna nadawców radiowych i telewizyjnych jest także władna publikować zalecenia skierowane do platform. Zdecydowała się na to po raz pierwszy w kontekście wyborów do europarlamentu w 2019 i opublikowała listę zaleceń[15], zawierającą te same sześć punktów co opisane wyżej dodatkowe wysiłki proponowane w tekście ustawy z 22 grudnia 2018 r.

Aktywność agencji rządowych

O ile obserwacja przemian prawodawstwa to znakomite narzędzie, by ocenić nasilenie działań przeciw dezinformacji we Francji, warta podkreślenia jest także coraz bardziej aktywna rola agencji rządowych w tej sferze. Rosnące uprawnienia CSA omówione zostały w poprzednim podrozdziale, a wspomnieć można o dwu innych organach – Krajowej Komisji Kontroli Prezydenckiej Kampanii Wyborczej (fr. *Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle*, CNCCEP) i ANSSI – z uwagi na ich kluczową rolę w odpieraniu działań w złych zamiarach, zwłaszcza podczas wyborów na urząd prezydenta w 2017. Trzeba zauważyć, że ich wysiłki skupiały się także na przeciwdziałaniu cyberatakom, ale agencje pracowały również ze sztabami wyborczymi kandydatów, aby poprawić ich kompetencje cyfrowe podczas warsztatów lub poprzez wydawanie konkretnych wytycznych. W dodatku szybka reakcja CNCCEP po ukazaniu się MacronLeaks miała podstawowe znaczenie w radzeniu sobie z wpływem tej kampanii dezinformacyjnej. Publikując dzień później materiał dla prasy, komisja wezwała media, by „nie informować o treści tych danych, zwłaszcza na stronach internetowych, przypominając, że rozpowszechnianie fałszywych informacji to naruszenie prawa, w szczególności karnego"[16]. Tradycyjne media potraktowały temat informacji zawartych w przeciekach ostrożnie, a niektóre zwróciły nawet uwagę odbiorców na podejrzany moment zdarzenia, tym samym edukując ich na swój sposób w zakresie umiejętności korzystania z mediów.

Działalność organizacji pozarządowych oraz inicjatywy trzeciego sektora

Obok działań rządowych i wdrożenia nowych ram legislacyjnych, kwestia dezinformacji wywołała także mobilizację innych podmiotów, przede wszystkim w obrębie mediów i społeczeństwa obywatelskiego. Przez rozmaite działania takie jak kampanie umiejętnego korzystania z mediów i inicjatywy weryfikacyjne (sprawdzające fakty) pełnią one aktywną rolę w walce z matactwami i mistyfikacjami we Francji.

Siła weryfikacji

W obliczu bezprecedensowego kryzysu, na tle wyraźnej utraty wiarygodności w oczach opinii publicznej, sytuacja skłoniła tradycyjne media francuskie, by przypuścić kontratak na zjawisko fałszywych informacji w celu odzyskania dawnej pozycji. Tworzenie stron, platform i blogów sprawdzających fakty należy do zasadniczych przeobrażeń na polu dziennikarstwa w ostatniej dekadzie. W latach 2008 i 2009 dwa dzienniki, „Libération" i „Le Monde", założyły własne blogi

– odpowiednio Désintox w przypadku „Libération" i Les Décodeurs pod egidą „Le Monde" – mając na uwadze prosty cel: sprawdzać informacje pojawiające się w internecie. Z czasem blogi przyciągnęły uwagę szerszego grona i zostały włączone jako rubryki w obręb portali obu gazet. Partnerstwa z innymi mediami pozwoliły im przyczynić się do rozwoju sprawdzania faktów we Francji. Za przykładem prasy tą samą drogą poszły skądinąd rozmaite media, na przykład swoje inicjatywy zorganizowały telewizje France 24 i Arte.

Wypada jednak wspomnieć, że duże media nie są jedynymi podmiotami zajmującymi się sprawdzaniem faktów. Jedną z najstarszych inicjatyw mających na celu odpieranie dezinformacji jest we Francji oparta na współpracy platforma hoaxbuster.com. Pierwotnie powstała w 2000 r. strona skupiała się na ujawnianiu bujd szerzących się w internecie przez łańcuszki e-mailowe. Przy szybkim rozwoju mediów społecznościowych ewoluowała w kierunku obalania nieprawdziwych pogłosek i informacji w sposób pedagogiczny, wyjaśniając czytającym, jak zauważyć takie fałszywki. HoaxBuster opiera się na udziale internautów, którzy nadsyłają pytania, prosząc platformę o weryfikację faktów zawartych w przeczytanym artykule, otrzymanym e-mailu czy zauważonym poście. Krajobraz inicjatyw sprawdzania faktów uzupełniają wreszcie wyspecjalizowane blogi, np. Les Surligneurs, skupione na weryfikacji aspektów prawnych tytułów materiałów w mediach czy przemów politycznych.

Aby walczyć z szerzeniem się *fake newsów* dotyczących pandemii COVID-19, rząd Francji stworzył internetowy serwis z odwołaniami do sprawdzających fakty artykułów na ten i powiązane tematy, nazwany Désinfox Coronavirus. Został on wprawdzie skasowany niedługo potem w efekcie skargi krajowego związku zawodowego dziennikarzy, którzy ostro skrytykowali tendencyjność doboru źródeł, ponieważ strona zbierała informacje jedynie z kilku[17].

W tabeli 4 znajduje się nieroszczący sobie praw do kompletności przegląd inicjatyw sprawdzających fakty aktywnych obecnie we Francji.

Przenosząc uwagę na nieco inny obszar i patrząc bardziej globalnie, warto zauważyć, że pięć mediów francuskich – AFP, „Le Monde", „Libération", France 24, „20 Minutes" – otrzymało w 2019 certyfikat Międzynarodowej Sieci Fact-Checkingowej (ang. *International Fact-Checking Network*) i działa wspólnie z Facebookiem i Instagramem na rzecz przeglądania zamieszczanych tam treści, w tym postów organicznych i opłacanych oraz obrazów, wideo i linków.

Wspieranie umiejętności korzystania z mediów i informacji

O ile mnożenie się weryfikujących fakty stron, blogów i tematycznych serwisów zapewnia cenne narzędzia dostrzegania dezinformacji w sieci, niemało pracy dodatkowej trzeba jeszcze wykonać w sprawie uświadamiania odbiorców. *De facto* muszą oni, aby móc w ogóle użyć narzędzi fact-checkingowych, niejako zrozumieć problem, który dezinformacja tworzy i rozwinąć własne zdolności sprawdzania faktów. W następstwie ataków terrorystycznych we Francji w 2015 r. poświęcono więcej uwagi zapobieganiu szerzenia teorii spiskowych i zachowań niebezpiecznych, często powiązanych z fałszywymi informacjami internetowymi. Ocenia się, że w roku 2016 około 55 istotnych inicjatyw zwiększania kompetencji medialnych i informacyjnych przejawiało we Francji aktywność[18], a można przypuszczać, że ich liczba od tamtej pory wzrosła. Co więcej, zgodnie z raportem *Wyniki indeksu umiejętności korzystania z mediów i informacji 2019* autorstwa Inicjatywy Polityk Europejskich w Instytucie Społeczeństwa Otwartego – Sofia to właśnie we Francji widać największe postępy, a kraj ten zyskał cztery punkty i przesunął się o cztery miejsca na liście[19] między 2017 i 2019 r. Indeks zawiera szacunki odporności 35 państw europejskich na fałszywe informacje, używając wskaźników wolności mediów, edukacji i zaufania do dziennikarstwa.

Tabela 4. Główne strony i inicjatywy fact-checkingowe działające we Francji od roku 2000.

TYTUŁ MACIERZYSTY	NAZWA	MEDIUM	KRÓTKI OPIS	DATA POWSTANIA
HoaxBuster	HoaxBuster	Sieć	Internetowa platforma oparta na współpracy, obalająca fałszywki i pogłoski	2000
„Libération"	Désintox	Sieć, następnie telewizja	Blog (2008–2013), później rubryka na stronie dziennika „Libération" (2013–2018) oraz program wideo nagrywany we współpracy z Arte France (2012–obecnie)	2008
„Le Monde"	Les Décodeurs	Sieć (częściowo radio)	Blog (2009–2014), rubryka internetowa od 2014, partnerstwo z radiem France Inter w latach 2012–2013	2009
Franceinfo	Le Vrai du Faux	Radio	Cotygodniowy program radiowy, od sierpnia 2012 r. codzienny	2012
France 24	Intox	Sieć	Rubryka internetowa w dziale „Les Observateurs" (Obserwatorzy)	2014
„20 Minutes"	Fake Off	Druk i sieć	Seria artykułów	2017
„Libération"	CheckNews	Sieć	Serwis odpowiadający na pytania internautów o wiadomości w mediach i rozprawiający się z pogłoskami	2017
Les Surligneurs	Les Surligneurs	Sieć	Strona skupiająca się na kwestiach prawnych	2017
AFP	Factuel	Sieć	Blog sprawdzający wiadomości z różnych regionów, dostępny w 18 językach	2017
France 2	Faux et usage de faux	Telewizja	Część telewizyjnego programu informacyjnego	2019

Źródło: zestawienie własne oparte na danych skompilowanych przez Laurenta Bigota w artykule *Le fact checking en France, en une chronologie*, La Revue des médias (październik 2019).

Ostateczne wyniki wskazują, że po zgromadzeniu 59 punktów i zdobyciu 15 miejsca Francja znajduje się w drugiej grupie państw, osiągając dobre rezultaty i wychodząc ponad średnią (patrz Mapa, strona 8).

Z działań na rzecz rozwijania tych kompetencji, które głównie odbywają się w szkole, najczęściej korzystają dzieci i młodzież. Dziennikarze i weryfikatorzy faktów regularnie prowadzą warsztaty czy niewielkie konferencje na temat mediów i informacji, a współcześnie coraz mocniej skupiają się na tym, jak dostrzec dezinformację w sieci. Do najbardziej znanych inicjatyw należy Tydzień Prasy i Mediów w Szkole (fr. *La semaine de la presse et des médias à l'école*), organizowany od 1989 r. przez francuskie Centrum Edukacji Medialno-Informacyjnej (fr. *Le Centre pour l'éducation aux médias et à l'information*, CLEMI). Zachęcanie dzieci do stawania się mądrzejszymi i rozsądniejszymi obywatelami w sieci to ważkie zadanie, które CLEMI stawia sobie za cel. Centrum jest częścią krajowego Ministerstwa Edukacji Narodowej i Młodzieży, ale współpracuje z licznymi podmiotami prywatnymi i trzeciego sektora, by realizować swoją misję. Niedawnym przykładem jest wspólna inicjatywa dziennikarzy „Le Monde" i AFP oraz stowarzyszenia *Entre les lignes*, by prowadzić warsztaty pomagające młodzieży odróżniać w sieci informacje prawdziwe i fałszywe oraz analizować zdjęcia i wideo i zauważać w nich ślady manipulacji lub fałszerstwa.

Sprawdzanie faktów i umiejętność korzystania z mediów i informacji to dwie dobrze rozwinięte we Francji branże, uzupełniające ramy prawne ustanowione przez rząd do walki z dezinformacją. Niemniej, jeśli mowa o inicjatywach pozarządowych w tym obszarze, spostrzec można pewien brak centrów badawczych i ośrodków analitycznych specjalnie poświęconych zagadnieniu.

Działalność mediów społecznościowych w poszczególnych krajach

W miarę jak liczba ich użytkowników i globalne wpływy rosły przez ostatnią dekadę, platformy społecznościowe mierzą się z rosnącym naciskiem ze strony prawodawców, by moderowały treści na swoich serwerach. Relacje szefów firm z głowami państw czy rządami ewoluowały w różnych kierunkach. Od wyborów w 2017 r. prezydent Macron często spotykał się z interesariuszami ze świata mediów społecznościowych, a niedawno promował pogłębiony dialog między nimi a władzami publicznymi z zamiarem wspólnej pracy nad rozwiązywaniem nowych problemów, przed którymi stoją.

Eksperyment Facebooka

Między styczniem a lutym 2019 r. międzyministerialna grupa zadaniowa złożona z ekspertów wysokiego szczebla i stałych sprawozdawców z kilku ministerstw, kancelarii premiera i niezależnych autorytetów pracowała z Facebookiem nad prekursorskim eksperymentem. Jak stwierdza list przewodni, cel stanowiło „zbadanie ogólnych ram regulacji sieci społecznościowych, począwszy od walki z nienawiścią w sieci, na zasadzie dobrowolnej współpracy Facebooka niewymaganej przez przepisy prawa”[20]. Pomysł polegał zatem na przyjrzeniu się zasadom moderacji na tej platformie, zasobom przydzielonym przez nią do tego zadania i stronie organizacyjnej oraz na wymyśleniu nowego instrumentu, by odpowiednio wypośrodkować między swobodami obywatelskimi – a szczególnie wolnością wypowiedzi – i ochroną porządku publicznego w sieciach społecznościowych.

Raport wskazuje, że wymiana zdań między reprezentantami Facebooka i francuskich ministerstw skupiała się głównie na treściach nienawistnych, ale wnioski płynące z projektu można zastosować do wszelkich kwestii, o które zahaczają treści zamieszczane w mediach społecznościowych, włączając w to dezinformację. Specjalny nacisk położono na globalny wymiar i globalne skutki rozpowszechniania treści w sieci oraz na fakt, że rezultaty francuskiej inicjatywy powinny być możliwe do przeniesienia i zastosowania w dowolnym kraju członkowskim UE. Zespół zalecił utworzenie nowego systemu regulacji opartego na pięciu filarach:

1. „Publiczna polityka regulacyjna gwarantująca wolności osobiste i swobodę działalności gospodarczej platform.

2. Regulacje normatywne skupione na rozliczalności sieci społecznościowych, wdrażane przez niezależne władze administracyjne i oparte na trzech obowiązkach nałożonych na platformy:
   - obowiązek przejrzystego działania w porządkowaniu treści,
   - obowiązek przejrzystego działania w stosowaniu regulaminu i moderacji treści,
   - obowiązek dochowania należytej staranności względem użytkowników.

3. Dialog polityczny między operatorami, rządem, ustawodawcą i społeczeństwem obywatelskim.

4. Niezależna władza administracyjna działająca we współpracy z innymi organami państwa i otwarta na społeczeństwo obywatelskie.

5. Ogólnoeuropejska współpraca, wzmacniająca zdolności Państw Członkowskich do podejmowania działań wobec światowych platform i zmniejszająca ryzyko polityczne związane ze stosowaniem filarów w każdym Państwie Członkowskim”[21].

Wnioski wysnute z projektu są co najmniej tak interesujące jak sam pomysł i przebieg zadania. Taka współpraca między czołowymi podmiotami prywatnymi i instytucjami publicznymi wysokiego szczebla na poziomie ministerialnym wzmacnia wzajemne zrozumienie swoistych wyzwań, z którymi mierzą się obie strony, i daje większe szanse na wprowadzenie nowych rozwiązań niełatwych problemów wyłaniających się w związku z treściami w sieci. Przyjęte przez rząd francuski podejście oparte na współpracy odbiega od mniej elastycznych postaw w innych państwach Europy, które uszczegółowią inne rozdziały raportu.

Podsumowanie

Jako kraj mocno przywiązany do wolności wypowiedzi Francja od 1881 r. buduje ramy prawne zapobiegające rozpowszechnianiu fałszywych informacji. Przecieki, które nastąpiły podczas prezydenckiej kampanii wyborczej w 2017 r., stanowiły jednak przewrót w myśleniu i uświadomiły francuskim politykom, jakie wyzwania dezinformacja internetowa stawia systemowi demokratycznemu. Nowa ustawa, uchwalona w grudniu 2018 r., jest wymierzona dokładniej przeciw zjawisku dezinformacji internetowej i ma na celu przeciwdziałanie fałszywym informacjom w okresach poprzedzających wybory. Obok wysiłków władz państwowych odbywają się liczne inicjatywy pozarządowe, ogniskujące się głównie na sprawdzaniu faktów i poprawie umiejętności korzystania z mediów i informacji przez społeczeństwo. Francja stała się też ostatnio sceną nowych prób współpracy między podmiotami publicznymi i prywatnymi, które mają pozwolić na lepsze zrozumienie wyzwań i następstw walki z dezinformacją.

Zważywszy, że fałszywe informacje to zjawisko ogólnoświatowe, którego skuteczne zwalczanie wymaga współpracy, warto wreszcie wspomnieć o kilku francuskich interesariuszach uczestniczących w działaniach na skalę ponadpaństwową. Działalność taka najczęściej odbywa się na poziomie unijnym; wymienić można stowarzyszenie branżowe znad Sekwany – *Association des Agences-Conseils en Communication* – sygnatariusza Unijnego kodeksu postępowania w zakresie zwalczania dezinformacji zainicjowanego przez Komisję Europejską w 2018 r. Ponadto Komisją Specjalną ds. Obcych Ingerencji we Wszystkie Procesy Demokratyczne w Unii Europejskiej, w tym Dezinformacji (INGE), powstałą w Parlamencie Europejskim w czerwcu 2020 r., kieruje francuski eurodeputowany Raphaël Glucksmann. Troje posłów z Francji zasiada w tej komisji, dwóch kolejnych pełni rolę zastępstwa. Działania zwalczające dezinformację na poziomie krajowym są kluczowe, aczkolwiek to właśnie zaangażowanie i współpraca na poziomie paneuropejskim są dziś zapewne najistotniejsze, toteż europejskie oraz krajowe władze publiczne powinny poświęcać im szczególną uwagę i wiele starań.

PRZYPISY

1 Kilka przykładów wprowadzających w błąd tweetów mozna znaleźć w artykule Jeana-Marca Manacha, *On a examiné les «Macron Leaks» pour vous, voilà ce qu'on y a trouvé*, Slate 2017, [online]: http://www.slate.fr/story/145221/le-macronleaks-est-une-fakenews.

2 Noémie Bonnin, *Les réseaux sociaux première source d'info en ligne chez les personnes sensibles aux théories du complot*, Francetvinfo 2019, [online]: https://www.francetvinfo.fr/internet/reseaux-sociaux/info-franceinfo-les-reseaux-sociaux-premiere-source-d-info-en-ligne-chez-les-personnes-sensibles-aux-theories-du-complot_3191963.html.

3 Ibidem.

4 *Une enquête ouverte sur le piratage d'En Marche!*, „Les Échos" 2017, [online]: https://www.lesechos.fr/2017/05/une-enquete-ouverte-sur-le-piratage-d-en-marche-167537.

5 *Deklaracja Praw Człowieka i Obywatela*, artykuł XI, tłum. Stanisław Posner, Warszawa 1907 (oryg. 1789), [online]: https://polona.pl/item/deklaracja-praw-czlowieka-i-obywatela,NzI1NTM1MTI/24/#info:metadata.

6 Loi du 29 juillet 1881 sur la liberté de la presse, artykuł 27, [online]: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/2020-11-27/.

7 Basile Ader, *Coronavirus et « fake news »*, Auguste Debouzy 2020, [online]: https://www.august-debouzy.com/fr/blog/1412-le-coronavirus-et-les-fake-news.

8 *Video: Macron slams RT, Sputnik news as 'lying propaganda' at Putin press conference*, France 24 2017, [online]: https://www.france24.com/en/20170530-macron-rt-sputnik-lying-propaganda-putin-versailles-russia-france-election.

9 Loi n° 2018-1202 du 22 décembre 2018, artykuł 1, [online]: https://www.legifrance.gouv.fr/jorf/id/JORFARTI000037847566.

10 Ibidem; Décret n° 2019-297 du 10 avril 2019 relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général, art. 1, [online]: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038359165.

11 Loi n° 2018-1202 du 22 décembre 2018, op. cit., art. 6.

12 Loi n° 2018-1202 du 22 décembre 2018, op. cit., art. 8.

13 Loi n° 2018-1202 du 22 décembre 2018, op. cit., art. 11.

14 Ibidem.

15 Recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations, Conseil supérieur de l'audiovisuel, [online]: https://www.csa.fr/Reguler/Espace-juridique/Les-textes-reglementaires-du-CSA/Les-deliberations-et-recommandations-du-CSA/Recommandations-et-deliberations-du-CSA-relatives-a-d-autres-sujets/Recommandation-n-2019-03-du-15-mai-2019-du-Conseil-superieur-de-l-audiovisuel-aux-operateurs-de-plateforme-en-ligne-dans-le-cadre-du-devoir-de-cooperation-en-matiere-de-lutte-contre-la-diffusion-de-fausses-informations.

16 Recommandation aux médias suite à l'attaque informatique dont a été victime l'équipe de campagne de M. Macron, Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle, [online]: http://www.cnccep.fr/communiques/cp14.html.

17 *Le gouvernement supprime sa page controversée « désinfox coronavirus »*, „Le Monde" 2020, [online]: https://www.lemonde.fr/actualite-medias/article/2020/05/05/le-gouvernement-supprime-sa-page-controversee-desinfox-coronavirus_6038753_3236.html.

18 European Audiovisual Observatory, *Mapping of media literacy practices and actions in EU-28*, Strasbourg 2016, [online]: https://rm.coe.int/1680783500.

19 Open Society Institute – Sofia, *Just think about it. Findings of the Media Literacy Index 2019*, [online]: https://osis.bg/wp-content/uploads/2019/11/MediaLiteracyIndex2019_-ENG.pdf.

20 *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, Mission report "Regulation of social networks – Facebook experiment"*, version 1.1, May 2019, [online]: https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf.

21 Ibidem.

Michał Krawczyk

Zjednoczone Królestwo

Wstęp

Na początku marca 2018 r. Wielka Brytania stała się ofiarą bezprecedensowych działań ze strony rosyjskich służb specjalnych, które dokonały zamachu z wykorzystaniem broni chemicznej na jej terytorium[1]. Celem ataku był Siergiej Skripal, były rosyjski oficer wojskowy oraz podwójny agent brytyjskich służb wywiadowczych[2]. Niespotykana po rozpadzie Związku Sowieckiego sytuacja doprowadziła do poważnego kryzysu dyplomatycznego oraz miała swoją kontynuację w cyberprzestrzeni, gdzie Moskwa rozpoczęła operację informacyjną. Rosyjskie media publiczne stworzyły w ciągu kilku tygodni 138 sprzecznych[3] ze sobą wersji wydarzeń, które następnie były rozpowszechniane w brytyjskiej przestrzeni informacyjnej za pomocą mediów społecznościowych. Celem było odwrócenie uwagi, wprowadzenie chaosu i podważenie zaufania do oficjalnych komunikatów[4]. Ówczesna Premier Wielkiej Brytanii Theresa May opisała te zdarzenia jako „falę dezinformacji", z którą Wielka Brytania zderzyła się w ciągu kilku dni po zamachu na Skripala[5]. Nie był to pierwszy raz, gdy Wielka Brytania musiała mierzyć się z dezinformacją oraz manipulacją *online*. Już wybory prezydenckie w Stanach Zjednoczonych w 2016 r. pośrednio skupiły uwagę Londynu na tym problemie, szczególnie poprzez działalność brytyjskiej firmy Cambridge Analytica, która stała się głośna ze względu na skandal związany z pozyskaniem przez nią danych 87 milionów użytkowników platformy Facebook i wykorzystaniem ich do stworzenia zaawansowanych modeli osobowości użytych następnie do prowadzenia ukierunkowanej (ang. *targeting*) kampanii prezydenckiej dla m.in. Donalda Trumpa oraz Teda Cruza[6]. Działalność Cambridge Analytica za oceanem zwróciła uwagę także na rozległą aktywność firmy w Wielkiej Brytanii, szczególnie w kontekście kampanii referendalnej dotyczącej Brexitu[7]. Wszystkie te zdarzenia doprowadziły do zwiększenia świadomości i zainteresowania

problemem dezinformacji i manipulacji *online* wśród opinii publicznej, mediów oraz klasy politycznej. Uruchomiło to w konsekwencji działania mające na celu rozpoznanie problemu, jego definicję oraz walkę z nim, w które zaangażowali się politycy, media oraz organizacje pozarządowe.

Dezinformacja w Wielkiej Brytanii

W styczniu 2017 r. parlament Zjednoczonego Królestwa sformułował potrzebę zorganizowania dochodzenia parlamentarnego (ang. *parliamentary inquiry*) dotyczącego zagadnienia dezinformacji i *fake news*, którą powtórzył po przedterminowych wyborach z czerwca 2017 r. W rezultacie w Izbie Gmin rozpoczęła działalność Komisja ds. Cyfryzacji, Kultury, Mediów i Sportu (ang. *Digital, Culture, Media and Sport Committee*). Głównym rezultatem przeprowadzonych badań, analiz oraz szeregu konsultacji i przesłuchań był raport *Disinformation and 'fake news'*, wydany w dwóch wersjach: raport okresowy z 29 lipca 2018 r. oraz raport końcowy z 18 lutego 2019 r. Pierwszy z nich porządkował dotychczas znaną wiedzę ogólną na temat zjawiska, próbował rozwiązać kwestie definicyjne, charakteryzował narzędzia służące do rozprzestrzeniania nieprawdziwych informacji i prezentował przykłady nieprawidłowości w przestrzeni informacyjnej oraz dotychczas udokumentowanych operacji informacyjnych. Raport końcowy skupiał się na zagadnieniu roli oraz odpowiedzialności platform internetowych, kwestii gromadzenia i wykorzystywania danych przez prywatne organizacje, roli płatnych reklam politycznych oraz na zagranicznych operacjach wpływu.

Zaprezentowano także rozbudowany zestaw rekomendacji dotyczących przyszłych działań legislacyjnych i organizacyjnych. Do najważniejszych postulatów można zaliczyć:

1. Regulację mediów społecznościowych i stworzenie nowych definicji prawnych oraz rozwiązań legislacyjnych dla firm technologicznych, aby umożliwić egzekwowanie od platform społecznościowych odpowiedzialności za materiały publikowane na ich łamach.
2. Stworzenie regulacji i obowiązkowego kodeksu etyki, których przestrzeganie miałoby być nadzorowane przez niezależnego regulatora z ustawowymi prawami do monitorowania działalności poszczególnych firm technologicznych.
3. Ochrona danych użytkowników i nadzór nad ich przetwarzaniem za pomocą algorytmów oraz AI przez firmy technologiczne.
4. Kompetencje cyfrowe (ang. *digital literacy*) powinny stać się czwartym filarem podstawowej edukacji, na równi z czytaniem, pisaniem i liczeniem.

Raport stanowi ważny wkład w proces przeciwdziałania dezinformacji w Wielkiej Brytanii. Zawiera on kompleksową analizę zagadnienia dotykającą wielu płaszczyzn oraz prezentuje rozbudowany zestaw rekomendacji dla działań rządu, które zostały wzięte pod uwagę przy tworzeniu rządowej strategii walki z zagrożeniami *online* (ang. *Online Harms White Paper*).

Kolejnym elementem brytyjskich działań w obszarze walki z dezinformacją była opublikowana w kwietniu 2019 r. przez rząd biała księga *Online Harms White Paper*, w której przedstawiono rządowe propozycje walki z zagrożeniami w sieci. Zagrożenia zostały zdefiniowane jako „treści lub działania *online* szkodzące użytkownikom, w szczególności dzieciom lub zagrażające »brytyjskiemu sposobowi życia« poprzez obniżenie poziomu bezpieczeństwa narodowego lub przez podważanie naszych [tj. brytyjskich – przyp. aut.] praw i obowiązków…”[8]. Wyrażone w białej księdze stanowisko identyfikuje dezinformację oraz manipulację jako jeden z typów szkodliwej działalności *online*, które powinny zyskać większą uwagę ze strony państwa oraz do walki z którymi potrzebne jest podjęcie zdecydowanych działań legislacyjnych. W kontekście dezinformacji podniesione zostało zarówno ryzyko wykorzystywania jej przez wrogie państwa (ang. *hostile states*) do podważania wartości i zasad demokratycznych oraz jako bezpośrednie zagrożenie dla społeczeństwa i życia obywateli. W przypadku zagrożeń zewnętrznych

z nazwy wymieniona została Federacja Rosyjska, określona jako państwo będące głównym źródłem dezinformacji, natomiast w obu przypadkach podkreślono rolę platform społecznościowych, które ze względu na swoją charakterystykę, model biznesowy oraz używanie algorytmów mogą sprzyjać szerzeniu się nieprawdziwych informacji.

Online Harms White Paper przedstawia zjawisko dezinformacji oraz manipulacji w cyberprzestrzeni jako ważne z punktu widzenia bezpieczeństwa narodowego i społecznego. Wskazuje także na potrzebę przedstawienia odpowiedniej legislacji i działań ze strony rządu, które będą odpowiadały wyzwaniom epoki cyfrowej. Dokument ten jest kolejnym krokiem na brytyjskiej ścieżce walki z dezinformacją w cyberprzestrzeni. Zapowiadane w nim działania w obszarze dezinformacji zostaną przedstawione w dalszej części rozdziału.

Istniejące regulacje dotyczące dezinformacji

W Zjednoczonym Królestwie nie funkcjonuje obecnie jeden organ nadzorujący platformy społecznościowe oraz zamieszczane na nich treści. Podobnie nie istnieje prawo odnoszące się do dezinformacji czy manipulacji *online* i zakazujące ich w sposób bezpośredni. Kwestia nielegalnej manipulacji oraz rozróżnienia pomiędzy rzetelnym przekazem informacji a treściami dezinformującymi nie jest natomiast nowością z perspektywy działań podejmowanych przez rząd Zjednoczonego Królestwa. Początek aktywności w tym obszarze to ustawa *Broadcasting Act 1990*, zakazująca stosowania urządzeń i technik w celu przekazywania wiadomości i wpływania na jednostki bez ich wiedzy. Ustawa dawała prawo nadzoru *Independent Television Commission*, następnie zastąpionemu przez *Office of Communications* (Ofcom).

Organy regulujące

Ofcom na mocy ustawy *Communication Act 2003* został wyposażony w kompetencje do kontrolowania i egzekwowania standardów treści w radiu i telewizji. Pomimo braku kompetencji regulacyjnych w obszarze mediów społecznościowych czy treści *online*, ustawa ta umożliwia Ofcom szereg aktywności kontrolnych związanych ze standardami nadawców, pluralizmem mediów oraz umiejętnością korzystania z nich[9]. Takie funkcje łączą się natomiast pośrednio z problemem dezinformacji i manipulacji w cyberprzestrzeni, które stały się przedmiotem prowadzonych przez Ofcom badań i analiz. Działania mające na celu zminimalizowanie fali nieprawdziwych wiadomości, które są realizowane poprzez kontrolę nadawców, a także akcje informacyjne i *fact-checkingowe* podjęto również w kontekście pandemii COVID-19. Do aktywności związanych z zagrożeniami *online* należy publikacja dokumentu przedstawiającego doświadczenia Ofcom w regulacji radia i telewizji, które mogą stanowić podstawę przyszłych wytycznych dotyczących szkodliwych treści *online*; uruchomienie programu *Making Sense of Media* działającego na rzecz podnoszenia umiejętności korzystania z treści *online* oraz szereg raportów, np. *Online Nation* badający, w jaki sposób treści i usługi *online* są oferowane użytkownikom oraz przedstawiający zachowanie użytkowników Internetu[10]. Ofcom zwraca uwagę, że fakt istnienia regulacji nadawców telewizyjnych i radiowych oraz równoczesny jej brak w przypadku treści *online* „doprowadził do »loterii standardów«, która pozwala platformom mediów społecznościowych wykorzystać luźne ramy prawne, podczas gdy tradycyjni nadawcy muszą przestrzegać surowych przepisów dotyczących ochrony odbiorców”[11]. Równocześnie Ofcom wzywa do wprowadzenia większej ilości regulacji dotyczących mediów społecznościowych, w szczególności Facebooka, YouTube'a i Twittera, które miałyby przede wszystkim wymagać od platform szybkiego i skutecznego usuwania nieodpowiednich treści pod groźbą nałożenia kary[12].

Kolejnym organem regulującym, który ma pewne kompetencje w obszarze dezinformacji i manipulacji, jest *Advertising Standards Authority* (ASA), będąca organizacją przemysłu reklamowego o kompetencjach samoregulujących (ang. *self-regulatory organisation*). Rolą ASA jest regulacja

treści reklam, promocji i marketingu bezpośredniego, do czego służy m.in. możliwość prowadzenia dochodzeń dotyczących ich zgodności z kodeksem praktyk reklamowych (ang. *The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing*)[13, 14].

Kwestia reklam politycznych oraz kampanii związanych z ważnymi tematami społecznymi czy politycznymi na platformach społecznościowych jest istotnym aspektem ogólnego problemu dezinformacji, o czym wspomina m.in. raport *Disinformation and 'fake news'*[15]. ASA ma ograniczony zakres działań w tym obszarze, ponieważ regulacje dotyczące reklam politycznych zostały wyłączone z jej nadzoru pod koniec lat 90. XX w. Pomimo tego do jej aktywności zalicza się dochodzenia, kontrole i orzeczenia związane z reklamami i kampaniami prowadzonymi wokół spraw społecznie wrażliwych, jak np. ochrona środowiska, które także są często przedmiotem dezinformacji oraz zorganizowanych operacji informacyjnych. Ponadto ASA należy do grupy konsultacyjnej uruchomionej przez brytyjską Komisję Wyborczą (ang. *The Electoral Commission*), która ma na celu m.in. koordynację podejmowanych przez jej członków działań zmierzających do walki z dezinformacją w obszarze reklamy i marketingu[16].

Przywołana powyżej brytyjska Komisja Wyborcza jest kolejnym organem regulacyjnym, który działa w obszarze dezinformacji i manipulacji *online* w kontekście reklam politycznych. Jej główna rola jako regulatora skupia się na monitorowaniu oraz egzekwowaniu zasad dotyczących finansowania kampanii politycznych i wydatkowania środków przez komitety wyborcze. To dotyczy także pieniędzy wydawanych na kampanie cyfrowe. Komisja posiada uprawnienia do prowadzenia dochodzeń, kontroli oraz sankcjonowania nieprzepisowych praktyk. Wszystkie dotyczą jednak sytuacji, w której prowadzone jest już śledztwo, a więc nie mogą być użyte w przypadku kontroli bieżących kampanii i reklam politycznych, prowadzonych w świecie cyfrowym, a w szczególności na platformach społecznościowych, których obecny status prawny umożliwia brak współpracy z Komisją Wyborczą. Komisja w jednym ze swoich oficjalnych dokumentów apeluje o zwiększenie uprawnień w kwestii udostępnienia dokumentów od osób i organizacji trzecich, co miałoby umożliwić pozyskanie danych od dostawców usług cyfrowych[17]. Ponadto można zwrócić uwagę, że do tej pory kwestia kontroli i przejrzystości finansowania reklam i kampanii politycznych na platformach społecznościowych zależała wyłącznie od woli samych platform. W jednej ze swoich rekomendacji dla rządu Komisja wnosi, aby oddolne działania platform zostały poddane obserwacji i ocenie, a w razie stwierdzenia niesatysfakcjonujących działań i wyników, aby kwestia ta stała się przedmiotem legislacji i regulacji ze strony rządu Wielkiej Brytanii[18].

Podczas gdy reklamy polityczne nadawane przez telewizję czy radio są przedmiotem ścisłej kontroli przez Ofcom, a działania poszczególnych komitetów wyborczych przez Komisję Wyborczą, to te same aktywności na platformach społecznościowych pozostają w swego rodzaju szarej strefie. Rodzi to szczególne zagrożenie ze względu na możliwość bezpośredniego i indywidualnego kierowania (ang. *targeting*) oraz personalizowania reklam i treści dla konkretnych grup społecznych czy indywidualnych użytkowników, którego mechanizm pozostaje bez jakiejkolwiek kontroli z zewnątrz. Efektem są nowego rodzaju zagrożenia dla procesów wyborczych.

Kolejnym organem regulującym w szeroko rozumianym obszarze dezinformacji i manipulacji *online* jest Biuro Rzecznika Informacji (ang. *The Information Commissioner's Office*, ICO), będące pozaresortowym organem publicznym odpowiadającym przed parlamentem Zjednoczonego Królestwa. ICO zajmuje się kwestiami związanymi z wolnością przepływu informacji oraz prywatnością danych[19] i nadzoruje przestrzeganie m.in. *Data Protection Act 2018*, *General Data Protection Regulation* (GDPR) oraz *Privacy and Electronic Communications Regulations 2003*. Zgodnie z prawem ICO może podjąć działania w celu zmiany zachowania organizacji lub jednostek, które zbierają, przetwarzają

i przechowują dane osobowe. Jego kompetencje obejmują prowadzenie dochodzeń i audytów, egzekwowanie przepisów karnych oraz nakładanie kar. Ze względu na swoje zadania ICO bada m.in. wykorzystywanie danych oraz personalizowanie treści przez platformy mediów społecznościowych. ICO skorzystało z uprawnień do prowadzenia śledztw i karania podmiotów łamiących prawo w tym zakresie m.in. w 2018 r., kiedy zastosowało najwyższą możliwą karę pieniężną – 500 tysięcy funtów dla Facebooka za dwukrotne wykroczenie przeciwko *Data Protection Act 1998*. Dochodzenie ICO wykazało, że Facebook naruszył prawo przez zaniechanie ochrony danych osobowych, które zostały następnie wykorzystane m.in. przez Cambridge Analytica do nielegalnego tworzenia profilów psychologicznych użytkowników podczas wyborów prezydenckich w Stanach Zjednoczonych w 2016 r. ICO zajmuje się więc ochroną danych osobowych i kontrolowaniem ich wykorzystania w obszarze dezinformacji i manipulacji *online*. Jak sama organizacja podkreśliła w wydanym przez siebie raporcie *Investigation into the use of data analytics in political campaigns*, niekontrolowane wykorzystanie danych milionów użytkowników korzystających z mediów społecznościowych jest ogromnym zagrożeniem dla prawidłowego przepływu informacji i odpowiedniego funkcjonowania procesów wyborczych. Manipulowanie i dezinformowanie stało się o wiele łatwiejsze i wydajniejsze właśnie dzięki nielegalnemu wykorzystaniu danych osobowych pochodzących najczęściej z platform społecznościowych i braku bezpośredniej jurysdykcji jednego regulatora nad sposobem działania tych platform[20].

Ostatnim organem, który można zaliczyć do regulatorów w obszarze dezinformacji i manipulacji *online* jest Urząd Ochrony Konkurencji i Rynku (ang. *Competition and Markets Authority*, CMA). CMA jest jednostką odpowiedzialną za wzmacnianie konkurencji biznesowej oraz zapobieganie i ograniczanie działań antykonkurencyjnych. W ramach swoich kompetencji CMA wielokrotnie podnosił zarzuty wobec największych platform społecznościowych, które jego zdaniem ze względu na swój charakter oparty na finansowaniu z reklam oraz model biznesowy dążący do monopolizacji rynku mają negatywny wpływ na przestrzeń informacyjną oraz dostęp do niezależnych mediów. Jak można przeczytać w raporcie *Online platforms and digital advertising*, wydanym przez CMA: „(...) Wreszcie, obawy związane z platformami internetowymi finansowanymi z cyfrowych reklam mogą prowadzić do szerszych szkód społecznych, politycznych i kulturowych poprzez upadek niezależnych i wiarygodnych mediów informacyjnych, wynikające z tego rozprzestrzenianie się *fake news* oraz upadek lokalnej prasy (...)"[21]. CMA w swoich działaniach w obszarze dezinformacji skupia się więc na zapobieganiu monopolizacji rynku i przestrzeni informacyjnej przez kilka największych platform, lobbowaniu na rzecz ścisłych regulacji dla dużych firm technologicznych oraz kontrolowaniu przestrzegania praw konsumentów przez te firmy.

Działania rządowe

Poza opisaną wyżej białą księgą *Online Harms* rząd Zjednoczonego Królestwa podjął wiele innych inicjatyw i aktywności w obszarze zwalczania dezinformacji. Znajdują się wśród nich zmiany doktrynalne, nowo powstałe jednostki badawcze i naukowe, projekty edukacyjne oraz wiele innych. Do najważniejszych zaliczają się następujące:

- *Fusion Doctrine* – wprowadzona w 2018 r. w ramach rządowego Przeglądu Zdolności Bezpieczeństwa Narodowego (ang. *National Security Capability Review*). Według niej służby wywiadowcze będą odpowiedzialne za identyfikację platform, które odpowiedzialne są za rozprzestrzenianie dezinformacji. Doktryna ta wskazuje, iż komunikację strategiczną należy traktować z powagą równą działaniom finansowym czy militarnym. Szczegóły *Fusion Doctrine* nie zostały nigdy upublicznione[22].
- *National Security Communications Team* (NCST) – po wzmożonej aktywności aktorów rozprzestrzeniających dezinformację w 2018 r., rząd Wielkiej Brytanii zapowiedział znaczącą

rozbudowę NSCT. Ich głównym zadaniem jest przeciwdziałanie zagrożeniom dla bezpieczeństwa narodowego i walka z ich „elementami komunikacyjnymi", w tym m.in. dezinformacją. Wśród działań NCST można wymienić akcję informacyjną *Don't Feed the Beast* mającą na celu edukację społeczeństwa w zakresie rozpoznawania dezinformacji.

- *Rapid Response Unit* – jednostka wchodząca w skład *Government Communication Service* (GCS), która została stworzona w ramach rządowej polityki „przywracania debaty publicznej opartej na faktach"[23]. Rolą *Rapid Response Unit* jest „monitorowanie wiadomości i informacji publikowanych lub udostępnianych *online* w celu szybkiej, dokładnej i rzetelnej identyfikacji pojawiających się problemów". Działania te mają pomóc Rządowi „(...) zrozumieć obecne środowisko medialne i ocenić skuteczność komunikacji publicznej"[24].
- *The RESIST Model* – zestaw narzędzi (ang. *toolkit*) stworzony z myślą o rządowych pracownikach i menedżerach wyższego szczebla oraz specjalistach ds. komunikacji w sektorze publicznym. Celem jest wyposażenie jego odbiorców w kompleksową wiedzę na temat zagrożenia dezinformacją. Zawiera także opis sześciu kroków zalecanych w celu jego zmniejszenia[25].
- *Centre for Data Ethics and Innovation* – jednostka powstała w ramach *Department for Digital, Culture, Media & Sport*. Jej cel stanowi rozwój wiedzy na temat technologii opartych na danych oraz przełomowych rozwiązań opartych m.in. na AI i algorytmach. Bada także wykorzystanie danych i algorytmów do wpływania na przestrzeń informacyjną i jej „patologizację"[26].
- *Open Information Partnership* – program łączący organizacje oraz ekspertów zajmujących się ujawnianiem i zwalczaniem dezinformacji. Zapoczątkowana w 2019 r. sieć łączy dziennikarzy śledczych, organizacje pozarządowe, think tanki, akademików, aktywistów i fact-checkerów z ponad 20 krajów. Głównym celem jest wymiana wiedzy i umiejętności oraz dofinansowanie projektów organizacji członkowskich. Stworzony i prowadzony przez Biuro Spraw Zagranicznych (ang. *Foreign Office*)[27].

Proponowana legislacja oraz plan działania Wielkiej Brytanii

Przywołane wcześniej dwa najważniejsze brytyjskie dokumenty traktujące o problemie dezinformacji oraz o roli państwa w zwalczaniu tego zagrożenia – czyli raport *Disinformation and 'Fake News'* definiujący i charakteryzujący zjawisko oraz proponujący szeroką gamę rekomendacji dla rządu, a także *Online Harms White Paper* przedstawiający plany rządu w obszarze zwalczania cyfrowych zagrożeń – są kluczowe dla zrozumienia kierunku rozwoju strategii do walki z dezinformacją w Wielkiej Brytanii.

Rządowe plany przedstawione w białej księdze *Online Harms* zakładają wprowadzenie restrykcyjnych przepisów dotyczących firm technologicznych, które będą musiały wziąć odpowiedzialność za działania swoich użytkowników, ich bezpieczeństwo oraz za treści publikowane w ich serwisach. W przypadku nieprzestrzegania przepisów lub uchybienia im twórcy dokumentu wnoszą o karanie platform społecznościowych wysokimi grzywnami lub o blokowanie do nich dostępu. W razie naruszeń i nierespektowania prawa do odpowiedzialności mogliby zostać pociągnięci nawet osobiście członkowie kierownictwa wyższego szczebla.

Proponowane ramy prawne zakładają ponadto:

- Powstanie niezależnego regulatora kontrolującego treści *online* i działania platform społecznościowych. Posiadać ma on rozległe kompetencje w kwestii kontroli, egzekwowania oraz karania[28]. Po konsultacjach związanych z wydaniem białej księgi na regulatora zaproponowany został Ofcom, co argumentowane jest rozległym doświadczeniem organizacji w regulacji telewizji i prasy[29].

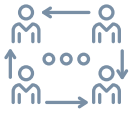
- Powstanie nowego dokumentu należytej staranności (ang. *duty of care*), który będzie nakładał obowiązki i wymagania na firmy technologiczne oraz określał ich odpowiedzialność za treści publikowane na ich platformach. Przestrzeganie przepisów należytej staranności będzie kontrolowane i egzekwowane przez niezależnego regulatora.
- Stworzenie *Code of Practice*, w którym regulator będzie wskazywał konkretne czynności, jakie dostawcy usług cyfrowych będą musieli podjąć w celu realizacji *duty of care* oraz w kontekście zwalczania i minimalizacji danych zagrożeń.
- Kluczową rolę odgrywać ma przejrzystość, zaufanie i odpowiedzialność. Regulator będzie miał prawo do żądania od firm corocznych raportów, które będą musiały zawierać działania podejmowane przez daną firmę wobec szkodliwych treści *online* oraz co ważne, regulator będzie miał prawo do zażądania wglądu w działanie algorytmów. Wszystkie raporty zostaną opublikowane i udostępnione opinii publicznej, aby ułatwić obywatelom podjęcie świadomej decyzji o korzystaniu z usług danej platformy.
- W przypadku zagrożeń związanych z bezpieczeństwem narodowym firmy technologiczne będą musiały poddać się jeszcze dokładniejszej kontroli i wykazać konkretne kroki podjęte w celu przeciwdziałania rozprzestrzenianiu się danych treści.
- Regulator powinien lobbować wśród platform internetowych na rzecz większego dostępu niezależnych badaczy i naukowców do wewnętrznych danych, a same firmy powinny skupić się na tworzeniu nowych bezpiecznych technologii. Rząd zapowiedział również nową strategię dotyczącą umiejętności korzystania z mediów *online*[30].

Nowe regulacje prawne dotyczące firm technologicznych i platform społecznościowych zapowiadają ogromne zmiany w kontekście walki z dezinformacją. Nowa rzeczywistość regulacyjna będzie wymagać od nich dostosowania się do wysokich standardów narzucanych przez rząd. Pomimo że inne państwa oraz UE także planują regulacje dotyczące sfery cyfrowej, to nikt jeszcze nie próbował objąć regulacjami tak rozległych obszarów świata *online*. Dlatego w tym kontekście Wielka Brytania wyłania się jako lider międzynarodowych wysiłków na rzecz bezpiecznej przestrzeni informacyjnej. Następstwem publikacji białej księgi jest trwający właśnie proces konsultacji publicznych, w tym etap oficjalnej odpowiedzi rządu na kwestie podniesione przez interesariuszy. Do tej pory rząd przedstawił swoje cząstkowe stanowisko, a przedstawienie raportu końcowego z konsultacji, po której ustawa może zostać przedstawiona w parlamencie, jest prognozowana na okres do końca 2021 r. Pierwotne zapowiedzi wskazywały na szybsze tempo prac, jednak w chwili pisania tego raportu nie zostały podane żadne szczegóły co do dalszych terminów i planów wobec koncepcji przedstawionej w *Online Harms White Paper*. Według nieoficjalnych informacji pojawiających się z otoczenia parlamentu i rządu, przyjęcie ustawy może przedłużyć się do 2023 lub 2024 r.[31].

Zagrożenia i ryzyka *Online Harms White Paper*

Podnoszone wątpliwości dotyczą m.in. problemu z brakiem dokładnej definicji dezinformacji w przedstawionym dokumencie oraz z zagadnieniem oceny celowości w procesie jej rozprzestrzeniania. Niektóre z firm argumentują, że nie będą w stanie określić celu badanej czynności bazując na niejasnych definicjach i przesłankach[32]. Jako kolejne zagrożenie wprowadzenia norm prawnych przedstawionych w *Online Harms White Paper* podnosi się ryzyko naruszenia wolności wypowiedzi oraz wprowadzenie częściowej cenzury Internetu. Jak ocenia organizacja *Index on Censorship*, planowane działania obejmują zbyt dużo różnorodnych obszarów, a „szeroki zakres różnych zagrożeń, którym rząd planuje przeciwdziałać w ramach przedstawionych planów, wymaga szeregu różnych, dopasowanych rozwiązań"[33]. Ponadto *Index of Censorship* zarzuca brak jasnych definicji oraz potencjał dla arbitralnych i niekonsultowanych

społecznie decyzji dotyczących treści publikowanych *online*. Według przedstawicieli firm technologicznych planowane działania mogą w negatywny sposób wpłynąć na brytyjski przemysł cyfrowy oraz jego innowacyjność. W szczególności ucierpieć mają start-upy oraz mikro- i małe przedsiębiorstwa[34]. Wreszcie podnoszony jest problem z oceną prawdziwego stopnia zagrożenia, które niesie ze sobą dezinformacja. Podczas gdy pewne jej formy, jak fałszywe wiadomości na temat leków czy szczepionek, mogą mieć konsekwencje dla zdrowia i życia ludzi, to jej inne odmiany, jak np. niegroźne formy teorii spiskowych rozprzestrzeniane na YouTubie, mogą nie być warte „regulowania Internetu" i ryzyk, jakie to ze sobą niesie dla wolnego i demokratycznego społeczeństwa[35].



Trzeci sektor

Wielka Brytania jest przykładem rozbudowanego systemu niezależnych mediów, organizacji pozarządowych i szerokiej gamy organizacji *fact-checkingowych* zajmujących się problemem dezinformacji oraz manipulacji *online*.

Organizacje *fact-checkingowe*

Wyróżniającą się organizacją *fact-checkingową* jest założony w 2009 r. Full Fact. To niezależny organ posiadający od 2014 r. status organizacji charytatywnej i funkcjonujący dzięki wpłatom darczyńców. Full Fact prowadzi przede wszystkim rozległe działania *fact-checkingowe* oraz analityczne w obrębie największych platform społecznościowych, a także skupia się na analizowaniu przestrzeni informacyjnej w kontekście wyborów oraz innych procesów demokratycznych. W styczniu 2019 r. Full Fact nawiązał współpracę z Facebookiem, dla którego świadczy usługi weryfikacji treści na platformie, które zostały oznaczone jako fałszywe przez brytyjskich użytkowników[36]. Organizacja pracuje także obecnie nad stworzeniem narzędzia do automatycznego *fact-checkingu* w ramach inicjatywy Google AI Impact Challenge[37]. Wśród innych aktywności można wymienić badania i publikacje z zakresu dezinformacji, jej psychologicznych aspektów oraz teorii spiskowych[38].

Full Fact jest organizacją należącą do *International Fact-Checking Network* (IFCN)[39], zrzeszającej inicjatywy *fact-checkingowe* z całego świata. Poza nią do IFCN należą także trzy inne brytyjskie organizacje:

- FactCheckNI – pierwsza niezależna organizacja tego typu w Irlandii Północnej, działająca od 2016 roku[40].
- Ferret Fact Service – pierwsza organizacja *fact-checkingowa* w Szkocji, założona w 2017 roku dzięki grantowi Google Digital News Initiative[41].
- Logically – organizacja łącząca zaawansowane techniki AI oraz największy na świecie zespół weryfikatorów do walki z dezinformacją[42].

Media

Działania organizacji medialnych są kolejnym elementem budowania krajowej odporności na zagrożenia w przestrzeni informacyjnej. Skupiają się one głównie na ułatwianiu dostępu do zweryfikowanych informacji, edukacji i szkoleń z zakresu umiejętności korzystania z mediów oraz rozpoznawania dezinformacji i manipulacji. Swoje zespoły, serwisy bądź narzędzia dedykowane do realizacji tych zadań posiada większość znaczących telewizji, gazet i rozgłośni radiowych. Należą do nich serwis BBC Beyond Fake News zapewniający dopływ rzetelnych informacji związanych z pandemią COVID-19, oferujący szkolenia *online* i materiały edukacyjne, a także prowadzący podobne inicjatywy w innych krajach, np. w Indiach, Nigerii oraz Mjanmie[43]. Swoją inicjatywę rozwija także The Guardian, który w partnerstwie m.in. z Google realizuje projekt NewsWise. Jest to program mający na celu edukację dzieci w zakresie umiejętności korzystania z mediów i informacji. Efektem ma być wyposażenie ich w wiedzę i umiejętności do sprawnej nawigacji we współczesnej skomplikowanej przestrzeni informacyjnej[44]. Warto odnotować także

inicjatywę Associated Press – AP Fact Check, globalną sieć *fact-checkingową* weryfikującą informacje z wielu regionów świata dzięki zaangażowaniu lokalnych dziennikarzy[45].

Szkolnictwo wyższe

Najciekawszą brytyjską inicjatywą z sektora nauki jest projekt prowadzony przez Oxford Internet Institute – *The Computational Propaganda Research Project* (COMPROP). W jego ramach naukowcy zajmują się zagadnieniem interakcji pomiędzy algorytmami, automatyzacją i polityką. Badania obejmują różne obszary nauki, takie jak socjologia, komunikacja, informatyka oraz nauki polityczne. Wśród licznych efektów pracy COMPROMP znajdują się publikacje dotyczące dezinformacji na różnych platformach społecznościowych, sposobu rozprzestrzeniania się nieprawdziwych informacji czy zagadnienia monetyzacji dezinformacji[46]. Ponadto w ramach realizowanego przez COMPROP projektu stworzono narzędzie *The CompProp Navigator*, będące internetowym przewodnikiem po zasobach ułatwiających i umożliwiających lepsze zrozumienie problemu dezinformacji oraz reagowanie na niego[47].

Inne

Istnieje także szereg innowacyjnych inicjatyw, najczęściej łączących nowoczesne rozwiązania z obszaru ICT oraz aktywności *fact-checkingowe* lub pracę niezależnych dziennikarzy. Najciekawsze z nich to: *Sereley*, aplikacja mobilna do analizy obrazu i wideo w czasie rzeczywistym, wykrywająca manipulacje oraz edycje obrazu i dźwięku[48]; *Eyewitness media verification*, czyli narzędzie umożliwiające weryfikację i uwierzytelnianie podczas tworzenia spontanicznych materiałów przez naocznych świadków wydarzeń[49]; *Kendraio Verify* mające na celu umożliwienie wspólnej weryfikacji treści przez dziennikarzy z całego świata, którzy będą mogli tworzyć „łańcuch weryfikowalnych faktów" i realizować dziennikarstwo oparte na współpracy[50].

Działania platform społecznościowych

Największe platformy społecznościowe jak Facebook, Twitter oraz YouTube podjęły działania na rzecz przeciwdziałania dezinformacji w Wielkiej Brytanii, szczególnie w kontekście wyborów parlamentarnych z 2019 r. oraz *infodemii* (termin oznaczający szybkie i niekontrolowane rozprzestrzeniania się fałszywych i zmanipulowanych informacji na temat pandemii COVID-19). W ostatnim czasie, we współpracy z brytyjskim rządem, platformy te uzgodniły pakiet działań na rzecz walki z dezinformacją o szczepionkach. Zadeklarowano, że firmy nie będą czerpać profitów z nieprawdziwych wiadomości na ten temat oraz podejmą bliską współpracę z organami zdrowia publicznego w celu promowania prawdziwych i rzetelnych informacji[51]. Wśród innych aktywności platform społecznościowych w obszarze walki z dezinformacją można wyróżnić wspominaną już wcześniej współpracę Facebooka z organizacją *fact-checkingową* Full Fact; wprowadzenie przez YouTube panelu ze sprawdzonymi informacjami wyświetlanego nad listą filmów po wyszukaniu niektórych fraz[52]; informowanie przez Twitter, gdy chcemy polubić lub podać dalej wiadomość zawierającą informację oznaczoną jako „sporna"[53]. Są to w większości jednak działania skupione na *fact-checkingu*, transparentności informacji oraz wydajniejszych działaniach moderacyjnych.

W odniesieniu do rządowych planów przedstawionych w *Online Harms White Paper* największe firmy technologiczne nie zajęły samodzielnego stanowiska. W wielu swoich wypowiedziach CEO Facebooka Mark Zuckerberg podkreślał potrzebę regulacji kwestii prawnych oraz zwiększenia roli państwowych regulatorów. Akcentował jednak, że powinno się to stać przy współpracy z największymi firmami oraz w drodze wspólnie wypracowanego konsensusu[54]. Jedynym oficjalnym dokumentem w tej sprawie jest komentarz opublikowany przez Internet Association (IA), grupę lobbingową reprezentującą takie podmioty jak Facebook, Twitter, YouTube, Microsoft oraz Amazon[55].

Organizacja handlowa podkreśla w nim wzmożone działania gigantów technologicznych na rzecz prywatności i transparentności oraz pisze o woli współpracy z rządem w tym zakresie. Podkreśla jednak, że proponowane podejście jest zbyt ogólne i poszczególne rozwiązania powinny być dopasowane do charakteru problematyki. Zwraca także uwagę na potencjalne szkody, jakie mogą zostać wyrządzone brytyjskiemu sektorowi nowych technologii oraz w odniesieniu do wartości wolności słowa i wypowiedzi[56]. Ponadto IA podnosi wątpliwości oraz problemy przedstawione w tym rozdziale, w podrozdziale *Zagrożenia i ryzyka*. Potwierdza też chęć współtworzenia nowych regulacji razem z rządem, pisząc: „IA wspiera zbalansowane, proporcjonalne regulacje, które realizują wspólny cel ochrony ludzi przed zagrożeniami *online* i zapewnienia, iż Internet będzie nadal mógł dostarczać zysków dla ekonomii i społeczeństwa"[57].

Podsumowanie

Działania Wielkiej Brytanii na rzecz walki z dezinformacją oraz manipulacją *online*, rozpoczęte w 2017 r., są przykładem niezwykle kompleksowego podejścia i próby regulacji całego systemu mediów społecznościowych. Jest to ambitna próba, która ma na celu zwiększenie kontroli państwa nad działalnością gigantów cyfrowych oraz umożliwienie pojedynczym konsumentom podejmowanie świadomych decyzji o korzystaniu z ich usług dzięki zwiększeniu transparentności oraz ułatwieniu dostępu do wewnętrznych danych i rozwiązań technologicznych stosowanych przez te organizacje. Planami przedstawionymi w *Online Harms White Paper* Londyn pozycjonuje siebie jako lidera światowych zmagań z regulowaniem rynku cyfrowego i działań mediów społecznościowych oraz walki z dezinformacją. Oczywiście na obecnym etapie, to jest w fazie planowania, pojawia się wiele kwestii spornych, niejasności i zagrożeń podejmowanych przez przedstawicieli firm technologicznych, mediów czy organizacji pozarządowych. Wszyscy jednak podkreślają potrzebę wprowadzenia regulacji dezinformacji i przestrzeni informacyjnej *online*, aby móc wyjść z obecnej sytuacji, w której brakuje rozwiązań prawnych dla tych problemów. Uwaga wszystkich pochylających się nad rozwiązaniem podobnych problemów na świecie powinna zatem skupić się na kolejnych działaniach rządu Wielkiej Brytanii i efektach, przedłużającego się, wprowadzenia założeń *Online Harms White Paper* w życie.

PRZYPISY

1 BBC News, *Russian spy: What happened to Sergei and Yulia Skripal?*, 2018, [online]: https://www.bbc.com/news/uk-43643025.

2 BBC News, *Sergei Skripal: Who is the former Russian intelligence officer?*, 2018, [online]: https://www.bbc.com/news/world-europe-43291394.

3 Gordon Ramsay, Sam Robertshaw, *Weaponising news, RT, Sputnik and targeted disinformation*, King's College London Centre for the Study of Media, Communication & Power 2019, s. 7, [online]: https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf.

4 DFRLab, *UK Poisoning: Russia Recycles Responses*, 2018, [online]: https://medium.com/dfrlab/uk-poisoning-russia-recycles-responses-77e1d357b777.

5 GOV.UK, *PM statement on the Salisbury investigation: 5 September 2018*, 2018, [online]: https://www.gov.uk/government/speeches/pm-statement-on-the-salisbury-investigation-5-september-2018.

6 Cecilia Kang, Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, The New York Times 2018, [online]: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

7 Information Commissioner's Office, *RE: ICO Investigation into use of personal information and political influence*, 2020, [online]: https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf.

8 HM Government, *Online Harms White Paper*, 2019, s. 6, [online]: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

9 *Written evidence submitted by Ofcom (FNW0107)*, s. 1, [online]: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/fake-news/written/48434.pdf.

10 Ofcom, *Raising awareness of online harms*, [online]: https://www.ofcom.org.uk/about-ofcom/annual-reports-and-plans/2019-20-annual-report/raising-awareness-of-online-harms.

11 Aliya Ram, Nic Fildes, *Ofcom outlines case for regulating social media networks*, Financial Times 2018, [online]: https://www.ft.com/content/a16935a4-bb39-11e8-94b2-17176fbf93f5.

12 Ibidem.

13 The Advertising Standards Authority, *How we handle complaints*, [online]: https://www.asa.org.uk/about-asa-and-cap/the-work-we-do/how-we-handle-complaints.html.

14 The Advertising Standards Authority, *Advertising codes*, [online]: https://www.asa.org.uk/codes-and-rulings/advertising-codes.html.

15 House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report*, 2019, s. 57, [online]: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

16 Oficjalny list dyrektora The Advertising Standards Authority Guya Parkera do przewodniczącego Komisji Cyfryzacji, Kultury, Mediów i Sportu Damiana Collinsa, 2019, [online]: https://www.asa.org.uk/uploads/assets/uploaded/50fe478e-ebc2-4f94-b4cf223bacdf48c1.pdf.

17 The Electoral Commission, *Digital Campaigning, Increasing transparency for voters*, 2018, [online]: https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf.

18 Ibidem, s. 23.

19 Information Commissioner's Office, *Who we are*, [online]: https://ico.org.uk/about-the-ico/who-we-are/.

20 Information Commissioner's Office, Investigation into the use of data analytics in political campaigns, 2018, [online]: https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

21 Competition & Markets Authority, *Online platforms and digital advertising*, 2020, s. 9, [online]: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

22 HM Government, *National Security Capability Review*, 2018, s. 10, [online]: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.

23 Government Communication Service, *Alex Aiken introduces the Rapid Response Unit*, 2018, [online]: https://perma.cc/837J-UF2U.

24 Ibidem.

25 Government Communication Service, *RESIST Counter-disinformation toolkit*, 2019, s. 8–16, [online]: https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/.

26 Centre for Data Ethics and Innovation, *About us*, [online]: https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about.

27 Open Information Partnership, [online]: https://openinformationpartnership.org.

28 HM Government, *Online Harms White Paper*, 2019, s. 44, op. cit.

29 Department for Digital, Culture, Media & Sport, *Online Harms White Paper – Initial consultation response*, 2020, [online]: https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response.

30 Digital Action, *Online Harms White Paper: Seven Experts Perspectives*, 2019, s. 2, [online]: www.politico.eu/wp-content/uploads/2019/04/Seven-expert-perspectives-on-the-UK-online-harms-White-Paper-.pdf.

31 BBC News, *Online Harms bill: Warning over 'unacceptable' delay*, 2020, [online]: https://www.bbc.com/news/technology-53222665.

32 Global Partners Digital, *Unpacking 'Harmful Content': Disinformation*, 2020, [online]: https://www.gp-digital.org/unpacking-harmful-content-disinformation/.

33 Index on Censorship, *Index on Censorship submission to Online Harms White Paper consultation*, 2019, [online]: https://www.indexoncensorship.org/2019/07/governments-online-harms-white-paper-risk-damaging-freedom-of-expression-in-the-uk/.

34 Internet Association, *Internet Association Initial Response To The Online Harms White Paper*, 2019, [online]: http://uk.internetassociation.org/wp-content/uploads/sites/2/2019/05/IA_Initial-OHWP-Response_30-09-19_UK.pdf.

35 The Guardian, *The Guardian view on online harms: white paper, grey areas*, 2019, [online]: https://www.theguardian.com/commentisfree/2019/apr/08/the-guardian-view-on-online-harms-white-paper-grey-areas.

36 Full Fact, *Full Fact to start checking Facebook content as third-party factchecking initiative reaches the UK*, 2019, [online]: https://fullfact.org/blog/2019/jan/full-fact-start-checking-facebook-content-third-party-factchecking-initiative-reaches-uk/.

37 Full Fact, *Automated Fact Checking*, [online]: https://fullfact.org/about/automated/.

38 Ibidem.

39 International Fact-Checking Network, *Verified signatories of the IFCN code of principles*, [online]: https://www.ifcncodeofprinciples.poynter.org/signatories.

40 FactCheckNI, https://factcheckni.org/.

41 The Ferret, *About us*, [online]: https://theferret.scot/about-us/.

42 Logically, *About Us*, [online]: https://www.logically.ai/about.

43 BBC, *Beyond Fake News*, [online]: https://www.bbc.co.uk/beyondfakenews/.

44 The Guardian, *NewsWise: who we are and what we do*, 2019, [online]: https://www.theguardian.com/newswise/2018/jun/12/newswise-who-we-are-and-what-we-do.

45 AP Fact Check, [online]: https://apnews.com/hub/ap-fact-check.

46 Oxford Internet Institute: The Project on Computational Propaganda, *About*, [online]: https://comprop.oii.ox.ac.uk/about/.

47 Oxford Internet Institute, *Oxford experts launch new online tool to help fight disinformation*, 2019, [online]: https://www.oii.ox.ac.uk/news/releases/oxford-experts-launch-new-online-tool-to-help-fight-disinformation/.

48 Serelay, *Our products*, [online]: https://www.serelay.com/our-products/.

49 Google News Initiative, *Eyewitness media verification*, [online]: https://newsinitiative.withgoogle.com/dnifund/dni-projects/eyewitness-media-verification/.

50 Google News Initiative, *Kendraio Verify*, [online]: https://newsinitiative.withgoogle.com/dnifund/dni-projects/kendraio-verify/.

51 GOV.UK, *Social media giants agree package of measures with UK Government to tackle vaccine disinformation*, 2020, [online]: https://www.gov.uk/government/news/social-media-giants-agree-package-of-measures-with-uk-government-to-tackle-vaccine-disinformation.

52 The Irish News, *YouTube adds fact-check panels to search results in the UK*, 2020, [online]: https://www.irishnews.com/magazine/technology/2020/09/23/news/youtube-adds-fact-check-panels-to-search-results-in-the-uk-2076531/.

53 Sky News, *Twitter is warning users when they attempt to 'like' misinformation*, 2020, [online]: https://news.sky.com/story/twitter-is-warning-users-when-they-attempt-to-like-misinformation-12140940.

54 Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas*, The Washington Post, 2019, [online]: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

55 Internet Association, *Internet Association Initial Response To The Online Harms White Paper*, 2019, op. cit.

56 Ibidem, s. 3–6.

57 Ibidem, s. 9.

Jakub Tuszyński

Państwa Trójmorza

Wstęp

Inicjatywa Trójmorza stanowi forum współpracy polityczno-gospodarczej dwunastu państw UE położonych między morzami Adriatyckim, Bałtyckim oraz Czarnym, w którego skład wchodzą: Austria, Bułgaria, Chorwacja, Czechy, Estonia, Litwa, Łotwa, Polska, Rumunia, Słowacja, Słowenia oraz Węgry. Celem Inicjatywy jest wzmocnienie rozwoju regionu przez określanie priorytetowych projektów w trzech filarach – energetycznym, transportowym i cyfrowym – oraz ich wspólną realizację. Stosownie do ustaleń zawartych w komunikacie Komisji Europejskiej *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym - odpowiedź Unii Europejskiej* (opisanym szerzej w rozdziale dotyczącym polityk i legislacji UE), wszystkie te sektory są narażone na zagrożenia hybrydowe, w tym na dezinformację i propagandę. Przykładowo *Hybrid CoE* w raporcie pt. *Assessing Energy Dependency in the Age of Hybrid Threats*[1] wskazuje na więzy (współ)zależności między państwami będącymi dostawcami energii a jej odbiorcami. Regularne dostawy energii wiążą się w opinii Centrum ze stosunkami geopolitycznymi, które z kolei pociągają za sobą zagrożenia hybrydowe. Zagrożone są jednak nie tylko poszczególne sektory, ale również same państwa Trójmorza. Wzmożona infrastrukturalna i gospodarcza integracja tego regionu wymaga opracowania transgranicznych metod jej zabezpieczania. Z tego względu Instytut Kościuszki aktywnie propaguje ideę budowy Cyfrowego Trójmorza, które w swoich założeniach obejmuje także aktywne przeciwdziałanie zagrożeniom hybrydowym na wschodniej flance NATO. Współdziałanie w ramach tej nowej platformy na pewno wzmocniłoby już istniejące inicjatywy Sojuszu Północnoatlantyckiego takie jak NATO STRATCOM (misją tego centrum jest poprawa zdolności komunikacyjnych Sojuszu przy wykorzystaniu nowoczesnych technologii oraz narzędzi analitycznych).

Niektóre z działań podejmowanych przez poszczególne państwa w celu realizacji założeń Cyfrowego Trójmorza zasługują na szczególną uwagę. Z tego względu w niniejszym rozdziale szerzej zostaną opisane inicjatywy Litwy (jako przedstawiciela regionu skupionego na budowaniu partnerstw międzynarodowych), Estonii (posiadającej zaawansowany system instytucjonalno-prawny), a także Słowacji i Bułgarii – ze względu na aktywną działalność społeczeństwa obywatelskiego. Omówione zostaną również najciekawsze działania pozostałych państw regionu, z wyłączeniem Polski, której poświęcono osobny rozdział raportu.

Legislacja i polityka państw w zakresie przeciwdziałania zjawisku dezinformacji

Estonia

Estonia od czasu cyberataku w 2007 r., podczas którego zostały zaatakowane strony m.in. estońskiego parlamentu, ministerstw i banków, rozwija zdolności składające się na cyberodporność (ang. *cyber-resilience*) i intensyfikuje działania w obszarze rozwoju instytucjonalno-prawnego, mającego na celu ochronę państwa przed zagrożeniami hybrydowymi, w tym kampaniami dezinformacyjnymi. Przykładem nasilenia tych działań jest Koncepcja Bezpieczeństwa Narodowego[2] (est. *Eesti julgeoleku-poliitika alused*) z 2017 r., która porusza m.in. problematykę budowy odporności systemowej i wzmocnienia jedności społeczeństwa. Szczególną uwagę poświęcono odporności społeczeństwa na wpływy z zewnątrz, którym należy przeciwdziałać poprzez promowanie wspólnych wartości oraz budowanie zaufania do państwa i jego instytucji. Wskazano również, że obrona psychologiczna rozumiana jako świadomość obywateli na temat wrogich operacji informacyjnych jest ważnym elementem budującym odporność i jedność społeczeństwa.

Coroczne raporty Estońskiej Służby Bezpieczeństwa Wewnętrznego[3] (est. *Kaitsepolitseiamet*) wymieniają zagrożenia hybrydowe jako jedno z wyzwań, przed którymi państwo to musi stanąć, i zwracają szczególną uwagę na działalność Kremla w obszarze operacji informacyjnych oraz propagandy historycznej. W raporcie za 2019 r.[4] *Kaitsepolitseiamet* wskazał, że stronie rosyjskiej „brakuje pomysłów oraz środków"[5] na prowadzenie operacji wpływu z powodu sankcji gospodarczych nałożonych na Rosję, co „poskutkowało forsowaniem dotychczasowych narracji, zwłaszcza w kwestii swojej interpretacji historii"[6].

Estonia podjęła również kroki legislacyjne w celu uregulowania rynku medialnego, głównie w drodze ustawy o działalności mediów (est. *Meediateenuste seadus*), która nakłada na dostawców usług medialnych obowiązek weryfikacji informacji przed publikacją. Drugim istotnym aktem jest ustawa o mediach publicznych (est. *Eesti Rahvusringhäälingu seadus*), która określa ramy działania mediów publicznych. Estońskie media zobligowane są również do przestrzegania samoregulacyjnego kodeksu etycznego[7] wymagającego od dziennikarzy m.in. dogłębnego zapoznania się z badaną sprawą, przedstawienia racji obu stron oraz oparcia się na faktach.

Estonia uświadamia społeczeństwo o problemie zagrożeń hybrydowych przy pomocy takich inicjatyw jak Estoński Kurs Obrony Narodowej (est. *Kõrgemaid riigikaitsekursuseid*), który jest koordynowany przez think tank *International Centre for Defence and Security* (ICDS). Kurs skupia się przede wszystkim na omówieniu koncepcji estońskiej polityki bezpieczeństwa, polityki zagranicznej i obronnej, a także szeroko pojętej koncepcji obrony narodowej. W programie znajduje się również tematyka związana z nowoczesnym obliczem wojny (w tym wojny informacyjnej). Kurs jest przeznaczony dla polityków, wysokich urzędników, członków Estońskich Sił Obrony (est. *Eesti Kaitsevägi*), liderów opinii oraz organizacji pozarządowych.

Walkę z fałszywymi treściami prowadzi również estoński nadawca publiczny (est. *Eesti Rahvusringhääling*, ERR), który stworzył specjalną rubrykę[8], a na jej łamach publikuje poradniki, artykuły, audycje radiowe i materiały (również dla młodzieży). Innym przykładem działań ERR w tym

zakresie była publikacja materiałów z okazji Media Literacy Week (ros. *Неделя медиаграмотности*)[9], który odbył się w dniach 26–30 października 2020 r., zwracał uwagę na problemy wynikające z nadmiaru informacji i przedstawiał sposoby zaradzenia temu zjawisku. Wydarzenie kierowano przede wszystkim do młodzieży – w jego ramach zostały przeprowadzone warsztaty i debaty z ekspertami, którzy udzielali rad na temat rozpoznawania fałszywych informacji. Inicjatywę zorganizowało Ministerstwo Edukacji i Badań (est. *Haridus- ja Teadusministeerium*).

Litwa

Litwa podejmuje szerokie spektrum działań od uchwalania aktów prawnych przez tworzenie dokumentów strategicznych po inicjatywy na arenie międzynarodowej. Jednym z najważniejszych z punktu widzenia omawianej problematyki dokumentów w litewskim prawodawstwie jest ustawa o dostępie do informacji publicznej (lit. *Lietuvos Respublikos visuomenės informavimo įstatymas*)[10], która określa kompetencje Litewskiej Komisji Radiofonii i Telewizji (lit. *Lietuvos radijo ir televizijos komisija*, LRTK). Ustawa ta daje Komisji prawo do tymczasowego bądź trwałego zawieszenia koncesji nadawczej konkretnego operatora lub dostawcy usług VOD za m.in.: szerzenie propagandy wojennej, podżeganie do wojny lub nienawiści, ośmieszanie, poniżanie, podżeganie do dyskryminacji, przemocy, brutalnego traktowania fizycznego grupy osób lub osoby do niej należącej ze względu na wiek, płeć, orientację seksualną, pochodzenie etniczne, rasę, narodowość, obywatelstwo, język, pochodzenie, status społeczny, przekonania, przekonania, poglądy lub religię[11]. Decyzja LRTK musi zostać usankcjonowana przez sąd administracyjny w Wilnie (lit. *Vilniaus apygardos administracinis teismas*).

Problem dezinformacji jest również poruszany w białej księdze polityki obronnej Litwy (lit. *Lietuvos gynybos politikos Baltoji knyga*)[12], która zawiera następujące działania:

1) monitorowanie i analizowanie przestrzeni informacyjnej, aby określić cele, skalę i środki operacji informacyjnych;

2) prowadzenie kampanii informacyjnych, aby zwiększać świadomość opinii publicznej;

3) promowanie współpracy w ramach NATO i UE.

Przestrzeń informacyjną monitoruje Departament Komunikacji Strategicznej Litewskich Sił Zbrojnych (ang. *Strategic Communications Department of the Lithuanian Armed Forces*, LAF), a eksperci LAF wspomagają Litewską Komisję Radiofonii i Telewizji w jej działaniach dotyczących przeciwdziałania rozprzestrzenianiu się fałszywych treści. LAF prowadzi działalność edukacyjną na różnych szczeblach, od instytucji państwowych po szkoły. Ostatnia metoda opisana w białej księdze sprowadza się do promowania współpracy bilateralnej i wielostronnej z instytucjami NATO i UE oraz z ich państwami członkowskimi, która miałaby polegać na wymianie doświadczeń, najlepszych praktyk oraz analizy celów, skutków i taktyk wykorzystanych w czasie ataków przeprowadzonych w przestrzeni informacyjnej.

Litwa jest również aktywna na polu międzynarodowym. Warto wskazać chociażby wspólne oświadczenie wydane w listopadzie 2020 r. po 26. posiedzeniu[13] Bałtyckiej Rady Ministrów[14] (ang. *Baltic Council of Ministers*, BCM), w której w skład wchodzą Litwa, Łotwa i Estonia. W oświadczeniu Wilno wyraża poparcie dla działań UE w zakresie zwalczania dezinformacji oraz wzywa ją do aktywniejszej pomocy krajom i społeczeństwom w regionie w budowaniu odporności na destabilizujące wpływy Rosji, a także do dalszego wspierania niezależnych, pluralistycznych mediów w krajach Partnerstwa Wschodniego. W ramach oświadczenia wskazano również priorytety dla prezydencji Litwy w tej radzie w 2021 r., a jednym z nich jest właśnie walka z dezinformacją, co oznacza, że państwa bałtyckie uznają to zjawisko za istotny problem, któremu trzeba się przeciwstawić.

Za pozytywne na pewno należy uznać działania państwa litewskiego mające na celu rozwijanie świadomości społecznej, że zagrożenia hybrydowe bezpośrednio wpływają na życie obywateli, a także ujęcie tego problemu w dokumentach strategicznych oraz próby znalezienia odpowiedzi w formule współpracy na arenie międzynarodowej.

Pozostałe kraje

Dla większości z pozostałych państw Trójmorza impulsem do bardziej zdecydowanego zwalczania zagrożeń w przestrzeni informacyjnej była pandemia koronawirusa i kampanie dezinformacyjne z tym związane (Austria, Bułgaria, Łotwa, Rumunia, Węgry); dla niektórych przyczynkiem stała się dezinformacja w kwestii 5G (Chorwacja) oraz wzmożenie działań hybrydowych na terenie Europy Środkowo-Wschodniej po agresji Rosji na Ukrainę (Czechy).

Rząd **Austrii** utworzył 13 marca 2020 r. cyfrowy sztab kryzysowy[15] (niem. *Digitaler Krisenstab*), który wszedł w skład Urzędu Kanclerza Federalnego (niem. *Bundeskanzleramt*). Jego zadaniem jest wspieranie współpracy mediów, społeczeństwa obywatelskiego i ośrodków akademickich w zwalczaniu rozprzestrzeniania się fałszywych informacji na temat koronawirusa oraz zapewnienie szybkiej wymiany informacji na temat narracji dezinformacyjnych. Jednym z działań podjętych przez sztab była kampania informacyjna skierowana do imigrantów, którą przeprowadzono w 16 językach[16].

Bułgaria podjęła próby uregulowania problemu dezinformacji[17]. Jedną z nich był projekt ustawy o stanie wyjątkowym z marca 2020 r., który wprowadzał poprawkę w bułgarskim kodeksie karnym penalizującą rozpowszechnianie fałszywych informacji na temat COVID-19. W myśl projektu za taki czyn miało grozić do trzech lat pozbawienia wolności – lub do pięciu i grzywna w wysokości od 10 000 BGN do 50 000 BGN w przypadku wystąpienia w jego następstwie poważnych szkód. Poprawkę zawetował jednak prezydent Bułgarii, Rumen Radew, który stwierdził, że przepis ten narusza swobodę wypowiedzi[18].

Chorwacja razem z 14 państwami członkowskimi UE (w tym Austrią, Bułgarią, Czechami, Estonią, Łotwą, Litwą, Polską i Słowacją) podpisała 19 października 2020 r. list skierowany do wiceprzewodniczącej Komisji Europejskiej Margrethe Vestager, komisarza ds. rynku wewnętrznego Thierry'ego Bretona oraz wiceprzewodniczącej do spraw wartości i przejrzystości Very Jourovej[19]. Sygnatariusze listu sugerują, że „UE powinna przygotować strategię przeciwdziałania dezinformacji na temat technologii 5G" i wskazują, że w 10 państwach europejskich doszło do podpaleń masztów 5G oraz ataków na obsługę techniczną. Państwa członkowskie zaoferowały również swoją pomoc w realizacji tej inicjatywy. Jest to przykład działań dyplomatycznych podejmowanych przez Chorwację w zakresie przeciwdziałania zagrożeniom hybrydowym, jak i realizacji założeń przyjętych w Strategii Bezpieczeństwa Narodowego[20] (chorw. *Strategija nacionalne sigurnosti*) z 2017 r. Wskazano w niej na konieczność współpracy z UE i NATO m.in. w wymiarze dyplomatycznym w celu budowania odporności Chorwacji na takie zagrożenia, w tym dezinformację.

Agresja Rosji na Ukrainę oraz intensyfikacja działań hybrydowych w obszarze Europy Środkowo-Wschodniej skłoniły **Czechy** do przeprowadzenia w 2015 r. Narodowego Audytu Bezpieczeństwa. Zakończył się on w 2016 r. i przyjął formę raportu[21], w którym wskazano 10 zagrożeń dla bezpieczeństwa Czech, w tym zagrożenia hybrydowe i wpływ obcych państw (ang. *influence of foreign powers*). Wśród podanych problemów znalazły się m.in. podważanie zaufania do demokratycznego państwa prawa czy też rozsiewanie dezinformacji poprzez media i platformy społecznościowe. Efektem audytu było m.in. utworzenie Centrum Przeciwdziałania Terroryzmowi i Zagrożeniom Hybrydowym (cz. *Centrum proti terorismu a hybridním hrozbám*), które rozpoczęło działalność 1 stycznia 2017 r.[22] Centrum działa w ramach ministerstwa spraw wewnętrznych i zajmuje się monitorowaniem zagrożeń związanych z bezpieczeństwem wewnętrznym, w tym kampanii dezinformacyjnych. Centrum szerzy również

wiedzę na ich temat wśród ogółu społeczeństwa, czego przykładem może być analiza głównych narracji dezinformacyjnych w Czechach związanych z koronawirusem[23].

Łotwa była inicjatorem działania, w ramach którego 130 krajów ONZ wydało 12 czerwca 2020 r. oświadczenie w sprawie przeciwdziałania dezinformacji w kontekście kryzysu zdrowotnego. Zwrócono w nim uwagę na rolę i odpowiedzialność państw, organizacji regionalnych, systemu ONZ i innych zainteresowanych stron – takich jak środki masowego przekazu, platformy społecznościowe i organizacje pozarządowe – w pomocy ludziom w radzeniu sobie z dezinformacją oraz zwiększaniu odporności społeczeństwa[24].

Prezydent **Rumunii** Klaus Iohannis 16 marca 2020 r. wydał dekret[25] w sprawie wprowadzenia stanu wyjątkowego na terytorium Rumunii, który przyznaje specjalne uprawnienia Krajowemu Urzędowi Administracji i Regulacji Komunikacji (rum. *Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii*, ANCOM). Na podstawie artykułu 54. dekretu ANCOM ma możliwość zablokowania stron internetowych, które publikują treści „promujące fałszywe wiadomości dotyczące rozprzestrzeniania się COVID-19 (ang. „*evolution of COVID-19*") oraz środków ochrony i zapobiegania"[26]. Na podstawie dekretu uniemożliwiono działanie niektórych stron internetowych[27].

Słowacja w sierpniu 2020 r. została członkiem Europejskiego Centrum Doskonalenia w zakresie Przeciwdziałania Zagrożeniom Hybrydowym (ang. *The European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE*), mającym siedzibę w Helsinkach, którego zadaniem jest umożliwienie wymiany wiedzy i doświadczeń dotyczących takich niebezpieczeństw[28]. Tym samym dołączyła do grona innych państw Trójmorza wchodzących w skład tej organizacji – Łotwy, Litwy, Polski, Estonii, Austrii, Czech, Rumunii, Słowenii i Węgier[29]. *Hybrid CoE* w ramach swojej działalności m.in. publikuje raporty i przeprowadza szkolenia dla decydentów państw członkowskich z zakresu problematyki zagrożeń hybrydowych. Działania przeciwko dezinformacji podjęło również Ministerstwo Spraw Zagranicznych m.in. tworząc nowy departament, którego zadaniem jest przeciwdziałanie tym zagrożeniom, jak również prowadząc warsztaty dla dyplomatów i pracowników ministerstw[30]. Powyższe działania są efektem zapowiedzi nowego słowackiego rządu, który ogłosił w 2020 r., że walka z zagrożeniami hybrydowymi będzie jednym z priorytetów na najbliższe cztery lata[31].

Na początku 2020 r. wydana została Biała Księga Obrony Republiki **Słowenii** (słow. *Bela knjiga o obrambi Republike Slovenije*)[32], która zapowiada podjęcie kompleksowych działań krajowych w celu przeciwdziałania zagrożeniom hybrydowym. W ramach tych aktywności rozwijana będzie współpraca w zakresie identyfikacji zagrożeń hybrydowych i reagowania na nie. Wzmocniona zostanie świadomość sytuacyjna, odporność na wrogie działania wywiadowcze, cyberbezpieczeństwo i bezpieczeństwo informacyjne oraz obrona, komunikacja strategiczna i mechanizmy zarządzania kryzysowego, z uwzględnieniem różnych metod operacji hybrydowych.

Węgierski parlament przyjął 29 marca 2020 r. ustawę o zwalczaniu koronawirusa (węg. *2020. évi XII. törvény a koronavírus elleni védekezésről*), która ustanawia specjalny porządek prawny na czas pandemii i m.in. nowelizuje węgierski kodeks karny, wprowadzając karę pozbawienia wolności od roku do lat pięciu za rozpowszechnianie *fake newsów* związanych z koronawirusem podczas trwania stanu zagrożenia[33]. *Amnesty International*[34] i *International Press Institute*[35] wskazują, że nowe regulacje mogą prowadzić do ograniczenia wolności słowa.

Inicjatywy pozarządowe w państwach Trójmorza

Bułgaria

Center for the Study of Democracy (CSD) jest interdyscyplinarnym think tankiem założonym w 1989 r.[36], w swojej działalności w obszarze dezinformacji skupia się przede wszystkim na badaniu wpływu Rosji na terenie Europy. Efektem tej działalności jest m.in. raport *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* napisany we współpracy z *Center for Strategic and International Studies*, który opisywał działania Rosji w pięciu krajach środkowoeuropejskich w połowie ubiegłej dekady. CSD organizuje również liczne panele eksperckie[37] oraz prowadzi edukację na temat problemu dezinformacji. W dobie koronawirusa CSD zidentyfikowało również narracje dezinformacyjne w Bułgarii i krajach ościennych[38], jak i wzięło udział w tworzeniu raportów dla Agencji Praw Podstawowych Unii Europejskiej, w ramach których opisano wpływ koronawirusa na prawa podstawowe we wszystkich państwach członkowskich UE. W raportach z marca 2020 r.[39] oraz lipca[40] tego samego roku omówiono m.in. działania podejmowane przez bułgarski rząd w celu przeciwdziałania zjawisku dezinformacji. Zostały opisane nieudane próby nowelizacji ustawy o radiu i telewizji (bułg. *Закон за радиото и телевизията*), które zakładały penalizację rozpowszechniania fałszywych informacji. Uwagi do projektu zgłosiły zarówno instytucje publiczne, jak i organizacje pozarządowe, które skrytykowały brak jasnych definicji dezinformacji oraz uznały proponowane poprawki za „nieuzasadnione rozszerzenie uprawnień organów władzy publicznej w zakresie nadzoru nad mediami internetowymi”[41], co może prowadzić do naruszenia wolności słowa i wolności mediów. W lipcowym raporcie wskazano również główne narracje dezinformacyjne w Bułgarii, czyli m.in. propagandę sukcesu Rosji w zwalczaniu koronawirusa.

Litwa

Sztandarowym przykładem inicjatywy zajmującej się zwalczaniem dezinformacji w Europie Środkowo-Wschodniej jest Debunk.eu. Organizacja ta wykorzystuje w swojej pracy sztuczną inteligencję, która potrafi „wykrywać i identyfikować dezinformację w ciągu dwóch minut w czasie rzeczywistym”[42]. Materiał jest oceniany na podstawie m.in. treści, źródła oraz sposobu rozprzestrzeniania danej informacji w mediach społecznościowych, a następnie jest przydzielany do odpowiedniej kategorii[43]. Ochotnicy nazywani „elfami” oraz *fact-checkerzy* „weryfikują artykuły z potencjalnie najbardziej szkodliwymi narracjami, które średnio stanowią 2 procent treści”[44] odnalezionych przez AI. Po weryfikacji przez ludzi nieprawdziwe wiadomości są oznaczane jako dezinformacja, a dziennikarze automatycznie powiadamiani o przypadkach *fake newsów*, które w następnym kroku demaskują i opisują. Na końcu całego procesu artykuły są publikowane w mainstreamowych mediach, dzięki czemu mogą docierać do 90% litewskiej populacji[45].

Słowacja

Jednym z wiodących think tanków skupiających się na tematyce dezinformacji na Słowacji jest *Slovak Security Policy Institute* (SSPI)[46]. SSPI zajmuje się głównie badaniem i analizą wyzwań związanych z bezpieczeństwem, w tym problemem dezinformacji. Przykładem inicjatyw tworzonych przez SSPI jest Antipropaganda.sk[47], serwis *factcheckingowy* poświęcony przede wszystkim obalaniu mitów związanych z kwestiami polityki zagranicznej i bezpieczeństwa oraz dostarczaniu informacji w oparciu o zweryfikowane fakty. Organizacja wydała również w 2020 r. raport *Ocena podejścia Republiki Słowackiej do walki z zagrożeniami hybrydowymi* (słow. *Zhodnotenie prístupu Slovenskej republiky k boju s hybridnými hrozbami*)[48]. Celem raportu jest ocena podejścia Słowacji do walki z zagrożeniami hybrydowymi oraz zaproponowanie środków i sposobów na jego poprawę. W tekście omówiono budowanie odporności, tworzenie procesów wewnętrznych oraz zdolność i potencjał administracji państwowej

do zwalczania zagrożeń hybrydowych. Raport analizuje podstawowe dokumenty regulujące tę kwestię oraz identyfikuje słabe i mocne strony w walce z tymi zagrożeniami na poziomie systemowym. Na tej podstawie formułowana jest propozycja ram strategicznych i modelu instytucjonalnego, które zoptymalizowałyby podejście Słowacji w tej dziedzinie. Ich ewentualną implementację może wzbogacić zestaw rekomendacji.

Oprócz wymienionych inicjatyw warto również pokrótce wspomnieć o *European Values Center for Security Policy* z Czech (EVC) ze względu na działania podejmowane przez tę organizację[49]. EVC prowadzi m.in. program Kremlin Watch skupiający się na demaskowaniu rosyjskich operacji dezinformacyjnych w Europie. Bliźniaczymi inicjatywami są również *Red Watch* dotyczący działalności Chin w tym obszarze i „Balkans Watch Briefing", czyli comiesięczny newsletter podsumowujący najnowsze działania przeciw tym zagrożeniom na Bałkanach.

Media społecznościowe w wybranych państwach Trójmorza

Media społecznościowe stały się ważną częścią rzeczywistości, a tym samym narzędziem wpływu, podobnie jak tradycyjne środki przekazu – telewizja, radio i prasa. Jak wynika z badań[50] opublikowanych w czasopiśmie „Nature: Human Behaviour", których celem była obserwacja i analiza zachowania trzech tysięcy Amerykanów w Internecie w okresie poprzedzającym wybory prezydenckie w USA z 2016 r., to Facebook stanowił „kluczowy wektor rozprzestrzeniania niewiarygodnych stron internetowych"[51]. Jest to również najpopularniejsza[52] platforma społecznościowa w zdecydowanej większości państw z regionu Trójmorza. Działania Facebooka mające przeciwdziałać dezinformacji noszą nazwę *Third-Party Fact-Checking Program*. Program ten wszedł w życie w 2016 r.[53] i w jego ramach niezależne organizacje identyfikują *fake newsy* w postaci wiadomości, zdjęć oraz filmów na Facebooku i Instagramie. Po oznaczeniu wiadomości jako fałszywej jej zasięgi na Facebooku oraz Instagramie są ograniczane, a osoby, które wcześniej podały dalej fałszywą treść, są o tym fakcie informowane. Od 12 maja 2020 r. programem są objęte **Austria** oraz Szwajcaria[54]. *Fact-checkingiem* w Austrii zajmie się we współpracy z Austriacką Agencją Prasową (*Austria Presse Agentur*, APA) agencja informacyjna *Deutsche Presse-Agentur GmbH* (DPA), która od marca 2019 r. prowadzi weryfikację treści na terenie Niemiec. Ponadto od września 2020 r. trzecim podmiotem odpowiedzialnym za austriackiego

Tabela 1. Organizacje zajmujące się *fact-checkingiem* na Facebooku w regionie Trójmorza.

PAŃSTWO	ORGANIZACJE
Bułgaria	BRAK
Chorwacja	Faktograf.hr
Czechy	Demagog.cz, AFP – Hub
Estonia	Delfi
Litwa	Delfi
Łotwa	Delfi, Re:Baltica
Rumunia	AFP – Coverage
Słowacja	AFP-Hub
Słowenia	BRAK
Węgry	BRAK

Źródło: https://www.facebook.com/journalismproject/programs/third-party-fact-checking/partner-map?locale=de_DE

Facebooka jest Agence France-Presse (AFP)[55]. DPA, podobnie jak inni partnerzy współpracujący w ramach tego programu, jest certyfikowane przez *International Fact-Checking Network* (IFCN),[56] czyli niezależną organizację zrzeszającą domy medialne, agencje informacyjne oraz organizacje non-profit. Aby otrzymać certyfikację IFCN, organizacja musi przestrzegać zasad zawartych w kodeksie postępowania (ang. *Code of Principles*)[57], czyli bezstronności i uczciwości, przejrzystości źródeł, transparentności finansowania, organizacji i metodologii oraz polityki korekt (ang. *corrections policy*), czyli jasnej procedury opisującej sposób działania w przypadku wykazania pomyłki w przeprowadzonej analizie. Dopiero po spełnieniu powyższych warunków i podpisaniu kodeksu postępowania organizacja może zostać członkiem IFCN[58]. W prezentowanej powyżej tabeli znalazła się lista inicjatyw z regionu Trójmorza wchodzących w skład programu *fact-checkingowego* Facebooka[59]. Ze względu na fakt, że w dniu pisania niniejszego raportu żadna organizacja z Bułgarii i Węgier nie wchodziła w skład IFCN, państwa te nie mają reprezentantów. W przypadku Słowenii centrum dziennikarstwa śledczego nad Adriatykiem *Oštro, center za preiskovalno novinarstvo v jadranski regiji* zostało członkiem IFCN 23 listopada 2020 r., ale w okresie tworzenia tego rozdziału nie brało udziału w facebookowej inicjatywie.

Podsumowanie

Państwa Trójmorza nie prowadzą jednolitej polityki wobec dezinformacji. Część z nich skupia się na tworzeniu nowych instytucji (jak ma to miejsce w Czechach czy Austrii) lub wykorzystaniu już istniejących (przypadek Rumunii); inną drogę wybrały Węgry, które postanowiły penalizować rozpowszechnianie *fake newsów*, a podobne próby, chociaż dotychczas nieskuteczne, podjęła również Bułgaria. Można jednocześnie wyróżnić aktywność niektórych państw Trójmorza na arenie międzynarodowej, tutaj prym wiodły Litwa, Łotwa i Estonia, które sygnalizowały potrzebę aktywniejszej debaty w kwestii tego zjawiska. Ważną inicjatywą na arenie międzynarodowej w kontekście omawianej problematyki jest również działalność *Hybrid CoE*, do którego w 2020 r. dołączyła Słowacja. Tym samym zwiększyła się obecność państw Trójmorza w tej inicjatywie – uczestniczy w niej już 10 krajów, co wskazuje na duże zainteresowanie tematyką zagrożeń hybrydowych w regionie Europy Środkowo-Wschodniej i wyraża chęć aktywnego przeciwdziałania dezinformacji. Powstały również dokumenty strategiczne wskazujące zagrożenia hybrydowe jako kluczowe wyzwanie i stanowiące jednocześnie zapowiedź kontrdziałań, czego przykładem jest wspomniany wcześniej Narodowy Audyt Bezpieczeństwa (cz. *Audit Národní Bezpečnosti*) przeprowadzony w Czechach.

Na terenie państw Trójmorza aktywnie działają również organizacje pozarządowe i *fact-checkingowe* oraz wyspecjalizowane think tanki, które stanowią przykład działań oddolnych. Są one niezbędne dla budowania odporności społeczeństwa, pełnią również często funkcję uświadamiającą – poprzez organizowanie tematycznych warsztatów, prelekcji czy kampanii społecznych we współpracy z lokalnymi władzami. W kolejnych latach ważne będzie budowanie bardziej zharmonizowanego podejścia do tego problemu. Potrzeby w tym zakresie wskazała inicjatywa Cyfrowego Trójmorza, a sygnałem do pogłębionej współpracy regionalnej może być deklaracja krajów grupy wyszehradzkiej podpisana 17 lutego 2021 r. w Krakowie, w której czytamy, że kraje wyszehradzkie dostrzegają i uznają „potrzebę przeciwdziałania rozprzestrzenianiu się dezinformacji rozpowszechnianej w internecie w celu ochrony bezpieczeństwa obywateli i przedsiębiorstw”[60]. Wola współpracy w budowaniu odporności na zaburzenia informacyjne powinna objąć jak najwięcej krajów Trójmorza w jak najszerszym zakresie.

PRZYPISY

1 Hybrid CoE, *Assessing Energy Dependency in the Age of Hybrid Threats*, styczeń 2019, [online]: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Assessing_Energy_Dependency_in_the_Age_of_Hybrid_Threats-HybridCoE.pdf.

2 Government Office, *National Security Concept*, 2017, [online]: https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf.

3 Coroczne raporty można znaleźć pod adresem https://www.kapo.ee/en/content/annual-reviews.html.

4 Kaitsepolitseiamet, *Annual Review 2019*, [online]: https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202019.pdf.

5 Ibidem, s. 21.

6 Ibidem, s. 21.

7 The code of ethics for the Estonian press, [online]: http://www.asn.org.ee/english/code_of_ethics.html.

8 Eesti Rahvusringhääling, *Mediagramotnost*, [online]: https://rus.err.ee/k/mediagramotnost.

9 Андрей Крашевский, *Как ориентироваться в информационном шуме: в Эстонии началась неделя медиаграмотности*, ERR 2020, [online]: https://rus.err.ee/1151455/kak-orientirovatsja-v-informacionnom-shume-v-jestonii-nachalas-nedelja-mediagramotnosti.

10 Republic of Lithuania, *Law on the Provision of Information to the Public*, No I-1418, 02.07.1996, [online]: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/c4a1511305c611e8802fc9918087744d?jfwid=1clcwosx33.

11 Ibidem.

12 Ministry of National Defence Republic of Lithuania, *The White Paper on Lithuanian defence policy*, 2017, [online]: https://kam.lt/en/defence_policy_1053/important_documents/the_white_paper_on_lithuanian_defence_policy.html.

13 *Joint Statement of the 26th Baltic Council*, 2020, [online]: https://vm.ee/et/uudised/joint-statement-26th-baltic-council.

14 Która wchodzi w skład Rady Bałtyckiej.

15 David Christopher Jaklin, *Disinformation and Covid-19: The Case of Austria*, 30.04.2020, [online]: https://medium.com/@david.jaklin/disinformation-and-covid-19-the-case-of-austria-5440094a789c.

16 ORF.at, *Offensive der Regierung gegen „Fake News"*, 27.05.2020, [online]: https://orf.at/stories/3159533/.

17 Desislava Krusteva, Radoslava Makshutova, *Bulgaria: Legislative attempts to restrict disinformation in 2020*, [online]: https://www.dataguidance.com/opinion/bulgaria-legislative-attempts-restrict.

18 Ibidem.

19 HINA, *Croatia and 14 More EU Members Seek Strategy Against Disinformation About 5G*, [online]: https://www.total-croatia-news.com/news/47499-croatia-and-14-more-eu-members-seek-strategy-against-disinformation-about-5g.

20 The Republic of Croatia, *National Security Strategy*, 2017, [online]: https://www.morh.hr/wp-content/uploads/2018/04/strategy_18012018.pdf.

21 Ministry of the Interior of the Czech Republic, *National Security Audit*, Prague 2016, [online]: https://www.mvcr.cz/cthh/soubor/national-security-audit.aspx.

22 Centre Against Terrorism and Hybrid Threats, [online]: https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx.

23 Centre Against Terrorism and Hybrid Threats, *Coronavirus: An overview of the Main Disinformation Narratives in the Czech Republic*, [online]: https://www.mvcr.cz/cthh/clanek/coronavirus-an-overview-of-the-main-disinformation-narratives-in-the-czech-republic.aspx.

24 Ministry of foreign affairs of the Republic of Latvia, *Latvian-initiated global call to combat the "infodemic" in the context of COVID-19 is endorsed by 130 countries*, [online]: https://www.mfa.gov.lv/en/news/latest-news/66123-latvian-initiated-global-call-to-combat-the-infodemic-in-the-context-of-covid-19-is-endorsed-by-130-countries.

25 Official Gazette of Romania, Part I, No. 212/16.03.2020, *Decree On the establishment of the state of emergency in the territory of Romania*, [online]: https://rm.coe.int/16809e375d.

26 Ibidem.

27 Georgi Gotev, *Romania shuts down websites with fake COVID-19 news*, 2020, [online]: https://www.euractiv.com/section/all/short_news/romania-shuts-down-websites-with-fake-covid-19-news/.

28 Ministry of Foreign and European Affairs of the Slovak Republic, *Slovakia Becomes the Member of the Center of Excellence for Countering Hybrid Threats in Helsinki*, 2020, [online]: https://www.mzv.sk/web/en/news/current_issues/-/asset_publisher/lrJ2tDuQdEKp/content/slovensko-sa-stalo-clenom-centra-vynimocnosti-pre-hybridne-hrozby-v-helsinkach/10182.

29 The European Centre of Excellence for Countering Hybrid Threats, *Dates of accession for the Hybrid CoE Participating States*, 2020, [online]: https://www.hybridcoe.fi/wp-content/uploads/2020/09/Dates-of-accession-for-the-Hybrid-CoE-Participating-States-03082020.pdf.

30 Miroslava German Sirotnikova, *Pandemic Pushes Slovakia To Finally Target Disinformation*, 20.10.2020, [online]: https://balkaninsight.com/2020/10/20/pandemic-pushes-slovakia-to-finally-target-disinformation/.

31 Ibidem.

32 Ministry of Defence of the Republic of Slovenia, *Defence White Paper of the Republic of Slovenia*, 2020, [online]: https://www.gov.si/assets/ministrstva/MO/Dokumenti/WP2020.pdf.

33 Library of Congress, *Hungary: National Assembly Adopts Act Giving Government Special Powers during Coronavirus Pandemic*, 2020, [online]: https://www.loc.gov/law/foreign-news/article/hungary-national-assembly-adopts-act-giving-government-special-powers-during-coronavirus-pandemic/.

34 Amnesty International, *Hungary: Granting government unlimited powers under new Covid19 law is disturbing development*, 2020, [online]: https://www.amnesty.ie/hungary-granting-government-unlimited-powers-under-new-covid19-law-is-disturbing-development/.

35 International Press Institute, *Hungary seeks power to jail journalists for 'false' COVID-19 coverage*, 2020, [online]: https://ipi.media/hungary-seeks-power-to-jail-journalists-for-false-covid-19-coverage/.

36 Center for the Study of Democracy, *Mission*, [online]: https://csd.bg/about/mission/.

37 Dotychczasowe wydarzenia można zobaczyć na stronie https://csd.bg/events/.

38 https://www.facebook.com/csdbg/videos/vb.112284368050/2813510982261037/?type=3&theater oraz https://www.facebook.com/csdbg/videos/vb.112284368050/393224358378169/?type=3&theater.

39 Center for the Study of Democracy, *Coronavirus COVID-19 outbreak in the EU – Fundamental Rights Implications*, 2020, [online]: https://fra.europa.eu/sites/default/files/fra_uploads/bulgaria-report-covid-19-april-2020_en.pdf.

40 Center for the Study of Democracy, *Coronavirus COVID-19 outbreak in the EU Fundamental Rights Implications*, 2020, [online]: https://fra.europa.eu/sites/default/files/fra_uploads/bg_report_on_coronavirus_pandemic_july_2020.pdf.

41 Ibidem, s. 12.

42 Debunk.eu, *About Debunk EU*, [online]: https://debunk.eu/about-debunk/.

43 Eline Chivot, *5 Q's for Viktoras Daukšas, Head of Debunk.eu*, 2020, [online]: https://datainnovation.org/2019/02/5qs-for-viktoras-dauksas-head-of-debunk-eu/.

44 Ibidem.

45 Ibidem.

46 Slovak Security Policy Institute [online]: https://slovaksecurity.org/?lang=en.

47 Slovak Security Policy Institute, *Antipropaganda.sk*, [online]: https://slovaksecurity.org/projects/antipropaganda-sk/?lang=en&portfolioCats=115%2C114%2C112.

48 Slovak Security Policy Institute, *Zhodnotenie prístupu Slovenskej republiky k boju s hybridnými hrozbami*, [online]: https://slovaksecurity.org/projects/zhodnotenie-pristupu-slovenskej-republiky-k-boju-s-hybridnymi-hrozbami/?portfolioCats=32.

49 European Values Center for Security Policy, *About Us*, [online]: https://europeanvalues.cz/en/about-us/.

50 Mark Travers, *Facebook Spreads Fake News Faster Than Any Other Social Website, According To New Research*, 2020, [online]: https://www.forbes.com/sites/traversmark/2020/03/21/facebook-spreads-fake-news-faster-than-any-other-social-website-according-to-new-research/.

51 Andrew Guess, Brendan Nyhan, Jason Reifler, *Exposure to untrustworthy websites in the 2016 US election*, Nature Human Behavior 2020, s. 5, [online]: https://www.nature.com/articles/s41562-020-0833-x.

52 Vincos Blog, *World Map of Social Networks*, [online]: https://vincos.it/world-map-of-social-networks/.

53 Facebook, *How Our Fact-Checking Program Works*, [online]: https://www.facebook.com/journalismproject/programs/third-party-fact-checking/how-it-works.

54 Facebook, *Facebook weitet Faktenprüferprogramm auf Österreich und die Schweiz aus*, [online]: https://about.fb.com/de/news/2020/05/facebook-weitet-faktenprueferprogramm-auf-oesterreich-und-die-schweiz-aus/.

55 Facebook, *Facebook weitet Faktenprüferprogramm aus: AFP wird Partner in Deutschland, Österreich und der Schweiz*, 2020, [online]: https://about.fb.com/de/news/2020/09/facebook-weitet-faktenprueferprogramm-aus-afp-wird-partner-in-deutschland-oesterreich-und-der-schweiz/.

56 Facebook, *Partnering with Third-Party Fact-Checkers*, 2020, [online]: https://www.facebook.com/journalismproject/programs/third-party-fact-checking/selecting-partners.

57 Poynter Institute, *International Fact-Checking Network fact-checkers' code of principles*, [online]: https://www.poynter.org/ifcn-fact-checkers-code-of-principles/.

58 Listę sygnatariuszy można znaleźć pod adresem https://ifcncodeofprinciples.poynter.org/signatories.

59 Listę aktualnych partnerów programu można znaleźć pod adresem https://www.facebook.com/journalismproject/programs/third-party-fact-checking/partner-map.

60 *Wspólna deklaracja Grupy Wyszehradzkiej o wzajemnej współpracy przy projektach cyfrowych*, Kraków 2021, [online]: https://www.gov.pl/attachment/68d73604-b505-4d5f-82ab-67e3f65618fd.

REKOMENDACJE

Legislacja mająca na celu zwalczanie dezinformacji musi odpowiadać na konkretne problemy

Nowe inicjatywy rządowe oraz działania legislacyjne powinny konkretnie podejmować problemy dezinformacji, propagandy, operacji informacyjnych itp. Zbyt szerokie podejście do problemów środowiska online i próba walki z jego wszystkimi zagrożeniami za pomocą jednolitego systemu bez względu na rodzaj problemu, niesie ze sobą groźbę powstania mechanizmów wadliwych i nieefektywnych. Przykładem jest brytyjski *Online Harms White Paper*, krytykowany często za zbyt ogólne podejście do zagrożeń w sieci i proponowanie zbyt ogólnego i, co za tym idzie nieszczelnego systemu.

Włączenie walki z dezinformacją w całokształt działań na rzecz cyberbezpieczeństwa

Kampanie dezinformacyjne często łączą się z szerszymi szkodliwymi akcjami albo są ich częścią. Jeśli spojrzeć na *MacronLeaks* jako przykład, ofensywa dezinformacyjna nastąpiła po udanych cyberatakach na skrzynki pocztowe ruchu politycznego *En Marche!*. Ważne, by postrzegać dezinformację jako aspekt szkodliwych działań w cyberprzestrzeni i element wojny hybrydowej oraz wzmacniać odporność systemów i sieci teleinformatycznych oraz cyberobronność poszczególnych krajów.

Budowa wspólnego frontu anty-dezinfo

Działania związane z przeciwdziałaniem dezinformacji i innym zagrożeniom występującym w przestrzeni informacyjnej powinny zostać oparte na kooperacji publiczno-prywatnej. Delikatny charakter kwestii związanych z przestrzenią informacyjną, *fact-checkingiem* czy cenzurą, powoduje, iż decyzyjność i aktywność w tych obszarach nie może pozostawać jedynie w gestii np. organów państwowych lub dużych firm technologicznych. Potrzebne jest stworzenie środowiska składającego się z organów administracji publicznej, sektora prywatnego, organizacji pozarządowych, medialnych i naukowych. Tylko wspólne działanie i wzajemna kontrola mogą uwiarygodnić i zoptymalizować poszczególne decyzje podejmowane w kontekście walki z dezinformacją.

Zwiększenie kooperacji oraz intensyfikacja współpracy na poziomie UE

Dalsze wzmacnianie współpracy państw członkowskich Unii Europejskiej i koordynacyjnych kompetencji Europejskiej Służby Działań Zewnętrznych ze szczególnym uwzględnieniem Centrum Analiz Wywiadowczych UE (INTCEN) oraz *Hybrid Fusion Cell*. Stworzenie długoletnich i strategicznych programów finansujących transgraniczne i paneuropejskie ośrodki monitorujące media społecznościowe. Intensyfikacja współpracy z innymi organizacjami międzynarodowymi (m.in. z NATO, OBWE, Radą Europy) oraz wykorzystanie potencjału wywiadowczego delegacji UE.

Promocja współpracy między platformami społecznościowymi a rządem

Eksperyment wykonany przez Facebooka i ekspertów wysokiego szczebla z francuskich ministerstw na początku 2019 r. jawi się jako bardzo pouczający, i skłania do namysłu nad nowym podejściem do systemu regulacyjnego mediów społecznościowych. Promowanie takiej współpracy to dla przedstawicieli rządu i dla ustawodawców sposób, by lepiej zorientować się w kwestiach, z którymi mierzą się takie platformy, zaś dla firm z branży sposób, by zrozumieć problemy przez ich platformy powodowane i podjąć decyzję o wspólnych działaniach. Współpraca może przyjmować charakter dwustronny albo odbywać się na spotkaniach czy szczytach gromadzących przedstawicieli z kilku państw.

Kluczem edukacja

Podstawowym, długoterminowym działaniem powinno być wdrożenie do systemu edukacji obszaru rozwijającego kompetencje korzystania z mediów (szczególnie cyfrowych) oraz modyfikacja systemu kształcenia w kierunku rozwoju umiejętności krytycznego myślenia i poddawania w wątpliwość treści zawartych w mediach. Niestety obecny system edukacyjny do poziomu średniego włącznie nie promuje kompetencji krytycznego myślenia i nie zawiera elementów związanych z edukacją medialną. Ich budowa to nadrzędny cel, gdyż społeczeństwo nieanalizujące treści i czytające bez zrozumienia jest idealnym celem kampanii dezinformacyjnych.

Zwiększenie transparentności i dostępu do danych

Kluczem do skutecznej walki z przejawami dezinformacji online jest lepsze zrozumienie jej natury oraz środowiska, w jakim funkcjonuje. W tym celu kluczowa wydaje się potrzeba rozszerzenia transparentności działań poszczególnych platform społecznościowych, algorytmów przez nie używanych oraz stosowanych rozwiązań technicznych. Zwiększyć powinna się także dostępność danych powiązanych z dezinformacją dla ośrodków badawczych, naukowców, analityków oraz organizacji zajmujących się tym problemem.

Wsparcie rozwoju narzędzi informatycznych do analizy przestrzeni informacyjnej online

Wspieranie rozwoju wielojęzykowych narzędzi służących do monitorowania zagrożeń hybrydowych i dezinformacji, które zdolne byłyby do przetwarzania dużych ilości danych oraz maksymalnej automatyzacji gromadzenia i analizy danych.

Intensyfikacja walki ze skoordynowanymi zachowaniami nieautentycznymi

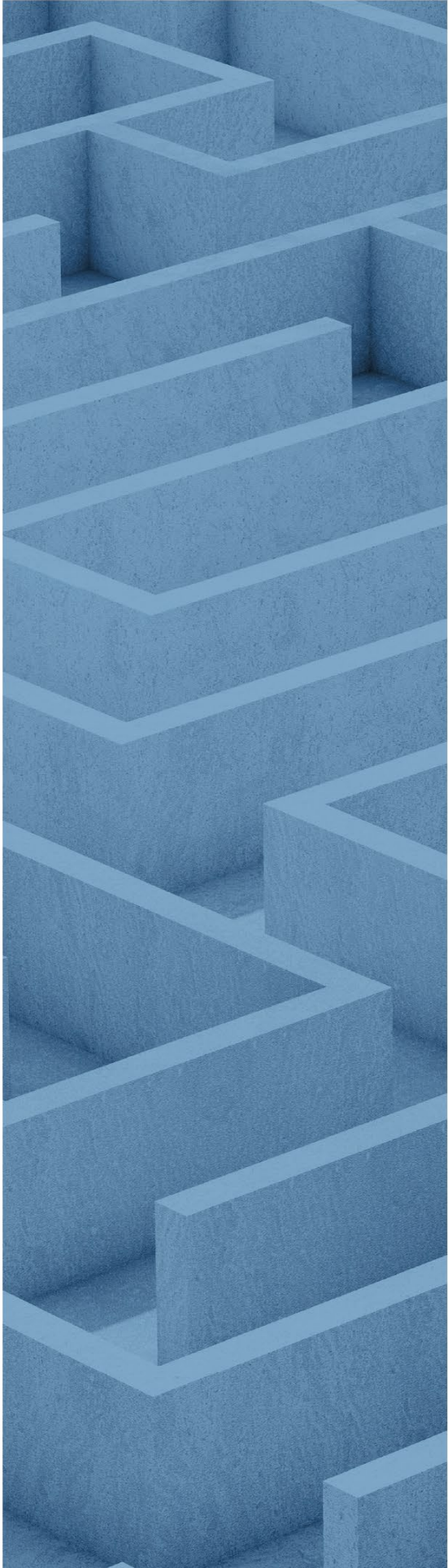
O ile moderacja treści przez sieci społecznościowe jest potrzebna w walce z dezinformacją internetową, odnoszące się do niej przepisy grzęzną często w debatach o progach i definicjach, które podmioty działające w złej wierze sprawnie obchodzą. Działając, nie należy tracić moderacji treści z oczu, ale uzupełnić ją powinien zwiększony wysiłek na rzecz przeciwdziałania problemowi skoordynowanych zachowań nieautentycznych.

Stworzenie narodowych komórek StratCom

W zakresie administracji państwowej wskazuje się na konieczność budowy międzyresortowych i międzyinstytucjonalnych komórek StratCom, które miałyby koordynować komunikację państwa oraz zwalczać dezinformację w sposób aktywny, posiadając własne kanały komunikacyjne. Komórka powinna budować scenariusze odpowiedzi na kampanie dezinformujące dzięki wyróżnieniu krytycznych obszarów podatnych na zewnętrzny wpływ informacyjny (jak w przypadku Polski polityka historyczna i relacje z Ukrainą) oraz być w stanie masowo uświadamiać społeczność o celach i narracjach dezinformacyjnych. Jednocześnie państwo powinno nadać ramy prawne dezinformacji i konsekwencjom jej świadomego rozpowszechniania, wzmacniając jednocześnie zaangażowanie mediów społecznościowych i sektora pozarządowego w monitoring i koordynowanie zwalczania dezinformacji.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki to wiodący pozarządowy ośrodek naukowo-badawczy o charakterze non-profit założony w 2000 r. Naszą misją jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz NATO. Instytut specjalizuje się w tworzeniu strategicznych rekomendacji i kierunków rozwoju kluczowych polityk publicznych, stanowiących merytoryczne wsparcie dla polskich i europejskich decydentów politycznych. Instytut Kościuszki jest pomysłodawcą i głównym organizatorem Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC, corocznej konferencji poświęconej strategicznym aspektom cyberprzestrzeni.



INSTYTUT KOŚCIUSZKI