Stosunki Międzynarodowe – International Relations
nr 3 (t. 54) 2018

ISSN 0209-0961
doi: 10.7366/020909613201805

Zewnętrzna ingerencja w wybory jako problem bezpieczeństwa międzynarodowego

Piotr Śledź

Uniwersytet Warszawski

Zasadniczym celem artykułu jest rozważenie, czy istnieją wystarczające przesłanki ku temu, aby można było postrzegać zagadnienie zewnętrznej ingerencji w wybory jako problem bezpieczeństwa międzynarodowego (w rozumieniu koncepcji politycznego wymiaru bezpieczeństwa) w odniesieniu do współczesnych realiów. Problem analizowany jest w kontekście okoliczności związanych z aktywnością podmiotów rosyjskich, towarzyszącą referendum w sprawie członkostwa Wielkiej Brytanii w Unii Europejskiej (2016 r.) oraz wyborom prezydenckim w USA (2016 r.) i we Francji (2017 r.). Pobocznym celem tekstu jest również ukazanie spectrum środków i metod wykorzystywanych do prowadzenia działań służących próbom wywarcia wpływu na wynik wyborów, ze szczególnym uwzględnieniem środków teleinformatycznych i wykorzystujących środowisko cyberprzestrzeni (w tym mediów społecznościowych), a także próba zdefiniowania kluczowych pojawiających się w tym kontekście w przestrzeni publicznej pojęć.

Słowa kluczowe: zewnętrzna ingerencja w wybory, bezpieczeństwo polityczne, bezpieczeństwo teleinformatyczne, propaganda, dezinformacja, fake newsy, postprawda, microtargeting, *big data*.

Wstęp

Natura zagrożeń bezpieczeństwa teleinformatycznego państw ulega ciągłym przeobrażeniom, podobnie jak społeczna percepcja tychże zagrożeń. Wynika to w szczególności z faktu, że w miarę postępu technologii informacyjnych lawinowo niemal rośnie liczba aktywności ludzkich przenoszonych do sieci. Społeczeństwa stają się w ten sposób bardziej uzależnione od internetu, a przez to wzrasta ich podatność na wszelkiego rodzaju zagrożenia mające źródła w przestrzeni teleinformatycznej. Implikuje to z kolei wzmożoną aktywność państw w cyberprzestrzeni. Działalność ta może wprawdzie mieć charakter defensywny i wynikać z realizacji podstawowego zadania, jakim jest zapewnienie swoim obywatelom i strukturom bezpieczeństwa, lecz od pewnego czasu coraz częściej przybiera ona również formy ofensywne, m.in. jako instrument realizacji celów polityki zagranicznej. Do scharakteryzowania tego typu

Piotr Śledź – doktorant na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego.

praktyk użyteczny wydaje się podział zaproponowany przez Marka Madeja, obejmujący z jednej strony wykorzystanie technologii IT jako środka walki cybernetycznej, z drugiej zaś – jako narzędzia pomocniczego, zwiększającego efektywność aktywności o charakterze nieofensywnym[1]. Przykładem pierwszego rodzaju działań państw mogą być cyberataki na systemy informatyczne obsługujące np. instytucje innego państwa[2]. W drugim z przywołanych wymiarów aktywność ta służyć może m.in. pozyskiwaniu informacji wywiadowczych lub uprawianiu propagandy z wykorzystaniem internetu jako medium. To właśnie ostatniemu z przywołanych aspektów poświęcone będą w przeważającej mierze rozważania w ramach niniejszego artykułu.

Wydarzenia ostatnich lat, szczególnie zaś zwycięstwo Donalda Trumpa w wyborach na prezydenta USA w 2016 r., uwidoczniły nowe zjawisko – próby ingerencji obcego państwa w przebieg wyborów za pomocą środków teleinformatycznych. Nie chodzi tu jednak bezpośrednio o sam proces wyborczy od strony technicznej, a więc np. o ataki na system zliczający oddane na kandydatów głosy, ale o takie kształtowanie preferencji społeczeństwa, aby doprowadzić do podjęcia przez ogół wyborców decyzji odpowiadającej interesom państwa, które tego typu działania podejmuje. Za drugi, równorzędny cel takich praktyk uznać można wywarcie presji wewnętrznej i międzynarodowej na państwo będące obiektem tychże manipulacji – ukazanie słabości jego instytucji oraz podważenie ich pozycji i wiarygodności, podobnie jak samego państwa jako podmiotu w stosunkach międzynarodowych, a także dezorientacja społeczeństwa, w tym wywołanie poczucia niepewności i chaosu. Rodzi to wiele pytań o potencjalne ograniczenie suwerenności, stanowiącej, jak określił to Jean Bodin, „główne znamię państwa”[3] – najbardziej zasadniczy atrybut państwowości jako takiej.

Zagrożenia dla suwerenności państwowej stanowią rdzeń problematyki bezpieczeństwa politycznego, a więc, tak jak pojęcie to definiują Barry Buzan, Ole Wæver i Jaap de Wilde, „stabilności porządku społecznego na poziomie organizacyjnym”[4]. Jako przykłady takich zagrożeń Buzan wymienia: wymuszenie na rządzie realizacji jakiejś konkretnej polityki bądź próby pozakonstytucyjnego obalenia go, secesjonizm oraz osłabianie struktur państwa w perspektywie planów agresji zbrojnej[5]. Przedmiot zagrożeń natury politycznej stanowią, jego zdaniem, przede wszystkim sfera idei

---

[1] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Polski Instytut Spraw Międzynarodowych, Warszawa 2007, s. 334–335. Przywołany podział odnosił się wprawdzie do działalności podmiotów pozapaństwowych w cyberprzestrzeni, ale wydaje się równie adekwatny do charakterystyki tego typu praktyk stosowanych przez państwa.

[2] Dla przykładu można w tym kontekście wymienić m.in. rosyjskie cyberataki na Estonię z 2007 r. czy też unieszkodliwienie systemów sterujących pracą irańskich elektrowni jądrowych za pośrednictwem wirusa Stuxnet przez osoby działające w imieniu USA i Izraela. Zob. szerzej M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, „e-Politikon” 2013, nr 6, s. 100–102.

[3] Za: E. Zieliński, *Nauka o państwie i polityce*, Dom Wydawniczy Elipsa, Warszawa 2006, s. 19.

[4] B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, Lynne Riener Publishers, Boulder–Londyn 1998, s. 141 (tłum. P.Ś.).

[5] B. Buzan, *People, States & Fear. An Agenda for International Security Studies in the Post-Cold War Era*, wyd. 2, ECPR Press, Colchester 2007, s. 109.

państwa, a więc jego tożsamość narodowa oraz przewodnia ideologia, a także instytucje państwowe. Celem niniejszego opracowania będzie zatem rozważenie, czy (a jeśli tak, to na ile) zewnętrzna ingerencja w wybory może zostać uznana za zagrożenie bezpieczeństwa w jego politycznym wymiarze, zgodnie z ramami nakreślonymi przez przedstawicieli tzw. szkoły kopenhaskiej. Logika tejże idei przedstawiona zostanie nieco szerzej w pierwszej sekcji artykułu.

Kolejny cel badawczy stanowić będzie zaprezentowanie, w drugiej, empirycznej sekcji tekstu, nowych środków, za pomocą których jedno państwo może podejmować próby ingerencji w wybory odbywające się w innym. Wyjaśnienia wymaga w tym kontekście również, jakie właściwości tego instrumentarium sprawiły, że ranga problemu, który *de facto* istniał od dekad, stała się dziś tak wysoka.

Zadaniem niniejszego artykułu nie jest stawianie tez lub hipotez o charakterze aprioryczny ani przedstawienie jasnych odpowiedzi na pytania związane z przedmiotową tematyką, ale – przede wszystkim – zainicjowanie debaty poświęconej zagadnieniu zewnętrznej ingerencji w proces wyborczy jako problemowi bezpieczeństwa narodowego i międzynarodowego w wymiarze politycznym, będącemu jednym ze znaków czasów obecnych, który w dodatku ma szanse na stałe wpisać się w krajobraz kampanii wyborczych w państwach Zachodu, a w miarę rozwoju technologicznego – zyskać jeszcze większe znaczenie.

Idea bezpieczeństwa politycznego

Związek pomiędzy funkcjonowaniem instytucji państwowych a bezpieczeństwem obywateli dostrzeżony został na długo przed sformułowaniem przez przedstawicieli tzw. szkoły kopenhaskiej koncepcji bezpieczeństwa politycznego. Pisał o tym już choćby Monteskiusz w swoim najsłynniejszym eseju *O duchu praw*[6]. Jednak to właśnie tej grupie naukowców zawdzięczamy pierwsze w miarę spójne ramy teoretyczne odnoszące się do innych gałęzi bezpieczeństwa międzynarodowego niż tradycyjnie rozumiane bezpieczeństwo militarne. Zostały one przedstawione na łamach publikacji *Security: A New Framework for Analysis*.

Podstawą dla wyróżniania kolejnych tego typu obszarów jest, w rozumieniu Buzana, Wævera i de Wilde'a, proces sekurytyzacji. Polega on na tym, że dane zagadnienie przedstawiane jest (i finalnie za takie uznawane) jako egzystencjalne zagrożenie dla bezpieczeństwa, wymagające podjęcia nadzwyczajnych środków zaradczych, przy jednoczesnym usprawiedliwieniu tego typu działań wykraczających poza standardowe procedury[7]. Bezpieczeństwo rozumiane jest tu jako przetrwanie danego podmiotu będącego punktem odniesienia (o pewnym szczególnym charakterze) w omawianym

[6] Zob. Monteskiusz, *O duchu praw*, tłum. M. Sczaniecki, w: *Historia idei politycznych: wybór tekstów*, t. 2, wybór i oprac. S. Filipowicz et al., Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 1998, s. 18–19.

[7] B. Buzan, O. Wæver, J. de Wilde, op. cit., s. 23–26.

procesie. Owymi nadzwyczajnymi środkami zaradczymi stosowanymi w obliczu zagrożenia o szczególnej wadze i naturze, przełamującymi dotychczasowe reguły i normy towarzyszące danej polityce, mogą być m.in. utajnienie pewnych jej obszarów, nakładanie nowych obowiązków na obywateli (takich jak obciążenia podatkowe czy pobór do wojska), ograniczenie określonych praw obywatelskich lub działania służące skupieniu energii i zasobów społeczeństwa w celu zwalczenia zagrożenia. Poszczególne zagrożenia zostają uznane za egzystencjalne i stają się przedmiotowymi zagadnieniami bezpieczeństwa, kiedy zaistnieją jako takie w wymiarze intersubiektywnego dyskursu, a więc powszechnej percepcji społeczeństwa osadzonej w określonym kontekście. Problemy bezpieczeństwa, zgodnie z tym modelem, stają się nimi, gdy są za takie powszechnie uważane, niezależnie od ich realnej wagi. Stwierdzenie to doprowadziło autorów do stworzenia koncepcji sektorów bezpieczeństwa, a więc specyficznych, możliwych do zidentyfikowania typów relacji i interakcji pomiędzy tworzącymi je jednostkami (tu: podmiotami bezpieczeństwa jako zasadniczymi punktami odniesienia, aktorami bezpośrednio dokonującymi sekurytyzacji oraz aktorami funkcjonalnymi wpływającymi pośrednio na dynamikę danego sektora)[8]. Choć wyróżnili oni pięć zasadniczych sektorów, ich spectrum pozostaje otwarte.

Za jeden z sektorów bezpieczeństwa Buzan, Wæver i de Wilde uznali wymiar polityczny dotyczący ram instytucjonalnych umożliwiających funkcjonowanie państwa[9]. Jako egzystencjalne zagrożenia dla bezpieczeństwa politycznego państw wzmiankowani autorzy uznają traktują okoliczności zagrażające ich suwerenności stanowiącej konstytutywny element państwowości – fundamentalne prawo do autonomicznego decydowania o własnych sprawach, w tym o formie politycznej danego państwa, bez presji zewnętrznej. Zagrożenia te dotyczyć mogą w szczególności podważania legitymacji (w wymiarze wewnętrznym i zewnętrznym), a także autorytetu władz państwowych oraz ich uznania za takowe. Definiując państwo jako związek idei, bazy fizycznej i instytucji, autorzy ci wyróżniają zagrożenia względem struktury władz (np. w kontekście reprezentowanej przez nie ideologii), a także integralności terytorialnej państwa oraz samego jego istnienia (przykładowo choćby poprzez działanie na rzecz erozji tożsamości narodowej lub podważanie prawa danego państwa do niepodległości)[10]. Napięcia prowadzące do zagrożeń bezpieczeństwa politycznego mogą pochodzić z zewnątrz i być efektem działalności innych państw lub mieć charakter endogeniczny. Aktorami sekurytyzującymi w odniesieniu do omawianego sektora bezpieczeństwa są przede wszystkim rządy narodowe[11], w interesie których leży podniesienie do rangi egzystencjalnego zagrożenia problemów godzących bezpośrednio w ich działalność.

[8] Ibidem, s. 7–8, 27–29.

[9] Oprócz państw podmiotami bezpieczeństwa politycznego mogą być inne silnie zintegrowane struktury, jak niektóre organizacje międzynarodowe (np. Unia Europejska), grupy subpaństwowe czy ruchy o charakterze transnarodowym (polityczne, społeczne lub religijne).

[10] Ibidem, s. 141–161.

[11] Rząd nie jest jednak w kontekście tychże działań w pełni utożsamiany z państwem.

Podmioty bezpieczeństwa politycznego mogą mieć również charakter zbiorowy. Zagrożenia te dotyczyć mogą całej społeczności międzynarodowej, jeśli zagrożone są reguły i instytucje nadające kształt porządkowi międzynarodowemu, jak choćby prawo międzynarodowe, lub określonej grupy państw w kontekście ich integracji regionalnej.

Koncepcja bezpieczeństwa w wymiarze politycznym (podobnie jak całość teorii bezpieczeństwa międzynarodowego tzw. szkoły kopenhaskiej) sformułowana została pod koniec XX w. Posiłkowała się zatem przykładami zaczerpniętymi z rzeczywistości zimnowojennej oraz krótkiego okresu bezpośrednio po zakończeniu tejże konfrontacji. Wydaje się, że znaczenie pewnych, dostrzegalnych już wówczas, megatrendów rozwojowych zostało przez jej autorów nieco zlekceważone. Dotyczy to zwłaszcza procesów globalizacji i rewolucji informacyjnej. Upowszechnienie się internetu i mediów elektronicznych, ponadnarodowych ze swej natury, z jednej strony ograniczyło możliwości oddziaływania państwa na przestrzeń informacyjną, z drugiej natomiast – okazały się one być dla ich władz użytecznym instrumentarium mogącym służyć jako płaszczyzna bezpośredniej partycypacji politycznej obywateli[12], ale także stanowić narzędzie realizacji celów rządzących w prowadzonej polityce wewnętrznej i międzynarodowej. Dotyczy to w szczególności rywalizacji informacyjnej, a więc psychologicznej. Na przestrzeni ostatnich kilku lat byliśmy świadkami pojawienia się pewnych nowych jej form, wykorzystujących techniki umożliwiające działania na nieosiągalną wcześniej skalę, rzucające wyzwanie tradycyjnie rozumianej suwerenności państwowej w dość nieoczekiwany sposób.

Charakterystyka współczesnych prób zewnętrznej ingerencji w wybory

Rozważania dotyczące ingerencji w wybory przez inne państwo za pomocą środków teleinformatycznych odnosiły się będą do jednego podmiotu inicjującego tego typu działania, a więc do Federacji Rosyjskiej. Wynika to przede wszystkim ze skali stosowania przez Moskwę manipulacji za pośrednictwem internetu i nowych mediów, nieporównywalnej z jakimkolwiek innym podmiotem, a także z dość jasno sprecyzowanych celów, które im przyświecają w kontekście rosyjskiej polityki zagranicznej. Na przestrzeni minionych kilku lat Rosjanie byli podejrzewani o usiłowanie wywarcia wpływu na rezultaty:

– referendum dotyczącego członkostwa Wielkiej Brytanii w Unii Europejskiej w czerwcu 2016 r.[13],

[12] Chodzi o wykorzystanie technologii informacyjnych w relacjach państwa (lub władz lokalnych) z obywatelami – m.in. poprzez głosowania, konsultacje czy też realizację usług publicznych. Zob. np.: T. Gajowniczek, *Elektroniczna demokracja – istota pojęcia i problemy definicyjne*, w: W. Tomaszewski, D.M. Mościcka, A. Jurkun (red.), *Demokracja a wybory. Współczesne dylematy i wyzwania*, Instytut Nauk Politycznych UWM, Olsztyn 2015, s. 20–22; L. Porębski, *Lokalny wymiar elektronicznej demokracji*, Księgarnia Akademicka, Kraków 2012, s. 40–47.

[13] Zob. np. M. Czarnecki, *Jak rosyjskie trolle wkręcały Brytyjczyków w sprawie brexitu i muzułmanów*, „Gazeta Wyborcza", 15.11.2017.

– wyborów prezydenckich w Stanach Zjednoczonych w listopadzie 2016 r.[14],
– wyborów prezydenckich we Francji w kwietniu i maju 2017 r.[15]

We wszystkich trzech przypadkach celem było doprowadzenie do podjęcia przez wyborców takiej decyzji, której następstwami byłyby: 1) osłabienie spoistości geopolitycznego Zachodu oraz jego instytucji, takich jak Unia Europejska czy NATO, 2) podważenie liberalno-demokratycznego modelu państwowości, 3) pogłębienie chaosu w polityce wewnętrznej tychże państw, 4) rozbudzenie nastrojów nacjonalistycznych[16]. Kroki te doprowadzić miałyby finalnie do kontestacji filarów obecnego porządku międzynarodowego, takich jak prawo międzynarodowe czy instytucje wielostronne. W tym celu Rosjanie działali w szczególności na rzecz wspierania nacjonalistycznych i populistycznych kandydatów oraz ruchów. Wpisuje się to w rosyjską wizję przekształcenia globalnego układu sił w multipolarny, o której pisze m.in. Stanisław Bieleń[17]. Zwycięstwo zwolenników wystąpienia Wielkiej Brytanii z UE znacząco ograniczyło potencjalny wzrost znaczenia Europy jako jednolitego aktora geopolitycznego oraz jeden z filarów Zachodu, doprowadzając do sytuacji, gdy jedno z najpotężniejszych państw struktury (do tego stały członek Rady Bezpieczeństwa ONZ) decyduje się nie uczestniczyć już w projekcie integracji europejskiej, a negocjacje ze Wspólnotą dotyczące warunków Brexitu pogłębiają jeszcze polityczne antagonizmy pomiędzy Zjednoczonym Królestwem a Europą kontynentalną. Ewentualna wygrana wyborcza Marine Le Pen, oznaczająca antyeuropejski kurs Francji, służyłaby podobnym celom jako uderzenie w kolejny z filarów Zachodu i Unii Europejskiej.

Przypadek wyborów prezydenckich w USA w 2016 r. był jednak jeszcze bardziej spektakularny, gdyż działania Moskwy skierowane były przeciwko wciąż największemu globalnemu mocarstwu w wymiarze politycznym, gospodarczym, militarnym oraz *soft power*. Ingerując w przebieg wyborów, Rosja jako *challenger* rzuciła globalnemu liderowi wyzwanie, czyniąc to w sposób niejako asymetryczny. Jej działania zmierzające do wyborczego zwycięstwa Donalda Trumpa miały na celu osłabienie USA na kilku płaszczyznach – podważenie wiarygodności amerykańskich instytucji i służb, pogłębienie podziałów społecznych oraz delegitymizację przywództwa tego państwa. Dodatkowo zapowiedzi Trumpa z kampanii wyborczej dotyczące bardziej izolacjonistycznej polityki zagranicznej USA, w kontekście m.in. NATO, obecności

---

[14] Zob. np. M.A. Piotrowski, *Amerykańskie oceny dotyczące ingerencji Rosji w przebieg wyborów prezydenckich w USA*, „Biuletyn PISM" 2017, nr 8.

[15] Zob. np. L. Daniels, *How Russia hacked the French election*, Politico.eu, 23.04.2017, https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/ (data dostępu: 18.06.2018).

[16] Jako inne przesłanki dla tego typu działań Rosji James Rogers i Andriy Tyushka wyliczają również m.in. próby desynchronizacji rozwoju pozostałych państw poradzieckich oraz byłych demoludów, dyskredytowanie ich rządów oraz odpychanie tych państw od Zachodu, czy też chęć zdezorientowania i zdemotywowania zachodnich elit politycznych. Za: J. Rogers, A. Tyushka, *'Hacking' into the West: Russia's 'anti-hegemonic' Drive and the Strategic Narrative Offensive*, „Defence Strategic Communications" 2017, nr 2, s. 51–55.

[17] S. Bieleń, *Identyfikacja Rosji w stosunkach międzynarodowych*, w: S. Bieleń, M. Raś (red.), *Polityka zagraniczna Rosji*, Difin, Warszawa 2008, s. 24–26.

w Azji Wschodniej czy protekcjonistycznego nastawienia w handlu zagranicznym również w sposób oczywisty współgrały ze strategicznymi oczekiwaniami Federacji Rosyjskiej. Profesor Roman Kuźniar określił wskazane działania Moskwy za pomocą frazy „Jeśli nie możesz ich pokonać, wybierz im swojego prezydenta”[18].

Bardzo trudno rozsądzić, na ile rosyjskie działania, o których mowa w niniejszym tekście, doprowadziły w 2016 r. do zwycięstwa Donalda Trumpa oraz zwolenników Brexitu, a na ile stało się to niezależnie od nich. Pamiętać trzeba o licznych problemach w polityce wewnętrznej obu państw, dotyczących m.in. kwestii społecznych (w szczególności – imigracji) i gospodarczych, czy też z drugiej strony – relatywnego osłabienia pozycji międzynarodowej obu państw – dość trafnie zdiagnozowanych i wykorzystanych jako element platformy wyborczej populistów. Cechą wspólną w obu przypadkach był także sprzeciw wobec politycznego mainstreamu oraz identyfikowanemu z nim zjawiska politycznej poprawności. Okoliczności te niewątpliwie były istotne w kontekście decyzji wyborców w Stanach Zjednoczonych i Wielkiej Brytanii. Przekaz rzeczonych środowisk rozpowszechniany był kanałami internetowymi, zarówno na użytek wewnątrzpaństwowej walki politycznej, jak i wskutek działań Federacji Rosyjskiej.

Realizacji wspomnianych założeń Kremla posłużyło, jak zostało to już wskazane, instrumentarium wykorzystujące środki teleinformatyczne, które wcześniej nie były na tak dużą skalę używane w tego typu celach. Należy zatem przedstawić owe środki oraz charakter działań podejmowanych za ich pomocą w omawianym kontekście. Zacząć trzeba od scharakteryzowania internetu jako medium służącego do walki informacyjnej. Może ona oczywiście być prowadzona w sposób tradycyjny, gdy portale internetowe, podobnie jak pozostałe kanały przekazu medialnego, starają się kształtować rzeczywistość wedle określonej linii politycznej. Warto jednak skupić się przede wszystkim na specyficznych, interaktywnych środkach realizacji tego celu. Dochodzi bowiem do sytuacji, w której granica pomiędzy twórcą a odbiorcą treści w internecie na swój sposób zaciera się. Media społecznościowe, takie jak Facebook, Twitter czy rosyjski VKontakte, lub też wszelkiego rodzaju fora internetowe i blogosfery umożliwiają każdemu użytkownikowi publikowanie niemalże dowolnych treści, do których dostęp może mieć nieograniczone w praktyce grono odbiorców. Jest to zatem przekaz w żaden sposób niezapośredniczony (w porównaniu choćby do mediów tradycyjnych) – znikają wszelkiego rodzaju filtry, owi *gatekeepers*, o których piszą Sarah Dooley, Emma Moore i Alexander Averin[19]. Użytkownik jest nie tylko twórcą treści, ale też to głównie na nim spoczywa odpowiedzialność za selekcję przyswajanych przezeń informacji z internetu. Paradoksalnie nieco, mając dostęp

[18] R. Kuźniar, *Trumputin*, „Rzeczpospolita”, 13.02.2017.

[19] S. Dooley, E. Moore, A. Averin, *Change and 21st century media*, w: J. Althuis, L. Haiden (red.), *Fake News: A Roadmap*, NATO Strategic Communication Center of Excellence, Riga 2018, s. 39. Chodzi tu o selekcję dostarczanych odbiorcy treści dokonywaną przez określone osoby bądź wynikającą z pewnych utrwalonych wzorców.

do niezliczonych źródeł informacji, wyszukuje on, przetwarza i udostępnia jednak zwykle te, które w największym stopniu odpowiadają jego subiektywnym kryteriom. Prowadzi to do zaistnienia zjawiska określanego metaforycznie jako „komora echo" (ang. *echo chamber*) – tworzenia na własne potrzeby zamkniętego, jednolitego ideowo obiegu informacji, będącego wypadkową wcześniejszych poglądów jego uczestników oraz prowadzącego głównie do umacniania ich w tych przekonaniach, co w efekcie przyczynia się z kolei do większej polaryzacji społeczeństwa[20].

Media społecznościowe, jak i w nieco szerszym rozumieniu środowisko współczesnej cyberprzestrzeni, okazują się użytecznym narzędziem prowadzenia walki informacyjnej z racji na swoje właściwości. Wymienić można tu m.in.:

– dostępność (w kontekście upowszechnienia się urządzeń przenośnych z dostępem do internetu, takich jak smartfony czy tablety),
– szybkość rozpowszechniania się informacji,
– ogromna liczba informacji przekazywanych każdego dnia,
– anonimowość użytkowników,
– brak ograniczeń przestrzennych oraz związanych z treścią udostępnianych informacji (np. z propagowaniem treści ekstremistycznych)[21].

Powyższy katalog uzupełnić można ponadto o kwestie wynikające z własności cyberprzestrzeni jako takiej, w tym stosunkowo niskie koszty prowadzenia działań ofensywnych czy też trudności w określeniu stanu prawnego tego typu aktywności (w tym samego faktu ich legalności)[22]. Odnośnie do mediów społecznościowych możemy również mówić o pewnych ich specyficznych właściwościach umożliwiających dokonywanie motywowanych politycznie manipulacji. Do cech tych należą: 1) obecność elementu wartościującego (tzw. polubień czy też lajków – treści, które zyskują ich więcej, *a priori* uznane zostają przez odbiorców za bardziej wartościowe), 2) aktywność decydentów politycznych (lub ich sztabów) oraz liderów opinii (umożliwia to zarówno nawiązanie bezpośredniej interakcji, w tym tzw. hejt, a więc ataki słowne połączone z propagandą dyfamacyjną, jak również m.in. kradzież tożsamości i podszywanie się pod daną osobę), 3) element komercyjny (m.in. w kontekście wykupywania reklam lub płatnego pozycjonowania treści wyświetlanych odbiorcom).

Manipulacje te służyć mogą w kontekście wyborów przede wszystkim dwóm zasadniczym celom politycznym – zdobywaniu poparcia społecznego dla preferowanego kandydata, partii bądź opcji (w kontekście referendów), co oczywiste, ale również zniechęcaniu potencjalnych wyborców pierwotnie zamierzających głosować inaczej do podjęcia takiej decyzji oraz demobilizowaniu ich. Realizacji tych celów

[20] Ibidem, s. 39–40. Podobnym zjawiskiem przywoływanym przez autorów jest tzw. bańka filtrująca, a więc sytuacja, w której w okopywaniu się na dotychczasowych stanowiskach użytkowników wspierają algorytmy automatycznie selekcjonujące treści.

[21] *Social Media as a Tool of Hybrid Warfare*, NATO Strategic Communication Center of Excellence, Riga 2016, s. 5–6.

[22] Za: M. Madej, op. cit., s. 330–334.

(w szczególności drugiego z wymienionych) sprzyjają dwa zjawiska – postprawda i fake newsy. Aby mówić o ich użyteczności w kontekście manipulacji przedwyborczych, należy je wpierw zdefiniować.

Pojęcie postprawdy rozpowszechnił Ralph Keyes, autor książki *The Post-truth Era: Dishonesty and Deception in Contemporary Life* z 2004 r. Odnosił je do ówczesnej rzeczywistości, w której manipulowanie prawdą ma charakter użytkowy, jest racjonalizowane i nie rodzi pośród ludzi oporów natury moralnej[23]. Prawdziwy renesans przeżywa ono jednak od 2016 r. i brytyjskiego referendum oraz wyborów prezydenta USA. Z tej perspektywy należy w omawianym kontekście zdefiniować postprawdę jako budowanie dyskursu politycznego, w którym forma staje się nadrzędna względem treści – fakty i prawda schodzą na dalszy plan, ustępując emocjom i przekazowi *stricte* politycznemu[24]. Często posiłkuje się ona w dodatku funkcjonującymi w społeczeństwie stereotypami, utrwalając je[25].

Orężem postprawdy są fake newsy. Chelsea McManus i Celeste Michaud na podstawie swoich rozważań wyprowadzają jego następującą definicję: „rozpowszechnianie fałszywych informacji kanałami medialnymi (w formie drukowanej, transmitowanej bądź internetowej), które może być dokonane umyślnie (dezinformacja) albo być wynikiem nieporozumienia lub zaniedbania (mylna informacja)”[26]. Oczywiście plotki czy fałszywe pogłoski nie są zjawiskiem nowym i towarzyszą człowiekowi prawdopodobnie od kiedy posiadł on zdolność mowy, jednak to, co wcześniej obecne było głównie w przekazach ustnych, dziś rozpowszechniane jest przez media masowe, a dzięki internetowi zyskało zasięg globalny. Wynika to w dużej mierze z motywacji czysto komercyjnych, implikujących poszukiwanie tematów o wysokiej atrakcyjności dla potencjalnych odbiorców. W przypadku mediów internetowych zjawisko to określa się często mianem *clickbait*[27].

Postprawda i fake newsy mogą zatem służyć zarówno agitacji wyborczej, jak i demobilizowaniu elektoratu przeciwników. W kontekście promowania preferowanego kandydata lub opcji oprócz konwencjonalnych działań realizowanych w ramach prowadzenia kampanii wyborczej mamy do czynienia z dwoma zasadniczymi rodzajami aktywności: 1) służącymi rozszerzaniu zasięgu związanych z nim treści na portalach społecznościowych i różnorakich stronach internetowych (najczęściej poprzez szeroko

---

[23] R. Keyes, *The Post-truth Era: Dishonesty and Deception in Contemporary Life*, St. Martin’s Press, New York 2004, s. 12–13.

[24] Pół żartem można by zatem powiedzieć, że postprawdę dość trafnie, choć mimowolnie, zdefiniował Adam Mickiewicz w balladzie *Romantyczność*, mówiąc ustami podmiotu lirycznego: „czucie i wiara silniej mówi do mnie niż mędrca szkiełko i oko”. Za: https://wolnelektury.pl/media/book/pdf/ballady-i-romanse-romantycznosc.pdf (data dostępu: 22.06.2018).

[25] J. Bartkowski, *Prawda jako dobro wspólne i jako kapitał społeczny*, w: T.W. Grabowski, M. Lakomy, K. Oświecimski (red.), *Postprawda jako zagrożenie dla dyskursu publicznego*, Wydawnictwo Naukowe Akademii Ignatianum, Kraków 2018, s. 36.

[26] C. McManus, C. Michaud, *Never mind the buzzwords: Defining fake news and post-truth*, w: J. Althuis, L. Haiden (red.), op. cit., s. 19 (tłum. P.Ś.).

[27] Chodzi tu o generowanie kliknięć, czyli wejść na daną stronę bądź podstronę, co skutkuje większymi wpływami od reklamodawców lub lepszym pozycjonowaniem danej witryny w wyszukiwarkach internetowych.

pojęty spam), 2) polegającymi na saturacji środowiska informacyjnego – chodzi o powstawanie baniek informacyjnych promujących określony zestaw poglądów poprzez skoordynowane tworzenie i udostępnianie treści przez aktywistów, liderów opinii oraz zwolenników[28]. Z kolei gdy celem jest propaganda dyfamacyjna wymierzona w kandydata lub opcję, której ewentualne zwycięstwo jest niepożądane, dochodzi m.in. do takich procederów, jak: 1) rozpowszechnianie plotek i fake newsów na temat adwersarza, 2) próby blokowania, usuwania lub manipulowania udostępnianymi przez niego treściami, 3) zdobywanie prywatnych informacji i wykorzystywanie ich do zniesławiania, ośmieszania lub grożenia stronie przeciwnej, 4) manipulacje psychologiczne lub socjotechniczne prowadzące do wymuszenia na odbiorcach określonych zachowań, 5) tworzenie „mgły informacyjnej" – rozmywanie faktów lub ich dezinterpretacja, m.in. poprzez kreowanie teorii spiskowych[29].

Wskazane wyżej zadania związane z prowadzeniem wojny informacyjnej w internecie mogą być realizowane przez konkretne osoby (określane powszechnie mianem trolli) lub w sposób zautomatyzowany (za pomocą tzw. botów). Za najsłynniejszą centralę zrzeszającą osoby zajmujące się propagandą polityczną w internecie na użytek zewnętrzny uchodzi bazująca w Sankt Petersburgu Agencja Badań Internetu[30]. Wspomina o niej m.in. odtajniona część raportu autorstwa amerykańskiej wspólnoty służb wywiadowczych US Intelligence Community, poświęconego rosyjskiemu zaangażowaniu w wybory na prezydenta USA w 2016 r. Autorzy uznają, że agencja zrzesza „zawodowych trolli" i jest powiązana z rosyjskimi służbami specjalnymi[31].

Z kolei boty stanowią w tym kontekście typ oprogramowania komputerowego, które automatycznie wchodzi w interakcje z użytkownikami mediów społecznościowych, imitując przy tym ludzkie zachowanie – oprócz działań *stricte* propagandowych (np. samoczynnego udostępniania treści na podstawie algorytmu), mogą gromadzić informacje o użytkownikach tychże portali[32]. Boty te często wyposażone są w zdolność samouczenia się, co pozwala im na bardziej wiarygodne udawanie ludzi[33]. W ostatnich latach ok. połowa całości ruchu sieciowego generowana jest przez boty[34].

---

[28] *Social Media as a Tool…*, s. 18.

[29] Ibidem, s. 19–20.

[30] Właśc. ros. Агентство интернет-исследований.

[31] *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community, 6.01.2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf (data dostępu: 23.06.2018).

[32] S. Lightfoot, *Political Propaganda Spread Through Social Bots*, The New School, New York 2017, s. 3, 8.

[33] Tragikomicznym przykładem może być tu opracowany w marcu 2016 r. przez Microsoft bazujący na sztucznej inteligencji chatbot (z którym można było prowadzić konwersacje za pośrednictwem Twittera) o nazwie Tay. Zaledwie 16 godzin od uruchomienia operator był zmuszony do jego dezaktywacji, gdyż pod wpływem interakcji sieciowych Tay zaczął głosić treści o charakterze rasistowskim, antysemickim oraz popierające polityczną agendę Donalda Trumpa. Zob. E. Hunt, *Tay, Microsoft AI chatbot, gets a crash course with racism from Twitter*, „The Guardian", 24.03.2016.

[34] I. Zeifman, *Bot Traffic Report 2016*, Incapsula.com, 24.01.2017, https://www.incapsula.com/blog/bot-traffic-report-2016.html (data dostępu: 24.06.2018).

Do celów zewnętrznej ingerencji wyborczej za pośrednictwem internetu wykorzystywane są również bardziej tradycyjne metody walki cybernetycznej, a więc ataki hakerskie. Chodzi tu w szczególności o wykradanie danych, zarówno poprzez włamania do lokalizacji, w których są one przechowywane, jak i przez przechwytywanie transmisji tychże danych oraz wykorzystanie w tym celu czynnika ludzkiego[35]. Zasadniczej motywacji dla tego typu działań nie stanowi już jednak zniszczenie przechwyconych danych, wykorzystanie ich do szantażu lub zmanipulowanie treści, jak ma to miejsce przy okazji regularnych ataków hakerskich[36], ale przede wszystkim możliwość potencjalnego wykorzystania zdobytych informacji do celów propagandowych. Wyborom prezydenckim w USA w 2016 r. oraz brytyjskiemu referendum o członkostwie w UE towarzyszyły analogiczne działania ze strony Rosji. W lipcu 2015 r. rosyjski wywiad (w ocenie służb amerykańskich był to Główny Zarząd Wywiadowczy – GRU) uzyskał dostęp do serwera Krajowego Komitetu Partii Demokratycznej i w okresie sięgającym co najmniej czerwca 2016 r. przechwytywał z niego dane[37]. Wykradzione e-maile zostały później opublikowane na portalu Wikileaks. Wskazywały one m.in. na preferencje aparatu partyjnego w prawyborach względem Hillary Clinton kosztem Berniego Sandersa, ujawnienie jej części pytań przez dziennikarkę CNN przed prawyborczą debatą, kontrowersyjne wypowiedzi kandydatki w trakcie zamkniętych spotkań w różnych gronach (dotyczące m.in. planów przeprowadzenia skrytej interwencji w Syrii, polityki Chin czy przyjmowania uchodźców), jak również pewne kontrowersje związane z finansowaniem fundacji Clinton Global Initiative[38]. Mogło to niewątpliwie zniechęcić potencjalnych wyborców Partii Demokratycznej, przyczyniając się do ich demobilizacji skutkującej porażką wyborczą Hillary Clinton. Inny przykład wycieku danych stanowią tzw. *Macronleaks* tuż przed głosowaniem w wyborach na prezydenta Francji w 2017 r. Z racji na swoją specyfikę ten przykład zostanie nieco szerzej omówiony w dalszej części tekstu.

Zupełnie nowym fenomenem w prowadzeniu kampanii wyborczych w sieci jest zagadnienie *big data*. Pojęcie to jest szerokie i dość niejasne, a przez to trudno definiowalne. Wartościowa wydaje się jednak definicja zaproponowana przez Justina Lane'a mówiąca w tym kontekście o „ogromnych ilościach danych elektronicznych, które są indeksowane oraz możliwe do przeszukiwania za pomocą systemów obliczeniowych, przechowywane na serwerach i analizowane przez algorytmy, ponieważ ilość tych danych jest zbyt duża, by możliwe było ich interpretowanie przez człowieka"[39].

---

[35] Za: M. Madej, op. cit., s. 343–344.

[36] Zob. P. Dawidziuk, B. Łącki, M.P. Stolarski, *Sieć Internet – znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa*, w: M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 50–51, 53–54, 59–60.

[37] *Assessing Russian Activities…*, op. cit.

[38] *18 revelations from Wikileaks' hacked Clinton emails*, BBC, 27.10.2016; https://www.bbc.com/news/world-us-canada-37639370 (data dostępu: 27.06.2018).

[39] J. Lane, *Big data and anthropology: Concerns for data collection in a new research context*, „Journal of Anthropological Society of Oxford" 2016, nr 1, s. 75 (tłum. P.Ś.). Autor podkreśla przy tym, że mianem

Skala wykorzystania *big data* na potrzeby kampanii wyborczych rośnie, a charakter tych działań ewoluuje w ostatnich latach niezwykle dynamicznie. W kampanii przed wyborami prezydenta USA w 2012 r. sztaby Baracka Obamy i Mitta Romneya gromadziły, pozyskane ze źródeł internetowych, terenowych oraz od instytucji finansowych, dane dotyczące płci, wieku, adresu, numeru telefonu, wcześniejszego uczestnictwa w wyborach, lokalizacji geograficznej, lat edukacji czy statusu kredytowego; służące przede wszystkim celom analitycznym – przewidywaniu wyników głosowań oraz badaniu reakcji (*responsiveness*) wyborców na poszczególne działania w ramach kampanii[40]. Postrzeganie roli *big data* w prowadzeniu kampanii wyborczej zmieniło się jednak na podstawie doświadczeń kampanii z 2016 r. – referendalnej w sprawie członkostwa Wielkiej Brytanii w Unii Europejskiej oraz przy okazji wyborów prezydenta USA.

Nastąpiło to za sprawą firmy Cambridge Analytica[41] i stworzonych przez nią narzędzi inżynierii wyborczej. Momentem przełomowym było potraktowanie mediów społecznościowych (w szczególności Facebooka) jako swoistego rezerwuaru *big data*. Pozyskiwane z nich informacje (na podstawie aktywności użytkowników tego typu portali – ich komentarzy, polubień czy też, jak w przypadku Cambridge Analytica, specjalnie spreparowanych do tego celu kwestionariuszy[42]) pozwalają stosownym algorytmom na zrekonstruowanie osobowości danej jednostki[43]. Ta technika badania ludzkiej osobowości (tu: rynku) nazywana jest psychografią. Znajduje zastosowanie nie tylko w marketingu politycznym, ale także w odniesieniu do przedsięwzięć *stricte* komercyjnych, związanych z wymianą określonych dóbr i usług. Firma Cambridge Analytica przy wykorzystaniu danych pozyskanych w kontrowersyjnych okolicznościach od Facebooka była w stanie stworzyć profile psychologiczne ok. 230 milionów Amerykanów[44]. Dane te stanowiły bazę pod działania określane mianem microtargetingu. Chodzi o tworzenie na podstawie algorytmów indywidualnie sprofilowanego przekazu politycznego zgodnego z kampanijną agendą – treści i symboli odwołujących się do emocji konkretnej osoby oraz do jej cech osobowości – jak również dostarczenie

tym określać można również cały „przemysł" badania, pomiaru oraz kupna i sprzedaży danych zebranych przez takie firmy, jak m.in. Google, Facebook czy Twitter.

[40] Zob. D.W. Nickerson, T. Rogers, *Political campaigns and big data*, „Journal of Economic Perspectives" 2014, nr 2, s. 53–58. Według autorów sztab Baracka Obamy miał zgromadzić w trakcie kampanii ok. 50 terabajtów tego typu danych.

[41] Podobnie jak wcześniej jej spółki-matki pod nazwą Strategic Communication Laboratories (SCL).

[42] Chodzi tu zwłaszcza o testy psychologiczne.

[43] R.J. González, *Hacking the citizenry? Personality profiling, 'big data' and the election of Donald Trump*, „Anthropology Today" 2017, nr 3, s. 9–10.

[44] C. Cadawalladr, *'I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower*, „The Guardian" 17.03.2018. Wiemy już również, że strona rosyjska miała do tychże danych dostęp. Za: D. O'Sullivan, D. Griffin, P. Di Carlo, *Cambridge Analytica's Facebook data was accesed from Russia, MP says*, CNN Tech, 17.07.2018, https://money.cnn.com/2018/07/17/technology/cambridge-analytica-data-facebook-russia/index.html (data dostępu: 18.07.2018).

go potencjalnie możliwym do przekonania (*persuadable*) wyborcom[45]. Microtargeting został wykorzystany w kampanii prowadzonej przez zwolenników opuszczenia przez Wielką Brytanię Unii Europejskiej, a także przez polityków Partii Republikańskiej w kilku kampaniach wyborczych w Stanach Zjednoczonych (również przed wyborami prezydenckimi w 2016 r.)[46]. W kampanii Donalda Trumpa tego typu działania przeprowadzono w ostatnich jej tygodniach w sześciu tzw. *swing-states* – w Michigan, Wisconsin, Iowa, Pensylwanii, Ohio oraz na Florydzie[47]. We wszystkich z wymienionych zwyciężył ostatecznie kandydat Republikanów, mimo przewagi Hillary Clinton w przedwyborczych sondażach.

Ciężar gatunkowy omawianych środków jako narzędzi wywierania wpływu na decyzje wyborców wynika ze skali działań, jakich prowadzenie umożliwiają. Z końcem roku 2017 dostęp do internetu miało ok. 4,15 mld ludzi – a zatem więcej jest dziś użytkowników sieci, niż osób, które nie mają do niej dostępu[48]. W Europie odsetek ten wynosi ok. 85%, a w Ameryce Północnej – aż 95%[49]. Gdy mowa o mediach społecznościowych, to według szacunków korzysta z nich prawie 3,2 mld aktywnych użytkowników[50]. Pole do manipulacji przy okazji kampanii wyborczych, szczególnie w demokratycznych państwach Zachodu, jest zatem ogromne, z czego niewątpliwie zdają sobie sprawę podmioty próbujące dokonać ingerencji w tego typu procesy. Możemy jednak mówić jedynie o potencjalnych zasięgach, gdyż nie sposób określić liczby osób, których decyzje wyborcze zostały ukształtowane dzięki opisywanym środkom. Przede wszystkim nie dysponujemy pełnym dostępem do danych o zasięgach poszczególnych informacji umieszczanych na stronach internetowych czy w mediach społecznościowych – są to zwykle dane bardzo skrzętnie strzeżone przez największe koncerny branży IT i administratorów poszczególnych stron[51]. Gdybyśmy je zresztą nawet znali, to niemożliwe byłoby określenie na podstawie samej liczby wyświetleń danej strony, jak zawarte na niej treści wpłynęły na polityczne poglądy i decyzje odbiorców[52].

---

[45] Na podstawie R.J. González, op. cit., s. 9–10. Przekaz ten klasyfikowany jest na podstawie jednego z 32 typów osobowości nakreślonych według danych dotyczących m.in. osobistych preferencji, nawyków konsumpcyjnych czy też gustu czytelniczego i filmowego, i dopasowywany do każdego z nich.

[46] C. Cadawalladr, *The great British Brexit robbery: How our democracy was hijacked*, „The Guardian" 6.05.2017.

[47] R.J. González, op. cit., s. 9.

[48] Dane za: https://www.internetworldstats.com/stats.htm (data dostępu: 29.06.2018).

[49] Ibidem.

[50] Za: https://wearesocial.com/blog/2018/01/global-digital-report-2018 (data dostępu: 29.06.2018). Najwyższy odsetek użytkowników social mediów w społeczeństwie przypada na obie Ameryki, Europę oraz Azję Wschodnią i Australię.

[51] Wyszukiwane zapytania mogą być rejestrowane przez samą wyszukiwarkę Google z ruchu sieciowego bądź za pomocą stosownego oprogramowania (jak np. przez należącą do Amazona witrynę Alexa).

[52] Wskaźniki, takie jak komentarze czy polubienia, są z kolei łatwe do zmanipulowania przez trolle lub boty. Opisując zasięgi poszczególnych treści, często robi się to w odniesieniu do serwisu Twitter (zob. np. R. Meyer, *The Grim Conclusion of the Largest-Ever Study of Fake News*, The Atlantic, 8.03.2018, https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/

Wobec wyzwania, jakim są próby zewnętrznego oddziaływania na wyniki wyborów, nie udało się jeszcze stworzyć katalogu skutecznych środków zaradczych. Pewne wysiłki były jednak w tym zakresie podejmowane. Należą do nich m.in. inicjatywy o charakterze prawno-instytucjonalnym. Przykładem tego typu działań jest amerykańska ustawa z maja 2016 r. *Countering Foreign Propaganda and Disinformation Act* ustanawiająca ramy dla współpracy instytucji federalnych w rzeczonym celu oraz powołująca Global Engagement Center jako naczelny organ dla jego realizacji. Inny rodzaj środków prawnych wymierzonych w koordynowane z zewnątrz operacje natury informacyjno-psychologicznej stanowią kary dla firm będących właścicielami platform społecznościowych służących udostępnianiu fake newsów, co ma z założenia wymuszać na nich większą kontrolę treści – na takie rozwiązanie zdecydowały się choćby Niemcy[53]. Tworzy się również instytucje pracujące na rzecz przeciwdziałania zewnętrznej agresji informacyjnej, również wielonarodowe, jak założone w 2017 r. wspólnie przez Unię Europejską i NATO European Centre of Excellence for Countering Hybrid Threats czy *stricte* natowskie NATO Communications Centre of Excellence (oba służące raczej celom edukacyjnym) i NATO Cooperative Cyber Defense Centre of Excellence[54]. Działalność instytucji oraz egzekucja właściwych norm prawnych mają jednak charakter reaktywny i *per se* nie zapobiegają opisywanemu problemowi. Przykładem częściowo skutecznych działań reaktywnych jest weryfikowanie prawdziwości komunikatów w czasie rzeczywistym (*fact checking*). W trakcie debat w kampanii prezydenckiej w USA w 2016 r. wysiłki te podejmowały m.in. Washington Post czy też sztab Hillary Clinton (odnośnie do wypowiedzi Donalda Trumpa). Niektóre media społecznościowe i portale internetowe pozostawiają ponadto swoim użytkownikom możliwość weryfikowania udostępnianych treści i zgłaszania moderatorom tych informacji, które są ich zdaniem fałszywe bądź zmanipulowane. Sam fakt istnienia (czy raczej – kształtowania się) określonego katalogu środków zaradczych względem problemu zewnętrznej ingerencji w wybory dowodzi jego rangi dla państw narażonych na tego typu zagrożenie.

Potencjalne działania proakytwne, *stricte* prewencyjne, rodzą z kolei wątpliwości co do ewentualnego ograniczenia wolności wypowiedzi i związanego z tym

[data dostępu: 18.07.2018]). Wydaje się to błędem, gdyż z jednej strony jest on główną areną walki informacyjnej polegającej na manipulowaniu treściami przez osoby bądź algorytmy (zob. R. Gorwa, *Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere*, Working Paper No. 2017/04, University of Oxford, Oxford 2017, s. 24–27), z drugiej natomiast – nie jest to najbardziej masowe z mediów społecznościowych. W badaniu Pew Research Center ze stycznia 2018 r. tylko 24% spośród badanych Amerykanów było użytkownikami Twittera (przy 68% zarejestrowanych na Facebooku), co sytuowało go dopiero na siódmym miejscu pośród tego typu serwisów (zob. A. Smith, M. Anderson, *Social Media use in 2018*, Pew Research Center, 1.03.2018, http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/ [data dostępu: 18.07.2018]).

[53] J. Althuis, S. Strand, *Countering fake news*, w: J. Althuis, L. Haiden (red.), op. cit., s. 69–71.

[54] Powołane do życia po rosyjskich atakach cybernetycznych na Estonię z 2007 r., choć realizujące także pewne zadania w zakresie opisywanej tematyki.

pola do nadużyć ze strony państw dysponujących takim instrumentarium (podobnie jak i w kontekście koncernów z branży IT). W ocenie udostępnianych treści zawsze będzie istniał bowiem pewien element arbitralności, co rodzić może ryzyko wykorzystywania tego przez rządy do działań mających znamiona cenzury prewencyjnej, jak dzieje się to w niektórych państwach niedemokratycznych. Niemożliwość weryfikacji wszystkich udostępnianych newsów, z racji na ich ogromną ilość, przez państwowych funkcjonariuszy, może prowadzić do ograniczeń natury strukturalnej, np. zmniejszenia dostępu do niektórych źródeł czy też usług sieciowych. Z drugiej strony umiejętnie spreparowana informacja (np. odwołująca się do emocji odbiorców bądź dokonująca mizinterpretacji faktów), z racji na rolę czynnika abstrakcyjnego, będzie trudna do sklasyfikowania jako fake newsy przez bezosobowy algorytm. Choć pojawiają się pomysły, aby systemy takie wykorzystywały np. *machine learning*[55], na dziś rozwiązania te nie zapewniają odpowiedniej skuteczności. Dlatego też kluczowa, gdy chodzi o walkę z wrogą zewnętrzną propagandą polityczną, wydaje się być praca u podstaw w postaci edukowania społeczeństwa – nauka identyfikowania fałszywych informacji, rozpoznawania przyświecających ich rozpowszechnianiu celów oraz przeciwdziałania temu zjawisku; jak również (w kontekście microtargetingu) uwrażliwienie na pewnego rodzaju mechanizmy manipulacji psychologiczno-emocjonalnych. Jest to jednak działanie długookresowe, polegające na kształtowaniu nawyków w społeczeństwie, w związku z czym potencjał manipulacji politycznych przy użyciu opisywanych narzędzi wciąż pozostaje duży. Mechanizmy przeciwdziałania próbom wpływania na politykę w danym kraju (za pomocą kierowanej z zewnątrz propagandy), w tym na wybory, wykorzystujące w tym celu środowisko internetowe i tzw. nowe media, mają na chwilę obecną charakter rudymentarny.

Niemniej jednak niektóre z nich okazały się skuteczne. Przykładem są w tym kontekście wybory prezydenckie we Francji w 2017 r. Wspierana przez Kreml kandydatka Frontu Narodowego, Marine Le Pen, nie odniosła w nich sukcesu, pomimo szeroko zakrojonej dezinformacji rozsiewanej kanałami internetowymi. Było to w dużej mierze efektem pracy osób odpowiedzialnych za kampanię Emmanuela Macrona w sieci. Serwery ruchu En Marche! padły ofiarą wielu ataków hakerskich, m.in. z użyciem stron phishingowych[56]. Sztab kandydata rozmyślnie doprowadził do tego, że hakerzy weszli w posiadanie wielu loginów i haseł (prawdziwych oraz sztucznie spreparowanych), przez co, gdy doszło do wycieku danych znanego jako *Macronleaks*, część udostępnionych opinii publicznej informacji okazała się fałszywa

[55] Ibidem, s. 73. Zob. też np. aplikacje do *fact checking* stworzone przez brytyjską organizację Full Fact; https://fullfact.org/automated (data dostępu: 4.07.2018). Przeciwdziałaniu efektowi „kabiny echo" służyć ma z kolei program (w formie dodatku do przeglądarek internetowych) Open Mind stworzony przez grupę studentów Uniwersytetu Yale, zob. https://openmind.press/ (data dostępu: 4.07.2018).

[56] Termin *phishing* odnosi się w tym kontekście do stron z umieszczonym skryptem logowania, imitujących prawdziwe witryny internetowe, służących hakerom do wykradania loginów i haseł zmylonych użytkowników.

lub całkowicie bezwartościowa, co znacznie ograniczyło negatywny wpływ ataku na poparcie dla Macrona[57]. Oprócz tego sztab obecnego prezydenta Francji, we współpracy z firmą Liegey Muller Pons, wykorzystał algorytmy zbliżone w swej naturze do tych oferowanych przez Cambridge Analytica (analizujące wypowiedzi ok. 300 tysięcy rozmówców w ramach kampanii typu *door-to-door* oraz aktywność użytkowników na profilach En Marche! w mediach społecznościowych) do mobilizacji wolontariuszy oraz promowania politycznej agendy kandydata pośród wyborców[58].

Próba oceny wpływu zewnętrznej ingerencji w wybory jako zagrożenia dla bezpieczeństwa międzynarodowego w wymiarze politycznym

Omawiana w niniejszym artykule kwestia rodzi liczne niejednoznaczności. Przed przystąpieniem do analizy problemu z punktu widzenia idei politycznego wymiaru bezpieczeństwa międzynarodowego warto skoncentrować się jeszcze na dwóch wątkach: czy nowe metody wpływania na wyniki wyborów z zewnątrz są skuteczniejsze niż tradycyjne, a także czy Rosja, jako podmiot podejmujący tego typu działania, faktycznie zrealizowała przyświecające im cele. Odpowiedzi na tak postawione pytania nie są oczywiste.

Rozważając kwestię skuteczności wykorzystywania środowiska nowych mediów jako instrumentarium zewnętrznej ingerencji w wybory, należy podkreślić, że obliczone na ten cel próby podejmowane były już w przeszłości, szczególnie w okresie zimnowojennym. Często realizowano je rękoma funkcjonariuszy służb specjalnych. Do przykładów takich działań zaliczyć można inspirowaną i koordynowaną przez CIA operację Kondor (polegającą na eliminowaniu, także fizycznym, lewicowych polityków w takich państwach, jak Argentyna, Boliwia, Chile, Paragwaj czy Urugwaj), a także szereg nieskutecznych działań mających na celu niedopuszczenie do zwycięstwa wyborczego w 1970 r. późniejszego prezydenta Chile – Salvadora Allende[59]. Podobnie rzecz miała się z operacją Gladio, z inspiracji CIA zakrojoną na szeroką skalę przy wykorzystaniu bogatego spektrum środków (propagandowych, jak również *stricte* militarnych), służącą powstrzymaniu Włoskiej Partii Komunistycznej przed przejęciem władzy[60]. Z kolei Związek Radziecki stosował w tym celu strategię infiltracji środowisk opiniotwórczych

---

[57] A. Logeswaran, *How Macron's team thwarted the hackers with one simple trick*, World Economic Forum, 11.06.2017, https://www.weforum.org/agenda/2017/05/how-macrons-team-thwarted-the-hackers-with-one-simple-trick/ (data dostępu: 5.07.2018).

[58] V. Polonski, *#MacronLeaks changed political campaigning. Why Macron succeded and Clinton failed*, World Economic Forum, 12.05.2017, https://www.weforum.org/agenda/2017/05/macronleaks-have-changed-political-campaigning-why-macron-succeeded-and-clinton-failed/ (data dostępu: 5.07.2018).

[59] T. Paszewski, *Polityka Stanów Zjednoczonych wobec Ameryki Łacińskiej a demokracja – doświadczenia okresu zimnej wojny*, „Polski Przegląd Dyplomatyczny" 2007, nr 1, s. 105–108.

[60] D. Ganser, *The ghost of Machiavelli: An approach to Operation Gladio and terrorism in cold war Italy*, „Crime, Law & Social Change" 2006, nr 2, s. 114–117.

i budowania grup wpływów w określonych państwach Zachodu[61]. Ważnym instrumentem zewnętrznego oddziaływania na wybory są również media tradycyjne. Aby nie szukać daleko, wspomnieć można choćby o rosyjskich mediach o międzynarodowym zasięgu, nadających w językach poszczególnych państw, takich jak RT (dawniej Russia Today) czy Sputnik[62]. Niezwykle trudno oszacować, czy próby wpływania na przebieg kampanii wyborczej przy użyciu tradycyjnego zestawu środków były mniej skuteczne niż fake newsy i algorytmy. Porażki Marine Le Pen we francuskich wyborach prezydenckich w 2017 r. oraz Teda Cruza w kampanii prawyborczej Partii Republikańskiej rok wcześniej pokazują, że skuteczność nowych instrumentów nie jest bynajmniej pełna.

Gdyby zaś zastanowić się nad tym, co zyskała Rosja, przyczyniając się do zwycięstwa Donalda Trumpa oraz decyzji Brytyjczyków o opuszczeniu Unii Europejskiej, również pojawią się pewne wątpliwości. Wydaje się, że, o ile Kremlowi udało się osiągnąć względne zyski w zakresie realizacji swoich długoterminowych celów, o tyle, gdy mowa o codziennej praktyce politycznej, Rosja poniosła pewne straty. Z pewnością działania prezydenta USA wpisują się w rosyjskie dążenia budowy multipolarnego układu sił. Kampanijne zapowiedzi Trumpa zwiastowały chaos i osłabienie pozycji USA – w szczególności z powodu jego izolacjonistycznych postulatów. Zwycięstwo Trumpa, atakującego w kampanii m.in. mniejszości narodowe, religijne i etniczne czy imigrantów, nie pozostało bez wpływu na trend polaryzacji amerykańskiego społeczeństwa. Indukowany zewnętrznie chaos informacyjny spowodował spadek zaufania Amerykanów do przekazów medialnych[63]. Kreml, poprzez swoje zaangażowanie na rzecz wyborczego zwycięstwa kontrowersyjnego miliardera, podminował w pewnym stopniu legitymację urzędu prezydenta USA oraz demokracji jako systemu sprawowania władzy (w jej zachodnim, liberalnym kształcie). Dysfunkcje przywództwa Trumpa, wynikające z jego osobistych cech oraz z wątpliwości dotyczących okoliczności wyborczego zwycięstwa, pogłębiają dodatkowo chaos w polityce wewnętrznej USA, osłabiając poszczególne gałęzie funkcjonowania państwa, a w efekcie jego pozycję międzynarodową i miejsce w globalnym układzie sił. Rosja zyskała wizerunkowo w efekcie swoich działań, objawiając się jako podmiot zdolny, pomimo niedostatku pewnych zasobów, wpływać w sposób fundamentalny na politykę globalnego mocarstwa numer jeden. Chaotyczna i często konfrontacyjna polityka Trumpa wobec Chin, której elementem jest m.in. konfrontacja celna, w pewnym stopniu przyczynia się finalnie do osłabiania Państwa Środka, co również sprzyja Rosji obawiającej się rosnącego znaczenia swojego wschodniego sąsiada. Trump pogłębił dodatkowo podej-

---

[61] R. Kuźniar, *Polityka i siła. Studia strategiczne – zarys problematyki*, Wydawnictwo Naukowe Scholar, Warszawa 2006, s. 97.

[62] Ich działalność w zakresie dywersji informacyjnej przed wyborami prezydenckimi w USA w 2016 r. opisuje (z zaznaczeniem ważnych manipulacji i przeinaczeń) wspominany już raport US Intelligence Community. Zob. *Assessing Russian activities…*, op. cit.

[63] Zob. N. Newman, R. Fletcher, *Bias, Bullshit and Lies. Audience Perspectives on Low Trust in the Media*, Reuters Institute for the Study of Journalism, Oxford 2017, s. 5–7, 41–42.

rzenia o sprzyjanie Moskwie swoimi wypowiedziami przy okazji szczytu USA–Rosja w Helsinkach 16 lipca 2018 r. i spotkania z Władimirem Putinem.

Jeśli chodzi natomiast o Brexit, to Rosja osiągnęła niewątpliwie swój cel, jakim było rozbicie dotychczasowego kształtu Unii Europejskiej, zrzeszającej najbogatsze i najbardziej znaczące państwa Europy Zachodniej. Decyzja ta wymusiła również dymisję umiarkowanie proeuropejskiego premiera Davida Camerona i wzrost znaczenia przeciwników Unii Europejskiej w łonie rządzącej Partii Konserwatywnej, co doprowadziło do zaostrzenia jej stanowiska względem współpracy z kontynentalnymi partnerami. Brexit był także paliwem politycznym dla prorosyjskich środowisk w Wielkiej Brytanii, takich jak Partia Niepodległości Zjednoczonego Królestwa (United Kingdom Independence Party, UKIP). Z drugiej strony warto rozważyć, czy rezygnacja Wielkiej Brytanii, wcześniej blokującej przez wiele lat plany pogłębiania zakresu przedmiotowego integracji europejskiej, nie stworzyła w pewnym sensie okazji do podjęcia tego typu działań, na co wskazywać mogą przesłanki w postaci decyzji o uruchomieniu Stałej Współpracy Strukturalnej w dziedzinie bezpieczeństwa i obrony (PESCO) czy planów utworzenia oddzielnego budżetu dla strefy euro.

Także w odniesieniu do Donalda Trumpa wskazać można na pewne okoliczności niekorzystne z punktu widzenia Rosji. Cieniem na pełnieniu przez Trumpa swojej funkcji kładzie się również śledztwo nadzorowane przez specjalnego prokuratora, Roberta Muellera, dotyczące rosyjskich prób ingerencji w wybory prezydenckie z 2016 r. Ujawnione zostały kontakty najbliższych współpracowników Trumpa z przedstawicielami Federacji Rosyjskiej w trakcie kampanii wyborczej[64]. Prezydent USA musi zatem stale udowadniać swoją niezależność od Rosji i podkreślać podmiotowość prowadzonej względem Moskwy polityki, przynajmniej na poziomie deklaratywnym. Sam Trump twierdzi, że jest „najgorszym koszmarem Rosji"[65] i choć jego praktyka polityczna wykazuje pewną ambiwalencję w tej kwestii, można wskazać na podjęte działania, które istotnie są z perspektywy rosyjskich władz niekorzystne. Wspomnieć należy tu m.in. o zwiększonym zaangażowaniu USA w konflikt syryjski (w tym przeprowadzeniu ataków rakietowych), wydaleniu ze Stanów Zjednoczonych 60 rosyjskich dyplomatów po próbie otrucia Siergieja Skripala na terytorium Wielkiej Brytanii czy wydaniu zgody na sprzedaż broni Ukrainie. Obecna polityka USA osłabia również sojuszników Rosji, w tym Syrię czy (w kontekście wycofania się z JCPOA[66]) Iran. Ponadto badanie opinii publicznej instytutu Gallup wykazuje największy po zimnej

[64] Zob. https://themoscowproject.org/explainers/trumps-russia-cover-up-by-the-numbers-70-contacts--with-russia-linked-operatives/ (data dostępu: 8.07.2018). Lista obejmuje m.in. byłego Doradcę do spraw Bezpieczeństwa Narodowego Michaela Flynna, prokuratora generalnego Jeffa Sessionsa, szefa sztabu wyborczego Paula Manaforta, prawnika Donalda Trumpa Michaela Cohena, zięcia i Starszego Doradcę Trumpa Jareda Kushnera, oraz syna prezydenta, Donalda juniora.

[65] Za: S. Collinson, *Trump's toughness on Russia judged against his predecessors*, CNN, 9.06.2018, https://edition.cnn.com/2018/06/09/politics/trump-russia-historical-analysis/index.html (data dostępu: 8.07.2018).

[66] Joint Comprehensive Plan of Action – zawarte 14 lipca 2015 r. porozumienie nakładające na Iran ograniczenia dotyczące aktywności na rzecz rozbudowy programu nuklearnego tego państwa.

wojnie odsetek postaw antyrosyjskich wśród Amerykanów (aż 72%)[67], w związku z czym wybory prezydenckie w 2020 r. wygra prawdopodobnie, po raz pierwszy od czasów Ronalda Reagana, kandydat postulujący zaostrzenie relacji z Rosją. Ważnymi czynnikami w kontekście rosyjskim są też nieprzewidywalność i chaotyczność prezydentury Trumpa, mogące wynikać z braku wcześniejszych doświadczeń politycznych, przekładające się m.in. na ambiwalencję widoczną np. w jego polityce względem Chin czy Korei Północnej.

Próbując więc ocenić, czy zewnętrzna ingerencja w wybory, na kształt działań podejmowanych przez Federację Rosyjską w ostatnich latach, może być uznana za (pozamilitarne) zagrożenie bezpieczeństwa politycznego danego państwa, nie sposób sformułować jednoznacznych wniosków. Zasadnicze pytanie dotyczy w tym kontekście egzystencjalnego, z punktu widzenia funkcjonowania państwa i jego instytucji, charakteru tego zagrożenia. Patrząc wyłącznie na sam przedmiot rozważań, niewątpliwie jego natura spełnia wiele z przesłanek sformułowanych przez Buzana, Wævera i de Wilde'a. Jako że o egzystencjalności zagrożeń bezpieczeństwa politycznego państwa decyduje podminowanie jego suwerenności, patrząc wyłącznie na aspekt przedmiotowy omawianego zagadnienia, można by je za takowe uznać. Skoro Buzan stwierdza, że „wszystko, co daje się przedstawić jako pogwałcenie suwerenności […] może być zaprezentowane jako problem bezpieczeństwa"[68], pytanie o to, czy wybór dokonany przez uprawnionych do głosowania dzięki kampanii manipulacji kierowanej przez inne państwo (zainteresowane podjęciem określonej decyzji) jest suwerenny, wydaje się zasadne.

Warto przeanalizować pod tym kątem trzy obszary, w które, zdaniem Buzana, wymierzone są zagrożenia bezpieczeństwa politycznego, a więc tożsamość narodową, ideologię, wokół której państwo jest zorganizowane (składające się na ideę państwa) oraz będące jej wyrazicielami instytucje państwowe[69]. Stwierdzić można, że koordynowane z zewnątrz działania obliczone na wypaczenie wyników wyborów wymierzone są we wszystkie te trzy elementy. Generowanie i wzmacnianie podziałów społecznych osłabia wspólnotę narodową, przez co logika tożsamości narodowej zaczyna częściowo ustępować miejsca myśleniu w kategoriach trybalistycznych. Sprzyja temu wspomniane już zjawisko medialnej „komory echo". W dodatku przemoc słowna w sieci potrafi przerodzić się w rzeczywistą przemoc fizyczną[70]. Funkcjonowanie instytucji państwa podminowuje dodatkowo podważenie wewnętrznej legitymacji i autorytetu władzy pochodzącej ze zmanipulowanych wyborów – słabnie przez to poczucie identyfikacji

[67] Za: M. Brenan, *Americans, Particularly Democrats, Dislike Russia*, Gallup, 5.03.2018, https://news.gallup.com/poll/228479/americans-particularly-democrats-dislike-russia.aspx (data dostępu: 8.07.2018).

[68] B. Buzan, O. Wæver, J. de Wilde, op. cit., s. 150.

[69] B. Buzan, op. cit., s. 109.

[70] Przykład stanowić mogą starcia pomiędzy zwolennikami i przeciwnikami Donalda Trumpa przy okazji jego kampanijnych wieców, m.in. 11 marca 2016 r. w Chicago. Zob. M. Davey, J. Bosman, *Donald Trump's rally in Chicago canceled after violent scuffles*, „The New York Times" 11.03.2016.

ogółu z władzą państwa, jako obarczoną ciężkim grzechem pierworodnym, oraz rośnie jej podatność na krytykę. Za pewien przejaw tego zjawiska uznać można falę demonstracji z 20 lutego (rocznicy urodzin George'a Washingtona, tzw. Presidents' Day) 2017 r. pod hasłem *Not My President's Day*[71].

Jeśli za ideologię spajającą państwa Zachodu uznamy demokrację liberalną ze wszystkimi jej aksjonormatywnymi fundamentami, takimi jak m.in. zasada suwerenności narodu, prawa i wolności jednostki czy idea trójpodziału władzy, to wszelkiego rodzaju prawicowo-populistyczne, antysystemowe ugrupowania polityczne ów ład kontestują, podobnie jak lansująca ideę suwerennej demokracji Rosja. Ta wspólnota interesów sprawia, że partie o takim nastawieniu (m.in. brytyjski UKIP czy francuski Front Narodowy[72]) otrzymują szerokie wsparcie ze strony Kremla[73]. Kontestowanie liberalnej demokracji służy Rosji zarówno jako składowa budowania legitymacji autokratycznej władzy Władimira Putina w wymiarze wewnętrznym, jak i postulat w kontekście dążeń do multipolarnego układu sił oraz przekształcenia porządku międzynarodowego. W wymiarze jednostkowym przyczynia się również do osłabiania legitymacji *de facto* każdej władzy wybranej w demokratycznych wyborach, co odnosi się zwłaszcza do poszczególnych państw Zachodu. Rosyjska propaganda często przedstawia ich władze, funkcjonujące w realiach demokratycznych państw prawnych, jako te, które naruszają prawa i swobody obywatelskie[74].

Gdy zaś mowa o instytucjach państwowych, to rzeczone działania z jednej strony podważają ich autorytet i podają w wątpliwość skuteczność tychże organów, z drugiej z kolei ich celem może być obsadzenie stanowisk przez osoby prezentujące poglądy współgrające z agendą strony dokonującej tego rodzaju manipulacji bądź w jakiś sposób z nią powiązane. Pierwszy cel wiąże się z organizacyjną stabilnością porządku publicznego – słabość instytucji państwa niemal z automatu przekłada się na niższe społeczne poczucie bezpieczeństwa. Komunikat wysłany w stronę społeczeństwa państwa poddanego zewnętrznej ingerencji w wybory jest w tym przypadku następujący – skoro władze nie są w stanie zagwarantować uczciwego przebiegu wyborów, co leży w ich bezpośrednim interesie, to zapewnienie bezpieczeństwa państwu i jego obywatelom będzie dla nich tym bardziej problematyczne. Osłabia również, niejako siłą rzeczy, międzynarodowy wizerunek danego państwa. Drugi z przywołanych celów dotyczy wymuszania na rządzących konkretnej polityki, m.in. poprzez uczynienie nimi osób gotowych ją realizować, jak w przypadku niektórych przedstawicieli prezydenckiej

---

[71] Trudno jednak określić, co jest głównym aspektem sprzeciwu wobec prezydentury Donalda Trumpa ze strony części Amerykanów – oskarżenia o manipulacje wyborcze, prezydencka polityka (w szczególności imigracyjna) czy też jego specyficzny styl bycia.

[72] Od 11 marca 2018 r. funkcjonujący pod nazwą Zjednoczenie Narodowe.

[73] Zob. F. Wesslau, *Putin's friends in Europe*, European Coucil of Foreign Relations, 19.10.2016, https://www.ecfr.eu/article/commentary_putins_friends_in_europe7153 (data dostępu: 9.07.2018).

[74] Przykłady tego typu działań – zob. Aneks I do raportu *Assessing Russian activities…*, op. cit.

administracji Trumpa[75]. Przyjmując definicję polityki proponowaną przez Buzana, mówiącą, iż jest to „kształtowanie ludzkiego zachowania w celach zarządzania dużą grupą ludzi"[76], możemy powiedzieć, że temu właśnie służyć mają owe manipulacje – gdy chodzi zarówno o wywieranie wpływu na zachowanie obywateli przy urnach wyborczych, jak i o samo kształtowanie odpowiednich postaw społecznych w ramach sprawowania władzy.

Gdy więc mowa wyłącznie o aspekcie przedmiotowym omawianego zagadnienia, zewnętrzna ingerencja w wybory wpisuje się w kryteria uznania jej za zagrożenie egzystencjalne dla bezpieczeństwa politycznego państw. Wątpliwości budzi w tym kontekście jednak skala tego typu działań – to, czy jest ona na tyle duża, aby można było mówić o realnym wpływie na wyniki wyborów. Z perspektywy badacza stosunków międzynarodowych, niedysponującego stosownym warsztatem z zakresu nauk ścisłych, jak również z racji na niedostępność niektórych danych, udzielenie jednoznacznej odpowiedzi, wychodzącej poza ramy ekstrapolacji dotychczasowego stanu wiedzy w stosunku do nowego obszaru analizy, jest na chwilę obecną niemożliwe. Należałoby zapytać o zasięg poszczególnych fake newsów i ich rzeczywiste oddziaływanie na decyzje wyborcze elektoratu, co samo w sobie jest niezwykle trudne do oszacowania, także ze względu na konieczność dokonania rozdzielenia między propagandą zasiewaną z zagranicy a tą na użytek walki w polityce wewnętrznej. Niewiele wiemy także o skali wykorzystania w kampanii wyborczej microtargetingu. Nadchodzące lata prawdopodobnie dadzą nam pewne odpowiedzi na pytania, czy omawiane środki będą w dalszym środku stosowane, w jakiej formie[77] oraz o ich skuteczność.

Warto jednak zwrócić uwagę na jeszcze jedną wątpliwość. Liczba użytkowników mediów społecznościowych jest odwrotnie proporcjonalna do ich wieku[78]. Hipotetycznie więc to najmłodsi wyborcy powinni być najbardziej podatni na manipulacje wykorzystujące tego typu instrumentarium. Praktyka jednak tego nie potwierdza. W wyborach na prezydenta USA w 2016 r. to Hillary Clinton dość zdecydowanie

---

[75] Zob. M. Crowley, *All of Trump's Russia Ties, in 7 Charts*, Politico, https://www.politico.com/magazine/story/2017/03/connections-trump-putin-russia-ties-chart-flynn-page-manafort-sessions-214868 (data dostępu: 9.07.2018).

[76] B. Buzan, C. Jones, K. Little, *The Logic of Anarchy: Neorealism to Structural Realism*, Columbia University Press, New York 1993, s. 35.

[77] Przykład nowego instrumentarium manipulacji w kampaniach wyborczych, które może w nieodległej przyszłości odcisnąć na nich trwałe piętno, stanowi tzw. *deep fake*. Są to stworzone metodami bazującymi na rozwiązaniach technologicznych właściwych dla sztucznej inteligencji i *machine learningu* ekstremalnie realistyczne obrazy wideo przedstawiające wydarzenia (np. wypowiedzi decydentów politycznych), które nigdy nie miały miejsca. Sztucznie wygenerowane filmy od tych, które nie powstały w ten sposób, odróżnić można jedynie za pomocą narzędzi kryptograficznych, co jednak wymaga od odbiorców wysoce specjalistycznej wiedzy. Zob. K. Roose, *Here Come the Fake Videos, Too*, The New York Times, 4.03.2018, https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html (data dostępu: 18.07.2018).

[78] Zob. A. Smith, M. Anderson, op. cit.

zwyciężyła w grupie wiekowej wyborców od 18 do 44 lat[79], natomiast najmłodsi Brytyjczycy głosujący w referendum o członkostwie ich państwa w UE poparli jego pozostanie we Wspólnocie[80]. Im młodsi byli przedstawiciele badanej grupy, tym poparcie dla Clinton oraz członkostwa Wielkiej Brytanii w Unii Europejskiej było wyższe. Podobnie rzecz miała się z wynikami wyborów prezydenta Francji, w których Macron zwyciężył wśród najmłodszych wyborców[81]. Fakty te mogą zatem sugerować, że wpływ opisywanych działań na decyzje obywateli tych trzech państw przy urnach nie był decydujący. Pamiętajmy jednak, że w procesie sekurytyzacji kluczową rolę odgrywa percepcja danego zagrożenia, a niekoniecznie jego realna doniosłość.

Podsumowanie

Zakres przedmiotowy kwestii zewnętrznej ingerencji w wybory oraz znaczenia tego typu procesów z punktu widzenia ograniczenia suwerenności poszczególnych państw i narodów pozwalają myśleć o tymże zagadnieniu jako o zagrożeniu bezpieczeństwa politycznego, tak jak pojęcie to definiowali przedstawiciele szkoły kopenhaskiej. Sprzyja temu medialny oddźwięk, z którym kwestie te się spotykają. Nie sposób jednak określić jednoznacznie, jak próby te wpłynęły na wynik wyborów prezydenckich w USA i we Francji oraz na referendum w Wielkiej Brytanii, a także jaka była ostatecznie skala tychże działań. Wywoływanie chaosu informacyjnego służyć może m.in. temu, aby społeczeństwo postrzegało skalę podejmowanych manipulacji jako większą niż rzeczywista, nabierając przy tym wątpliwości co do swej politycznej podmiotowości i sprawczości. Podobnie niemożliwe jest wyznaczenie granicy pomiędzy propagandą prowadzoną w ramach walki politycznej w samych Stanach Zjednoczonych, Wielkiej Brytanii czy Francji a analogicznymi wysiłkami inicjowanymi na zewnątrz z intencją wypaczenia wyniku głosowania. Można wskazać choćby na poszczególne amerykańskie media bezpośrednio powielające przekaz rosyjski[82].

Jak już wspomniano, zadaniem niniejszego artykułu nie jest dawanie jednoznacznych odpowiedzi na pytania dotyczące natury i znaczenia zewnętrznej ingerencji w wybory z punktu widzenia bezpieczeństwa państw. Służyć ma on przede wszystkim zainicjowaniu debaty w tym przedmiocie. Dyskusja ta powinna toczyć się

[79] Zob. wyniki sondażu typu exit-poll dla CNN: https://edition.cnn.com/election/2016/results/exit-polls (data dostępu: 18.07.2018). Struktura demograficzna elektoratu Donalda Trumpa wydaje się dość typowa dla osób popierających Partię Republikańską i jej kandydatów.

[80] Zob. *EU referendum: The result in maps and charts*, BBC News, 24.06.2016, https://www.bbc.com/news/uk-politics-36616028 (data dostępu: 18.07.2016). Dostrzec należy jednak stosunkowo niską frekwencję w obwodach, w których do głosowania uprawnionych było najwięcej osób najmłodszej kategorii wiekowej.

[81] J. Burn-Murdoch, B. Ehrenberg-Shannon, A. Wisniewska, A. Rininsland, *French elections results: Macron's victory in charts*, „Financial Times" 9.05.2017. Odstępstwem od wskazanej reguły było w tym przypadku zdecydowane zwycięstwo Macrona także pośród najstarszych wyborców.

[82] Są to w szczególności portale internetowe związane ze skrajnie prawicowym ruchem Alt-right, takie jak Breitbart.com czy Alt-right.com, na łamach którego publikowano teksty Aleksandra Dugina – jednego z czołowych ideologów putinowskiej Rosji.

w szczególności wokół pytań o to, jak badać zagadnienie będące zasadniczym problemem niniejszego tekstu oraz jak pod wpływem opisywanego instrumentarium zmieni się (i czy w ogóle jakkolwiek) logika rządząca polityką w jej wewnątrzpaństwowym i międzynarodowym wymiarze. Gdy mowa o metodologii badań, zasadny wydaje się postulat integracji nauk informatycznych z naukami o polityce – szczególnie w wymiarze wypracowywania stosownej i efektywnej metodologii badania prób wpływania na politykę innego państwa przy wykorzystaniu instrumentarium stwarzanego przez nowe media. Ważny byłby w tym kontekście postulat integracji metod ilościowych z jakościowymi.

Na koniec dodać warto, że nawet jeśli opisywane manipulacje miały ostatecznie istotny wpływ na wyniki wyborów prezydenckich w USA czy referendum decydującego o członkostwie Wielkiej Brytanii w Unii Europejskiej, to nie były one jedyną przyczyną sukcesów polityków o prawicowo-populistycznej proweniencji. Przyjmowanie tego wytłumaczenia za obowiązujące, choć wygodne i kuszące dla wielu środowisk, wydaje się drogą na skróty. Niewątpliwie za takimi rozstrzygnięciami stało wiele problemów społecznych, zarówno natury gospodarczej, jak i wynikających z demografii czy różnic kulturowych. Faktem są również coraz głębsze podziały społeczne. Oferta polityczna środowisk bliższych mainstreamowi także uznana została przez wyborców za niezadowalającą. Przestrzec należy zatem przed traktowaniem działalności Rosji jako wyłącznego czynnika sprawczego w kontekście Brexitu czy wyboru Donalda Trumpa na prezydenta USA.

Foreign Electoral Intervention as a Problem of International Security

The main goal of the article is to consider whether there are sufficient premises to perceive the issue of foreign electoral intervention as a problem of international security (in the meaning of the concept of political dimension of security) in relation to contemporary political realities. The problem is analyzed on the basis of circumstances related to the activity of Russian entities accompanying the referendum on the membership of the United Kingdom in the European Union (2016) as well as the presidential elections in the US (2016) and France (2017). The secondary objective of the paper is to present the spectrum of means and methods used to conduct activity aimed at attempting to influence the elections' result, with particular emphasis on ICT and using the cyberspace (including social media) as well as an attempt to define key concepts emerging in this context in the public space.

Keywords: Foreign electoral intervention, political security, cybersecurity, propaganda, disinformation, fake news, post-truth, microtargeting, big data.