

DOI: <https://doi.org/10.34862/rbm.2020.1.5>

Andrzej Kozłowski  
Uniwersytet Łódzki  
andrzejk1234@gmail.com  
<https://orcid.org/0000-0001-7443-9401>

## **Rosyjskie „środki aktywne” w cyberprzestrzeni w wyborach prezydenckich w Stanach Zjednoczonych w 2016 roku**

**Streszczenie:** Przedmiotem badania przedstawionym w artykule jest zastosowanie starych metod rosyjskiego wywiadu: środków aktywnych przy wykorzystaniu nowoczesnych technologii na przykładzie wyborów prezydenckich w Stanach Zjednoczonych. Artykuł próbuje odpowiedzieć na pytanie, jakie były rosyjskie cele i czy zostały one osiągnięte, oraz analizuje wykorzystanie nowoczesnych środków, takich jak ataki hakerskie czy media społecznościowe. Autor przybliży również specyficzną sytuację polityczną w USA przed wyborami prezydenckimi. Wybory prezydenckie w 2016 roku są najbardziej znanym przykładem zastosowania na masową skalę środków aktywnych przez Rosjan, ale nie jedynym. Artykuł ten ma pomóc zrozumieć, w jaki sposób się je stosuje przy wykorzystaniu nowoczesnych technologii oraz jakie kwestie są akcentowane. W artykule wykorzystano metodę analizy krytycznej, której poddano dokumenty, książki i artykuły, metodę obserwacji polegającą na lekturze artykułów naukowych, wiadomości prasowych, oraz metodę historyczną, przedstawiającą genezę i znaczenie środków aktywnych w czasie zimnej wojny.

**Słowa kluczowe:** Rosja, Stany Zjednoczone, środki aktywne, wybory prezydenckie

### **Russian Active Measures in Cyberspace in the U.S. 2016 Presidential Election**

**Summary:** This research paper focuses on using the Russian intelligence old methods: the active measures supported and developed by the modern technology on the example of the presidential election in the United States. The paper tries to answer the questions about the aims of Russian engagement and attempt to measure effectiveness of these efforts. In addition, it presents and analyzes the usage of cyberattacks and massive information campaigns in social media and the extraordinary situation just before the presidential election. The case of using Russian social media in presidential election in 2016 is the most detailly accounted but not the only one when such a method was used. This paper should help to understand how the active measures were supported and developed by the new technology and what the most important aspects are. The several research methods were used in this article such as the critical analysis of the documents, research papers and books and the observation method was used to read research papers, press

news. Last but not least the historic research method was implemented to this article to examine and present the development and the significance of the active measures during the Cold War.

**Keywords:** Russia, The United States, active measures, presidential election

## Wstęp

Pojęcie „środki aktywne” pojawiło się po raz pierwszy w 1972 w ZSRR w słowniku kontrwywiadowczym wydanym przez Wyższą Szkołę KGB im. Feliksa Dzierżyńskiego (Darczewska, 2018, s. 49). Termin ten zdefiniowano jako: „działania kontrwywiadu umożliwiające przejrzenie zamiarów przeciwnika, pozwalające uprzedzić jego niepożądane kroki, wprowadzić przeciwnika w błąd, przechwycić jego inicjatywę, udaremnić jego akcje dywersyjne. Środki aktywne, w odróżnieniu od środków ochronnych, np. dotyczących zabezpieczenia reżimu tajności oraz ochrony tajemnicy państwowej i wojskowej, mają charakter ofensywny, umożliwiają wykrycie i przerwanie wrogiej działalności we wczesnym jej stadium, zmuszają przeciwnika do zdemaskowania się, pozwalają narzucić mu swą wolę, zmuszają do działań w niesprzyjających warunkach oraz kierunkach pożądanym dla organów kontrwywiadu. W praktyce działalności kontrwywiadowczej organów bezpieczeństwa państwowego do środków aktywnych zalicza się przedsięwzięcia mające na celu zbudowanie pozycji agenturalnych w obozie przeciwnika i jego otoczeniu, prowadzenie gier operacyjnych z przeciwnikiem, jego dezinformację, kompromitację i demoralizację, przerzut na terytorium ZSRR osób mających szczególną wartość operacyjną, zdobywanie informacji wywiadowczej itp.” (Darczewska, 2018, s. 49).

Były funkcjonariusz I Zarządu Głównego i archiwista wywiadu KGB Wasilij Mitrochin napisał, że obok klasycznej działalności wywiadowczej KGB próbowało zmienić bieg wypadków w polityce światowej, wykorzystując środki aktywne do m.in. manipulacji medialnej (Andrew, Mitrochin, 2013, s. 362). Podsumowując, celem środków aktywnych jest rozbrojenie przeciwnika poprzez wpłynięcie na jego procesy decyzyjne w obszarze polityki, gospodarki, społeczeństwa oraz wojska i doprowadzenie do autodestrukcji. Wykorzystanie „środków aktywnych” może polegać nie tylko na fałszowaniu istniejących wydarzeń, ale również kreowaniu i wykorzystaniu istniejących wydarzeń i zjawisk, tak aby ich rezultat doprowadził do osiągnięcia pożądanym z punktu widzenia Kremla celów. Proces ten odbywa się za pomocą wielu różnych instrumentów: politycznych, ekonomicznych, militarnych, społecznych czy informacyjnych (Kozłowski, 2018). W czasach

zimnej wojny naturalnym przeciwnikiem, na którym wykorzystywano „środki aktywne”, były Stany Zjednoczone. Wydarzenia z 2016 roku pokazały, że nie uległo to dużej zmianie (Andrew, Mitrochin, 2013, s. 362).

Zastosowanie „środków aktywnych” współcześnie niewiele różni się od sposobów ich użycia w czasach zimnej wojny. Można je podzielić na dwie szerokie kategorie. Jedne są realizowane za pomocą działań dezinformacyjnych i propagandowych, a druga kategoria uwzględnia dywersje, prowokacje, operacje o charakterze paramilitarnym czy protesty. Narzędziem, które zrewolucjonizowało wykorzystanie „środków aktywnych”, był Internet, który zniósł bariery komunikacyjne i informacyjne. Umożliwia on dostęp do informacji w czasie rzeczywistym, pozwalając na przeprowadzenie błyskawicznych operacji informacyjnych. Taka cecha Internetu jak możliwość bezpośredniego dotarcia do ponad 4 mld internautów (Internet Live Stats, 2019) z każdym komunikatem, który dodatkowo można spreparować pod konkretną grupę odbiorców za pomocą tzw. mikrotargetowania, sprawia, że jest to idealne narzędzie do stosowania tzw. „środków aktywnych”. Dodając do tego jeszcze względną anonimowość oraz niewielkie koszty prowadzenia takich działań, wiadomo, dlaczego rosyjskie służby wykorzystały Internet do swoich operacji na dużą skalę (Darczewska, Żochowski, 2017, s.10).

### **Przykłady użycia środków aktywnych przed erą Internetu**

ZSRR wielokrotnie w czasach zimnej wojny stosował środki aktywne. Jednym z przykładów było podsycanie zamieszek na tle etnicznym w Stanach Zjednoczonych. Dokonywano tego poprzez fałszowanie informacji i inspirowanie teorii spiskowych, np. twierdząc, że Martin Luther King Jr.<sup>1</sup> został zamordowany przez rząd Stanów Zjednoczonych, czy wysyłając, rzekomo przez członków Ku Klux Klanu, paczki z ukrytymi materiałami wybuchowymi do Afroamerykanów<sup>2</sup>. Próbowano również dyskredytować amerykański wywiad, przedstawiając CIA jako sprawcę zamachu na prezydenta Johna F. Kennedy’ego w 1963 roku (Report

---

<sup>1</sup> Martin Luther King Jr. był amerykańskim pastorem baptystycznym, liderem ruchu obywatelskiego oraz działaczem na rzecz równouprawnienia Afroamerykanów. Zasłynął marszem na Waszyngton, w którym wzięło udział 250 tys. osób, podczas którego wygłosił słynne przemówienie *I have a dream*. Przedstawił w nim wizję Stanów Zjednoczonych, gdzie wszyscy obywatele niezależnie od koloru skóry mają równe prawa. Został zamordowany w 1968 roku przez swoich przeciwników politycznych.

<sup>2</sup> Ku Klux Klan (KKK) to organizacja rasistowska założona w Stanach Zjednoczonych w XIX wieku po wojnie secesyjnej. Głównym celem grupy była walka o utrzymanie supremacji białych.

Of The Select Committee On Intelligence, 2019, Vol. 2, s. 7). Szerzenie chaosu w społeczeństwie, wykorzystywanie problemów wewnętrznych i destabilizacja państwa poprzez pogłębianie napięć to charakterystyczny element rosyjskiej strategii zastosowania środków aktywnych.

Najbardziej znany epizod zastosowania środków aktywnych to operacja „INFEKTION” z początku lat 80. XX wieku. Była to kampania, która miała na celu przekonanie opinii publicznej na świecie, a w szczególności przywódców i społeczeństwa państw afrykańskich, że wirus HIV został stworzony w Forcie Detrick w Stanach Zjednoczonych jako broń biologiczna (Selvage, Nehring, 2019). Taka historia po raz pierwszy pojawiła się na łamach w mało znanej, lokalnej indyjskiej gazecie „Patriot”. Pismo zostało w 1962 roku stworzone przez KBG. Autora artykułu przedstawiono jako renomowanego amerykańskiego naukowca antropologa. W innym artykule opublikowanym na łamach tej samej gazety, autorstwa dwóch Niemców z NRD, podających się za francuskich badaczy, rozwinęto temat, przedstawiając liczne spreparowane badania, oraz zaprezentowano oparte na nich wnioski. Następnie artykuł ten został omówiony w ponad 40 różnych sowieckich gazetach, magazynach, audycjach radiowych i telewizyjnych. Kolejnym etapem było rozprowadzanie fałszywej informacji na Zachodzie. Dokonywano tego przez publikowanie wiadomości za pośrednictwem prosowieckich, lewicowych mediów oraz prawicowych organizacji, skłonnych do szerzenia teorii spiskowych (Singer, Brooking, 2019, s. 147–148). Trwająca cztery lata operacja zakończyła się sukcesem. Jej efekty były widoczne na początku XXI wieku. W 2001 roku portal [allafrica.com](http://allafrica.com) informował, że prezydent Namibii, twierdził, że to właśnie Amerykanie stoją za stworzeniem wirusa (Gliwa, 2019). Przeprowadzone przez RAND Corporation i Oregon State University badania wykazały, że 50% Afroamerykanów uważa, że AIDS został stworzone przez człowieka, a 25%, że w tym procesie uczestniczyło państwowe laboratorium badawcze (Boghardt, 2009, s. 19).

W opinii przedstawicieli Departamentu Stanu za pomocą operacji INFEKTION Związek Radziecki dążył do podważenia wiarygodności Stanów Zjednoczonych, szerzenia postaw antyamerykańskich na świecie, izolowania USA na arenie międzynarodowej, wywoływania napięć między sojusznikami, w szczególności w państwach, które gościły amerykańskich żołnierzy. Departament Stanu uważał również, że celem ZSRR mogło być odwrócenie uwagi od rozwoju własnego zaawansowanego arsenału broni biologicznej (United States Department of

State, 1987) i to pomimo podpisania Konwencji o broni biologicznej<sup>3</sup>.

Przed nastaniem ery Internetu stosowanie środków aktywnych było o wiele trudniejsze. Szerzenie dezinformacji i tworzenie fałszywych narracji było czasochłonne i wymagało zaangażowania zdecydowanie większej liczby zasobów. W tamtym okresie większość mediów o największym zasięgu i reputacji miała wystarczająco dużo czasu, żeby móc sprawdzić, czy informacje są prawdziwe, a te, które uznano za mało wiarygodne czy nawet fałszywe, odrzucano i rezygnowano z ich publikacji. Nie miały one możliwości, poza nielicznymi wyjątkami, dotrzeć do szerokiego grona odbiorców. Internet i bezpośredni, niekontrolowany dostęp do informacji zmienił znacznie tę perspektywę, a obecnie każda informacja, niezależnie od tego, czy jest prawdziwa, czy fałszywa, może zostać opublikowana, rozpowszechniona i dodatkowo znajdzie grono zwolenników, którzy w nią uwierzą. Ten fakt wykorzystali Rosjanie w 2016 roku.

### **Tło wyborów prezydenckich w 2016 roku w Stanach Zjednoczonych**

Środki aktywne wykorzystywane przez ZSRR, a potem Rosję służą osiągnięciu celów polityki zagranicznej i szkodzeniu przeciwnikom politycznym. W 2015 roku relacje między Stanami Zjednoczonymi a Rosją były dalekie od atmosfery „resetu” z początku prezydentury Baracka Obamy<sup>4</sup>. Ponowne dojście do władzy Władimira Putina w 2012 roku w Rosji oraz takie wydarzenia, jak udzielenie azylu w tym państwie byłemu pracownikowi amerykańskiej NSA Edwardowi Snowdenowi<sup>5</sup> oraz przede wszystkim aneksja Krymu w 2014 roku<sup>6</sup> i będąca tego następstwem wojna na Ukrainie oraz zestrzelenie pasażerskiego samolotu

<sup>3</sup> Konwencja o broni biologicznej jest traktatem podpisanym 10 kwietnia 1972 roku. Na jej mocy sygnatariusze zobowiązują się do nierozwijania, przekazywania oraz nabywania broni biologicznej. Obecnie 178 państw jest stroną Konwencji.

<sup>4</sup> Obejmując urząd prezydenta w 2009 roku, Barack Obama postawił sobie za jeden z celów polityki zagranicznej poprawę relacji z Rosją. W marcu 2009 roku w Genewie sekretarz stanu Hillary Clinton i minister spraw zagranicznych Rosji Siergiej Ławrow nacisnęli symboliczny przycisk „reset”.

<sup>5</sup> Edward Snowden był byłym pracownikiem CIA oraz amerykańskiej firmy Booz Allen Hamilton, która realizowała kontrakty dla NSA. Wykradł on i opublikował tajne informacje o działalności amerykańskiego wywiadu radioelektronicznego na całym świecie. Obecnie przebywa w Rosji.

<sup>6</sup> W wyniku drugiej rewolucji na Majdanie prezydent Ukrainy Wiktor Janukowycz zrezygnował z pełnienia funkcji prezydenta i uciekł do Rosji. Praktycznie w tym samym czasie wybuchły zamieszki na Krymie, a następnie pojawiły się tam uzbrojone jednostki bez oficjalnych emblematów państwowych i przejęły kontrolę nad półwyspem. W wyniku referendum, które nie zostało uznane przez społeczność międzynarodową, Krym został przyłączony do Rosji.

malezyjskich linii lotniczych nad Donbasem<sup>7</sup>, spowodowały, że relacje między Waszyngtonem a Moskwą stały się najgorsze od końca zimnej wojny. Zbliżające się wybory prezydenckie w Stanach Zjednoczony mogły to zmienić. Przyczyną potencjalnej zmiany miał być Donald Trump, ekscentryczny miliarder, który odnosił się z sympatią do rosyjskiego przywódcy i zapowiadał rewolucyjne zmiany w polityce zagranicznej (Klare, 2017). Prezydent Rosji Władimir Putin przyznał na konferencji prasowej po szczycie w Helsinkach, że chciał, żeby prezydent Trump wygrał wybory (Murray, 2018). Potwierdziła to amerykańska wspólnota wywiadowcza (Office of the Director of National Intelligence, 2017).

Wsparcie dla kandydatury Trumpa nie było jedynym powodem zaangażowania się Rosji w wybory prezydenckie w 2016 roku. Murowaną faworytką do zwycięstwa była Hillary Clinton z Partii Demokratycznej. Oznaczałoby to kontynuację polityki sankcji i wzmacniania sojuszu transatlantyckiego administracji Baracka Obama. Clinton, która pełniła funkcję sekretarz stanu w trakcie prezydentury Obamy, uchodziła za zwolenniczkę twardej, „jastrzębiej” polityki względem Rosji. Była pierwszą osobą w administracji Baracka Obamy, która ostrzegała, że kontynuowanie „resetu” z Rosją nie ma sensu i należy go zakończyć, zanim będzie za późno (Isikoff, Corn, 2018, s. 60). Stała się również osobistym wrogiem Władimira Putina, który oskarżył ją o ingerowanie w wewnętrzne sprawy Rosji w 2011 roku. Wtedy, będąc sekretarz stanu, Clinton poparła protestującą opozycję<sup>8</sup>. Wybór Hillary Clinton na prezydenta z rosyjskiej perspektywy oznaczał kontynuację polityki Obamy, albo nawet jej zaostrenie, co było niekorzystne dla Rosji. Donald Trump proponował alternatywne rozwiązania.

Należy również zwrócić uwagę, że sytuacja przedwyborcza w USA była wyjątkowa. Po pierwsze niespotykane duża liczba osób wyrażała niezadowolenie z kandydatów Partii Demokratycznej i Partii Republikańskiej. Po drugie, aż 39% uprawnionych do głosowania identyfikowało siebie jako niezależnych wyborców, którzy nie sympatyzują z żadną partią polityczną. Po trzecie większa niż zazwyczaj część społeczeństwa (jeden na ośmiu wyborców) miała podjąć decyzję, na kogo

<sup>7</sup> Samolot Boeing 777 linii lotniczych Malaysia Airlines został zestrzelony nad terytorium Ukrainy kierowanym pociskiem rakietowym ziemia-powietrze Buk M nr 322, należącym do stacjonującej w Kursku 53. Rakietowej Brygady Przeciwlotniczej Sił Zbrojnych Federacji Rosyjskiej.

<sup>8</sup> W 2011 roku odbyły się w Rosji wybory parlamentarne. Obserwatorzy donosili o licznych przypadkach oszustw wyborczych, w tym dorzucania głosów do urn wyborczych. Na znak protestu przeciwko tym działaniom na ulice rosyjskich miast wyszły dziesiątki tysięcy protestujących. Poparła ich sekretarz stanu Hillary Clinton. Słowa te wystarczyły, aby ubiegający się wtedy o urząd prezydenta Władimir Putin oskarżył Amerykanów, w szczególności Clinton, o inspirowanie protestów (Isikoff, Corn, 2018, s. 64).



zagłosuje, w ostatnim tygodniu kampanii wyborcze (Jamieson, 2018, s. 39).

### **„Środki aktywne” w kampanii prezydenckiej w 2016 roku. „Hakowanie i ujawnianie”**

Rosjanie prowadzili swoje operacje we wszystkich amerykańskich stanach, co świadczy o jej skali oraz zaangażowaniu dużych zasobach. Nowym elementem była cyberprzestrzeń. Rosjanie zastosowali strategię, którą eksperci określili mianem strategii „hakowania i ujawniania” (hacking and leaking). Polegała ona na wykorzystaniu hakerów, którzy włamywali się do systemów i sieci teleinformatycznych instytucji i osób, ważnych dla przebiegu procesu wyborczego, a potem ujawniania w Internecie wykradzionych informacji. Celem ataków były Krajowe Komitety Partii Demokratycznej (DNC) i Partii Republikańskiej (RNC) oraz Komitet Kampanii do Kongresu Partii Demokratycznej. Rosjanie wniknęli tak głęboko w systemy, że byli w stanie pozyskać praktycznie każdą informację, wliczając w to wszystkie e-maile czy śledzić czaty. Ofiarą hakerów zostały również pojedyncze osoby, takie jak m.in. John Podesta – szef sztabu Hillary Clinton, któremu włamano się do skrzynki poczty elektronicznej (Whittaker, 2019). Cyberataki stały się prostym i tanim narzędziem nielegalnego pozyskiwania tajnych i poufnych informacji, które nierzadko mogły być wykorzystywane jako tzw. kompromat<sup>9</sup>. Należy dodać, że osoba, która dokonuje takiego włamania, jest bardzo trudna do wykrycia ze względu na architekturę cyberprzestrzeni<sup>10</sup>.

Celem hakerów były również infrastruktura wyborcza w Stanach Zjednoczonych<sup>11</sup>. Najczęściej spotykaną aktywnością było skanowanie systemów teleinformatycznych systemów wyborczych w poszukiwaniu potencjalnych luk. Nie było to równoznaczne z włamaniem. Czynność ta prowadzona jest w celu rozpoznania potencjalnych obiektów do przeprowadzenia ataku. Rosjanie jednak oprócz skanowania dokonali również włamań. Pierwszą taką aktywność

<sup>9</sup> Termin ten określa kompromitujące materiały na temat polityka lub innej osoby publicznej.

<sup>10</sup> Cyberprzestrzeń ze względu na swoją architekturę sprzyja działaniom ofensywnym, gwarantując m.in. łatwość ukrycia prawdziwej tożsamości atakującemu, szybkość przeprowadzenia ataku czy relatywnie niewielkie środki, które są do tego potrzebne. Tylko zaawansowane narzędzia i długi, powolny proces umożliwiają identyfikację sprawcy.

<sup>11</sup> Departament Bezpieczeństwa Wewnętrznego definiuje infrastrukturę wyborczą jako urządzenia do przechowywania informacji, miejsca głosowania i miejsce liczenia głosowaniu, których celem jest wsparcie procesu wyborczego. W skład infrastruktury wyborczej według DHS wchodzi również całość technologii informacyjnej wliczająca w to bazy danych wyborców, maszyny do głosowania oraz inne systemy, które wspierają proces wyborczy (Office of the Press Secretary of Department of Homeland Security, 2017).

wykryto w lipcu 2016 roku w stanie Illinois, gdzie podejrzania wzbudziły ogromne ilości danych wychodzące z sieci. Badania przeprowadzone przez FBI wykazały, że zewnętrzny podmiot nielegalnie pobiera informacje z bazy danych zarejestrowanych wyborców. Uzyskano ponad pół miliona rekordów danych amerykańskich wyborców (Shawn, 2018).

Rosyjskim hakerom udało się również włamać do systemów komputerowych w jednym z okręgów wyborczych na Florydzie, czyli tzw. „swing states”, oraz umieścić złośliwe oprogramowanie w systemach producenta sprzętu wykorzystywanego w wyborach prezydenckich w 2016 roku (Wines, 2019). Według dostępnych informacji Rosja nie skorzystała jednak z możliwości i bezpośrednio nie manipulowała wynikami wyborów. Nie wpłynęła również w żaden sposób na listy Amerykanów uprawnionych do głosowania (Report Of The Select Committee On Intelligence, Vol. 1, 2019, s. 4). Wciąż nie wiadomo, dlaczego tak się stało. Prawdopodobnie celem była destabilizacja systemu demokratycznego w Stanach Zjednoczonych poprzez pogłębienie chaosu oraz podważenie legitymizacji przysłego prezydenta. Amerykanie mieli się zastanawiać, czy to oni z pewnością wybrali prezydenta, czy może była to sprawka zagranicznego mocarstwa, a doniesienia o możliwości zhakowania systemów wyborczych miały podtrzymywać niepewność w społeczeństwie.

Za przeprowadzanie cyberataków odpowiedzialne były dwie grupy hakerskie: APT 28, która powiązana jest z rosyjskimi wywiadem wojskowym GRU, oraz APT 29, która pracuje dla rosyjskiego kontrwywiadu FSB (Galante, Ee, 2018, s. 6). Rosjanie próbowali również odwrócić uwagę śledczych poprzez utworzenie fikcyjnego rumuńskiego hakera o pseudonimie Guccifer 2.0, który miał stać za włamaniami do DNC. Na dowód opublikował on w Internecie kilka skradzionych dokumentów, w których informowano o prywatnych darczyńcach czy dokumentach dotyczących zbierania funduszu przez Komitet Partii Demokratycznej. Nie były to wstrząsające materiały, ale zapowiadały, że dużo poważniejsze informacje mogą pojawić się w Internecie. Śledztwo służb i analiza lingwistyczna szybko uwodniła, że Guccifer 2.0 nie jest tym, za kogo się podaje, i za jego stworzeniem stoją rosyjskie służby (Isikoff, Corn, 2018, s. 199).

Pozyskanie informacji to pierwszy atak strategii „hakowania i ujawniania” (*hacking and leaking*). Równie ważne, jeśli nawet nie ważniejsze, jest rozprowadzanie informacji, tak by dotarły one do jak najszerszego grona odbiorców. Rolę tzw. przekazników informacji odgrywało wiele platform.



Najbardziej tradycyjnym były strony internetowe, na których magazynowano wykradzione w wyniku ataków hakerskich informacje. Główną rolę odgrywał tutaj portal Wikileaks<sup>12</sup>. Istniał od dawna i zdążył zdobyć reputację oraz nawiązać niezbędne kontakty z mediami na całym świecie<sup>13</sup>. Czyniło to tę platformę, założoną przez Julianna Assange'a, atrakcyjnym miejscem do umieszczenia skradzionych dokumentów (House Permanent Select Committee on Intelligence, s. 30).

W 2016 roku utworzono również specjalną stronę internetową DCleaks, która miała skupiać się wyłącznie na pozyskiwaniu tajnych informacji dotyczących kampanii prezydenckiej w 2016 roku. Informacje przez te portale były publikowane w najbardziej strategicznych momentach kampanii, tak aby zaszkodzić kandydaturze Hillary Clinton (Newman, 2018). Publikacja wykradzonych informacji miała na celu zachwiać jednością Partii Demokratycznej. Opublikowane wiadomości wskazywały, że kierownictwo DNS faworyzowało Clinton oraz że wysmiewano jej głównego kontrkandydata w prawyborach Berniego Sandersa. Ujawnione informacje miały na celu nastawić negatywnie zwolenników tego polityka do Clinton oraz zasiania niepokoju w Partii Demokratycznej (Isikoff, Corn, 2018, s. 253).

### **Media społecznościowe – główny przekaznik informacji**

Drugim i o wiele ważniejszym sposobem dystrybucji było rozpowszechnianie informacji w mediach społecznościowych. Takie amerykańskie narzędzia, jak Facebook, Twitter czy Google, zostały wykorzystane do ataku na Stany Zjednoczone. W odróżnieniu od „Operation Infektion” nie trzeba było tworzyć z kilkuletnim wyprzedzeniem własnych gazet, które rozpowszechniały fałszywą informację. Założenie konta na jednym z mediów społecznościowych, które może posłużyć do szerzenia fałszywych informacji, zajmuje kilka minut. Jest to anonimowy proces, co więcej, jedna osoba może dysponować wieloma kontami. Tworzona są również boty<sup>14</sup>, które automatycznie retweetują najważniejsze informacje zalewające Internet.

To nie jedyne właściwości mediów społecznościowych, które powodują, że są

<sup>12</sup> Portal internetowy Wikileaks został założony w 2006 roku przez Juliana Assange'a. Celem było umożliwienie publikowania anonimowo dokumentów rządowych i korporacyjnych bez narażenia się na reperkusje ze strony władz.

<sup>13</sup> Sławę platformie przyniosła publikacja tajnych informacji Pentagonu o wojnach w Iraku i Afganistanie oraz depech dyplomatycznych Departamentu Stanu.

<sup>14</sup> Bot to prosty program komputerowy, która wchodzi w zaprogramowaną interakcję na Twitterze.

to skuteczne narzędzia do szerzenia dezinformacji. Pierwszą cechą jest homofilia, czyli tzw. „upodobanie do podobieństwa”. Umożliwia ona ludziom gromadzenie się w wielkiej, podobnie myślącej grupie. W mediach społecznościowych polega na tym, że klikając „lubię to” lub „podziel się”, internauci wchodzi w interakcje i przekazują informacje o tym, co nas interesuje. Algorytmy mediów społecznościowych działają w ten sposób, że jeżeli użytkownicy reagują pozytywnie na jakąś treść, to zobaczą więcej podobnych informacji. W ten sposób tworzone jest środowisko ludzi zamykających się w „bańkach informacyjnych”. Użytkownik otrzymuje, a następnie przesyła innym informacje, które są zbliżone ideologicznie lub politycznie. Powstaje wrażenie, że poglądy użytkownika są wyznawane przez zdecydowaną większość, dlatego muszą być słuszne. Inne informacje, które mogą zaprzeczyć przekazywanej tezie, nie przenikają przez bańkę informacyjną (Singer, Brooking, 2019, s. 170–172). Analizując media społecznościowe, należy również wspomnieć o „efekcie potwierdzenia”. Najkrócej można to określić, że ludzie lubią mieć rację i nie znoszą sprzeciwu. Efektem pokazania ich błędów czy pomyłek jest to, że oponent jeszcze bardziej się opiera. Kombinacja homofilii i efektu potwierdzenia prowadzi do sytuacji, że każda grupa wierzy, że to ona ma rację, a cała reszta jest niedouczona i po prostu gorsza (Singer, Brooking, 2019, s. 173).

Media społecznościowe były wykorzystywane przez Rosjan nie tylko do publikowania wykradzionych informacji, ale również do tworzenia i rozpowszechniania fałszywych informacji czy targetowanych reklam politycznych (Report Of The Select Committee On Intelligence, 2019, Vol. 2, s. 3)<sup>15</sup>. Głównym podmiotem odpowiedzialnym za te działania była Agencja Badań Internetowych (Internet Research Agency – IRA) z siedzibą w Petersburgu, zwaną potocznie „fabryką trolli”<sup>16</sup>. Celem jej działań było tworzenia setek tysięcy kont w mediach społecznościowych, które podszywały się pod obywateli Stanów Zjednoczonych i rozpowszechniały skrajne, konfrontacyjne opinie polityczne, ideologiczne i społeczne oraz służyły do organizowania protestów w świecie realnym. Nacisk kładziono na kwestie społeczne dzielące Amerykanów, takie jak etniczność, imigracja czy posiadanie broni. Głównym celem było wywołanie negatywnych emocji i doprowadzenie do protestów oraz zwrócenie Amerykanów przeciwko sobie i rządowi (Report Of The Select Committee On Intelligence, 2019, Vol. 2, s. 6).

<sup>15</sup> Reklamy polityczne były publikowane bez informacji, kto jest ich autorem, co jest obowiązkowe przy reklamach politycznych w stacjach telewizyjnych w Stanach Zjednoczonych.

<sup>16</sup> Jej twórcą jest Jewgienija Pirożokina, bliska współpracowniczka Władimira Putina.

IRA na dużą skalę wykorzystwała również reklamy polityczne na Facebooku. Były one kierowane do konkretnych grup osób o różnych poglądach – od lewicowych, po prawicowe, ale również adresowane do grup zainteresowanych kontrowersyjnymi tematami, jak np. dostęp do broni czy prawa mniejszości, np. czarnoskórej. Poruszano również tematy, które budziły skrajne emocje, takie jak brutalność policji, kwestie islamu, prawo do samoobrony czy prawa człowieka. Osoby, które zostały zidentyfikowane jako religijne i o patriotycznym nastawieniu, dostawały informacje wspierające np. działania policji. Do społeczności Afroamerykanów adresowano reklamy, które sprzeciwiały się brutalności i rasizmowi policji. W Teksasie stawiano na promowanie ruchu secesjonistycznego. Celem takich działań było pogłębienie stereotypów, podziałów w społeczeństwie oraz zwiększanie nieufności do rządu federalnego. Część reklam nie była fałszywa oraz nie miała politycznego charakteru i dotyczyła innych popularnych kwestii. Działano w ten sposób, aby budować zasięgi oraz zwiększyć liczbę osób śledzących konta. Rosjanie utworzyli 120 stron, które wygenerowały ponad 80 tys. postów przez dwa lata. Posty te wyświetliły się w ramach News Feed Facebooka 29 mln Amerykanów. Facebook szacując „polubienia”, „udostępnienia” oraz „śledzenie”, doszedł do wniosku, że rosyjskie treści dotarły do 129 mln osób (Nimmo, 2018). Najpopularniejszymi historiami rozpowszechnianymi na tej platformie były fałszywa informacja o tym, że papież Franciszek udzielił poparcia Donaldowi Trumpowi, oraz historia, że Hillary Clinton sprzedawała broń do ISIS (Report Of The Select Committee On Intelligence, 2019, Vol. 2, s. 6).

IRA również udało się zaangażować nieświadomych Amerykanów do pomocy w celu podpisywania petycji czy udziału w różnych wydarzeniach, Rosjanie poprzez swoje fałszywe strony na Facebooku zorganizowali 129 różnych wydarzeń, które miały mieć miejsce w świecie rzeczywistym. Nie wiadomo dokładnie, ile z nich się odbyło, ale warto wspomnieć o jednym, szczególnie ważnym. W maju w 2016 roku w Houston w Teksasie odbyły się dwie manifestacje. Jedna, zorganizowana przez United Muslims of America, wspierała muzułmanów w Stanach Zjednoczonych. W tym samym miejscu urządzano kontrmanifestację. Doszło do konfrontacji, a obie grupy musiała rozdzielać policja. Po badaniach okazało się, że za organizacją tych wydarzeń stały dwie strony na Facebooku, które zostały utworzone przez Rosjan (Allbright, 2017).

Innym przykładem prób wpływania na amerykańskie społeczeństwo było wykorzystanie morderstwa Setha Richa, pracownika DNC. Rosyjskie sieci trolli

w Internecie szerzyły fałszywe informacje, jakoby Rich miał być whistleblowerem, który przekazał Wikileaks tajne dokumenty. Spreparowano nawet wypowiedź prominentnego członka Partii Republikańskiej Newta Gingricha, byłego spikera Izby Reprezentantów, który rzekomo miał powiedzieć, że Ritch został zamordowany. Organizacja FactCheck zajmująca się identyfikowaniem nieprawdziwych informacji wydała oświadczenie, że wypowiedź jest nieprawdziwa. Potrzebowała na to jednak czasu i fałszywa informacja została rozpowszechniona w Internecie i dotarła do Amerykanów (Jamieson, 2018, s. 26).

Inną platformą mediów społecznościowych wykorzystaną przez Rosjan był Twitter. Zidentyfikowano 36 tys. zautomatyzowanych rosyjskich kont, które wyprodukowały prawie półtora miliona unikalnych tweetów. Ponadto natrafiono na prawie 3 tys. kont obsługiwanych przez ludzi pochodzących z IRA i GRU (Report Of The Select Committee On Intelligence 2019, Vol. 2, s. 8). Konta te szerzyły rasistowskie, antymuzułmańskie i antyimigranckie treści oraz rozpowszechniały wykradzione przez hakerów informacje (House Permanent Select Committee on Intelligence, s. 35). Przykładowo Rosjanie stworzyli fałszywe konto na Twitterze Partii Republikańskiej ze stanu Tennessee. Konto to urosło do takich rozmiarów, że miało większą liczbę obserwujących niż oficjalne, autentyczne konto. Prawie 1,5 mln użytkowników Twittera było narażone na działalność rosyjskich trolli (Jamieson, 2018, s. 11). Platformy Google odgrywały o wiele mniejszą rolę. Na promocję ponad 1 tys. filmów, które trwały 43 godziny na 18 kanałach YouTube, wydano niewiele, bo tylko 5 tys. dolarów. Efekt był mizerny, jedynie 3% z nich cieszyło się oglądalności powyżej 5 tys. (House Permanent Select Committee on Intelligence, s. 35).

Poza mediami społecznościowymi ważną rolę odgrywały kontrolowane przez państwo rosyjskie telewizję RT i Sputnik, które szeroko omawiały wykradzione treści, ale również prezentowały Hillary Clinton jako kryminalistkę, która w przeszłości miała uniknąć pięciu zarzutów federalnych. Zarzucano jej również wspieranie ekstremistów islamskich. Kandydatka Partii Demokratycznej miała być również chora psychicznie i w przypadku wyboru na prezydenta doprowadzić do wojny między Rosją a USA (Office of the Director of National Intelligence, s. 4). Cały amerykański proces wyborczy był przedstawiony jako skorumpowany. W Stanach Zjednoczonych RT jest głównie oglądana na kanale YouTube, gdzie ma 3 mln subskrybentów. Ponadto należy również podkreślić, że treści RT i Sputnika były prezentowane Amerykanom przez przeglądarkę Google

jako wiarygodne źródła informacji, wyświetlane na równi z CNN, Fox News czy innymi mediami głównego nurtu (House Permanent Select Committee on Intelligence, s. 32). Od 2013 roku RT współpracowała blisko z Wikileaks, będąc jedynym rosyjskojęzycznym partnerem medialnym portalu założonego przez Juliana Assange'a i mając dostęp do najświeższych informacji. Bliska współpraca była również widoczna w 2016 roku, kiedy RT publikowało kompromitujące Hillary Clinton wiadomości pochodzące z Wikileaks (Office of the Director of National Intelligence, s. 3). W ramach bliskiej współpracy Julian Assange udzielał się jako komentator i uczestnik programów telewizyjnych, w których krytykował Stany Zjednoczone. Programy z jego udziałem o Hillary Clinton cieszyły się dużym powodzeniem. Obejrzało je ponad 9 mln użytkowników (Office of the Director of National Intelligence, 2017, s. 4).

### Podsumowanie

Rosjanie połączyli dawną taktykę użycia środków aktywnych z nowymi technologiami i ruszyli na nowe pole walki: cyberprzestrzeń. Rosyjskie ataki na wybory prezydenckie w 2016 roku były zaawansowaną, trwającą przez długi okres operacją. W jej ramach przeprowadzono działania hakerskie, których celem były partie polityczne w Stanach Zjednoczonych oraz najważniejsze osoby. IRA używając na dużą skalę mediów społecznościowych, szerzyła dezinformacje, które pogłębiały podziały w amerykańskim społeczeństwie. Celem Rosji było zwiększenie nieufności do liderów politycznych, pogłębienie podziałów w amerykańskim społeczeństwie, podważenie zaufania do procesu wyborczego, osłabienie instytucji federalnych oraz zaszkodzenie reputacji Stanów Zjednoczonych jako najstarszej i najstabilniejszej demokracji nowożytnego świata (Report Of The Select Committee On Intelligence, 2019, Vol. 1, s. 67).

Żaden raport instytucji federalnej nie odpowiedział na pytanie, czy zastosowanie środków aktywnych wpłynęło na wynik wyborów i zwycięstwo Donalda Trumpa. Pytanie to wciąż pozostaje bez odpowiedzi, ale na pewno rosyjskie działania wpłynęły na kształt kampanii (Nimmo, 2018). Były dodatkowym ciężarem dla zespołu Clinton, dały również dodatkową amunicję dla zespołu Donalda Trumpa. Fałszywe jest stwierdzenie, że to Rosjanie wybrali na prezydenta Donalda Trumpa, zrobili to Amerykanie, którzy jednak byli celem rosyjskich środków aktywnych. Należy wziąć pod uwagę to, że Hillary Clinton zabrakło do zwycięstwa 80 tys. głosów w trzech kluczowych stanach, a na operacje dezinformacyjne Rosjan

narażony było ponad 150 mln Amerykanów (Stone, Gordon, 2017).

Użycie środków aktywnych podczas wyborów prezydencki miało szereg konsekwencji i pozwoliło osiągnąć część celów, która są tożsame z polityką zagraniczną Rosji. Po pierwsze wybór Donalda Trumpa osłabił sojusz transatlantycki i zantagonizował relacje między państwami europejskimi i Stanami Zjednoczonymi. Plotki o wycofaniu się USA z NATO (Jones, 2019), określenie Unii Europejskiej jako przeciwnika przez Donalda Trumpa (Roth, Smith, 2019) czy słowa kanclerz Angeli Merkel o tym, że Europa nie może polegać już na Stanach Zjednoczonych, tylko to potwierdzają (Sharkov, 2019). Jednocześnie znacznie pogorszył się odbiór Stanów Zjednoczonych wśród społeczeństw Europy, Afryki i Ameryki Łacińskiej (Wike *et al.*, 2018). W Wielkiej Brytanii, która jest najstarszym sojusznikiem USA na starym kontynencie, ponad kilkadziesiąt tysięcy osób protestowało przeciwko wizycie Trumpa (Johnson, 2019). Żaden amerykański prezydent nie powodował tak negatywnych reakcji.

Być może jednak największym sukcesem rosyjskich operacji było zakorzenienie w świadomości Amerykanów przekonania, że ich prezydent został wybrany przez interwencję obcego mocarstwa. Prawie połowa Amerykanów wierzy, że prezydent Trump był w zмовie z Rosjanami (Kahn, 2018). Sytuacja ta utrudnia dialog polityczny pomiędzy dwoma stronami sporu: Partią Republikańską i Partią Demokratyczną<sup>17</sup>. Ponadto wybór tak kontrowersyjnej osoby, jaką jest Donald Trump, pogłębił również podziały społeczne i etniczne w Stanach Zjednoczonych. Jest to oczywiście dłuższy proces i nie trwa od 2016 roku, ale wybór osoby na prezydenta, która słynie z rasistowskich i szowinistycznych komentarzy, pogłębił to zjawisko. Biorąc pod uwagę, że celem rosyjskich środków aktywnych zawsze było szerzenie chaosu u przeciwnika, można powiedzieć, że udało im się tego dokonać, a skutki ingerencji w 2016 roku Amerykanie odczuwają do dzisiaj.

## Bibliografia

- Allbright, C. (2017, November 1). A Russian Facebook page organized a protest in Texas. A different Russian page launched the counterprotest. *The Texas Tribune*. Dostęp: <https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-1/> [11.08.2019].
- Andrew, Ch., Mitrochin, W. (2013). *Archiwum Mitrochina*. Poznań: Wydawnictwo Rebis.

<sup>17</sup> Ostatnio obie partie podzieliło wszczęcie przez Izbę Reprezentantów śledztwa w sprawie potencjalnego impeachmentu Trumpa. Wcześniej obie strony nie potrafiły dojść do porozumienia w sprawie ustawy wzmacniającej bezpieczeństwo wyborów przed obcą ingerencją. Republikanie ją zablokowali.



- Boghardt, T. (2009). Soviet Bloc Intelligence and Its AIDS Disinformation Campaign. *Studies in Intelligence*, 53(4), 1–24. Dostęp: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/soviet-bloc-intelligence-and-its-aids.html> [10.08.2019].
- Darczewska, J. (2018). Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy. *Przegląd Bezpieczeństwa Wewnętrznego*, 10(18), 40–67. Dostęp: <https://www.abw.gov.pl/pl/pbw/publikacje/przegląd-bezpieczenstwa-10/1411,Przegląd-Bezpieczenstwa-Wewnetrznego-nr-18-10-2018.html> [30.09.2019].
- Darczewska, J., Żochowski, P. (2017). *Środki Aktywne. Rosyjski towar eksportowy* (Punkt Widzenia 64). Warszawa: Ośrodek Studiów Wschodnich. Dostęp: [https://www.osw.waw.pl/sites/default/files/pw\\_64\\_pl\\_srodki\\_aktywne\\_net.pdf](https://www.osw.waw.pl/sites/default/files/pw_64_pl_srodki_aktywne_net.pdf) [30.09.2019].
- Galante, L., Ee S. (2018, September 11). *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents*. Washington: Atlantic Council. Dostęp: [https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining\\_Russian\\_Election\\_Interference\\_web.pdf](https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining_Russian_Election_Interference_web.pdf) [16.08.2019].
- Gliwa, S. (2019, 6 sierpnia). Polska poligonem doświadczalnym walki informacyjnej? *CyberDefence24*. Dostęp: <https://www.cyberdefence24.pl/polska-niemoc-w-walce-z-fake-news-analiza> [7.08.2019].
- House Permanent Select Committee on Intelligence. (2018, March 22). *Report on Russian Active Measures*. Dostęp: [https://docs.house.gov/meetings/IG/IG00/20180322/108023/HRPT-115-1\\_1-p1-U3.pdf](https://docs.house.gov/meetings/IG/IG00/20180322/108023/HRPT-115-1_1-p1-U3.pdf) [22.11.2019].
- Isikoff, M., Corn, D. (2018). *Rosyjska ruletka. Jak Putin zhakował Amerykę i wygrał wybory za Donalda Trumpa*. Warszawa: Wydawnictwo Agora.
- Jamieson, H.K. (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know*. New York: Oxford University Press.
- Johnson, J. (2019, June 4). *Tens of Thousands Flood Streets in UK to Protest Trump and 'Everything He Stands For'*. Dostęp: <https://www.commondreams.org/news/2019/06/04/tens-thousands-flood-streets-uk-protest-trump-and-everything-he-stands> [11.08.2019].
- Jones, T. (2019, August 9). US threatens to withdraw troops from Germany. *Deutsche Welle*. Dostęp: <https://www.dw.com/en/us-threatens-to-withdraw-troops-from-germany/a-49959555> [11.08.2019].
- Kahn, Ch. (2019, March 26). Despite report findings, almost half of Americans think Trump colluded with Russia: Reuters/Ipsos poll. *Reuters*. Dostęp: <https://www.reuters.com/article/us-usa-trump-russia-poll/despite-report-findings-almost-half-of-americans-think-trump-colluded-with-russia-reuters-ipsos-poll-idUSKCN1R72S0> [18.08.2019].
- Klare, T. M. (2017, February 14). China First, Russia Second, America Third: Trump's Real Foreign Policy. *The Nation*. Dostęp: <https://www.thenation.com/article/china-first-russia-second-america-third-trumps-real-foreign-policy/> [11.08.2019].
- Kozłowski, A. (2018, 17 września). Środki aktywne – cyfrowa broń Kremla [Security Case Study 2018]. *CyberDefence24*. Dostęp: <https://www.cyberdefence24.pl/srodki-aktywne--cyfrowa-bron-kremla-security-case-study-2018> [30.07.2019].
- Murray, S. (2018, July 16). Putin: I wanted Trump to win the election. *Politico*. Dostęp: <https://www.politico.com/story/2018/07/16/putin-trump-win-election-2016-722486> [24.10.2019].

- Newman, H. L. (2018, March 25). Yes, Even Elite Hackers Make Dumb Mistakes. *Wired*. Dostęp: <https://www.wired.com/story/guccifer-elite-hackers-mistakes/?verso=true> [18.08.2019].
- Nimmo, B. (2018, February 27). #ElectionWatch: Beyond Russian Impact. *Atlantic Council's Digital Forensic Research Lab (DFRLab)*. Dostęp: <https://medium.com/dfrlab/electionwatch-beyond-russian-impact-2f5777677cc0> [11.08.2019].
- Office of the Director of National Intelligence. (2017, January 6). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Dostęp: [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf) [22.11.2019].
- Office of the Press Secretary of Department of Homeland Security. (2017, January 6). *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector*. U.S. Department of Homeland Security. Dostęp: <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical> [22.11.2019].
- Report of The Select Committee On Intelligence United States Senate On Russian Active Measures Campaigns And Interference In The 2016 U.S. Election. (2019). *Russian Efforts Against Election Infrastructure with Additional Views* (vol. 1, Report 116-XX, 116<sup>th</sup> Congress). Dostęp: [https://www.intelligence.senate.gov/sites/default/files/documents/Report\\_Volume1.pdf](https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf) [22.11.2019].
- Report of The Select Committee On Intelligence United States Senate On Russian Active Measures Campaigns And Interference In The 2016 U.S. Election. (2019). *Russia's Use Of Social Media With Additional Views* (vol. 2, Report 116-XX, 116<sup>th</sup> Congress). Dostęp: [www.intelligence.senate.gov/sites/default/files/documents/Report\\_Volume2.pdf](http://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf) [22.11.2019].
- Roth, A., Smith, D. (2018, July 15). Trump calls European Union a 'foe' – ahead of Russia and China. *The Guardian*. Dostęp: <https://www.theguardian.com/us-news/2018/jul/15/donald-trump-vladimir-putin-helsinki-russia-indictments> [11.08.2019].
- Selvage, D., Nehring, Ch. (2019, July 22). *Operation "Denver": KGB and Stasi Disinformation regarding AIDS*. Washington: Wilson Center. Dostęp: <https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids> [7.08.2019].
- Sharkov, D. (2018, October 5). Angela Merkel: Europe Can No Longer Rely On U.S. Protection. *Newsweek* (U.S. Edition). Dostęp: <https://www.newsweek.com/europe-cannot-fully-rely-us-protection-anymore-says-germanys-merkel-919410> [11.08.2019].
- Shawn, E. (2018, 8 April). Russian 'hack' of 2016 voter rolls leaves Galesburg, Illinois, reeling. *Fox News*. Dostęp: <https://www.foxnews.com/politics/russian-hack-of-2016-voter-rolls-leaves-galesburg-illinois-reeling> [16.08.2019].
- Singer, W.P., Brooking, T.E. (2019). *Nowy rodzaj wojny. Media społecznościowe jako broń*. Kraków: Vis-à-vis. Etiuda.
- Stone, P., Gordon, G. (2017, July 12). *Trump-Russia investigators probe Jared Kushner-run digital operation*. Dostęp: <https://www.mcclatchydc.com/news/nation-world/national/article160803619.html> [11.08.2019].
- United States Department of State. (1987). *Soviet Influence Activities: A Report on Active Measures and Propaganda 1986–87*. Washington: U. S. Department of State. Dostęp: <https://www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf> [22.11.2019].

- Whittaker, Z. (2019, April 18). *Mueller report sheds new light on how the Russians hacked the DNC and the Clinton campaign*. Dostęp: <https://techcrunch.com/2019/04/18/mueller-clinton-arizona-hack/> [16.08.2019].
- Wike, R., Stokes, B., Poushter, J., Silver, L., Fetterolf, J., Devlin, K. (2018). *Trump's International Ratings Remain Low, Especially Among Key Allies*. Washington: Pew Research Center. Dostęp: [https://www.pewresearch.org/global/wp-content/uploads/sites/2/2018/10/Pew-Research-Center\\_U-S-Image-Report\\_UPDATED\\_2018-10-01.pdf](https://www.pewresearch.org/global/wp-content/uploads/sites/2/2018/10/Pew-Research-Center_U-S-Image-Report_UPDATED_2018-10-01.pdf) [11.08.2019].
- Wines, M. (2019, April 18). *Russians Breached Florida County Computers Before 2016 Election, Mueller Report Says*. *The New York Times*. Dostęp: <https://www.nytimes.com/2019/04/18/us/florida-russia-2016-election-hacking.html> [16.08.2019].