SPRAWY MIĘDZYNARODOWE

2022, t. 75, nr 2
ISSN 0038-853X
e-ISSN 2720-0361
DOI 10.35757/SM.2022.75.2.13

Recenzje

TOMASZ PAWŁUSZKO
Uniwersytet Opolski
ORCID: 0000-0002-5572-3199
tomasz.pawluszko@uni.opole.pl

Robert Kupiecki, Filip Bryjka, Tomasz Chłoń, *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe „Scholar", Warszawa 2022, ss. 315

Przedmiotem recenzji jest monografia Roberta Kupieckiego, Filipa Bryjki i Tomasza Chłonia, która wypełnia istotną lukę tematyczną na polskim rynku wydawniczym, trudno bowiem znaleźć w obiegu akademickim i eksperckim przekrojową publikację na temat dezinformacji w stosunkach międzynarodowych. Zapotrzebowanie na wiedzę w tym obszarze znacząco wzrosło w związku z eskalacją konfliktu rosyjsko-ukraińskiego w lutym 2022 r. Recenzowana praca została wydana w połowie 2022 r. w uznanym warszawskim wydawnictwie Scholar jako efekt grantu Organizacji Traktatu Północnoatlantyckiego (*NATO's Public Diplomacy Division*) przy współpracy z Wydziałem Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Jak czytamy we wstępie, zasadnicza część publikacji powstała jednak przed pełnoskalową inwazją Rosji na Ukrainę.

Struktura książki jest stosunkowo harmonijna i odpowiada kwestiom wymienionym w podtytule. Część pierwsza dotyczy zagadnień pojęciowych (środowiska i koncepcji dezinformacji oraz związanych z nią zagrożeń), druga podejmuje temat rozpoznania zjawiska dezinformacji, a trzecia porusza kwestie przeciwdziałania mu i budowania odporności. Każda z nich składa się z czterech rozdziałów i podsumowania.

We wstępie Autorzy przyznają, że dezinformacja jako technika komunikacji zbudowana na kłamstwie ma długą historię. Jest ona pochodną ludzkich słabości poznawczych, które współcześnie wykorzystywane są w przestrzeni informacyjnej przez rozmaitych uczestników stosunków międzynarodowych. W recenzowanej książce badana jest dezinformacja jako narzędzie polityki zagranicznej, ponieważ to państwa dysponują największymi zdolnościami technicznymi i finansowymi, aby kierować swoje działania do całych społeczeństw innych państw (lub własnego) w celu wpływania na ich zachowania i decyzje. W epoce internetu i innych mediów masowych doszło do zdemokratyzowania przekazu informacji. Tym samym podmioty rozpowszechniające nieprawdę czy wytwarzające dezinformację mogą mieć ogromny wpływ na całe społeczeństwa. Waga problemu uzasadnia podjęcie projektu, jaki zamierzyli sobie Autorzy.

Punktem wyjścia pierwszej części książki jest ewolucja rozumienia bezpieczeństwa narodowego. Wpłynęły na to takie procesy jak: rozszerzenie kategorii bezpieczeństwa na kwestie niemilitarne, delegitymizacja wojen międzypaństwowych oraz rozwój technologii militarnych (nowe rodzaje broni czy oddziaływania psychologiczne i asymetryczne). Doprowadziło to

do poszerzenia tematyki bezpieczeństwa poprzez uwzględnienie nowych podmiotów, obszarów problemowych, wymiarów, oceny zagrożeń i perspektyw analitycznych (te celne uwagi zawarte są na stronach 18–19). Szczególnie ważną perspektywą jest spojrzenie tzw. szkoły kopenhaskiej, która w połowie lat dziewięćdziesiątych XX w. zaczęła promować ideę społecznego konstruowania bezpieczeństwa. Wypowiedzi dotyczące bezpieczeństwa mogą nie tylko odzwierciedlać zagrożenia, ale też je konstruować. Rozwój technologiczny i jego coraz większa oczywistość dla kolejnych pokoleń żyjących w XXI w. doprowadziły do uznania kwestii informacyjnych za kluczowe (Autorzy przytaczają przykłady wyborów prezydenckich w USA czy paniki wokół epidemii COVID-19). Konkludując, można zgodzić się z Autorami, że informacja urasta do rangi jednego z głównych zasobów strategicznych, nawet jeśli trudno określić skalę i skuteczność działań posługujących się informacją czy dezinformacją.

Na stronie 25 Autorzy prezentują interesujące zestawienie narzędzi wykorzystywanych w operacjach dezinformacyjnych. Przytaczają również próbę oszacowania globalnych kosztów dezinformacji, które w 2018 r. miały wynieść ok. 78 mld dol. Skutków tego procesu może doświadczać co czwarta firma na świecie. W epoce internetu dezinformacja może stanowić narzędzie w walce o umysły i emocje ludzi na skalę niespotykaną nigdy w historii. Jako przykład Autorzy analizują oddziaływanie tzw. postprawdy, czyli sytuacji, gdy uznane autorytety i fakty są zestawiane na równi z masowo powielanymi opiniami o wątpliwym pochodzeniu i jakości. Nadmiar informacji oraz istnienie tzw. baniek informacyjnych w mediach społecznościowych powodują, że spora liczba ludzi skłonna jest przyjąć opinie niesprawdzone lub nieoparte na wiedzy (s. 30).

W podrozdziale 1.3 Autorzy wprowadzają model ekosystemu informacyjnego jako otoczenia społeczeństwa i przedstawiają osiem składników tej koncepcji (s. 31–33). Następnie omawiane są procesy poznawcze u ludzi oraz ich konsekwencje dla przetwarzania informacji. Przedstawiono tu rozmaite heurystyki (s. 37) i techniki eksploatujące deficyty poznawcze człowieka. Wiedza ta ma ogromne znaczenie w polityce, ponieważ – jak podają Autorzy na podstawie badań Eurostatu z grudnia 2021 r. – średnio jedynie 23 proc. ludności państw UE weryfikuje informacje, a w żadnym z nich wskaźnik ten nie przekracza 50 proc. populacji. Co więcej, osoby powyżej 65 roku życia siedmiokrotnie częściej powielają nieprawdziwe informacje niż ludzie młodsi.

W rozdziale drugim Autorzy dokonują historycznego przeglądu studiów nad kłamstwem jako narzędziem polityki i dezinformacji. Dzieje ludzkości pełne są kulturowych wzorców zawierających kłamstwo wykorzystywane w charakterze techniki wpływania na otoczenie społeczne. Autorzy klasyfikują rodzaje propagandy oraz liczne bliskie jej typy operacji informacyjnych (s. 56–58). Bardzo użyteczne jest dla czytelników zestawienie na stronie 60, zawierające klaryfikację jedenastu pojęć, takich jak: *fakt*, *informacja*, *opinia*, *analiza* czy *dowód*. Sam termin *dezinformacja* zostaje szerzej opisany w rozdziale trzecim, gdzie zyskuje inne synonimy, jak: *socjotechnika*, *inżynieria społeczna*, *technika społecznej manipulacji* etc. (s. 65–66).

Autorzy podkreślają, że wspólne cechy wielu definicji dezinformacji dotyczą przekazu opartego na fałszywych informacjach, którego celem jest oddziaływanie na odbiorcę, by działał nie zgodnie z własnymi interesami, ale zamiarami dezinformatora. Mało precyzyjne jest natomiast stwierdzenie, że ważną cechą dezinformacji jest fakt, że dezinformator nie liczy się z kosztami swego działania innymi niż własne (s. 69). Chodzi zapewne o spowodowanie strat wśród adresatów działania.

Interesującym zabiegiem jest przegląd definicji dezinformacji zawartych w niektórych polskich dokumentach strategicznych. Zestawienie z dokumentami międzynarodowymi ogłoszonymi przez NATO i UE sugeruje konieczność przeglądu polskich doktryn bezpieczeństwa z perspektywy omawianego problemu (s. 70–73). Postulat ten wsparty jest udostępnionymi przez badaczy z Uniwersytetu Oksfordzkiego danymi z 2019 r., które pokazują, że w latach 2017–2019 podwoiła się liczba dezinformacji w mediach społecznościowych na świecie. Ponadto ponad siedemdziesiąt państw używa propagandy komputerowej do manipulowania opinią publiczną. Prym wiodą tu reżimy autorytarne, ale zjawisko widoczne jest również w społeczeństwach demokratycznych, zwłaszcza w okresach kampanii wyborczych.

Nieoczywistym wnioskiem z rozdziału trzeciego jest opinia, że odporniejsze na dezinformację zewnętrzną są państwa autorytarne, ponieważ zdecydowanie bardziej angażują się w kontrolowanie źródeł informacji. Wydaje się, że jest to stwierdzenie nieudokumentowane (brakuje danych i przypisów) i niejasne, ponieważ przy określeniu obiektu oddziaływania zatarto rozróżnienie na państwo i społeczeństwo (w przypadku reżimów autorytarnych podano państwo, a przy demokracjach – społeczeństwo). Państwa autorytarne, kontrolując obieg informacji, są w stanie stosować

dezinformację przeciwko własnym obywatelom, co czyni to zjawisko faktem, niezależnie od tego, czy jest wobec danego państwa zewnętrzne czy też nie. Lepszym obiektem oceny pozostają w tym względzie społeczeństwa, a nie państwa. Wartościowym stwierdzeniem jest za to pogląd, że promowane w demokracji wartości polityczne (np. wolność, otwartość i tolerancja) zarówno sprzyjają odporności społeczeństw, jak i czynią społeczeństwa otwarte podatnymi na wrogie oddziaływania.

W rozdziale czwartym otrzymujemy ważne zestawienie typów dezinformacji (ramka na s. 84) i rodzajów kłamstwa (s. 85–88). Autorzy trafnie tłumaczą na kilku przykładach, że procesy wykorzystywania nowych technologii informacyjnych do budowania mitów politycznych stanowią poważne zagrożenie dla państw demokratycznych (cyberataki, dezinformacja w procesach wyborczych, hejt, manipulacje na forach internetowych etc.). Rozdział kończy się nietypowym podsumowaniem, składającym się z pytań i odpowiedzi, co dobrze uzupełnia eseistyczny styl wywodu.

Druga część książki dotyczy procesów rozpoznawania dezinformacji. W rozdziale pierwszym dowiadujemy się, czym jest bezpieczeństwo informacyjne państwa (s. 103–105). Autorzy podkreślają wiodącą rolę Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego w systemie polskim oraz opisują doktrynalne i ustawowe elementy systemu bezpieczeństwa informacji. Istotnym wątkiem są kwestie wolności słowa i praw jednostki. Autorzy zauważają, że niski poziom debaty publicznej może prowadzić do dezinformacji i błędnych decyzji władz państwa, ale wolność opinii pozostaje elementem demokracji. Błędne wypowiedzi ekspertów nie noszą zatem znamion dezinformacji wywiadowczej zgodnie z art. 132 kodeksu karnego (s. 109).

W kolejnych podrozdziałach znalazły się oparte na przykładach analizy agentów wpływu, tzw. pożytecznych idiotów, trolli internetowych i botów (s. 110–115). Następnie czytelnik otrzymuje analizę specyfiki dezinformacji wojskowej wraz z przydatną terminologią. Wydaje się jednak, że w pracy tego typu opisy takich pojęć, jak *agent, funkcjonariusz służb* i *oferent* warto byłoby umieszczać nie w przypisie, ale raczej w tekście głównym, podobnie jak w przypadku wcześniej wprowadzonych terminów (s. 117).

W rozdziale drugim części drugiej przedmiotem analizy jest rozpoznawanie dezinformacji skierowanej do masowego odbiorcy. Autorzy sumiennie relacjonują procesy legislacyjne i omawiają narzędzia prawne (s. 125–127) dotyczące zwalczania dezinformacji w internecie. Problem ten jest

i będzie istotny w perspektywie rozwoju kolejnych narzędzi dezinformacji, ponieważ liczba użytkowników internetu zbliża się do pięciu miliardów, a 90 proc. wszystkich światowych danych wytworzono w ciągu dwóch pierwszych dekad XXI w. Kolejnym problemem jest fakt, że wiadomości fałszywe rozprzestrzeniają się sześć razy szybciej niż prawdziwe (s. 128–130). W następnych częściach omawianego rozdziału Autorzy analizują modele analizy i rozpoznawania dezinformacji opracowane w Wielkiej Brytanii (model RESIST) oraz przykłady zwalczanych przekazów. Wszystko zdefiniowane jest tu prosto i precyzyjnie.

Rozdział trzeci drugiej części książki to dalszy ciąg potoczystego wywodu prezentującego sposoby obrony przed dezinformacją. Autorzy omawiają myślenie krytyczne, sprawdzanie faktów (stosują tu niestety anglicyzm *fact-checking*) i wywiad jawnoźródłowy (OSINT). Godna uwagi jest rekonstrukcja elementów przekazów informacyjnych, które często zawierają sensacyjne tytuły oraz emocjonalne komunikaty pisemne i wizualne, a nie odwołują się do źródeł. Następnie Autorzy przechodzą do przedstawienia procesu weryfikowania informacji (s. 142–148), a na kolejnych stronach omawiają model analizy dezinformacji SCAME (s. 154–156).

Rozdział czwarty – i ostatni w części drugiej – dotyczy militaryzacji informacji w rosyjskiej kulturze strategicznej. Omówione są tu wątki historyczne i doktrynalne oraz elementy rosyjskiego ekosystemu dezinformacji, a dodatkowo wymieniono kilkadziesiąt (!) instytucji, które mogą wpływać na procesy informacyjne w Rosji i poza jej granicami. Dalsza część wywodu dotyczy rosyjskich ingerencji w wybory w państwach demokratycznych, ze szczególnym uwzględnieniem USA. Rozdział ten pokazuje, jak w praktyce może działać inspirowana przez państwo operacja dezinformacyjna w przestrzeni masowej komunikacji realnej i wirtualnej innego państwa. W następnych częściach omówione są wybrane dezinformacyjne działania wojskowe i polityczne (s. 172–185). Rozdział kończy się zwięzłym i informatywnym podsumowaniem.

Część trzecia rozwija podjęty w poprzednim bloku wątek przeciwdziałania dezinformacji poprzez budowę odporności. Autorzy skupili się w szczególności na problemach demokracji amerykańskiej oraz internetowej aktywności różnych rosyjskich instytucji w celu ingerencji w procesy wyłaniania władz w innych krajach. Podjęto tu także temat edukacji medialnej i przeciwdziałania informacji na poziomie jednostki. Wartością dodaną jest analiza rozwiązań instytucjonalnych w tym zakresie, które

przyjęto w takich europejskich państwach, jak Francja, Wielka Brytania i Włochy. Autorzy dowodzą, że edukacja medialna może wpływać na odporność państw i społeczeństw na dezinformację.

Po rozważeniu tych problemów Autorzy przechodzą na poziom analizy korporacji i instytucji społeczeństwa obywatelskiego. W tabeli 13 na stronie 224 zestawiają działania głównych korporacji internetowych mające na celu zwalczanie dezinformacji. W tabeli 14 na stronie 228 podają z kolei kontrprzykłady nieskutecznych, szkodliwych czy pozorowanych działań głównych platform mediów społecznościowych. W bardzo wartościowym fragmencie wywodu podkreślono, że coraz częściej pojawiają się dezinformacje na zamówienie, toteż największe serwisy celują w działania prewencyjne, monitorując treści, które naruszają regulamin, i likwidując profile i konta posługujące się fałszywymi informacjami. Skuteczność takich kroków nie jest jednak optymalna. Kolejną grupą interesariuszy w procesie zwalczania dezinformacji są organizacje społeczeństwa obywatelskiego i *think tanki* (s. 236, tab. 15). Wartością dodaną jest zestawienie inicjatyw będących przykładami prewencji i walki z dezinformacją (s. 238–241) oraz próba opisu wyzwań dla dziennikarstwa przyszłości (s. 244–246). Autorzy wspominają przy tym również o polskich inicjatywach (s. 246–247).

Ostatni rozdział książki przenosi czytelnika na poziom państwowy i międzynarodowy. Autorzy proponują w nim zestawienie przykładowych działań władz różnych państw przeciwko dezinformacji (s. 251) i rozwijają wybrane wątki w celu uogólnienia. Do kluczowych obszarów działań państw przeciwko dezinformacji należą: tworzenie struktur, regulacje prawne, cyberbezpieczeństwo, edukacja władz i urzędników, ostrzeżenia, decyzje administracyjne, działania dyplomatyczne i współpraca ze społeczeństwem. Autorzy gorzko konstatują, że tak naprawdę niewiele państw podjęło aktywne kroki przeciwko dezinformacji (na stronach 256–263 omówiono kilka modeli instytucjonalnych). Rozdział wieńczą analiza wydarzeń związanych z eskalacją wojny rosyjsko-ukraińskiej i podsumowanie analogiczne do poprzednich rozdziałów. Książka nie ma jednak osobnego zakończenia.

Publikacja Roberta Kupieckiego, Filipa Bryjki i Tomasza Chłonia opisuje ważne procesy, stawia liczne pytania i proponuje uczciwe odpowiedzi. Jest to kompleksowy, aktualny i ambitny projekt skupiający się na zagrożeniach internetowych. Na uznanie zasługują dobór tematów, układ treści, baza źródłowa i przejrzyste grafy. Książka napisana jest przejrzystym językiem i nie zawiera żargonu z obszaru cyberbezpieczeństwa.

Wydaje się, że recenzowany tom mógł przyjąć formułę prostszego i krótszego raportu analitycznego (o czym świadczą bardzo udane podsumowania poszczególnych części), ale Autorzy wybrali perspektywę bardziej akademicką, z rozbudowanym blokiem omawiającym pojęcia, wypowiedzi i klasyfikacje, co też było potrzebne z racji braku podobnych opracowań na polskim rynku. Publikacja przysłuży się kształceniu ekspertów, polityków, dziennikarzy, studentów i wszystkich, którzy czują się odpowiedzialni za bezpieczeństwo informacyjne państwa polskiego. Podsumowując, należy stwierdzić, że książka jest kamieniem milowym polskich badań w tym temacie i przez wiele lat będzie obowiązkowym punktem odniesienia dla wszystkich analityków bezpieczeństwa.