ARTYKUŁY

„Polityka i Społeczeństwo” 1(23) / 2025
DOI: 10.15584/polispol.2025.1.19

Agnieszka Warchoł*

WPŁYW PODMIOTÓW ZEWNĘTRZNYCH W CYBERPRZESTRZENI NA BEZPIECZEŃSTWO PROCESU WYBORCZEGO W PAŃSTWIE

Streszczenie

Celem niniejszego artykułu jest przedstawienie wpływu podmiotów zewnętrznych względem państwa na bezpieczeństwo procesu wyborczego. Główna teza publikacji zawiera się w stwierdzeniu, że współcześnie, za sprawą cyberprzestrzeni, podmioty zewnętrzne zintensyfikowały działania w zakresie wpływu na proces wyborczy podmiotu państwowego. W pracy zastosowane zostały takie metody badawcze, jak: analiza i krytyka źródeł, analiza i krytyka piśmiennictwa, metoda porównawcza, studium przypadku. Cyberprzestrzeń odgrywa kluczową rolę w procesie wyborczym, a w obliczu transnarodowych zagrożeń konieczne jest podnoszenie świadomości społeczeństwa w tym zakresie, dbałość o cyberbezpieczeństwo państwa, ale także niezbędna jest odpowiednia współpraca międzynarodowa, np. wymiana informacji, wspólne ćwiczenia i koordynacja działań. Zapewnienie bezpieczeństwa procesu wyborczego wymaga kompleksowego podejścia, które obejmuje zarówno aspekty techniczno-technologiczne, prawne, instytucjonalne, jak i społeczne.

Słowa kluczowe: cyberprzestrzeń, wybory, państwo, bezpieczeństwo

Wstęp

Rok 2024 określany jest mianem roku wyborczego za sprawą rekordowej liczby państw, w których zaplanowano wybory. Instytut V-Dem w raporcie pt. *Domocracy Report 2024. Democracy Winning and Losing at the Ballot* podaje, że obejmuje to aż 60 państw, w tym tych najbardziej zaludnionych, jak: Rosja, Indie, Bangladesz, Stany Zjednoczone Ameryki, Indonezja, Meksyk czy Pakistan, co sprawia, że do wyborów w tym roku miała się udać blisko połowa światowej populacji[1].

* Uniwersytet Komisji Edukacji Narodowej w Krakowie, e-mail: agnieszka.kura @up.krakow.pl, ORCID: 0000-0003-0786-6440.

[1] *Democracy Report 2024. Democracy Winning and Losing at the Ballot*, s. 40–41, V-Dem Institute, https://www.v-dem.net (15.06.2024).

Wybory to proces, na który składa się wiele działań i procedur zmierzających do wyłonienia spośród kandydatów przedstawicieli danej wspólnoty. Wybory są aktem politycznym, kreującym politykę państwa i wyłaniającym osoby odpowiedzialne za jej prowadzenie[2]. Według Ryszarda Herbuta, wybory są „formą zbiorowej decyzji podjętej przez określoną wspólnotę polityczną"[3]. Wraz z pojawieniem się kolejnej płaszczyzny funkcjonowania państwa, jaką jest cyberprzestrzeń, oraz powszechną informatyzacją życia społecznego, wzrasta ryzyko zewnętrznej ingerencji w poszczególne etapy procesu wyborczego. To do cyberprzestrzeni przenosi się życie społeczne, a granica między światem realnym a wirtualnym ulega zatarciu. Internet, jako główny komponent cyberprzestrzeni, stał się nieodłącznym elementem funkcjonowania większości ludzi na świecie. Z danych opublikowanych na platformie Statista, w kwietniu 2024 roku z Internetu korzystało 67% światowej populacji[4].

Zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, cyberprzestrzeń to „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3[5] ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami"[6]. Cyberprzestrzeń, z uwagi na swoją specyfikę, jest atrakcyjną płaszczyzną działalności różnego rodzaju podmiotów zarówno z sektora publicznego, jak i prywatnego. Zdaniem Mirona Lakomego, ujęcie podmiotowe zagrożeń w cyberprzestrzeni powinno uwzględniać przede wszystkim te podmioty, które dążąc do realizacji partykularnych interesów, dopuszczają się szkodliwej aktywności względem państwa, korzystając przy

[2] *Leksykon politologii*, red. A. Antoszewski, R. Herbut, Wrocław 2004, s. 499.

[3] *Ibidem.*

[4] *Number of internet and social media users worldwide as of April 2024*, Statista, https://www.statista.com (15.05.2024).

[5] System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2024, poz. 34). Zob. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, art. 3, pkt 3 (Dz.U. 2005, nr 64, poz. 565).

[6] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2017, poz. 1932).

tym z przestrzeni teleinformatycznej[7]. Można zatem wyróżnić zarówno podmioty indywidualne, jak np. haker, kraker, haktywista, szpieg, amator, terrorysta – w zależności od motywu, który kieruje ich działaniem, oraz organizacje, m.in.: inne państwa, organizacje terrorystyczne, korporacje, organizacje przestępcze, ruchy społeczne. Ich motywacje do działania na szkodę państwa w cyberprzestrzeni mogą mieć charakter: polityczny, wojskowy, religijny, gospodarczy, społeczny czy indywidualny (jak np. rozwój umiejętności czy rozrywka)[8].

Celem niniejszego artykułu jest przedstawienie wpływu podmiotów zewnętrznych względem państwa na bezpieczeństwo procesu wyborczego. Główna teza publikacji zawiera się w stwierdzeniu, że współcześnie, za sprawą cyberprzestrzeni, podmioty zewnętrzne zintensyfikowały działania w zakresie wpływu na proces wyborczy podmiotu państwowego. W ramach szczegółowych rozważań podjęta została próba udzielenia odpowiedzi na następujące pytania badawcze: Jaka jest rola cyberprzestrzeni w procesie wyborczym? Jakie techniki wykorzystują podmioty zewnętrzne do ingerencji w proces wyborczy danego państwa? Czy giganci technologiczni mogą mieć wpływ na wynik wyborów w poszczególnych państwach? W jaki sposób zewnętrzni aktorzy mogą wpływać na wynik wyborów w państwie, w którym możliwe jest głosowanie przez Internet? Aby udzielić odpowiedzi na postawione pytania, zastosowane zostały takie metody badawcze, jak: analiza i krytyka źródeł i piśmiennictwa, metoda porównawcza, studium przypadku. W przygotowaniu niniejszej pracy przydatne okazały się raporty, np. *Democracy Report 2024. Democracy Winning and Losing at the Ballot* i *How foreign actors targeted Polish information environment ahead of parliamentary election*, stenogramy z nagrań i sprawozdania z prac organów wybranych państw, a także akty prawne oraz literatura przedmiotu.

Obca ingerencja

17 sierpnia 2023 roku Sejm Rzeczypospolitej Polskiej podczas 81. posiedzenia podjął uchwałę w sprawie obcej ingerencji w proces wyborczy w Polsce[9]. „Rzeczpospolita Polska wszelką obcą ingerencję w polski

[7] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 82.

[8] A. Warchoł, *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku*, Kraków 2017, s. 69.

[9] W tym wypadku ważny jest kontekst polityczny. Tekst uchwały powstał w celu potępienia słów krytyki względem Prawa i Sprawiedliwości ze strony polityków niemieckich, w tym wymienionego w uchwale Manfreda Webera.

proces wyborczy uznaje za akt wrogi wobec państwa polskiego i będzie ją zdecydowanie zwalczać"[10] – głosi ostatnie zdanie uchwały. Zewnętrzna ingerencja w wybory była już wielokrotnie odnotowywana w wielu państwach świata. Zazwyczaj przejawia się ona w takich działaniach, jak np.: ataki na infrastrukturę wyborczą, kampanie dezinformacyjne, finansowanie kampanii wyborczych, wycieki danych i informacji newralgicznych z punktu widzenia państwa, manipulacja – zarówno w świecie realnym, jak i wirtualnym, np. z wykorzystaniem mediów społecznościowych.

W październiku 2023 roku amerykański wywiad przesłał do ponad 100 ambasad USA na różnych kontynentach świata informacje, z których wynika, że Federacja Rosyjska wykorzystuje szpiegów, media społecznościowe oraz rosyjskie media państwowe do podważania zaufania w uczciwość wyborów i legitymizację nowo wybranych demokratycznych władz poszczególnych państw[11]. Ma to na celu wywołanie chaosu i destabilizacji w państwach demokratycznych oraz poczucia strachu ze strony społeczeństwa i niechęci w stosunku do władz państwowych. Podobne dane, dotyczące wpływu Rosji na procesy polityczne w kraju, zostały upublicznione także w Wielkiej Brytanii w 2020 roku w raporcie parlamentarnej komisji do spraw wywiadu i bezpieczeństwa dotyczącym zagrożeń ze strony Rosji, w tym cyberzagrożeń i dezinformacji[12].

Najczęściej przywoływanym w literaturze przedmiotu przykładem zewnętrznej ingerencji w proces wyborczy za pośrednictwem cyberprzestrzeni, a dokładnie mediów społecznościowych, są wybory prezydenckie w 2016 roku w Stanach Zjednoczonych Ameryki, w których ogromną rolę odegrała firma Cambridge Analytica[13]. Przedsiębiorstwo zgromadziło ogromną ilość danych (m.in. z Facebooka, obecnie – Meta), na podstawie których zidentyfikowało osoby szybko wpadające w złość i mające tendencje do myślenia spiskowego[14]. Następnie za pośrednictwem platformy były im podsuwane spreparowane profile, teksty, grupy i spersonalizowane reklamy, które miały na celu prowokować do okre-

[10] Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 17 sierpnia 2023 r. w sprawie obcej ingerencji w proces wyborczy w Polsce (M.P. 2023, poz. 893).

[11] J. Landay, S. Lewis, *US intelligence report alleging Russia election interference shared with 100 countries*, Reuters, https://www.reuters.com (12.05.2024).

[12] *Russia*, Intelligence and Security Committee of Parliament, https://isc.independent.gov.uk (16.05.2024).

[13] A. Warchoł, *Ochrona praw i wolności człowieka w dobie Internetu* [w:] *Cyberprzestrzeń jako pole zmagań o bezpieczeństwo informacyjne*, red. W. Fehler, Siedlce 2022, s. 180–181.

[14] R. Foroohar, *Nie czyń zła. Jak Big Tech zdradził swoje ideały i nas wszystkich,* Warszawa 2020, s. 209.

ślonych zachowań oraz wywoływać emocjonalne zaangażowanie[15]. Przełożyło się to na wynik wyborów prezydenckich w Stanach Zjednoczonych i wybór Donalda Trumpa na urząd Prezydenta USA, a także na wyniki referendum w sprawie Brexitu w Wielkiej Brytanii[16].

Z początkiem 2023 roku zostały ujawnione działania izraelskiej grupy, tzw. *Team Jorge,* która miała ingerować w 33 kampanie wyborcze, z czego – według *Team Jorge* – 27 zakończyło się sukcesem dla jej zleceniodawców[17]. Narzędzia, z jakich korzystała grupa, to m.in. oprogramowanie umożliwiające zarządzanie fałszywymi profilami w mediach społecznościowych, rozpowszechnianie dezinformacji oraz wpływ na opinię publiczną, cyberataki na przeciwników politycznych swoich klientów, a także współpraca z innymi podmiotami zajmującymi się manipulacjami wyborczymi, np. ww. Cambridge Analytica. W 2015 roku obie firmy współpracowały przy próbie wpłynięcia na wybory w Nigerii[18].

Zakłócenie przeprowadzenia demokratycznych wyborów za pośrednictwem cyberprzestrzeni, w świetle prawa międzynarodowego, może być uznane za cyberoperację negatywnie wpływającą na funkcjonowanie i bezpieczeństwo systemu politycznego, gospodarczego, wojskowego lub społecznego danego państwa[19]. Współcześnie państwa samodzielnie decydują o kwalifikacji cyberoperacji jako ewentualnie naruszającej wskazaną przez nie normę prawa międzynarodowego[20]. Jak przypomniano w *Stanowisku Rzeczypospolitej Polskiej dotyczącym zastosowania prawa międzynarodowego w cyberprzestrzeni*, „istniejące prawo międzynarodowe, w tym *Karta Narodów Zjednoczonych*, stosuje się do cyberprzestrzeni. Tym samym państwa są zobowiązane do przestrzegania prawa międzynarodowego w cyberprzestrzeni"[21].

Z uwagi na specyfikę cyberprzestrzeni wysoce problematyczne jest przypisanie odpowiedzialności za daną cyberoperację konkretnemu

[15] A. Warchoł, *Wolność opinii w cyberprzestrzeni* [w:] *10 lat nauk o bezpieczeństwie. Potencjał, problematyka, perspektywy*, red. A. Polończyk, P. Swoboda, Kraków 2021, s. 641–642.

[16] C. Cadwalladr, *The great British Brexit robbery: how our democracy was hijacked*, The Guardian, https://www.theguardian.com (15.05.2024).

[17] S. Kirchgaessner, *How undercover reporters caught 'Team Jorge' disinformation operatives on camera*, The Guardian, https://www.theguardian.com (17.02.2025).

[18] S. Kirchgaessner [i in.], *Revealed: the hacking and disinformation team meddling in elections*, The Guardian, https://www.theguardian.com (17.02.2025).

[19] *Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni, Ministerstwo Spraw Zagranicznych*, Gov.pl, https://www.gov.pl (15.05.2024).

[20] J. Kulesza, *O wojnie w cyberprzestrzeni Polska zadecyduje sama*, Uniwersytet Łódzki, https://www.uni.lodz.pl (12.05.2024).

[21] *Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego…*

podmiotowi państwowemu. W świetle prawa międzynarodowego nie każdy cyberatak to atak[22], stąd należy unikać zbyt częstego posługiwania się tym terminem w odniesieniu do incydentów cyberbezpieczeństwa, a po drugie – proces atrybucji jest skomplikowany i wieloetapowy[23]. Dodatkowo szczególnie problematyczne jest wykazanie powiązania między atakującym podmiotem a władzami państwa[24], gdyż w prosty sposób można zaprzeczyć, że dana cyberoperacja odbywała się za wiedzą, akceptacją czy na zlecenie władz państwowych. Ponadto, z uwagi na potencjalne konsekwencje, państwa unikają obarczania odpowiedzialnością za cyberoperacje innych aktorów państwowych, gdyż tego typu wskazanie winowajcy wymaga podjęcia określonych działań o charakterze politycznym, np. na szczeblu dyplomatycznym[25]. W ostatnim czasie miały miejsce dwie sytuacje, które niektórzy eksperci nazywają mianem bezprecedensowych[26]. Na początku maja 2024 r. Niemcy wezwały swojego ambasadora w Rosji Otto Grafa Lambsdorffa na konsultacje w Berlinie w związku z cyberatakami na niemiecką partię polityczną oraz niemieckie firmy z branży logistycznej, zbrojeniowej, lotniczej, usług IT, a także fundacje i stowarzyszenia, za które odpowiedzialnością obarczono rosyjskie instytucje państwowe[27]. W oficjalnym komunikacie niemieckiego rządu odpowiedzialność za cyberoperacje przypisano grupie APT28, którą powiązano z rosyjskim wywiadem wojskowym[28]. Druga sytuacja dotyczy wezwania przez czeski rząd ambasadora Rosji Alexandra Zmejevskiego w związku z rosyjskimi atakami w cyberprzestrzeni na czeskie instytucje i infrastrukturę krytyczną[29]. W tym przypadku również doszło do bezpośredniego powiązania APT28 z rosyjskim wywiadem wojskowym GRU[30].

---

[22] Ł. Olejnik, A. Kurasiński, *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Warszawa 2022, s. 153.

[23] N. Tsagourias, M. Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, „European Journal of International Law", 2020, vol. 31, iss. 3, s. 942.

[24] A.E. Levite [i in.], *Managing U.S.-China Tensions Over Public Cyber Attribution*, s. 9, Carnegie Endowment for International Peace, https://carnegie-production-assets.s3.amazonaws.com (12.06.2024).

[25] *Ibidem.*

[26] Zob. Ł. Olejnik, *X, X.com*, https://x.com (12.06.2024).

[27] *Ambasador Niemiec opuścił Rosję. MSZ wezwało go na konsultacje*, Rzeczpospolita, https://www.rp.pl (12.06.2024).

[28] *Zurechnung der russischen Cyber-Kampagne*, Deutsche Vertretungen in Russland, https://germania.diplo.de (12.06.2024).

[29] *Lipavský si předvolal ruského velvyslance*, Novinky, https://www.novinky.cz (17.06.2024).

[30] *Prohlášení MZV ke kyberútokům ruského aktéra APT28 na Česko*, Ministry of Foreign Affairs of the Czech Republic, https://mzv.gov.cz (12.06.2024).

Sposoby zewnętrznej ingerencji

Według danych z raportu pt. *How foreign actors targeted Polish information environment ahead of parliamentary elections*, przygotowanego przez Alliance4Europe, OKO.press i ośrodek DFRLab, przed wyborami parlamentarnymi w Polsce, które odbyły się 15 października 2023 roku, zagraniczni aktorzy próbowali wpłynąć na proces wyborczy[31]. Autorzy raportu wymieniają podmioty rosyjskie i białoruskie, które, wykorzystując różne techniki ataków, dążyły do wywołania podziałów społecznych oraz podważenia zaufania do instytucji publicznych w Polsce[32]. Raport posługuje się definicjami oraz przywołuje ramy ingerencji w wybory opublikowane w raporcie z 2018 roku przez *think tank* Atlantic Council of United States, w którym wyróżniono kilka rodzajów działań zakłócających zaobserwowanych w latach 2014–2018, mających bezpośredni związek z ingerencją w wybory. Są to: zakłócenia infrastruktury, manipulacja głosami, upublicznianie danych uzyskanych nielegalnie (tzw. publikacje strategiczne), wykorzystywanie fałszywej tożsamości do wzmacniania zaangażowania użytkowników, wzmacnianie nastrojów, fabrykowanie treści[33]. W Polsce działania na rzecz zabezpieczenia i ochrony infrastruktury Państwowej Komisji Wyborczej i Krajowego Biura Wyborczego przed ingerencją z zewnątrz prowadzi Agencja Bezpieczeństwa Wewnętrznego (dalej: ABW)[34]. W tym zakresie ABW współpracuje z Ministerstwem Cyfryzacji w ramach krajowego systemu cyberbezpieczeństwa[35].

Jednym ze sposobów zakłócenia infrastruktury wyborczej są cyberataki. W 2023 roku opinia publiczna dowiedziała się, że w wyniku cyberataku na Brytyjską Komisję Wyborczą, który został zidentyfikowany w 2022 roku, zewnętrzne podmioty uzyskały dostęp do danych 40 milionów wyborców w Wielkiej Brytanii, zarejestrowanych w latach 2014–2022[36]. W marcu 2024 roku Oliver Dowden wskazał, że podmioty powiązane z Chinami były odpowiedzialne za dwie cyberkampanie wymie-

[31] G. Gigitashvili, *How foreign actors targeted Polish information environment ahead of parliamentary elections*, DFRLab, https://dfrlab.org (15.06.2024).

[32] *Ibidem.*

[33] L. Galante, S. Ee, *Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents*, Atlantic Council, https://www.atlanticcouncil.org (12.05.2024).

[34] *Odpowiedź na interpelację nr 42611 w sprawie cyberzabezpieczenia wyborów parlamentarnych w Polsce w 2023 r.*, Sejm, https://www.sejm.gov.pl (16.05.2024).

[35] *Ibidem.*

[36] R. Mason, H. Farah, *Electoral Commission apologises for security breach involving UK voters' data*, The Guardian, https://www.theguardian.com (15.05.2024).

rzone w brytyjskie instytucje, w tym Brytyjską Komisję Wyborczą w latach 2021–2022[37].

Innym sposobem uzyskania wpływu są ukierunkowane ataki *phishingowe*, jak np. w 2016 roku na skrzynki pocztowe osób ze sztabu wyborczego Hillary Clinton, w tym na szefa jej kampanii wyborczej. Kradzież danych, a następnie utworzenie wielu kanałów dystrybucji wykradzionych informacji, które posłużyły do kampanii dezinformacyjnych, spowodowały niespotykane dotąd straty wizerunkowe Partii Demokratycznej i chaos wśród amerykańskiego społeczeństwa, co mogło przesądzić o wyniku wyborów korzystnym dla kontrkandydata Clinton – Donalda Trumpa [38].

Podobna sytuacja miała miejsce w 2021 roku w Polsce, kiedy zhakowana została skrzynka pocztowa Michała Dworczyka, ówczesnego ministra w rządzie Mateusza Morawieckiego. Według danych z raportów Mandiant i Google, kampanię *Ghostwriter*/UNC1151 z dużym prawdopodobieństwem można powiązać z rządem Białorusi. CERT Polska poinformował, że jedną z metod ataku UNC1151 był właśnie *phishing*, co miało na celu wyłudzenie danych do logowania do skrzynek pocztowych[39]. Następnie przejęte skrzynki były penetrowane z zamiarem uzyskania dostępu do wrażliwych danych[40]. Działania te, prowadzone w sferze informacyjnej, obok kryzysu migracyjnego na granicy polsko-białoruskiej, wpisują się w katalog działań wojny hybrydowej prowadzonych przez Mińsk i Moskwę przeciwko Polsce i innym państwom UE i NATO.

Czy giganci technologiczni, czyli największe światowe korporacje medialno-technologiczne, mogą mieć wpływ na wynik wyborów w poszczególnych państwach? – to pytanie, które bardzo często pojawia się w debacie publicznej, zwłaszcza po skandalu Cambridge Analytici, wspomnianym już we wcześniejszych fragmentach tekstu. Blokowanie kont polityków przed wyborami czy wykorzystanie algorytmów, które promują charyzmatycznych i zarazem kontrowersyjnych kandydatów – to działania, które w XXI wieku wpisują się w walkę wyborczą. Dodatkowo coraz częściej wykorzystywane narzędzia AI mogą pomóc kandydatom

[37] *House of Commons Official Report Parliamentary Debates*, Hansard, https://hansard.parliament.uk (16.05.2024).

[38] *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, NASK, https://cyberprofilaktyka.pl (16.05.2024); A. Haertle, *Jak Rosjanie hakowali amerykańskie wybory – krok po kroku*, Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl (16.06.2024).

[39] *Rozwój technik ataku grupy UNC1151/Ghostwriter*, CERT Polska, https://cert.pl (17.06.2024).

[40] *Ibidem.*

dotrzeć do szerokiego grona odbiorców, czyli potencjalnych wyborców. W 2020 roku Manoj Tiwari, polityk z Indii, wykorzystał sztuczną inteligencję, a konkretnie technologię *deep fake* do przetłumaczenia swojego przemówienia na dwadzieścia różnych lokalnych języków używanych w Indiach, aby dotrzeć do większej liczby wyborców. *Deepfake* Tiwariego dotarł do około 15 milionów osób w 5800 grupach WhatsApp[41]. Był to prawdopodobnie pierwszy przypadek wykorzystania technologii *deep fake* w kampanii wyborczej. Obecnie przykład wyborów w 2023 roku w Słowacji pokazuje[42], że *deep fakes* może mieć coraz większy wpływ na procesy polityczne, w tym wyborcze. Oznacza to, że o tym, ile i w jaki sposób fałszywe treści będą rozprzestrzeniane i będą mogły trafić do szerokiego grona odbiorców, decydują platformy internetowe. To one kształtują swoje polityki, regulaminy, na które nie mają wpływu podmioty z sektora publicznego. W związku z tym są to podmioty mające ogromny wpływ na kształtowanie rzeczywistości politycznej, m.in. poprzez kształtowanie preferencji wyborczych za pośrednictwem mediów społecznościowych, co z kolei przekłada się na kształt nowo wybranych władz w poszczególnych państwach czy skład organów w regionalnych instytucjach, jak np. w Parlamencie Europejskim. To z kolei ma wpływ na politykę tych organów względem gigantów technologicznych.

Cyfryzacja wyborów

Co kilka lat w Polsce wracają pomysły wprowadzenia powszechnego głosowania w wyborach przez Internet. Jak pisze Magdalena Musiał-Karg, „głosowanie przez Internet jest jedną z form głosowania elektronicznego, które jako jedno z tzw. alternatywnych sposobów głosowania należy do narzędzi demokracji elektronicznej”[43]. Demokracja

[41] C. Jee, *An Indian politician is using deepfake technology to win new voters*, Technology Review, https://www.technologyreview.com (16.04.2024).

[42] Fragment dotyczy rozmowy Michala Šimečki, lidera liberalnej partii Postępowa Słowacja, oraz Moniki Tódovej z dziennika Denník N. na temat manipulowania wyborami, m.in. poprzez kupowanie głosów od nielicznej mniejszości Romów w kraju. Zainteresowani zaprzeczyli prawdziwości nagrania. Dodatkowo, post był dźwiękowy, co sprawiło, że wykorzystano lukę w polityce firmy Meta, która dotyczy manipulacji mediami. Zgodnie z polityką firmy, niezgodne z jej zasadami są wyłącznie fałszowane filmy, a nie nagrania głosowe. Zob. K. Maciejewski, *AI wpłynęła na wynik wyborów w Słowacji? Polska szczególnie narażona na dezinformację*, Forsal, https://forsal.pl (16.06.2024).

[43] M. Musiał-Karg, *Głosowanie przez Internet. Skąd czerpać wzorce i jak wprowadzać innowacje wyborcze?*, Fundacja im. Stefana Batorego, https://www.batory.org.pl (16.06.2024).

elektroniczna łączy, z jednej strony, problematykę partycypacji politycznej, a z drugiej – nowoczesne technologie i ich wpływ na ustrój demokratyczny[44]. Głosowanie internetowe może przybierać dwie formy. Pierwsza odnosi się do głosowania w lokalu wyborczym przy wykorzystaniu tzw. *voting machines*, natomiast druga – do głosowania zdalnego, z dowolnego miejsca[45].

W pierwszych miesiącach 2024 roku w polskich mediach pojawiły się informacje, że w Kancelarii Prezesa Rady Ministrów takie scenariusze są rozważane, na początku w formie pilotażowej i wyłącznie w odniesieniu do głosującej Polonii w wyborach prezydenckich[46]. Co jakiś czas temat wraca, zazwyczaj w czasie kampanii wyborczej, i jest propozycją kandydatów w wyborach, albo przy okazji nadchodzących wyborów, będąc jednym z proponowanych rozwiązań na podniesienie frekwencji wyborczej, co jednak jest argumentem kontrowersyjnym. W Estonii *i-voting* funkcjonuje od 2005 roku. Wraz z każdymi następnymi wyborami liczba głosujących przez Internet rośnie. W marcu 2023 roku w wyborach parlamentarnych aż 51% głosów oddano *online*, co oznacza, że po raz pierwszy w historii więcej głosów oddano przez Internet niż tradycyjnie[47]. Jednak wprowadzenie głosowania elektronicznego nie przyczyniło się w Estonii do zwiększenia frekwencji wyborczej[48]. Oprócz argumentów związanych ze zwiększeniem frekwencji wyborczej, wśród potencjalnych zalet głosowania przez Internet z dowolnego miejsca, zwolennicy wymieniają zazwyczaj wygodę, oszczędność czasu, szybkość i dokładność liczenia wyników[49], ograniczenie błędów i poprawę integralności procesu wyborczego, a także kwestie bezpieczeństwa sanitarnego – ten argument pojawiał się najczęściej w okresie pandemii COVID-19[50].

---

[44] M. Hagen, *A typology of Electronic Democracy*, Martin Hagen, http://www.martin-hagen.net (16.06.2024).

[45] *Introducing Electronic Voting: Essential Considerations*, Idea, https://www.idea.int (17.06.2024).

[46] *Ta grupa wyborców ma głosować przez internet. Sprawdzianem wybory prezydenckie*, Rzeczpospolita, https://www.rp.pl (16.06.2024).

[47] *How did Estonia carry out the world's first mostly online national elections*, e-stonia.com, https://e-estonia.com (16.06.2024).

[48] Dla przykładu, w wyborach parlamentarnych w Estonii w 2005 roku frekwencja wyniosła 64,23%, w 2019 roku – 63,67% a w 2023 – 63,53%. Zob. Election Guide, https://www.electionguide.org (15.06.2024).

[49] M. Musiał-Karg, *op.cit.*

[50] M. Lisi, C. Luis, *(Un)ready for change? The debate about electronic voting in Portugal and its implementation before and after the pandemic era*, Frotiersin, https://www.frontiersin.org (17.06.2024); E. Sfîrnaciuc, M.-E. Vasilescu, E. Simion, *E-voting*

Przeciwnicy wprowadzenia takich rozwiązań wskazują, że głosowanie internetowe może doprowadzić do oszustw wyborczych[51]. Dodatkowo mogą występować problemy z infrastrukturą, np. jej obciążenie[52], problemy z mechanizmem weryfikacji (na co wskazuje się też w przypadku Estonii[53]), szyfrowaniem czy neutralnością sprzętu. Oprócz problemów związanych ze sprzętem, cyberatakami czy oszustwami wyborczymi występuje jeszcze obowiązek zapewnienia ochrony prywatności wyborców, co przejawia się w fundamentalnej zasadzie prawa wyborczego, jaką jest zasada tajności głosowania. Oznacza ona „zagwarantowanie każdemu wyborcy, że treść jego decyzji wyborczej nie będzie mogła być ustalona i ujawniona. Każdy wyborca musi oddawać głos w takich warunkach technicznych i politycznych, które wykluczając możliwość takiego ustalenia, stwarzają mu nieskrępowane możliwości dokonania wyboru"[54]. Tajność głosowania, zgodnie z Kodeksem wyborczym, zapewnia się poprzez „przygotowanie w lokalu wyborczym odpowiedniej liczby łatwo dostępnych miejsc umożliwiających każdemu wyborcy nieskrępowane zapoznanie się z kartą do głosowania oraz jej wypełnienie w sposób niewidoczny dla innych osób"[55]. Zasada tajności głosowania jest jednym z tzw. przymiotników wyborczych, które zagwarantował ustrojodawca w Konstytucji RP[56].

Nie bez znaczenia w sytuacji wyborów internetowych pozostaje także problem potencjalnej ingerencji podmiotów zewnętrznych. Wpływ zewnętrznych aktorów może przejawiać się nie tylko w ingerencji w wynik wyborczy, zakłócenia infrastruktury wywołane np. cyberatakami, manipulacji i dezinformacji w kampanii wyborczej, ale może występować także *post factum*, czyli po wyborach, i przejawiać się w podważaniu legitymizacji nowo wybranych władz bądź uczciwości procesu wyborczego na każdym jego etapie, co także łączy się z potencjalnymi próbami wykazania, iż nie została dotrzymana zasada tajności głosowania. Warto pamiętać słowa Andrew Heywooda, iż „głosowanie tajne jest zazwyczaj uważane za gwaranta uczciwych wyborów"[57].

---

protocols in context of COVID19, ResearchGate, https://www.researchgate.net (18.06.2024).

[51] M. Musiał-Karg, *op.cit.*

[52] C. Szumski, *EU elections in Estonia kick off with technical difficulties for online voting*, Euractiv, https://www.euractiv.com (18.06.2024).

[53] *What's (still) wrong with Estonian e-voting*?, Gafgaf, https://gafgaf.infoaed.ee (18.06.2024).

[54] L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu,* Warszawa 2010, s. 161.

[55] Ustawa z dnia 5 stycznia 2011 r. Kodeks wyborczy (Dz.U. 2011, nr 21, poz. 112).

[56] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r….

[57] A. Heywood, *Politologia*, Warszawa 2008, s. 285.

Zakończenie

Wpływ podmiotów zewnętrznych na proces wyborczy w danym państwie nie jest zagrożeniem nowym. Manipulacja, dezinformacja w kampaniach wyborczych czy zagraniczne finansowanie działań kandydatów są obserwowane od lat. Natomiast bez wątpienia cyberprzestrzeń dostarczyła nowych możliwości wywierania wpływu na proces wyborczy przy użyciu dodatkowych technik, narzędzi i metod. Z racji specyfiki cyberprzestrzeni wydają się one szczególnie atrakcyjne, gdyż nie wymagają wysokich kosztów, zapewniają względną anonimowość oraz szybkość i szeroki zasięg oddziaływania. Przykładem tego typu czynności są cyberataki na infrastrukturę wyborczą, co zagraża integralności procesu wyborczego. Dodatkowo, w sferze informacyjnej, kampanie dezinformacyjne istotnie podważają zaufanie do samej instytucji wyborów oraz dostarczają wprowadzających w błąd informacji dotyczących kandydatów, a także polaryzują społeczeństwo w niezwykle szybkim tempie i często przy wykorzystaniu narzędzi wykorzystujących sztuczną inteligencję.

Zaufanie obywateli do uczciwości wyborów jest kluczowe, stąd próby jego podważania przez aktorów zewnętrznych są szczególnie niebezpieczne. Pojawiają się też nowe wyzwania związane z próbami wprowadzenia głosowania internetowego przez poszczególne państwa, a jak wiadomo, wyzwania, które nie wywołały właściwej reakcji państwa, przekształcają się w zagrożenia. Bardzo ważna jest debata wokół zalet i wad *i-votingu*, zwłaszcza że temat ten wraca przy okazji kampanii wyborczych i jest podnoszony przez polityków, w tym z najwyższych szczebli władzy.

Podsumowując, cyberprzestrzeń odgrywa kluczową rolę w procesie wyborczym, a w obliczu transnarodowych zagrożeń konieczne jest podnoszenie świadomości społeczeństwa w tym zakresie, dbałość o cyberbezpieczeństwo państwa, ale także niezbędna jest odpowiednia współpraca międzynarodowa, np. wymiana informacji, wspólne ćwiczenia i koordynacja działań. Zapewnienie bezpieczeństwa procesu wyborczego wymaga kompleksowego podejścia, które obejmuje zarówno aspekty techniczno-technologiczne, prawne, instytucjonalne, jak i społeczne.

Bibliografia

Ambasador Niemiec opuścił Rosję. MSZ wezwało go na konsultacje, Rzeczpospolita, https://www.rp.pl (12.06.2024).

Cadwalladr C., *The great British Brexit robbery: how our democracy was hijacked*, The Guardian, https://www.theguardian.com (15.05.2024).

Democracy Report 2024. Democracy Winning and Losing at the Ballot, V-Dem Institute, https://www.v-dem.net (15.06.2024).

Foroohar R., *Nie czyń zła. Jak Big Tech zdradził swoje ideały i nas wszystkich*, Warszawa 2020.

Galante L., Ee S., *Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents*, Atlantic Council, https://www.atlanticcouncil.org (12.05.2024).

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2010.

Gigitashvili G., *How foreign actors targeted Polish information environment ahead of parliamentary elections*, DFRLab, https://dfrlab.org (15.06.2024).

Haertle A., *Jak Rosjanie hakowali amerykańskie wybory – krok po kroku*, Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl (16.06.2024).

Hagen M., *A typology of Electronic Democracy*, Martin Hagen, http://www.martin-hagen.net (16.06.2024).

Heywood A., *Politologia*, Warszawa 2008.

House of Commons Official Report Parliamentary Debates, Hansard, https://hansard.parliament.uk (16.05.2024).

How did Estonia carry out the world's first mostly online national elections, e-stonia.com, https://e-estonia.com (16.06.2024).

Introducing Electronic Voting: Essential Considerations, Idea, https://www.idea.int (17.06.2024).

Jee C., *An Indian politician is using deepfake technology to win new voters*, Technology Review, https://www.technologyreview.com (16.04.2024).

Kirchgaessner S., *How undercover reporters caught 'Team Jorge' disinformation operatives on camera*, The Guardian, https://www.theguardian.com (17.02.2025).

Kirchgaessner S. [i in.], *Revealed: the hacking and disinformation team meddling in elections*, The Guardian, https://www.theguardian.com (17.02.2025).

Kulesza J., *O wojnie w cyberprzestrzeni Polska zadecyduje sama*, Uniwersytet Łódzki, https://www.uni.lodz.pl (12.05.2024).

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Landay J., Lewis S., *US intelligence report alleging Russia election interference shared with 100 countries*, Reuters, https://www.reuters.com (12.05.2024).

Levite A.E. [i in.], *Managing U.S.-China Tensions Over Public Cyber Attribution*, Carnegie Endowment for International Peace, https://carnegie-production-assets.s3.amazonaws.com (12.06.2024).

Lipavský si předvolal ruského velvyslance, Novinky, https://www.novinky.cz (17.06.2024).

Lisi M., Luis C., *(Un)ready for change? The debate about electronic voting in Portugal and its implementation before and after the pandemic era*, Frontiersin, https://www.frontiersin.org (17.06.2024).

Maciejewski K., *AI wpłynęła na wynik wyborów w Słowacji? Polska szczególnie narażona na dezinformację*, Forsal, https://forsal.pl (16.04.2024).

Mason R., Farah H., *Electoral Commission apologises for security breach involving UK voters' data*, The Guardian, https://www.theguardian.com (15.05.2024).

Musiał-Karg M., *Głosowanie przez Internet. Skąd czerpać wzorce i jak wprowadzać innowacje wyborcze?*, Fundacja im. Stefana Batorego, https://www.batory.org.pl (16.06.2024).

Number of internet and social media users worldwide as of April 2024, Statista, https://www.statista.com (15.05.2024).

Odpowiedź na interpelację nr 42611 w sprawie cyberzabezpieczenia wyborów parlamentarnych w Polsce w 2023 r., Sejm, https://www.sejm.gov.pl (16.05.2024).

Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Warszawa 2022.

Prohlášení MZV ke kyberútokům ruského aktéra APT28 na Česko, Ministry of Foreign Affairs of the Czech Republic, https://mzv.gov.cz (12.06.2024).

Rozwój technik ataku grupy UNC1151/Ghostwriter, CERT Polska, https://cert.pl (17.06.2024).

Russia, Intelligence and Security Committee of Parliament, https://isc.independent.gov.uk (16.05.2024).

Sfîrnaciuc E., Vasilescu M.-E., Simion E., *E-voting protocols in context of COVID19*, ResearchGate, https://www.researchgate.net (18.06.2024).

Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni, Ministerstwo Spraw Zagranicznych, https://www.gov.pl (15.05.2024).

Szumski C., *EU elections in Estonia kick off with technical difficulties for online voting*, Euractiv, https://www.euractiv.com (18.06.2024).

Ta grupa wyborców ma głosować przez internet. Sprawdzianem wybory prezydenckie, Rzeczpospolita, https://www.rp.pl (16.06.2024).

Tsagourias N., Farrell M., *Cyber Attribution: Technical and Legal Approaches and Challenges*, „European Journal of International Law", 2020, vol. 31, iss. 3.

Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 17 sierpnia 2023 r. w sprawie obcej ingerencji w proces wyborczy w Polsce (M.P. 2023, poz. 893).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005, Nr 64, poz. 565).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2002, Nr 156, poz. 1301).

Ustawa z dnia 5 stycznia 2011 r. – Kodeks wyborczy (Dz.U. 2011, nr 21, poz. 112).

Warchoł A., *Ochrona praw i wolności człowieka w dobie Internetu* [w:] *Cyberprzestrzeń jako pole zmagań o bezpieczeństwo informacyjne*, red. W. Fehler, Siedlce 2022.

Warchoł A., *Wolność opinii w cyberprzestrzeni* [w:] *10 lat nauk o bezpieczeństwie. Potencjał, problematyka, perspektywy,* red. A. Polończyk, P. Swoboda, Kraków 2021.

Warchoł A., *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku. Praca doktorska*, Kraków 2017.

What's (still) wrong with Estonian e-voting?, Gafgaf, https://gafgaf.infoaed.ee (18.06.2024).

Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, NASK, https://cyberprofilaktyka.pl (16.05.2024).

Zurechnung der russischen Cyber-Kampagne, Deutsche Vertretungen in Russland, https://germania.diplo.de (12.06.2024).

The Impact of External Actors in Cyberspace on the Security of the Electoral Process in the State

Abstract

The objective of this article is to present the impact of external actors on the security of the electoral process. The central thesis of the article posits that, in the contemporary era, cyberspace has enabled external actors to intensify their efforts in influencing the electoral process of sovereign states. This study employs various research methods, including source analysis and criticism, literature analysis and criticism, the comparative method, and case studies. Cyberspace is pivotal in the electoral process, and in light of transnational threats, it is imperative to enhance public awareness on this issue, strengthen state cybersecurity measures, and promote international cooperation, such as information exchange, joint exercises, and coordinated activities. Securing the electoral process necessitates a comprehensive approach that encompasses technical, technological, legal, institutional, and social dimensions.

Keywords: cyberspace, elections, state, security