
Weronika Ratajczak

Wyższa Szkoła Biznesu i Nauk o Zdrowiu w Łodzi

ORCID 0009-0006-3176-5948

Dezinformacja i wojna informacyjna jako zagrożenie dla bezpieczeństwa międzynarodowego

Wprowadzenie

Dezinformacja i wojna informacyjna to kluczowe zagadnienia dotyczące bezpieczeństwa międzynarodowego. W ostatnich dekadach stały się one coraz powszechniejsze, a ich znaczenie wzrosło wraz z rozwojem technologii i mediów społecznościowych. Problem ten jest szczególnie istotny, gdyż manipulacja informacją może prowadzić do destabilizacji politycznej, gospodarczej i społecznej. W dobie mediów elektronicznych, globalnych sieci społecznościowych i szybkiego przepływu informacji manipulacje takie mogą więc prowadzić do osłabienia zaufania społecznego i demokracji. Skala tego zjawiska oddziałuje na społeczeństwa w sposób realny – według badań 80% badanych uznało, że dezinformacja negatywnie wpływa na procesy polityczne w ich kraju i na świecie¹.

Artykuł ma charakter teoretyczno-przeglądowy i został oparty na jakościowej analizie treści, obejmującej literaturę naukową, raporty organizacji

¹ *Internet Security & Trust 2019. Part 3: Social Media, Fake News & Algorithms* (2019). Centre for International Governance Innovation. <https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%203%20Social%20Media%2C%20Fake%20News%20%26%20Algorithms.pdf> [dostęp: 30.09.2025].

międzynarodowych oraz opracowania eksperckie poświęcone problematyce dezinformacji, wojny informacyjnej i bezpieczeństwa międzynarodowego. W ramach analizy uwzględniono zarówno ujęcia teoretyczne, jak i konkretne studia przypadków, które miały istotne znaczenie dla stabilności politycznej i bezpieczeństwa informacyjnego państw demokratycznych. Analiza ma również charakter interdyscyplinarny, uwzględnia zagadnienia z zakresu prawa międzynarodowego, cyberbezpieczeństwa.

Celem niniejszego artykułu jest analiza dezinformacji i wojny informacyjnej jako narzędzi stosowanych w konfliktach. W kontekście tych zagrożeń szczególną uwagę zwrócono na ramy prawne oraz przykłady ingerencji w demokratyczne procesy wyborcze. Praca ta podejmuje również próbę oceny skuteczności środków obronnych, takich jak inicjatywy prawne, działania sojuszy wojskowych oraz programy edukacyjne. Problem badawczy koncentruje się na określeniu, w jaki sposób dezinformacja wpływa na stabilność państw i jakie strategie są najbardziej efektywne w jej zwalczaniu. Postawiono następującą hipotezę: Dezinformacja oraz wojna informacyjna stanowią dziś jedno z kluczowych wyzwań dla bezpieczeństwa międzynarodowego.

Przegląd literatury pokazuje, że wiele prac naukowych koncentruje się na technikach i strategiach dezinformacji stosowanych przez państwa oraz inne podmioty. Badania wykazują, że dezinformacja jest nie tylko narzędziem wojny psychologicznej, ale także sposobem na osłabienie moralne przeciwnika. W literaturze przedmiotu często podkreśla się znaczenie współpracy międzynarodowej i edukacji społeczeństwa jako podstawowych elementów skutecznej obrony przed dezinformacją. Zarówno w teorii, jak i w praktyce, dezinformacja pozostaje wyzwaniem dla globalnego bezpieczeństwa. Celem obecnych badań jest zrozumienie mechanizmów działania dezinformacji oraz opracowanie efektywnych strategii zapobiegania jej negatywnym skutkom.

Dezinformacja i wojna informacyjna – współczesny wymiar

Dezinformacja definiowana jest jako proces świadomego rozpowszechniania fałszywych lub manipulowanych informacji² w celu osiągnięcia określonego efektu politycznego lub strategicznego³. W literaturze prawniczej i politologicznej podkreśla się, że celem dezinformacji jest często kompromitacja

² M. Hetmański (2003). *Społeczny charakter informacji*. Wydawnictwo Towarzystwo Naukowe KUL. Lublin, s. 10–25.

³ K. Pięta (2024). *Dezinformacja jako narzędzie manipulacji w sieci*. https://www.researchgate.net/publication/385909650_Disinformation_as_a_tool_of_manipulation_on_the_Internet [dostęp: 03.03.2025].

państwowych instytucji czy osób publicznych i „podważanie autorytetu i wiarygodności państw”⁴. Dezinformacja może być językowa, obrazowa lub demonstracyjna⁵. Można ją więc rozumieć jako instrument w wojnie informacyjnej, wykorzystywany m.in. do podgrzewania napięć społecznych, deprecjacji wiarygodnych źródeł czy osłabiania zaufania społecznego. Ma na celu stworzenie pozornie prawdziwego obrazu i kształtowanie opinii zgodnie z interesami dezinformującego państwa, prowadząc do bezpośredniej lub pośredniej szkody⁶. Działania dezinformacyjne bywają integralnym elementem hybrydowego nacisku – mogą one wywoływać chaos informacyjny w społeczeństwie, co stanowi według NATO realne zagrożenie dla bezpieczeństwa demokratycznych państw⁷.

Wojna informacyjna to termin szerszy, obejmujący strategiczne użycie informacji, manipulacji i propagandy jako narzędzi walki o przewagę nad przeciwnikiem⁸. Opisuje się wojnę informacyjną jako użycie informacji i sposobu jej kreowania w celu uzyskania przewagi strategicznej, przy czym obejmuje ona zmylenie, wprowadzenie w błąd i wpływanie tendencyjnie na świat, podważanie jego polityki i skłanianie do nieświadomego przyczyniania się do realizacji celów dezinformatora⁹. Innymi słowy, wojna informacyjna to agresywna działalność w sferze komunikacji, prowadząca m.in. do zakłócenia procesów podejmowania decyzji czy podziałów społecznych. Jest z nią związana również kwestia cyberwojny – ataki komputerowe często są skoordynowane z kampaniami propagandowymi, tworząc wymiar „hybrydowy” konfliktu.

Wojna informacyjna lub operacje informacyjne niewątpliwie wpływają na świadomość i wolę jednostek, organizacji, społeczeństw i narodów za pomocą środków informacyjno-technicznych i informacyjno-psychologicznych. Propaganda i dezinformacja są formami operacji psychologicznych, nazywanych też wojną psychologiczną lub kognitywną. Są to działania poniżej progu

⁴ R. Mueller (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. U.S. Department of Justice. <https://www.justice.gov/archives/sco/file/1373816/dl> [dostęp: 03.03.2025].

⁵ M. Świerczek (2018). „System matrioszek”, czyli dezinformacja doskonała. „Przegląd Bezpieczeństwa Wewnętrznego”, 19, s. 210–225.

⁶ D. Jemielniak (2013). *Życie wirtualne dzikich*. Wydawnictwo Poltext. Warszawa, s. 11.

⁷ D.L. Byman, C. Gao, C. Meserole, V.S. Subrahmanian (2023). *Deepfakes and international conflict*. The Brookings Institution. <https://www.brookings.edu/articles/deepfakes-and-international-conflict/> [dostęp: 01.03.2025].

⁸ M. Sawicka-Ickiewicz (2025). *Propaganda i informacja – zarządzanie informacją w przestrzeni medialnej. Od klasycznych środków masowego przekazu do internetowych mediów społecznościowych*. https://wiz.pb.edu.pl/akademia-zarzadzania/wp-content/uploads/sites/3/2025/04/4.4.-Magdalena-Ickiewicz-Sawicka-Propaganda-i-dezinformacja---zarzadzanie-informacja-w-przestrzeni-medialnej_with_metadata.pdf [dostęp: 20.05.2025].

⁹ M. Świerczak (2018). „System matrioszek”... *Op. cit.*

wojny konwencjonalnej, które prowadzą do dezinformacji i innych form manipulacji, podważania zaufania do instytucji oraz wywoływania chaosu informacyjnego, co z kolei ułatwia przeprowadzenie ataków destabilizujących.

Metodologia badania

Celem niniejszego artykułu jest analiza dezinformacji i wojny informacyjnej jako narzędzi stosowanych we współczesnych konfliktach w kontekście bezpieczeństwa międzynarodowego. Opracowanie ma charakter teoretyczno-przeglądowy i opiera się na analizie dostępnej literatury naukowej, raportów instytucji międzynarodowych oraz źródeł eksperckich.

W badaniu zastosowano metodę analizy treści w ujęciu jakościowym, polegającą na przeglądzie i krytycznym omówieniu kluczowych publikacji dotyczących operacji dezinformacyjnych, propagandy cyfrowej, regulacji prawnych oraz działań instytucji międzynarodowych. Uwzględniono zarówno ujęcia teoretyczne, jak i opisy przypadków, które miały znaczący wpływ na bezpieczeństwo polityczne i informacyjne państw demokratycznych.

Zebrany materiał posłużył do opracowania syntezy aktualnych zagrożeń informacyjnych z uwzględnieniem kontekstu technologicznego (m.in. wykorzystania sztucznej inteligencji i algorytmów) oraz przeglądu narzędzi przeciwdziałania dezinformacji. Artykuł nie zawiera badań własnych ani analizy statystycznej – jego celem jest uporządkowanie i interpretacja istniejącej wiedzy, a także identyfikacja obszarów wymagających dalszych, pogłębionych badań empirycznych.

Ramy prawne i inicjatywy instytucji międzynarodowych w zwalczaniu dezinformacji

Obowiązujące prawo międzynarodowe pełni istotną rolę w dziedzinie cyberbezpieczeństwa, uwzględniając zarówno kwestie dezinformacji, jak i operacji informacyjnych. W związku z tym coraz więcej instytucji na poziomie globalnym oraz europejskim angażuje się w zwalczanie problemu wiarygodności informacji dostępnych w internecie oraz mediach¹⁰. W wyniku tych działań wydano dokumenty, z których za kluczowe uznaje się Kodeks postępowania

¹⁰ W. Czerski (2021). *Test Craap – przykład narzędzia do walki z dezinformacją*. https://www.researchgate.net/publication/366102266_Test_Craap__przyklad_narzedzia_do_walki_z_dezinformacja [dostęp: 01.04.2025].

w zakresie zwalczania dezinformacji¹¹ oraz Plan Działania Przeciwno Dezinformacji¹². Komisja i Europejska Rada ds. Usług Cyfrowych zatwierdziły oficjalne włączenie dobrowolnego kodeksu postępowania w zakresie zwalczania dezinformacji do Aktu o usługach cyfrowych¹³. Te dokumenty bezsprzecznie zobowiązują największe korporacje, takie jak Google, Facebook oraz X (dawny Twitter), do podejmowania działań mających na celu zwalczanie dezinformacji. Zgodnie z raportem Komisji Europejskiej z dnia 29 października 2019 roku kroki podjęte przez sygnatariuszy zaczynają przynosić pierwsze rezultaty. Na przykład, Facebook usunął już ponad 2 miliardy fałszywych kont wykorzystywanych do rozpowszechniania dezinformacji¹⁴.

Z kolei Plan Działania na rzecz zwalczania dezinformacji powstał w odpowiedzi na apel Rady Europejskiej o przedstawienie skoordynowanej reakcji UE na wyzwania związane z dezinformacją, w tym w kontekście zbliżających się wyborów europejskich w 2019 r. Plan opiera się na istniejących inicjatywach Komisji oraz pracach grup zadaniowych ds. komunikacji strategicznej w ramach Europejskiej Służby Działań Zewnętrznych (ESDZ). Dezinformacja w rozumieniu tego planu to możliwe do zweryfikowania, nieprawdziwe lub wprowadzające w błąd informacje, tworzone i rozpowszechniane w celu uzyskania korzyści gospodarczych lub zamierzonego wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną¹⁵. Skoordynowana reakcja na dezinformację przedstawiona w Planie Działania opiera się na czterech filarach:

1. Zwiększenie zdolności instytucji Unii do wykrywania, analizowania i ujawniania dezinformacji.
2. Wzmocnienie skoordynowanej i wspólnej reakcji na dezinformację.
3. Mobilizowanie sektora prywatnego do zwalczania dezinformacji.
4. Podnoszenie świadomości i zwiększanie odporności społecznej¹⁶.

Warto w tym miejscu podnieść, że Rada Bezpieczeństwa ONZ do tej pory nie przyjęła jednolitej rezolucji dotyczącej dezinformacji ani cyberoperacji informacyjnych. Niektórzy autorzy postulują uznanie poważnych

¹¹ *Kodeks postępowania w zakresie zwalczania dezinformacji*. Unia Europejska. <https://digital-strategy.ec.europa.eu/pl/library/code-conduct-disinformation> [dostęp: 01.04.2025].

¹² *Wspólny komunikat do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu regionów* (2018). Plan działania na rzecz zwalczania dezinformacji. <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52018JC0036> [dostęp: 01.04.2025].

¹³ *Kodeks postępowania... Op. cit.*

¹⁴ R. Babraj (2020). *Dezinformacja w dobie cyfrowej rewolucji*. Cyberpolicy. <https://cyberpolicy.nask.pl/dezinformacja-w-dobie-cyfrowej-rewolucji> [dostęp: 01.04.2025].

¹⁵ *Wspólny komunikat do Parlamentu Europejskiego... Op. cit.*

¹⁶ *Ibidem*.

cyberataków z manipulacją informacją za „uzbrojony atak” według art. 51 Karty Narodów Zjednoczonych, co teoretycznie dawałoby poszkodowanemu prawo do samoobrony. Jednak praktyka wskazuje, że odwołanie konfliktu informacyjnego do ogólnych przepisów o użyciu siły jest trudne. W związku z tym kraje często polegają na mniej formalnych środkach – sankcjach, restrykcjach wizowych czy blokadach nadawania propagandowych mediów (np. sankcje UE wobec rosyjskich nadawców)¹⁷.

Nowoczesne technologie i sztuczna inteligencja jako narzędzia dezinformacji

Postęp technologiczny radykalnie zwiększa zdolność do prowadzenia dezinformacyjnych operacji¹⁸. Media społecznościowe i algorytmy umożliwiają wzmacnianie treści, a sztuczna inteligencja generowanie fałszywych informacji na dużą skalę¹⁹. Modele językowe oparte na SI, takie jak ChatGPT, umożliwiają szybkie tworzenie tekstów niemal nieodróżnialnych od ludzkich – postów społecznościowych, artykułów czy komentarzy²⁰. Szczególnym zagrożeniem są *deepfake*. *Deepfake* może posłużyć do sfalszowania apelu lub spreparowania wypowiedzi polityka. Uważa się, że – choć często fałszywe informacje się demaskuje – ich potencjał wprowadzenia chaosu jest duży, ponadto podważają one wiarygodność rzeczywistych komunikatów²¹.

Ewelina Bartuzi-Trokielewicz stwierdza, że ludzie mają tendencję do ufania temu, co widzą i słyszą, co sprawia, że to zjawisko jest istotne w kontekście społeczeństwa cyfrowego, które korzysta z audiowizualnego przekazu informacji i internetu jako głównego źródła wiedzy o świecie. *Deepfake* kojarzy się głównie z manipulacją obrazu, w szczególności twarzy – czyli

¹⁷ Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, Dz.U. 1947 nr 23 poz. 90.

¹⁸ *Fake news – dezinformacja online próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski* (2020). Krajowa Rada Radiofonii i Telewizji. Wydawnictwo Krajowej Rady Radiofonii i Telewizji.

¹⁹ *Techniki manipulacji w świecie deepfake'ów – jak sztuczna inteligencja zmienia oblicze dezinformacji* (2025, 16 maja). Portal Gov.pl. <https://www.gov.pl/web/ai/techniki-manipulacji-w-swiecie-deepfakeow---jak-sztuczna-inteligencja-zmienia-oblicze-dezinformacji> [dostęp: 15.04.2025].

²⁰ M. Fraser (2021, 13 stycznia). *Sztuczna inteligencja w służbie propagandy. Jak jeszcze można wykorzystać modele językowe?* CyberDefence24. <https://cyberdefence24.pl/technologie/sztuczna-inteligencja-w-sluzbie-propagandy-jak-jeszcze-mozna-wykorzystac-modele-jezykowe> [dostęp: 15.04.2025].

²¹ D.L. Byman i in. (2023). *Deepfakes and... Op. cit.*

podmianą wizerunku lub sterowaniem mimiką. Istnieją również techniki manipulacji głosem, pozwalające odtworzyć mowę dowolnej osoby (*voice cloning*), oraz łączone materiały audio-wideo, w których sztucznie wygenerowany głos i mimika (wraz z ruchem ust) współgrają ze sobą, tworząc realistyczne filmy. Treści *deepfake'ów*, jak inne materiały manipulacyjne, są tworzone według precyzyjnych schematów marketingowo-propagandowych²². Rozwój sztucznej inteligencji umożliwił łatwiejsze tworzenie dezinformacji.

Organizacja NewsGuard przeprowadziła audyt 10 wiodących narzędzi generatywnej sztucznej inteligencji (m.in. ChatGPT-4, OpenAI, Microsoft – Copilot, Meta AI czy Google – Gemini) i sprawdziła ich skłonność do powtarzania fałszywych narracji²³. Z analizy wynika, że chatboty częściej generują fałszywe informacje w języku rosyjskim, chińskim i hiszpańskim niż w angielskim. Jednocześnie przy języku rosyjskim i chińskim pojawia się ponad połowa zarówno błędnych odpowiedzi, jak i braków odpowiedzi. Zdaniem analityków, użytkownik zadający pytanie na temat wiadomości w tych językach najlepszym zachodnim chatbotom ma większe prawdopodobieństwo otrzymania odpowiedzi zawierającej dezinformację lub propagandę ze względu na poleganie chatbota na źródłach niższej jakości i narracjach kontrolowanych przez państwo w tych językach²⁴.

Niewątpliwie nowoczesne technologie radykalnie zwiększają możliwości siania dezinformacji. W marcu 2022 r. ukazało się zmanipulowane wideo z prezydentem Ukrainy, Wołodymyrem Zełenskim, w którym rzekomo namawiał on ukraińskich żołnierzy do poddania się – był to klasyczny *deepfake* (wiarygodność filmu została szybko obalona, a sam film usunięto). Tego typu przykład pokazuje, że AI potrafi kreować filmowe i dźwiękowe fałszywki, zdolne wywołać zamieszanie u odbiorców. W realnym świecie może umożliwiać reżimom automatyzację propagandy, masową profilację odbiorców i natychmiastowe generowanie zmanipulowanej treści²⁵.

Deepfake pobudza emocje takie jak strach, złość i frustracja, dopasowując się do potrzeb odbiorcy. Jak zauważa Ewelina Bartuzi-Trokielewicz, treści te naśladują znane formaty: wywiady, poradniki, relacje, rolki TikTok, reportaże, *livestreamy*, reklamy i konsultacje online. Zawierają fałszywe opinie i zapewnienia o braku ryzyka oraz gwarantowanym zysku, opierając się

²² Techniki manipulacji w świecie *deepfake'ów*... (2025, 16 maja). Op. cit.

²³ Sztuczna inteligencja. Modele AI generują rosyjską i chińską dezinformację (2025, 7 lutego). CyberDefence24. <https://cyberdefence24.pl/technologie/sztuczna-inteligencja-modele-ai-generuja-rosyjska-i-chinska-dezinformacje> [dostęp: 16.04.2025].

²⁴ Ibidem.

²⁵ N. Bochyńska (2022, 19 marca). *Deepfake z Zełenskim. Czy fejkowe materiały wideo zmieniają przebieg wojen informacyjnych?* CyberDefence24. <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-deepfake-z-zelemskim-czy-fejkowe-materialy-wideo-zmienia-przebieg-wojen-informacyjnych> [dostęp: 16.04.2025].

na narracjach spiskowych i odrzuceniu oficjalnych źródeł. Często stosują emocjonalne huśtawki, prowadzące odbiorcę przez strach, złość i ratunek w postaci produktu lub usługi²⁶.

Reakcje na zagrożenia informacyjne: przykłady ingerencji w procesy demokratyczne

Jak wcześniej wskazano, UE przyjęła konkretne regulacje i inicjatywy dotyczące dezinformacji – Kodeks postępowania w sprawie zwalczania dezinformacji dla platform cyfrowych (Facebook, Google, X itp.), który był doskonalony w kolejnych latach wraz z wejściem w życie Rozporządzenia o przeciwdziałaniu FIMI (Foreign Information Manipulation and Interference, 2022) i ma na celu zmobilizowanie państw członkowskich i firm do efektywniejszej walki z zagraniczną propagandą²⁷ oraz tworzy unijny zestaw narzędzi do przeciwdziałania dezinformacji w internecie²⁸. Unijna strategia Europact for Democracy (DSA) zaleca też wzmocnienie mechanizmów reagowania na zagrożenia informacyjne, m.in. poprzez wymianę informacji między krajami oraz zespoły szybkiego reagowania, np. mechanizm G7 do szybkiego odrzucania rosyjskich kampanii dezinformacyjnych²⁹. Z kolei NATO rozwija mechanizmy wykrywania i odpierania takich działań, np. Centrum ds. Komunikacji Strategicznej StratCom COE czy ćwiczenia przeciwko operacjom hybrydowym³⁰. Opisanie inicjatywy NATO, UE i organizacji regionalnych stanowią reakcję na konkretne przypadki ingerencji informacyjnej w procesy demokratyczne, których symbolem stały się wydarzenia z 2016 roku, m.in. wybory prezydenckie w USA.

Wybory w USA z 2016 r. to jedna z najbardziej znanych spraw ingerencji informacyjnej w procesy demokratyczne. Raporty wywiadów USA jednoznacznie potwierdziły udział rosyjskich służb specjalnych w kampanii

²⁶ *Techniki manipulacji w świecie deepfake'ów...* (2025, 16 maja). Op. cit.

²⁷ *EEAS Report on Foreign Information Manipulation and Interference Threats* (2023, 7 lutego). The Diplomatic Service of the European Union. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en [dostęp: 03.04.2025].

²⁸ P. Zegarow (2022, 1 lipca). *Nowy Kodeks Postępowania w zakresie zwalczania dezinformacji*. Cyberpolicy. <https://cyberpolicy.nask.pl/nowy-kodeks-postepowania-w-zakresie-zwalczania-dezinformacji> [dostęp: 03.04.2025].

²⁹ *G7 Rapid Response Mechanism (RRM) statement on Russian Influence Campaign* (2025, 17 stycznia). The Diplomatic Service of the European Union. https://www.eeas.europa.eu/eeas/g7-rapid-response-mechanism-rrm-statement-russian-influence-campaign_en [dostęp: 03.04.2025].

³⁰ D.L. Byman i in. (2023). *Deepfakes and...* Op. cit.

prezydenckiej. Według amerykańskich instytucji, to właśnie ujawnienie skradzionych dokumentów z obozu Hillary Clinton (za pośrednictwem operacji cybernetycznych) przyczyniło się do jej porażki i sukcesu Donalda Trumpa³¹. Uważa się, że operacje te obejmowały zarówno ataki hakerskie, jak i rozległe kampanie dezinformacyjne w mediach społecznościowych. Śledztwa amerykańskie wskazały na zdynamizowanie rosyjskiej propagandy internetowej oraz koordynację działań dezinformacyjnych wymierzoną w wyborców³².

Wątpliwości co do ingerencji pojawiły się także w Rumunii. Podczas wyborów parlamentarnych w 2024 roku kandydat prorosyjski, Călin Georgescu, zyskał niespodziewanie duże poparcie, pomimo deklaracji zerowych wydatków na kampanię. Jego szybki wzrost popularności, osiągnięty dzięki zmasowanej kampanii w mediach społecznościowych prowadzonej przez zagraniczne firmy i sieć ochotników, wzbudził podejrzenia. Prezydent Klaus Iohannis ujawnił dowody na 85 tysięcy cyberataków na instytucje wyborcze, wskazując na prawdopodobną rosyjską ingerencję. Kampania Georgescu charakteryzowała się wykorzystaniem tysięcy fałszywych kont w mediach społecznościowych i rozbudowaną strategią dezinformacji. Utworzono także 41 pododdziałów kont, odpowiadających poszczególnym okręgom w Rumunii, aby budować lokalne struktury³³. Według Exolyt, narzędzia analizującego ruch na TikToku, liczba obserwujących Georgescu wzrosła o 2 541% w listopadzie. W odpowiedzi na te doniesienia Sąd Konstytucyjny Rumunii unieważnił pierwszą turę wyborów³⁴.

Działania informacyjne prowadzone przez Rosję stanowią kolejny przykład operacji informacyjnych. Poza kampaniami wyborczymi Rosja prowadziła rozległe operacje informacyjne w regionie Europy Środkowo-Wschodniej. Jak podaje Polskie Radio, w trakcie pełnoskalowej inwazji w 2022 r. kremlowska propaganda nagłaśniała różne teorie – m.in. o rzekomej budowie „biologicznego laboratorium USA na Ukrainie”. Organizacje

³¹ M.A. Piotrowski (2017, 23 stycznia). *Amerykańskie oceny dotyczące ingerencji Rosji w przebieg wyborów prezydenckich w USA*. Polski Instytut Spraw Międzynarodowych. https://www.pism.pl/publikacje/Ameryka_skie_oceny_dotycz_ce_ingerencji_Rosji_w_przebieg_wybor_w_prezydenckich_w_USA_ [dostęp: 03.04.2025].

³² *Parlament Wielkiej Brytanii: Rosja wtrącała się w referendum w Szkocji i ingerowała w Brexit* (2020, 21 lipca). CyberDefence24. <https://cyberdefence24.pl/polityka-i-prawo/parlament-wielkiej-brytanii-rosja-wtracala-sie-w-referendum-w-szkocji-i-ingerowala-w-brexit> [dostęp: 03.04.2025].

³³ *Raport PAP: Rosja ingeruje w wybory – od Rumunii po Hiszpanię* (2025, 30 kwietnia). Polska Agencja Prasowa. <https://www.pap.pl/aktualnosci/raport-pap-rosja-ingeruje-w-wybory-od-rumunii-po-hiszpanie-0> [dostęp: 01.05.2025].

³⁴ *Ibidem*.

fact-checkingowe (np. EUvsDisinfo) i NATO wielokrotnie rozprawiały się z tymi kłamstwami³⁵.

Choć najgłośniej w kontekście dezinformacji wymienia się Rosję, inne mocarstwa również stosują operacje informacyjne. Chiny koncentrują się przede wszystkim na promocji swoich narracji za granicą i tłumieniu krytyki w internecie, ale zdarzały się także przypadki wykorzystania zasobów do oddziaływań politycznych. Niedawno ujawnione badania opisały chińską sieć Spamouflage, która od co najmniej kilku lat generuje antyamerykańskie i prochińskie treści w mediach społecznościowych. Początkowo propaganda ta była ogólnikowo prorządowa, ale z czasem sieć zaczęła korzystać z podziałów społecznych USA – m.in. odtwarzała treści ekstremistyczne skrajnej prawicy i lewicy, prowadząc zdywersyfikowane konta podszywające się pod Amerykanów³⁶.

Wnioski

Analiza przeprowadzona w niniejszym opracowaniu potwierdza, że dezinformacja oraz wojna informacyjna stanowią dziś jedno z kluczowych wyzwań dla bezpieczeństwa międzynarodowego. Ich rola wykracza poza tradycyjne działania propagandowe – stają się one złożonymi, wielowarstwowymi procesami, wykorzystującymi zarówno nowoczesne technologie (w tym sztuczną inteligencję), jak i mechanizmy psychologiczne, socjotechniczne oraz kulturowe.

Współczesna przestrzeń informacyjna, zdominowana przez media społecznościowe i algorytmy personalizujące treści, tworzy warunki sprzyjające szybkiemu rozprzestrzenianiu się zmanipulowanych lub fałszywych informacji. Jak wskazano w analizie przypadków, zjawisko to ma charakter transnarodowy – przykłady ingerencji w wybory w Stanach Zjednoczonych, działania dezinformacyjne w Europie Środkowo-Wschodniej czy działalność sieci powiązanych z Chinami (Spamouflage) dowodzą, że dezinformacja jest stosowana jako narzędzie wpływu politycznego, osłabiania spójności społecznej i podważania zaufania do instytucji demokratycznych.

Szczególną uwagę należy zwrócić na rozwój narzędzi opartych na sztucznej inteligencji, takich jak generatywne modele językowe, *voice cloning* czy *deepfaki*. Ich zdolność do tworzenia realistycznych, lecz fałszywych treści audiowizualnych znacząco utrudnia weryfikację przekazów i może

³⁵ *Jak kraje bałtyckie walczą z rosyjską dezinformacją* (2024, 26 grudnia). Polskie Radio. <https://www.polskieradio.pl/399/11185/artykul/3463725,jak-kraje-baltyckie-walczą-z-rosyjska-dezinformacja> [dostęp: 15.04.2025].

³⁶ D. Klepper (2024, 3 września). *China-linked 'Spamouflage' network mimics Americans online to sway US political debate*. The Associated Press. <https://apnews.com/article/china-disinformation-network-foreign-influence-us-election-a2b-396518bafd8e36635a3796c8271d7> [dostęp: 15.04.2025].

prowadzić do poważnych konsekwencji w sytuacjach kryzysowych – zarówno militarnych, jak i społeczno-politycznych.

Pomimo aktywności organizacji międzynarodowych – w szczególności Unii Europejskiej, NATO czy wybranych państw członkowskich – w zakresie tworzenia narzędzi prawnych i instytucjonalnych do przeciwdziałania dezinformacji, istniejące instrumenty pozostają w wielu aspektach nieskoordynowane i niedostosowane do tempa rozwoju technologicznego. Brakuje globalnych regulacji o zasięgu obowiązującym (np. w ramach ONZ), a środki takie jak sankcje czy blokady informacyjne mają charakter reaktywny i ograniczony w skuteczności.

Wnioski z analizy wskazują również na rosnące znaczenie odporności społecznej jako elementu bezpieczeństwa państw. Kluczowe znaczenie zyskują tu działania w obszarze edukacji medialnej i informacyjnej, które zwiększają zdolność obywateli do identyfikowania manipulacji, rozpoznawania źródeł informacji oraz rozumienia mechanizmów wykorzystywanych w operacjach psychologicznych. Edukacja ta powinna być realizowana zarówno na poziomie szkolnym, jak i w ramach działań społecznych oraz instytucjonalnych (np. przez biblioteki, media publiczne, NGO).

Zintegrowane podejście do przeciwdziałania dezinformacji powinno łączyć cztery kluczowe komponenty:

1. Regulacje prawne – zarówno na poziomie krajowym, jak i międzynarodowym.
2. Inwestycje w technologię weryfikacji informacji – rozwój narzędzi *fact-checkingowych*, systemów wykrywania botów i treści syntetycznych.
3. Wzmocnienie odporności społecznej – poprzez systemowe działania edukacyjne.
4. Koordynacja międzynarodowa – wymiana informacji, szybkie reagowanie i wspólne mechanizmy prewencji.

W świetle powyższego, artykuł podkreśla, że dezinformacja i wojna informacyjna nie są zagrożeniami przejściowymi czy wyłącznie technologicznymi – to złożone zjawiska o charakterze strukturalnym, wymagające długofalowych i interdyscyplinarnych strategii przeciwdziałania.

Bibliografia

- Babraj R. (2020). *Dezinformacja w dobie cyfrowej rewolucji*. Cyberpolicy. <https://cyberpolicy.nask.pl/dezinformacja-w-dobie-cyfrowej-rewolucji> [dostęp: 01.04.2025].
- Bochyńska N. (2022, 19 marca). *Deepfake z Zełenskim. Czy fejkowe materiały wideo zmieniły przebieg wojen informacyjnych?* CyberDefence24. <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-deepfake-z-zelenskim-czy-fejkowe-materialy-wideo-zmienia-przebieg-wojen-informacyjnych> [dostęp: 16.04.2025].

- Byman D.L., Gao C., Meserole C., Subrahmanian V.S. (2023). *Deepfakes and international conflict*. The Brookings Institution. <https://www.brookings.edu/articles/deepfakes-and-international-conflict/> [dostęp: 01.03.2025].
- Czerski W. (2021). *Test Craap – przykład narzędzia do walki z dezinformacją*. https://www.researchgate.net/publication/366102266_Test_Craap_przyklad_narzedzia_do_walki_z_dezinformacja [dostęp: 01.04.2025].
- EEAS Report on Foreign Information Manipulation and Interference Threats (2023, 7 lutego). The Diplomatic Service of the European Union. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en [dostęp: 03.04.2025].
- Fake news – dezinformacja online próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski* (2020). Krajowa Rada Radiofonii i Telewizji. Wydawnictwo Krajowej Rady Radiofonii i Telewizji.
- Fraser M. (2021, 13 stycznia). *Sztuczna inteligencja w służbie propagandy. Jak jeszcze można wykorzystać modele językowe?* CyberDefence24. <https://cyberdefence24.pl/technologie/sztuczna-inteligencja-w-sluzbie-propagandy-jak-jeszcze-mozna-wykorzystac-modele-jezykowe> [dostęp: 15.04.2025].
- Hetmański M. (2003). *Społeczny charakter informacji*. Wydawnictwo Towarzystwo Naukowe KUL. Lublin.
- Ickiewicz-Sawicka M. (2025). *Propaganda i informacja – zarządzanie informacją w przestrzeni medialnej. Od klasycznych środków masowego przekazu do internetowych mediów społecznościowych*. https://wiz.pb.edu.pl/akademia-zarzadzania/wp-content/uploads/sites/3/2025/04/4.4.-Magdalena-Ickiewicz-Sawicka-Propaganda-i-dezinformacja---zarzadzanie-informacja-w-przestrzeni-medialnej_with_metadata.pdf [dostęp: 20.05.2025].
- Internet Security & Trust 2019. Part 3: Social Media, Fake News & Algorithms* (2019). Centre for International Governance Innovation. <https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%203%20Social%20Media%2C%20Fake%20News%20%26%20Algorithms.pdf> [dostęp: 30.09.2025].
- Jak kraje bałtyckie walczą z rosyjską dezinformacją* (2024, 26 grudnia). Polskie Radio. <https://www.polskieradio.pl/399/11185/artykul/3463725,jak-kraje-baltyckie-walczą-z-rosyjska-dezinformacja> [dostęp: 15.04.2025].
- Jemielniak D. (2013). *Życie wirtualne dzikich*. Wydawnictwo Poltext. Warszawa.
- Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, Dz.U. 1947 nr 23 poz. 90.
- Klepper D. (2024, 3 września). *China-linked 'Spamouflage' network mimics Americans online to sway US political debate*. The Associated Press. <https://apnews.com/article/china-disinformation-network-foreign-influence-us-election-a2b396518bafd8e36635a3796c8271d7> [dostęp: 15.04.2025].
- Kodeks postępowania w zakresie zwalczania dezinformacji*. Unia Europejska. <https://digital-strategy.ec.europa.eu/pl/library/code-conduct-disinformation> [dostęp: 01.04.2025].

- Media and information literacy is first line of defence against disinformation* (2020, 28 października). UNESCO. <https://www.unesco.org/en/articles/media-and-information-literacy-first-line-defence-against-disinformation> [dostęp: 18.04.2025].
- Mueller R. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. U.S. Department of Justice. <https://www.justice.gov/archives/sco/file/1373816/dl> [dostęp: 03.03.2025].
- Parlament Wielkiej Brytanii: Rosja wtrącała się w referendum w Szkocji i ingerowała w Brexit* (2020, 21 lipca). CyberDefence24. <https://cyberdefence24.pl/polityka-i-prawo/parlament-wielkiej-brytanii-rosja-wtracala-sie-w-referendum-w-szkocji-i-ingerowala-w-brexit> [dostęp: 03.04.2025].
- Pięta K. (2024). *Dezinformacja jako narzędzie manipulacji w sieci*. ResearchGate. https://www.researchgate.net/publication/385909650_Disinformation_as_a_tool_of_manipulation_on_the_Internet [dostęp: 03.03.2025].
- Piotrowski M.A (2017, 23 stycznia). *Amerykańskie oceny dotyczące ingerencji Rosji w przebieg wyborów prezydenckich w USA*. Polski Instytut Spraw Międzynarodowych. https://www.pism.pl/publikacje/Ameryka_skie_oceny_dotycz_ce_ingerencji_Rosji_w_przebieg_wybor_w_prezydenckich_w_USA_ [dostęp: 03.04.2025].
- Raport PAP: Rosja ingeruje w wybory – od Rumunii po Hiszpanię* (2025, 30 kwietnia). Polska Agencja Prasowa. <https://www.pap.pl/aktualnosci/raport-pap-rosja-ingeruje-w-wybory-od-rumunii-po-hiszpanie-0> [dostęp: 01.05.2025].
- Sztuczna inteligencja. Modele AI generują rosyjską i chińską dezinformację* (2025, 7 lutego). CyberDefence24. <https://cyberdefence24.pl/technologie/sztuczna-inteligencja-modele-ai-generuja-rosyjska-i-chinska-dezinformacje> [dostęp: 16.04.2025].
- Świerczek M. (2018). „System matrioszek”, czyli dezinformacja doskonała. „Przegląd Bezpieczeństwa Wewnętrznego”, 19.
- Techniki manipulacji w świecie deepfake’ów – jak sztuczna inteligencja zmienia oblicze dezinformacji* (2025, 16 maja). Portal Gov.pl. <https://www.gov.pl/web/ai/techniki-manipulacji-w-swiecie-deepfakeow---jak-sztuczna-inteligencja-zmienia-oblicze-dezinformacji> [dostęp: 15.04.2025].
- Wspólny komunikat do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-społecznego i Komitetu regionów (2018). Plan działania na rzecz zwalczania dezinformacji <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52018JC0036> [dostęp: 01.04.2025].
- Zegarow P. (2022, 1 lipca). *Nowy Kodeks Postępowania w zakresie zwalczania dezinformacji*. Cyberpolicy. <https://cyberpolicy.nask.pl/nowy-kodeks-postepowania-w-zakresie-zwalczania-dezinformacji/> [dostęp: 03.04.2025].

Abstrakt

W erze globalnej cyfryzacji i nieograniczonego dostępu do informacji, wojna informacyjna oraz dezinformacja stały się istotnymi narzędziami walki o wpływy polityczne oraz destabilizację państw. Celem artykułu jest analiza mechanizmów i metod stosowanych w operacjach dezinformacyjnych oraz ich wpływu na bezpieczeństwo międzynarodowe. Omówiono zarówno przykłady historyczne, jak i współczesne – w tym ingerencje w procesy demokratyczne, manipulację opinią publiczną oraz wykorzystanie technologii sztucznej inteligencji w kampaniach dezinformacyjnych. Szczególną uwagę poświęcono strategiom obronnym podejmowanym przez państwa

i organizacje międzynarodowe w celu minimalizacji skutków wojny informacyjnej. Artykuł ma charakter teoretyczno-przeglądowy i opiera się na jakościowej analizie treści dostępnej literatury naukowej, raportów instytucji międzynarodowych oraz źródeł eksperckich.

Disinformation and Information Warfare as a Threat to International Security

Abstract

In the era of global digitalization and unlimited access to information, information warfare and disinformation have become important tools in the struggle for political influence and the destabilization of states. The aim of this article is to analyze the mechanisms and methods used in disinformation operations and their impact on international security. Both historical and contemporary examples are discussed—including interference in democratic processes, manipulation of public opinion, and the use of artificial intelligence technologies in disinformation campaigns. Particular attention is given to the defensive strategies adopted by states and international organizations to minimize the effects of information warfare. The article has a theoretical and review-based character and is based on a qualitative content analysis of available academic literature, reports of international institutions and expert sources.

Słowa kluczowe: dezinformacja, wojna informacyjna, bezpieczeństwo międzynarodowe, sztuczna inteligencja, deepfake

Keywords: disinformation, information warfare, international security, artificial Intelligence, deepfake

Weronika Ratajczak – studentka prawa oraz absolwentka kryminologii Wyższej Szkoły Biznesu i Nauk o Zdrowiu w Łodzi. Interesuje się tematyką prawa karnego, kryminalistyką oraz psychologią przestępczości, które zgłębia zarówno od strony teoretycznej, jak i praktycznej. Specjalizuje się w analizie prawnej oraz praktycznych aspektach stosowania prawa w odniesieniu do zjawisk przestępczych.