Zeszyty Naukowe
Zbliżenia Cywilizacyjne XVII (1)/2021

https://dx.doi.org/10.21784/ZC.2021.003

PAULINA BERLIŃSKA-WOJTAS
Uniwersytet Mikołaja Kopernika w Toruniu

Bezpieczeństwo informacyjne RP w dobie COVID-19

Information Security of the Republic of Poland In COVID-19 era

Streszczenie:
Celem artykułu jest udzielenie odpowiedzi na pytania poświęcone realizacji działań zapobiegających dezinformacji w dobie pandemii COVID-19 na poziomie międzynarodowym i krajowym. Autorka analizuje dokumenty i konkluzje unijne oraz *Strategii Bezpieczeństwa Narodowego RP 2020* oraz konfrontuje dokumenty z zadaniami podjętymi przez podmioty we współpracy z organizacjami społecznymi: projektami *EUvsDisinfo*, *Mythbusters* i *#Fakenews.* Autorka przeanalizowała trendy i zainteresowania społeczne związane z pandemią i dezinformacją wokół COVID-19.
Słowa kluczowe: Dezinformacja, cyberprzestrzeń, bezpieczeństwo informacyjne, pandemia, Unia Europejska

Abstract
The aim of the article is to answer questions dedicated to implementation of disinformation in the time of the COVID-19 pandemic at the international and national level. The author analyzes EU documents and projects as well as the *Security Strategy of the Republic of Poland 2020* and confronts them with tasks undertaken by entities cooperating with social organizations: *EUvsDisinfo*, *Mythbusters* and *#Fakenews* projects. The author analyzed trends and social interests with the COVID-19 pandemic and disinformation.
Keywords: Disinformation, cyberspace, information security, pandemia, European Union

Wstęp

Termin *bezpieczeństwo informacyjne państwa* został wprowadzony dopiero w drugiej połowie XX wieku. Mimo to, informacja ujmowana jako czynnik bezpieczeństwa była dostrzegana dużo wcześniej. Wyzwania z nią związane były doceniane przez wodzów, królów, a nawet kupców. Tradycyjnie, bezpieczeństwo informacyjne interpretowano jako syntezę kilku istotnych czynników: dostarczała wiedzy o przeciwniku, chroniła własne tajemnice i obejmowała umiejętność zdobywania informacji przez władców na temat rządzonych[1]. Ranga informacji dla bezpieczeństwa państwa była wielokrotnie potwierdzana przez wydarzenia historyczne i te najnowsze.

W literaturze przedmiotu wskazuje się, że bezpieczeństwo informacyjne jest równoznaczne z osiągnięciem stanu wolnego od zagrożeń: przekazywania informacji podmiotom do tego nieuprawnionym, działalności dywersyjnej czy szpiegostwa. Termin oznacza też wachlarz działań, systemów oraz metod, których zamiarem jest zabezpieczenie zasobów informacyjnych gromadzonych, przetwarzanych i przechowywanych w pamięciach komputerów oraz sieciach teleinformatycznych. Bezpieczeństwo informacyjne obejmuje też organizację przepływu informacji między organami władzy[2].

Środowisko informacyjne Polski uległo zmianie od czasu wstąpienia do struktur NATO oraz Unii Europejskiej. Obecność naszego kraju we Wspólnocie obliguje do wywiązywania się z realizacji zadań postawionych na szczeblu unijnym. Obszerny katalog zagrożeń dla bezpieczeństwa informacyjnego powiększył się o problemy związane z rozwojem społeczeństwa informacyjnego i cyfrowego. Globalna pandemia SARS-COV-2, przeniesienie zawodowych i prywatnych sfer życia codziennego do Internetu to okoliczności sprzyjające rozwojowi zupełnie nowych wyzwań dla bezpieczeństwa informacyjnego, w tym dezinformacji dedykowanej pandemii COVID-19.

---

1 Zob.: J. Piekałkiewicz, *Dzieje szpiegostwa*, Warszawa 1999.

2 P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa Polskiego*, Toruń 2015, s. 71-73.

W artykule zadaję pytania: jak Unia Europejska przeciwdziała dezinformacji o COVID-19? W jaki sposób Polska odpiera ataki informacyjne poświęcone pandemii COVID-19? Czy strategia walki z działaniami hybrydowymi wpisuje się w założenia i rekomendacje Rady Europejskiej z 16 czerwca 2020?

Korpus materiału źródłowego stanowi dokument *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*[3], monografie naukowe poświęcone bezpieczeństwu informacyjnemu i działaniom dezinformacyjnym oraz materiały prasowe dostępne w przestrzeni internetowej. W świetle strategii Rady Unii Europejskiej oraz konkluzji, nieodzowne okazały się dokumenty zawierające rekomendacje dla państw członkowskich UE*: Nowy program strategiczny na lata 2019-2024*[4]*, Konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych*[5] oraz projekty *EU vs Disinfo*, *Mythbusters* czy *#Fakehunter* mający zwalczać szerzenie dezinformacji poświęconej pandemii COVID-19 na terenie państw członkowskich Unii Europejskiej[6]. Dzięki narzędziu Google Trends przeanalizowano trendy i zainteresowania związane z pandemią i dezinformacją wokół COVID-19.

Bezpieczeństwo informacyjne, a zaburzenia informacyjne

W efekcie rozwoju społeczeństwa informacyjnego napędzanego przez rewolucję informacyjną, warunki bezpieczeństwa, charakter i metody rozwiązywania kryzysów o charakterze militarnym czy pozamilitarnym uległy zmianie. Informacja będąca zasobem strategicznym, przekształciła się w broń i cel potencjalnych ataków. W związku z postępem technologicznym, zmianie uległo też naturalne środowisko obiegu

[3] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp z dnia 1.10.2020].

[4] *Nowy program strategiczny na lata 2019-2024,* https://www.consilium.europa.eu/media/39919/a-new-strategic-agenda-2019-2024-pl.pdf [dostęp z dnia 6.11.2020].

[5] *Konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych*, Bruksela, 10.12.2019, https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/pl/pdf [dostęp z dnia 6.11.2020].

[6] EU vs Disinfo, https://euvsdisinfo.eu/reading-list/ [dostęp z dnia 6.11.2020].

informacji. Cyberprzestrzeń wraz z dostępem do Internetu – powszechnej platformy komunikacyjnej – stanowi nowe źródło przekazu i przetwarzania informacji. Dzięki swojemu interaktywnemu charakterowi poza odbiorem informacji umożliwia też jej tworzenie i kreowanie.

Zaburzenia informacyjne (ang. *information disorder*[7]) to ogólny termin obejmujący trzy typy wprowadzania w błąd: dezinformacji *sensu stricto*, *misinformation* (mylna informacja) oraz *mal-information* (zniekształcona informacja)[8]. Dezinformacja w swoim najbardziej popularnym wymiarze to […] *taki sposób przekazania informacji – prawdziwej lub fałszywej – aby wprowadzić w błąd przeciwnika/konkurenta*[9]. Literatura przedmiotu i raporty ukazują bardziej złożoną strukturę dezinformacji. Jedną z płaszczyzn jest utożsamienie jej z pewną formułą przekazu kładąc nacisk na ingerencję w procesy poznawcze. Za cel dezinformacji uznaje się […] *wywołanie u odbiorcy poglądu, decyzji, działania lub jego braku, w zgodzie z założeniem ośrodka, który planował proces wprowadzenia odbiorcy w błąd. W istocie jest to ingerencja w proces decyzyjny obiektu (tj. odbiorcy), lub grupy obiektów*[10] dostarczanych komunikatów, które są niezgodne ze stanem faktycznym, mogą zaś stanowić […] *element walki informacyjnej między konkurującymi podmiotami, stąd istotne jest dążenie do eliminowania wszelkich prób fałszowania informacji*[11].

Znaczna część narracji medialnych wykorzystuje zwroty „dezinformacja" i *fake news* w sposób synonimiczny. Należy jednak odróżnić dwa typy dezinformacji. Pierwszy z nich, *misinformation* – mylna informacja – to nieprawdziwe lub mylące informacje rozprzestrzeniane w sposób

7 *Council of Europe*, https://www.coe.int/en/web/freedom-expression/information-disorder, [dostęp z dnia 6.11.2020].

8 Dwa terminy nie posiadają jeszcze swoich odpowiedników w języku polskim. Zob. raport: *Information disorder: Toward an interdisciplinary framework for research and policy making*, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c, [dostęp z dnia 29.10.2020].

9 T. R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 83.

10 Kamil Basaj, Dezinformacja, czyli sztuka manipulacji, [w:] *Biuletyn Biura Analiz i Reagowania Rządowego Centrum Bezpieczeństwa.25*, s. 14–17, https://rcb.gov.pl/wp-content/uploads/BIULETYN-ANALITYCZNY-nr-25.pdf, [dostęp z dnia 1.11.2020].

11 K. Liedel, P. Piasecka, T.R. Aleksandrowicz*, Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 36.

nieświadomy lub przypadkowy. Natomiast drugi, *Mal-information* to informacja mająca swoje źródło w faktycznym i realnym stanie rzeczy. Wykorzystana w mylący bądź wypaczony sposób ma na celu wprowadzenie chaosu informacyjnego bądź do osiągnięcia jakiegoś celu[12]. *Fake news* definiuje się jako wiadomości o niskiej jakości, intencjonalnie zakładające fałszywe informacje[13], zaprzeczające najlepszym dostępnym dowodom[14] lub sprawnie funkcjonujący element *growing industries*[15].

Unia Europejska, WHO, Europol

W świetle wybuchu epidemii SARS-COV-2 w chińskiej miejscowości Wuhan, uznaną 11 marca 2020 roku przez Światową Organizację Zdrowia[16] za pandemię, Unia Europejska, Zachodnie Bałkany czy kraje Afryki[17] stanęły przed wyzwaniem infodemii dedykowanej pandemii COVID-19. WHO definiuje infodemię jako […] *nadmierną ilość informacji na temat jakiegoś problemu, utrudniającą znalezienie rozwiązania. Może powodować wprowadzanie w błąd, dezinformację i powstawanie pogłosek podczas stanu zagrożenia zdrowia. Infodemia może utrudniać skuteczną reakcję w zakresie zdrowia publicznego i wywoływać dezorientację i brak zaufania wśród obywateli*[18]*.* Równolegle wobec problemów związanych z infodemią wskazuje się na wzrost intensywności działań dezinformacyjnych w zakresie przeciwdziałania pandemii SARS-COV-2.

12 C. Wardle, H. Derakhshan, *Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information*, https://en.unesco.org/sites/default/files/f._jfnd_handbook_module_2.pdf [dostęp z dnia 12.11.2020].

13 Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang, Huan Liu. *Fake News Detection on Social Media: A Data Mining Perspective*. SIGKDD Explor. Newsl. 19, 2017/1, s. 22–36 DOI:https://doi.org/10.1145/3137597.3137600.

14 D. J. Flynn, B. Nyhan, J. Reifler, *The nature and origins of misperceptions: Understanding false and unsupported beliefs about politics.* [w:] *Political Psychology*, 38/2017, 127-150.

15 Zob: D. Sumpter, *From Facebook and Google to fake news and filter-bubbles – the alghoritms that control our lives*, Nowy York 2018.

16 Dalej: WHO - World Health Organization.

17 Zob.: sprawozdania specjalne ESDZ na stronie EUvsDisinfo, https://euvsdisinfo.eu/ [dostęp z dnia 6.11.2020].

18 *Coronavirus disease 2019 (COVID-19). Situation report-45*, https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4 [dostęp z dnia 3.11.2020].

W celu przeciwdziałania zadaniom w zakresie wywierania wpływu na obywateli Wspólnoty Europejskiej, wypracowano wspólne stanowisko dedykowane zwalczaniu dezinformacji na terenie państw członkowskich. 10 czerwca 2020 roku opublikowano *Wspólny Komunikat do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Społecznoekonomicznego i Komitetu Regionów. Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom*[19], w którym opierając się o plan działania na rzecz zwalczania dezinformacji z 2018 roku[20] skoncentrowano się na natychmiastowej reakcji na dezinformację wokół pandemii koronawirusa. Podobnie jak w dokumencie z 2018 roku zaznaczono, że fundamentem wszelkich aktywności przeciwdziałających dezinformacji są [...] *europejskie wartości i prawa podstawowe, w szczególności wolność wyrażania opinii. Określono w nim podejście obejmujące całe społeczeństwo, zakładające zacieśnioną współpracę między kluczowymi podmiotami, takimi jak organy publiczne, dziennikarze, badacze, weryfikatorzy informacji, platformy internetowe i społeczeństwo obywatelskie*[21]. Autorzy dokumentu pod nazwą *Konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych* z grudnia 2019 roku położyli szczególny nacisk na wykorzystywanie nowych technologii i sztucznej inteligencji w prowadzonych działaniach informacyjnych oraz wypracowania szczególnych narzędzi dyplomacji cyfrowej[22].

W komunikacie z 2020 roku, po wybuchu pandemii COVID-19, zniesiono akcent dyplomatyczny i uwypuklono główne wyzwania dotyczące

[19] *Wspólny Komunikat do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Społecznoekonomicznego i Komitetu Regionów. Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom*, 10.6.2020, Bruksela, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020JC0008&from=EN, [dostęp z dnia 6.11.2020].

[20] Zob.: *Joint Communication to the European Parliament, the European Council, the Council, the European economic and social comitee and the comitee of the region, Action Plan Against Disinformation*, 5.12.2018, Bruksela, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf, [dostęp z dnia 6.11.2020].

[21] Tamże.

[22] *Konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych*, Bruksela, 10.12.2019, https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/pl/pdf [dostęp z dnia 6.11.2020].

zwalczania infodemii polegające na proaktywnej i pozytywnej komunikacji, skoordynowanej i szybkiej reakcji unijnej polityki publicznej oraz *współpracy organów państw członkowskich, społeczeństwa obywatelskiego, platform mediów społecznościowych i na arenie międzynarodowej*[23]. Twórcy komunikatu podkreślili konieczność rozróżnienia pomiędzy fałszywymi formami treści lub tymi wprowadzającymi w błąd. W swojej propozycji uwzględnili też zamiar wprowadzenia w błąd, wyrządzenia szkody publicznej lub osiągnięcia korzyści ekonomicznych. Obecność takiego zamiaru, według komunikatu komisji z kwietnia 2018 roku[24] kwalifikuje te treści jako dezinformację. Podniesienie zdolności analitycznej i dostępu do platform internetowych, tuż obok zacieśnienia współpracy między instytucjami UE a działaniami państw Wspólnoty, mają stanowić element działań krótko- i długoterminowych w zakresie walki z dezinformacją na terenie UE. Obok wymienianych: jasnej i dostępnej komunikacji, rzetelnego informowania na poziomie krajowym i ogólnoeuropejskim[25] prowadzono ukierunkowaną strategię informacyjną zarządzaną we współpracy z innymi organizacjami, na przykład projektu autorstwa zespołu z WHO, *Mythbusters*[26], pakietu pomocowego *Drużyna Europy*[27] czy Europejskim Centrum Zapobiegania i Kontroli Chorób[28]. Warto nadmienić, że popularne platformy komunikacyjne o dużym czynniku widoczności jak Facebook, WhatsApp, Twitter, Mozilla czy TikTok są sygnatariu-

[23] *Wspólny Komunikat do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Społecznoekonomicznego i Komitetu Regionów. Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom*, 10.6.2020, Bruksela, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020JC0008&from=EN, [dostęp z dnia 6.11.2020], s. 3.

[24] *Zwalczanie dezinformacji w internecie: podejście europejskie COM(2018) 236, finał z dnia 26 kwietnia 2018 r.*, https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-236-F1-PL-MAIN-PART-1.PDF [dostęp z dnia 1.11.2020].

[25] Zob. m. in. treści pochodzące z Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób, https://www.ecdc.europa.eu/en [dostęp z dnia 6.11.2020].

[26] Witryna demaskująca treści dezinformacyjne dotyczące COVID-19: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters [dostęp z dnia 10.11.2020].

[27] https://ec.europa.eu/poland/news/200408_pandemia_reax_pl [dostęp z dnia 6.11.2020].

[28] https://www.ecdc.europa.eu/en/covid-19-pandemic [dostęp z dnia 10.11.2020].

szami kodeksu praktyk na rzecz walki z dezinformacją[29]. W październiku 2020 do walki z dezinformacją na temat korona wirusa dołączyła Wikipedia[30]. Ponadto, członkowie międzynarodowej inicjatywy *Journalism Trust Initiative*, w skład której wchodzą takie organizacje jak Reporterzy Bez Granic, Global Editors Network czy European Broadcasting Union opracowali wskaźniki wiarygodności dotyczące źródeł informacji[31]. Podobnie jak projekt *Global Disinformation Index* , inicjatywy mają na celu demaskację, rozbicie i obniżenie rangi witryn dezinformacyjnych[32]. Obok treści zawierających elementy dezinformacji bądź stanowiących *fake-news'y*, członkowie inicjatyw analizowali też sposób prowadzenia kampanii reklamowych przez firmy zamieszczające reklamy swoich produktów tuż obok dezinformacji poświęconych COVID19[33].

Europejski Urząd Policji (dalej: Europol) na początku 2020 roku sporządził sprawozdanie dedykowane cyberprzestępczości zorganizowanej między innymi wokół pandemii COVID-19[34]. Z analizy danych wynika, że w porównaniu z innymi działaniami przestępczymi to właśnie wybuch pandemii był najbardziej widocznym i uderzającym katalizatorem rozwoju przestępstw w sieci. Sprawozdawcy podkreślają wzrost cyberprzestępstw dedykowanych sprzedaży towarów nielegalnych[35] w tzw. darkwebie[36], na-

[29] Zob.: *Code of practise of disinformation*, online: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation [dostęp z dnia 6.11.2020]; N. Lomas, *TikTok joins the EU's Code of practise and disinformation*, shorturl.at/eotNO [dostęp z dnia 6.11.2020].

[30] *Rzetelne informacje o COVID-19 w Wikipedii. WHO ogłosiło współpracę z platformą*, 26.10.2020, https://www.cyberdefence24.pl/bezpieczenstwo-informacyjne/rzetelne-informacje-o-covid-19-w-wikipedii-who-oglosilo-wspolprace-z-platforma, [dostęp z dnia 1.11.2020].

[31] Strona internetowa projektu: *Journalism Trust Initiative:* https://jti-rsf.org/en/about [dostęp z dnia 10.10.2020].

[32] *Disinformation index:* https://disinformationindex.org/about/ [dostęp z dnia 11.10.2020].

[33] Zob. raport z października 2020: *Popular brands adevrtising next to COVID19 disinformation*, https://disinformationindex.org/wp-content/uploads/2020/10/Oct_23_2020-DisinfoAds-Popular-brands-advertising-next-to-COVID19-disinformation-.pdf [dostęp z dnia 11.11.2020].

[34] *Catching virus...*: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic [dostęp z dnia 2.11.2020].

[35] Por.: *European Drug Report 2020: keys and developments*, https://www.emcdda.europa.eu/publications/edr/trends-developments/2020_en [dostęp z dnia 10.11.2020].

[36] Zob.: E. Ormsby, *Darkweb*, przeł. A. M. Nowak, Kraków 2019.

silenie anonimowej sprzedaży niecertyfikowanych masek ochronnych i zestawów testowych czy zmodernizowanych kampanii phisignowych i ransomware'owych (z naciskiem na wzmożenie kampanii DDos[37]). Działania te w widocznym stopniu wykorzystują społeczną izolację i przeniesienie większości aktywności zawodowych i prywatnych do Internetu. Europol kładł nacisk zmasowaną aktywność dezinformacyjną organizacji podmiotów, które w bezpośredni sposób wykorzystują kryzys publicznej opieki zdrowotnej w celu osiągnięcia zysku lub wspierania interesów geopolitycznych[38].

Strategia Bezpieczeństwa Narodowego RP 2020

Strategia Bezpieczeństwa Narodowego RP 2020 (dalej: SBN), podpisana 12 maja 2020 roku przez Prezydenta RP Andrzeja Dudę, stanowi długo wyczekiwany dokument mający na celu uwzględnienie wszystkich wymiarów funkcjonowania bezpieczeństwa narodowego. Współcześnie strategia wyewoluowała do postaci dokumentu włączającego zagadnienia wykraczające poza te, wykorzystujące bitwy do celów wojny, jak pisał von Clusewitz[39], czy rozdziału i użycia środków wojennych dla urzeczywistnienia celów polityki, jak u Harta[40]. Strategia ma być:

> wyborem przez najwyższe organy władzy wykonawczej środków, narzędzi i sposobów ich osiągnięcia w ramach […] przemyślanej koncepcji działania na rzecz zapewnienia wolnych od wszelkich wyzwań i zagrożeń warunków bytu im rozwoju narodowego, a także łagodzenia lub usuwania skutków w razie ich wystąpienia[41].

[37] DDos – denial-of-service – rozproszone ataki typu „odmowa usługi". Ataki DDos są klasyfikowane jako jeden z rodzaj cyberprzestępstw, charakteryzujących się ograniczonymi barierami wejścia ze względu na niski koszt oraz wysoką osiągalność.
[38] *Catchinh…*: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic [dostęp z dnia 2.11.2020] s. 4.
[39] C. von Clausewitz, *O wojnie*, przeł. A. Cichowicz, L. Koc, Warszawa 1958.
[40] L. Hart, B.Henry, *Strategia: działania pośrednie*, przeł. E. Bagieński, Warszawa 1959.
[41] *Ocena zapisów Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020_prof. Waldemar Kitler*, 1.9.2020, https://cyberdefence24.pl/ocena-zapisow-strategii-bezpieczenstwa-narodowego-rzeczypospolitej-polskiej-2020prof-waldemar-kitler, [dostęp z dnia 11.11.2020].

W ramach dwóch aspektów bezpieczeństwa narodowego: przedmiotowego i podmiotowego, dostrzeżono rangę dwóch różnych obszarów działań cyberbezpieczeństwa oraz bezpieczeństwa informacyjnego. Włączono je do pierwszego z czterech filarów bezpieczeństwa. Oddzielając je od siebie, autorzy SBN potraktowali je priorytetowo. Autorzy Strategii za obligatoryjne uznali podniesienie odporności na zagrożenia w przestrzeni informacyjnej. W konsekwencji akcentowali konieczność *budowy zdolności do ochrony przestrzeni informacyjnej*, […] *zwiększenie skutecznych działań z zakresu jednolitej komunikacji strategicznej* oraz aktywnego przeciwdziałania *dezinformacji poprzez budowę zdolności i stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi*[42]. W opublikowanej na łamach strony cyberdefence24.pl ocenie zapisów nowej SBN, eksperci odnoszą się bezpośrednio do kwestii spornych wynikających z wyzwań, jakimi powinny podołać zapisy *Strategii…*[43]. Dotyczą między innymi dynamiki i nieprzewidywalności środowiska cyberzagrożeń i bezpieczeństwa informacyjnego, wskazywania działań Federacji Rosyjskiej jako głównego nurtu zagrożeń w przestrzeni cyber czy pominięcie pozostałych podmiotów politycznych i niepolitycznych (np. Chiny czy ISIS)[44]. Mimo zapisu o zwiększaniu świadomości społecznej, o niebezpieczeństwach wynikających z manipulacji informacjami, w sposób powierzchowny zaprezentowano możliwe zagrożenia w przestrzeni informacyjnej oraz nie wskazano precyzyjnych rozwiązań w walce z dezinformacją. Zagrożenia, mimo upływu lat, rozwoju technologii oraz nowych wyzwań o charakterze globalnym, zostały dokładniej opisane w dwóch dokumentach: projekcie Doktryny bezpieczeństwa informacyjnego RP[45]

[42] *Strategia...*, s. 21, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp z dnia 1.11.2020].

[43] *(Cyber)bezpieczna Polska. Strategia Bezpieczeństwa Narodowego okiem ekspertów*, 1.9.2020, https://www.cyberdefence24.pl/cyberbezpieczna-polska-strategia-bezpieczenstwa-narodowego-okiem-ekspertow [dostęp z dnia 20.11.2020].

[44] Tamże.

[45] *Doktryna bezpieczeństwa informacyjnego RP*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf, [dostęp z dnia 10.11.2020].

oraz Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej *na lata 2019-2024*[46].

Przykłady działań międzynarodowych i krajowych w walce z dezinformacją poświęconą COVID-19

Zainteresowanie pandemią COVID-19 od początku jej występowania bije rekordy popularności wśród użytkowników Internetu. Narzędzie Google Trends, umożliwiające analizę popularności fraz wpisywanych przez użytkowników sieci udostępniło osobną kategorię dedykowaną wyszukiwaniom związanym z pandemią COVID-19[47]. Fraza *disinformation* wpisywana na terytorium USA, związana bezpośrednio z minionymi wyborami prezydenckimi w Stanach Zjednoczonych została przez Google Trends oznaczona liczbą 68. Natomiast frazy *COVID, koronawirus COVID-19* czy *COVID-19 Polska* z wynikami odpowiednio 100, 94 i 60 w okresie 4 października – 14 listopada 2020 plasują się w czołówce wyszukiwań w wyszukiwarce Google z regionu Polski[48]. Fraza *fake news koronawirus* interesuje Polaków falowo: zainteresowanie nią wśród internautów odnotowano od 8-14 marca 2020 (wynik 100) oraz 8-24 października 2020 (wynik 64)[49]. Fraza *dezinformacja* nie cieszy się w Polsce popularnością – zainteresowanie nią wynosi mniej niż 1, nie pojawiła się w wynikach 25 najpopularniejszych wyszukiwań w sektorze dedykowanemu pandemii COVID-19 w Polsce.

Wśród przykładów działań UE, WHO, Polski i pozostałych podmiotów w zakresie zwalczania zagrożeń dezinformacyjnych i manipulacji informacją poświęconą pandemii COVID-19 są wymienione projekty:

[46] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024, dostęp z dnia 9.11.2020.

[47] Zobacz: *Coronavirus Search Trends*, https://trends.google.com/trends/story/US_cu_4Rjdh3ABAABMHM_en, [dostęp z dnia 20.11.2020].

[48] Google Trends: https://trends.google.com/trends/explore?geo=PL&q=dezinformacja,COVID-19 [dostęp 23.11.2020].

[49] Google Trends: https://trends.google.com/trends/explore?geo=PL&q=fake%20news%20koronawirus [dostęp z dnia 23.11.2020].

EUvsDisinfo, *Mythbusters* oraz raporty opracowane przez UNESCO[50] czy na przykład stworzona przez NATO *research task group*[51]. Na poziomie krajowym szczególnie interesującą inicjatywą jest projekt realizowany przez Polską Agencję Prasową i rząd – *#Fakehunter*[52].

Projekt *EUvsDifinfo*, autorstwa Europejskiej Służby Działań Zewnętrznych *East StratCom Task Force* została utworzona w 2015 roku w celu polepszenia narzędzi w prognozowaniu i reagowaniu powstającym kampaniom dezinformacyjnym. Autorzy projektu obrali za cel zwiększenie świadomości społecznej i zrozumienia operacji dezinformacyjnych przygotowywanych na Kremlu oraz pomoc obywatelom Unii Europejskiej w uodpornieniu się na cyfrowe informacje i manipulacje mediami[53]. Przeciwdziałanie dezinformacji poświęconej pandemii stanowi jeden z obszarów, którymi zajmuje się *East Stratcom TaskForce* Korzystając z usług analizy danych i monitorowania mediów zespół projektu identyfikuje, zestawia i ujawnia przypadki dezinformacji pochodzące z prokremlowskich mediów, które są rozpowszechniane w całej UE i krajach Partnerstwa Wschodniego. Zespół *EUvsDisinfo* gromadzi i kataloguje przypadki udokumentowanych działań dezinformacyjnych w bazie danych. Zgromadzony katalog to repozytorium typu *open source* z możliwością przeszukiwania – zawierającej ponad 6500 próbek pro kremlowskiej dezinformacji[54]. Baza danych jest aktualizowana co tydzień wraz z krótkim podsumowaniem trendów. Ponadto, zespół publikuje analizy i artykuły poświęcone ewolucji metod i praktyk dezinformacji oraz zestawienia międzynarodowych badań. Interesującą funkcjonalnością jest wprowadzenie interaktywnego quizu sprawdzającego umiejętność rozpoznawania dezinformacji w sieci[55].

[50] *Combating the disinfodemic: Working for truth in the time of COVID-19*, https://en.unesco. org/covid19/disinfodemic, [dostęp z dnia 2.11.2020].
[51] *How is NATO Responding to Disinformation on COVID-19*, https://shape.nato. int/news-archive/2020/video-how-is-nato-responding-to-disinformation-on-covid19 [dostęp z dnia 1.11.2020].
[52] *#Fakehunter*, https://fakehunter.pap.pl/, [dostęp z dnia 9.11.2020].
[53] *EUvsDisinfo*: https://euvsdisinfo.eu/about/ [dostęp z dnia 23.11.2020].
[54] EUvsDisinfo: https://euvsdisinfo.eu/disinformation-case/ [dostęp z dnia 20.11.2020].
[55] EUvsDisinfo: https://euvsdisinfo.eu/quizzes/euvsdisinfo/ [dostęp z dnia 20.11.2020].

Mythbusters jest jednym z projektów Światowej Organizacji Zdrowia, któremu w ramach funkcjonującej witryny internetowej poświęcono kolejną podstronę. *Mythbusters* zawiera szereg filmów wideo i infografik informujących o prawidłowym postępowaniu w przypadku rozszerzania się epidemii. Demaskuje popularne mity i w graficzny sposób odpowiada na pytania dotyczące między innymi mnożenia wirusa w określonych warunkach pogodowych. Wydaje się, że mimo rangi problemu szerzenia dezinformacji, została potraktowana przewidywalnie. Interesującą funkcjonalnością przedstawioną w formie poradnika jest instrukcja zgłaszania/raportowania treści dezinformacyjnych *online*[56] działająca na zasadzie hiperłączy. Ciekawą formą rozpowszechniania, choć ukrytą w treści strony, wiedzy o mechanice szerzenia dezinformacji poświęconej COVID-19 jest podlinkowanie gry *GOViral!*[57]. Gra polega na ocenie wiarygodności treści o COVID-19, wcielaniu się w postać trolla szerzącego dezinformację czy powielaniu treści, które potencjalnie mogą stanowić treści celowo wprowadzające w błąd.

#Fakehunter, społeczny projekt weryfikacji treści publikowanych w Internecie jest rodzimą odpowiedzią na zapotrzebowanie walki z dezinformacją. Platforma uruchomiona we współpracy Polskiej Agencji Prasowej i GovTechPolska – międzyresortowego zespołu działającego przy Premierze RP – działa na rzecz demaskowania nieprawdziwych informacji (*fake news*) dotyczących wirusa SARS-COV-2. Autorzy opracowali bazę około 800 artykułów zawierających link do źródeł polskojęzycznych oraz raport eksperta odnoszący się do rzetelności każdego omawianego artykułu. W ramach społecznego projektu, autorzy przygotowali wyzwanie dla użytkowników Internetu (*#Fakehunterchallenge*), którego istotą było zgłoszenie i zweryfikowanie jak największej ilości *fake newsów*[58]. Innowacją projektu jest wprowadzenie wtyczki współpracującej z przeglądarką Chrome umożliwiającą bieżące

[56] Zob.: https://www.who.int/campaigns/connecting-the-world-to-combat-coronavirus/how-to-report-misinformation-online [dostęp z dnia 20.11.2020].
[57] *GOViral!*: https://www.goviralgame.com/en [dostęp z dnia 11.2020].
[58] Podkreślam to, ponieważ autorzy nie różnicują *fake newsów* od *mal-information* czy *misinformation*.

zgłaszanie i raportowanie wiadomości. Wbrew praktykom i sprawdzonym rozwiązaniom z zagranicy, twórcy społecznej i rządowej platformy zwalczającej dezinformacje nie wprowadzili narzędzi edukujących w zakresie rozpoznawania dezinformacji.

W ramach działań pozarządowych należy wspomnieć o raporcie z września 2019 roku *Zjawisko dezinformacji w dobie polityki cyfrowej. Państwo, społeczeństwo, polityka, biznes*[59], raporcie Instytutu Kościuszki[60] analizującego trendy i narracje dezinformacji rozpowszechniane na platformach społecznościowych oraz platformie FakeNews.pl[61], projektowi Fundacji Przeciwdziałamy Dezinformacji.

Konkluzje

Analizując wpływ nowoczesnych technologii i rangi informacji rozumianej w kategoriach zasobu strategicznego państwa, trudno pomiąć cyberprzestrzeń rozumianej jako nowe środowisko walki. Cyberprzestrzeń może posłużyć jako przykład zmiany paradygmatu w myśleniu o sposobach prowadzenia walki i konfliktów pozamilitarnych, do których z powodzeniem zalicza się walka informacyjna. Prowadzona z sukcesami na dwóch różnych płaszczyznach, rzeczywistym i wirtualnym, może przebiegać w językach odnoszących się do potrzeb społecznych, tak czytelnych podczas pandemii COVID-19.

Działania skierowane na zwalczanie dezinformacji poświęconej koronawirusowi zarówno na szczeblu międzynarodowym i krajowym są umiarkowane, ograniczając się do pojedynczych przedsięwzięć. Ilość dokumentów, raportów i rekomendacji mówiących o konieczności prowadzenia skutecznych czynności skierowanych przeciw działaniom dezinformacji rosyjskiej czy chińskiej, skonfrontowana z przedsięwziętymi krokami jest nieproporcjonalnie wysoka. Projekt WHO, instytucji

[59] Nask Państwowy Instytut Wydawniczy, Warszawa 2019, https://akademia.nask.pl/badania/Raport_CP_Dezinformacja_ONLINE.pdfzespołu

[60] M. Krawczyk, K. Milulski, *COVID-19. Dezinformacja w polskiej cyberprzestrzeni*, Kraków 2020 https://ik.org.pl/wp-content/uploads/raport_dezinformacja_pl_v3.pdf [dostęp z dnia 13.11.2020].

[61] *Fakenews.pl*: https://fakenews.pl/ [dostęp z dnia 12.11.2020].

odwołującej się do zaufania społecznego i autorytetu wynikającego z jej rangi, zajmującej się zdrowiem na poziomie globalnym pozostawia dużo luk do wypełnienia wyłącznie na poziomie informacyjnym. Na poziomie krajowym, mimo wielokrotnego podkreślania znaczenia bezpieczeństwa informacyjnego, a zarazem konieczności walki ze wszelkimi przejawami dezinformacji, zrealizowano projekt, który pozostał bez echa w mediach masowego przekazu. Mimo intensywnych kampanii informacyjnych na temat pandemii koronawirusa dotychczas nie opublikowano żadnego spotu informacyjnego odnoszącego się do bezpieczeństwa informacyjnego czasie pandemii COVID-19. Przestrzeń związana z edukacją w zakresie rozpoznawania dezinformacji pozostaje niezagospodarowana. Wszak kampanie dezinformacyjne mają bezpośredni wpływ na zmierzch autorytetów, podważania zaufania do instytucji i rozwojowi wszelkich ruchów zagrażających bezpieczeństwu zdrowia publicznego. Mimo trudności, z jakimi boryka się państwo i jego instytucje w dobie COVID-19, nie należy zapominać o bezpieczeństwie informacyjnym kraju jak i konsekwencjach długofalowych kampanii dezinformacyjnych naruszających poczucie bezpieczeństwa Polaków.

Bibliografia:

I. Monografie:

Aleksandrowicz T. R., *Podstawy walki informacyjnej*, Wyd. Editions Spotkania, Warszawa 2016.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa Polskiego*, Wyd. Adam Marszałek, Toruń 2015.

Hart L., Henry B., *Strategia: działania pośrednie*, przeł. E. Bagieński, Wyd. Ministerstwa Obrony Narodowej, Warszawa 1959.

Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka*, Wyd. Difin, Warszawa 2012.

Ormsby E., *Darkweb*, przeł. A. M. Nowak, Wyd. Społeczny Instytut Wydawniczy Znak, Kraków 2019.

Piekałkiewicz J., *Dzieje szpiegostwa*, Wyd. Czytelnik, Warszawa 1999.

Sumpter D., *From Facebook and Google to fake news and filter-bubbles – the alghoritms that control our lives*, Wyd. Bloomsbury Sigma, Nowy York 2018.

von Clausewitz C., *O wojnie*, przeł. A. Cichowicz, L. Koc, Wyd. Test, Warszawa 1958.

II. Dokumenty:

Catching virus. Cybercrime disinformation: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic.

Doktryna bezpieczeństwa informacyjnego RP, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

European Drug Report 2020: keys and developments, https://www.emcdda.europa.eu/publications/edr/trends-developments/2020_en

Information disorder: Toward an interdisciplinary framework for research and policy making, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Commitee and the Commitee oh the Regions Action Plan Against Disinformation, Bruksela 2018, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf

Konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych, Bruksela, https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/pl/pdf

Konkluzje Rady w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych, Bruksela, 10.12.2019, https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/pl/pdf

Nowy program strategiczny na lata 2019-2024, https://www.consilium.europa.eu/media/39919/a-new-strategic-agenda-2019-2024-pl.pdf

Sprawozdania specjalne ESDZ na stronie EUvsDisinfo, https://euvsdisinfo.eu

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej *na lata 2019–2024*, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024.

Wspólny Komunikat do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Społecznoekonomicznego i Komitetu Regionów. Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom, Bruksela 2020, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020JC0008&from=EN.

Wspólny Komunikat do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Społecznoekonomicznego i Komitetu Regionów. Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom, Bruksela 2020, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020JC0008&from=EN.

Zjawisko dezinformacji w dobie polityki cyfrowej. Państwo, społeczeństwo, polityka, biznes, Nask Państwowy Instytut Wydawniczy, Warszawa 2019, https://akademia.nask.pl/badania/Raport_CP_Dezinformacja_ONLINE.pdf.

III. Artykuły:

Basaj K., Dezinformacja, czyli sztuka manipulacji, [w:] *Biuletyn Biura Analiz i Reagowania Rządowego Centrum Bezpieczeństwa*, https://rcb.gov.pl/wp-content/uploads/BIULETYN-ANALITYCZNY-nr-25.pdf.

Flynn D. J., Nyhan B., Reifler J., [w:] *The nature and origins of misperceptions: Understanding false and unsupported beliefs about politics.* [at:] *Political Psychology*, 38/2017, s. 127-150.

Shu K., Sliva A., Wang S., Tang J., Liu H., *Fake News Detection on Social Media: A Data Mining Perspective* [w:] *SIGKDD Explor. Newsl*. 19, 2017/1, s. 4-17.

IV. Źródła internetowe:

#Fakehunter, https://fakehunter.pap.pl/.

(Cyber)bezpieczna Polska. Strategia Bezpieczeństwa Narodowego okiem ekspertów, https://www.cyberdefence24.pl/cyberbezpieczna-polska-strategia-bezpieczenstwa-narodowego-okiem-ekspertow.

Code of practise of disinformation, online: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

Combating the disinfodemic: Working for truth in the time of COVID-19, https://en.unesco. org/covid19/disinfodemic.

Coronavirus disease 2019 (COVID-19). Situation report-45, https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4

Coronavirus Search Trends, https://trends.google.com/trends/story/US_cu_4Rjdh3ABAABMHM_en.

Council of Europe, https://www.coe.int/en/web/freedom-expression/information-disorder.

Disinformation index: https://disinformationindex.org/about/

EU vs Disinfo, https://euvsdisinfo.eu/reading-list/.

Fakenews.pl: https://fakenews.pl/.

GOViral! https://www.goviralgame.com/en.

How is NATO Responding to Disinformation on COVID-19, https://shape.nato.int/news-archive/2020/video-how-is-nato-responding-to-disinformation-on-covid19

https://www.cyberdefence24.pl/bezpieczenstwo-informacyjne/rzetelne-informacje-o-covid-19-w-wikipedii-who-oglosilo-wspolprace-z-platforma.

Journalist Trust Initiative: https://jti-rsf.org/en/about.

Krawczyk M., Milulski K*., COVID-19. Dezinformacja w polskiej cyberprzestrzeni*, Kraków 2020 https://ik.org.pl/wp-content/uploads/raport_dezinformacja_pl_v3.pdf.

Lomas N., *TikTok joins the EU's Code of practise and disinformation*, shorturl.at/cnzR6.

Mythbusters: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters.

Ocena zapisów Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020_prof. Waldemar Kitler, https://cyberdefence24.pl/ocena-zapisow-strategii-bezpieczenstwa-narodowego-rzeczypospolitej-polskiej--2020prof-waldemar-kitler.

Popular brands adevrtising next to COVID19 disinformation, https://disinformationindex.org/wp-content/uploads/2020/10/Oct_23_2020-DisinfoAds-Popular-brands-advertising-next-to-COVID19-disinformation-.pdf.

Rzetelne informacje o COVID-19 w Wikipedii. WHO ogłosiło współpracę z platformą.

Wardle C., Derakhshan H., *Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information*, https://en.unesco.org/sites/default/files/f._jfnd_handbook_module_2.pdf.

Zwalczanie dezinformacji w internecie: podejście europejskie COM(2018) 236, finał z dnia 26 kwietnia 2018 r., https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-236-F1-PL-MAIN-PART-1.PDF.