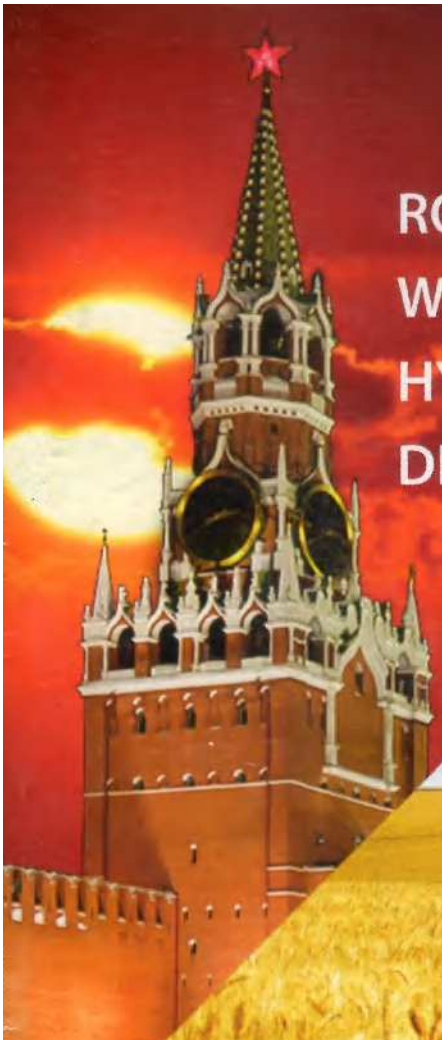
ROSYJSKA INGERENCJA W WYBORY: HYBRYDOWE ZAGROŻENIA DLA DEMOKRACJI



Anatoliy Kruglashov
Sergii Shvydiuk

Czernicwce 2019

ROSYJSKA INGERENCJA W WYBORY: HYBRYDOWE ZAGROŻENIA DLA DEMOKRACJI

Profesor, dr hab. **Anatoliy Kruglashov**
Kierownik Katedry Politologii i Zarządzania Publicznego
Czerniowiecki Uniwersytet Narodowy imienia Jurija Fedkowicza
Dr **Sergii Shvydiuk**
Docent Katedry Politologii i Zarządzania Publicznego
Czerniowiecki Uniwersytet Narodowy imienia Jurija Fedkowicza

e-mail: sershvyd@gmail.com

Wydrukowane20.03.2019
Odpowiedzialny za wydanie Anatoliy Kruglashov
Nakład 50 cop.

Tłumaczenie Sergii Shvydiuk

Czerniowce 2019

ROSYJSKA INGERENCJA W WYBORY: HYBRYDOWE ZAGROŻENIA DLA DEMOKRACJI

Atak Rosji na porządek światowy, utworzony po II wojnie światowej, rozpoczął się za długo przed aneksją Krymu i rozpoczęciem wojny na wschodzie Ukrainy w 2014 roku. Próby Kremla o przywrócenie Rosji statusu najpierw lidera regionalnego w Eurazji, a następnie – państwa o znaczeniu światowym, doprowadziły do wielopoziomowej polityki rewizjonistycznej Moskwy. W szczególności odrzucenie przez Putina w 2007 r. idei zbliżenia Ukrainy a NATO[1] było publicznym roszczeniem o rzeczywiste nakreślenie linii, określających obszary rosyjskich interesów w Europie, o które Rosja gotowa walczyć wszelkimi środkami. W tym czasie to zachowanie Putina otrzymało obojętność lub ugodową reakcję wielu przywódców światowych, co zostało potraktowane przez niego za dogodną okazję do podjęcia kolejnego kroku. I czekanie na ten krok nie trwało długo.

Już w sierpniu 2008 roku Rosja udała się do działań wojennych przeciwko Gruzji. I znowu reakcja Europejczyków była w większości powolna, tylko Stany Zjednoczone zareagowały nieco mocniej. W tym czasie jednak „kolektywny Zachód" nie był przygotowany do odpowiedniej reakcji na coraz bardziej agresywną politykę rosyjską. Dla rosyjskich elit politycznych i urzędników bezpieczeństwa państwa to stanowisko potwierdziło wiarę w ich zdolność do powrotu Rosji z międzynarodowej peryferii politycznej do centrum światowego systemu. Nie mając godnych i konstruktywnych sugestii dla partnerów w krajach postsowieckich, zarówno w wymiarze gospodarczym, technologicznym, bezpieczeństwa czy jakimkolwiek innym, Rosja przeszła z kuszących obietnic perspektywy integracji euroazjatyckiej na coraz bardziej sztywny kurs[2], a następnie do zniszczenia ustalonych zasad polityki międzynarodowej, demontażu mechanizmów ich przestrzegania i gwarancji bezpieczeństwa.

Naszym zdaniem wiodącą ideą takiej polityki była bezkompromisowa odmowa Rosji grać zgodnie z ogólnie przyjętymi zasadami, zamiast narzucanie własnych zasad gry wszędzie gdzie były sprzyjające warunki. Aby osiągnąć te

---

[1] Выступление и дискуссия на Мюнхенской конференции по вопросам политики безопасности. 10 февраля 2007 года, [електронний ресурс], http://kremlin.ru/events/president/transcripts/24034

[2] Мельничук Ігор, Інтеграційні проекти Російської Федерації на пострадянському просторі. – Чернівці: Рута, 2015. – 400 с.

cele, wykorzystano cały arsenał środków – od szantażu energetycznego i ukierunkowanej propagandy do użycia siły na terytorium innych państw.

Po aneksji Krymu i początku rosyjskiej agresji przeciwko Ukrainie do dyskursu publicystycznego a później i naukowego weszło pojęcie "wojny hybrydowej". Ten temat obecnie jest energicznie dyskutowany w literaturze naukowej ze względu na jego znaczenie nie tylko dla poszczególnych krajów, ale także dla bezpieczeństwa międzynarodowego na ogół. Wojna hybrydowa różni się od zwykłej wojny tym, że dla osiągnięcia przewagi nad rywalem są wykorzystane nie tylko, a czasem nie tyle metody militarne, ile informacyjne operacje wywrotowe i propagandowe. Także destrukcyjny wpływ na opinię publiczną, poparcie polarnych sił politycznych i radykalnych ruchów społecznych, ingerencja w sieci komputerowe organów państwowych i firm prywatnych, wykorzystanie instrumentów wpływu w organizacjach międzynarodowych, sieci społecznościowe i inne środki. Wśród ważnych celów takiej wojny jest aspiracja podzielenia i osłabienia NATO, zmiana prozachodnich rządów, stworze pretekstu dla wojny, zajęcie terytoriów, uzyskanie dostępu do rynków europejskich na własnych warunkach[3] etc. Takie działania mają na celu wewnętrzne osłabienie kraju przeciwnika, sprowokowanie kryzysów politycznych i społecznych, podzielenie społeczeństwa, do którego jest kierowana agresja hybrydowa. A w przypadku Ukrainy – stworzenie warunków dojścia do władzy lojalnych wobec Kremla lub otwarcie prorosyjskich sił.

Środowiskiem hybrydowego wpływu przede wszystkim występuje wewnętrzna przestrzeń informacyjna państwa i społeczeństwa obywatelskiego, funkcjonujących w ramach demokratycznego systemu politycznego. W ostatnich latach okazało się, że mianowicie demokratyczne instytucje, zasady i procedury, wartości i normy zachowania politycznego zostały zagrożone podważaniem ich witalności i skuteczności metodami hybrydowymi. W ten sposób podstawowe wolności demokratyczne – słowa, myśli, zrzeszania się, zgromadzenia – zostały systematycznie wykorzystywane dla rozprzestrzeniania "fake newsów" i dezinformacji, tworzenia destrukcyjnych organizacji i grup, do prowadzenia

[3] Chivvis Christopher S. Understanding Russian "Hybrid Warfare" and What Can be Done About it, Testimony of Chistopher S. Chivvis. The Rand Corporation. Before the Committee of Armed Services United States House of Representative, p. 1., [електронний ресурс], https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

prowokacyjnych, a często jawnie bezprawnych działań. W istocie, rozpoczęło się hybrydyczne pasożytnictwo na strukturach nośnych demokracji dla zniszczenia jej od wewnątrz, uniemożliwienia jej prawidłowego funkcjonowania.

Jednym z priorytetowych kierunków stosowania rosyjskich wysiłków hybrydowych została instytucja wyborów i procesy wyborcze, które w demokratycznym systemie politycznym i w demokratycznym reżimie politycznym zapewniają wyraz woli obywateli i kształtowanie legalnej władzy, obieg i odnowienie elity politycznej, określenie strategicznego kierunku rozwoju społeczeństwa i agendy władz. Dlatego kompromitowanie i dyskredytowanie procesu wyborczego, zniekształcanie wyników rzeczywistego wyrazu woli obywateli lub doprowadzanie do władzy pożądanych kandydatów wyraźnie wpisuje się w logikę „wojny hybrydowej".

W praktyce systematyczna ingerencja Rosji w wybory w różnych krajach stała się prawdziwym instrumentem osiągnięcia celów hybrydowych.

Na przykład podczas przedterminowych wyborów prezydenckich na Ukrainie w dniu 25 maja 2014 r. rosyjski propagandowy „Pierwszy kanał" poinformował o zwycięstwie Dmytra Jarosza, w tym czasie szefa „Prawego Sektora".

Rosyjskie media wykorzystały hipertroficzny obraz tej organizacji jako narzędzie demonizowania wizerunku porewolucyjnej Ukrainy, pokazując w niej zwycięstwo prawicowych radykalnych sił i zastraszając nimi tako własnych odbiorców jako i zagranicznych konsumentów rosyjskich mediów propagandowych[4]. W rzeczywistości kandydat ten zdobył mniej niż jeden procent głosów wyborców. Jednocześnie pojawienie się tej wiadomości poprzedził cyberatak na stronę Ukraińskiej Centralnej Komisji Wyborczej (CKW), który spowodował tymczasową awarię w jej pracy. I chociaż ten atak został rzekomo przeprowadzony w Ukrainie przez prorosyjską grupę „CyberBerkut", na razie nie ulega wątpliwości skąd dokładnie pochodziło

[4] Świątkowska, Joanna. Działania prowadzone w cyberprzestrzeni jako metoda ingerencji w demokratyczny proces wyborczy // Walka informacyjna : uwarunkowania, incydenty, wyzwania / pod redakcją naukową Hanny Batorowskiej. - Kraków : Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją, 2017. - S.258, [електронний ресурс], http://hdl.handle.net/11716/2031

polecenie na atak[5]. Niemal synchroniczna transmisja informacji o zwycięstwie D. Yarosha na kanale rosyjskim i faktyczna ingerencja w system informacyjny CKW Ukrainy pokazały, że takie fałszywe wiadomości to nie tylko praca propagandystów i grafików rosyjskiego kanału telewizyjnego. Jednoznacznym jest wniosek , że w ten sposób Rosja wykazała szczególne zainteresowanie wywieraniem wpływu na wybory ukraińskie i próbowała manipulować informacjami o ich przebiegu i wynikach.

Oczywiście że Ukraina nie była jedynym krajem docelowym takich ataków. Ich systematyczny charakter i niemal globalna geografia rozprzestrzeniania spowodowały coraz większe zaniepokojenie oraz potrzebę przestudiowania tego niebezpiecznego zjawiska i opracowania środków przeciwdziałania im przez zagrożone państwa. W związku z tym w listopadzie 2018 r. ogłoszono Raport ogólny Komitetu Nauki i Technologii Zgromadzenia Parlamentarnego NATO „Rosyjska ingerencja w wybory i referenda w Sojuszu"[6]. W tym Raporcie, opartym o wiele źródeł, podano informacje na temat ingerencji Rosji w proces wyborczy co najmniej pięciu państw członkowskich NATO w ciągu ostatnich kilku lat, w szczególności w wybory prezydenckie w USA w 2016 roku, referendum w sprawie Brexitu w 2016 roku i wybory powszechne w 2017 roku w Wielkiej Brytanii, w wybory francuskiego prezydenta w 2017 roku, wybory parlamentarne w Niemczech w 2017 roku i referendum w sprawie statusu Katalonii w 2017 roku.

Rosja wykorzystała zatem dość jednolity schemat: nieupoważniona ingerencja w sieci komputerowe partii politycznych i struktur rządowych; złamanie osobistej i zawodowej poczty elektronicznej, kradzież danych osobowych; systemowy wyciek skradzionych informacji wraz z masowym rozpowszechnianiem w mediach społecznościowych za pomocą botów, trolli i innych środków.

---

[5] Galante, Laura & Ee Shaun, Defining Russian Election Interference: an Analysis of Select 2-14 to 2018 Cyber Enabled Incidents. Atlantic Council, Scowcroft Center for Strategy and Security, September 2018, p. 7.

[6] Russian Meddling in Elections and Referenda in the Alliance. General Report by Susan DAVIS (United States) General Rapporteur - 181 STC 18 E fin. 11 November 2018, [електронний ресурс], https://www.nato-pa.int/sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSIAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf

Zdaniem mówcy Zgromadzenia, Susan Davis, Rosja interweniuje w wybory innych państw realizując następujące cele:

• zaostrzenie już istniejących napięć społecznych w społeczeństwach tych krajów;

• podważanie zaufania obywateli do liberalnych instytucji demokratycznych;

• promowanie osobowości i grup politycznych postrzeganych jako dostępne dla rosyjskich wpływów oraz dyskredytowanie tych, którzy są traktowane jako wrogo nastawieni;

• tworzenie atmosfery chaosu i niepewności w krajach zachodnich[7].

Konkretne cele interwencji rosyjskiej różnią się w zależności od okoliczności i nie są wzajemnie wykluczone. Zwłaszcza, interwencja Rosji ma na celu wzmocnienie wcześniejszych społecznych i politycznych napięć w społeczeństwie. Gdziekolwiek pojawiło się podejrzenie rosyjskiej interwencji, hakerzy i trolle wykazali się dość dobrym zrozumieniem niepokojącego nastroju, który dzieli kraj. W Stanach Zjednoczonych rosyjscy agenci publikowali płatne reklamy, które podburzyły religijne i polityczne sprzeczności podważające społeczeństwo obywatelskie. W Niemczech rosyjskie botnety wykorzystywały problem polityki uchodźców, próbując osłabić pozycję kanclerz Angeli Merkel i podważyć zaufanie do jej kursu politycznego. W Hiszpanii rosyjskie media i botnety gorliwie wspierały zwolenników katalońskiego separatyzmu[8]. Ze swej natury rosyjska interwencja uwzględnia i wykorzystuje istniejące linie pęknięć w społeczeństwach różnych krajów i zaostrza sprzeczności między różnymi grupami społecznymi, politycznymi lub etnicznymi maksymalizując istniejące wady.

Najgłośniejszy przypadek rosyjskiej interwencji – wybory prezydenckie w USA w 2016 roku. W tym kontekście naukowcy wyróżniają cztery główne obszary wpływu: kradzież informacji; selektywne rozpowszechnianie informacji; kampania propagandowa; wreszcie próby zepsucia systemu głosowania w całym kraju[9]. Wydarzeniom tym towarzyszyła skoordynowana krok po kroku kampania w mediach społecznościowych. Z ich pomocą przeprowadzano wycieki

---

[7] Ibid., p. 2.

[8] Ibid.

[9] Van De Velde. J. The Law of Cyber Interference in Elections. Available at SSRN 3043828 (2017)., p.10., [електронний ресурс], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828

informacyjne, rozpowszechniano fałszywe historie w celu delegitymizacji rządu USA.

W szczególności podczas kampanii wyborczej USA latem 2016 roku WikiLeaks opublikowało skradzione dokumenty elektroniczne Partii Demokratycznej. Założyciel WikiLeaks, Julian Assange przyznał się że ten wyciek próbuje uniemożliwić Hillary Clinton wygranie wyborów[10]. Według amerykańskich służb wywiadowczych odpowiedzialnymi za cyberataki, w tym te które doprowadziły do kradzieży dokumentów Partii Demokratycznej, są dwie grupy hakerów związane z Rosją, mianowicie Fancy Bear i Cozy Bear.

Tak więc we wspólnym oświadczeniu Departamentu Bezpieczeństwa Wewnętrznego i Biura Dyrektora Wywiadu Narodowego ds. Bezpieczeństwa Wyborczego z dnia 7 października 2016 roku. stwierdzono że „publikacja na stronach internetowych, takich jak DCLeaks.com i WikiLeaks, skradzionych e-mailów, a także działalność online postaci Guccifer 2.0, są zgodne z metodami i motywacją Rosjan. Dlatego te kradzieże i ujawnienie mają na celu zakłócenie procesu wyborczego w USA" [11].

W dniu 29 grudnia 2016 r. Departament Bezpieczeństwa Narodowego i Federalne Biuro Śledcze Stanów Zjednoczonych wydały wspólną analizę szczegółów technicznych narzędzi wykorzystywanych przez rosyjskich cywilów i służby wywiadowcze dla cyber-uszkodzenia komputerów i sieci wyborczych w Stanach Zjednoczonych, a także rządu USA, podmiotów politycznych i prywatnych[12].

Według amerykańskich organów ds. Bezpieczeństwa cybernetycznego działania rosyjskich grup hakerskich były skierowane w rząd i obywateli USA, w tym agencje rządowe, obiekty infrastruktury krytycznej, think tanki,

---

[10] Charlie Savage. Assange, Avowed Foe of Clinton, Timed Email Release for Democratic Convention. New York Times (JULY 26, 2016), [електронний ресурс], https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html

[11] Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. Release Date: October 7, 2016, [електронний ресурс], https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

[12] GRIZZLY STEPPE – Russian Malicious Cyber Activity. December 29, 2016. Reference Number: JAR-16-20296A, [електронний ресурс], https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

uniwersytety, organizacje polityczne i korporacje w celu kradzieży informacji. Jednocześnie ataki hakerów zostały zamaskowane jako działalność osób trzecich, w tym fałszywych postaci online, na przykład Guccifer 2.0, aby ukryć źródło ataku przed ofiarą i zwiększyć wiarygodność odbiorców takich informacji.[13].

Amerykański ekspert ds. Bezpieczeństwa cybernetycznego Dave Aitel uważa, że publikacja plików skradzionych przez rosyjskie służby specjalne w celu ingerencji z zewnątrz w wybory prezydenckie odpowiada definicji aktu cyberwojny.[14]. Według Michaela Jensena taka działalność rosyjskich trolli została dobrze przemyślana nie tylko jako atak informacyjny na Stany Zjednoczone, ale także jako kampania propagandowa przeciwko temu państwu. Autor potwierdza to swoją analizą 20348 tweetów utworzonych między 14 lipca 2014 a 26 września 2017 roku, wskazując również, że 2752 profile w Twitter są związane z działalnością rosyjskiej Agencji Badań Internetowych[15], znanej jako „fabryka trolli".

Z kolei rosyjscy urzędnicy zaprzeczali wszelkie zarzuty manipulacji i prób ingerowania w życie polityczne Stanów Zjednoczonych. Jednak te odrzucenia nie przekonały Waszyngtonu, który wprowadził nowe antyrosyjskie sankcje związane z ingerencją w kampanię prezydencką. W ich ramach Stany Zjednoczone wysłały 35 rosyjskich dyplomatów z kraju.[16].

W wyniku dalszych badań na Facebooku znaleziono co najmniej 120 sfałszowanych rosyjskich kont rozprzestrzeniających wiadomości, obejmując ponad 29 milionów obywateli amerykańskich. Strony te próbowali zorganizować 129 prawdziwych wydarzeń offline oznaczonych przez 33 800 osób w Stanach

---

[13] Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. Release Date: October 7, 2016, [електронний ресурс], https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

[14] Dave Aitel. Guest editorial: The DNC hack and dump is what cyberwar looks like. Ars Technica (Jun 17, 2016), [електронний ресурс], https://arstechnica.com/information-technology/2016/06/guest-editorial-the-dnc-hack-and-dump-is-what-cyberwar-looks-like/

[15] Jensen, Michael. "RUSSIAN TROLLS AND FAKE NEWS: INFORMATION OR IDENTITY LOGICS?" *Journal of International Affairs*, vol. 71, no. 1.5, 2018, p. 118, *JSTOR*, [електронний ресурс], www.jstor.org/stable/26508125.

[16] Obama expels 35 Russian diplomapts in retaliation for US election hacking, [електронний ресурс], https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack

Zjednoczonych. Chociaż informacji o tym, ile z tych wydarzeń zostało przeprowadzone i ile osób w nich uczestniczyło, nie ma.

Od stycznia 2018 r. na Twitterze znaleziono co najmniej 50258 rosyjskich kont, zawierających informacje dotyczące wyborów w USA[17].

Problemy rosyjskiej ingerencji w wybory prezydenckie w USA w rzeczywistości nie warto ograniczać „niezamawianą pomocą" dla obywateli amerykańskich aby rozwiązać dylemat wyboru pomiędzy D. Trampem a H. Clinton. Amerykańscy politycy wciąż debatują, o ile ta interwencja przyczyniła się do zwycięstwa urzędującego prezydenta. Poglądy na ten temat zależą w dużym stopniu od identyfikacji partyjnej. Tak, Demokraci i ich zwolennicy przywiązują dużą wagę do konsekwencji tej ingerencji w wyniki wyborów. Zamiast tego, wśród Republikanów bardziej rozpowszechniona tendencja do łagodzenia jego skutków. Takie partyjne ograniczenie debaty uniemożliwia Amerykanom ocenę, że jeśli wysiłki strony rosyjskiej na rzecz D. Trumpa do pewnego stopnia wpłynęli na amerykańskich wyborców, wówczas to stosunkowo krótkoterminowe działanie miało niższą skalę i negatywne skutki przed innymi bardziej destrukcyjnymi konsekwencjami takiej ingerencji. Wśród nich jest rozczarowanie wyborców wynikami wyborów, ich demokratycznym charakterem i samym amerykańskim systemem politycznym[18].

W Wielkiej Brytanii wykorzystano rozpowszechnianie dezinformacji, wpływ propagandowy na wyborców przez manipulowanie informacjami w mediach społecznościowych. W przeddzień i podczas referendum w sprawie Brexitu Rosjanie używali setki kont na Twitterze i na Facebooku, a także botnetów dla rozpowszechniania tysięcy wiadomości ze wzmianką o Brexitu[19].

We Francji, w przededniu wyborów prezydenckich, przeprowadzono masowe ataki na sieci komputerowe kandydata E. Macrona i jego partii politycznej, a 36 godzin przed wyborami opublikowano dziewięć gigabajtów skradzionych informacji w celu szkodzić temu kandydatowi. Wśród opublikowanych oryginalnych dokumentów znalazły się także liczne sfałszowane, które musiały zasiać wątpliwości i dezinformację wśród francuskich

[17] Russian Meddling in Elections and Referenda in the Alliance..., p. 5.

[18] Tomz Michael & Weeks Jessika L.P. Public Opinion and Foreign Electoral Intervention, p. 24–26., [електронний ресурс], https://web.stanford.edu/~tomz/working/TomzWeeks-ElectoralIntervention-2018-08-24.pdf

[19] Russian Meddling in Elections and Referenda in the Alliance..., p.7.

wyborców. Dzięki internetowym botom, skrajnie prawicowym aktywistom i WikiLeaks informacje te szybko rozprzestrzeniły się online[20]. Jednak w tym przypadku atak na kandydata na prezydenta Emanuela Macrona nie doprowadził do wyników pożądanych przez jego organizatorów i on zdobył znaczną przewagę w głosach nad przeciwnikiem[21].

W Niemczech interwencja polegała na zainfekowaniu komputerów rządowych trojanami wirusowymi i kradzieży dużej ilości informacji[22]. Rozprzestrzeniane przez tak zwane trolle Kremlowskie dezinformację oraz zniekształcone informacje przyczyniły się do osłabienia pozycji A. Merkel i jej popierających partii politycznych. I odwrotnie, zapewniły bezprecedensowy sukces wyborczy niemieckiej ultra-prawicy.

W Hiszpanii rozpowszechnianie informacji separatystycznych i wezwań do oddzielenia Katalonii również związane z działalnością rosyjskich botnetów. Pośrednim dowodem na to była niezwykle duża liczba repostów wiadomości rosyjskich agencji informacyjnych Russian Today i Sputnik przez konta wenezuelskie i anonimowe[23].

Wpływ na wyraz woli w Holandii związany z próbą Rosji przesunąć uwagę publiczną w sprawie dochodzenia rosyjskiego zaangażowania w zniszczenie lotu MH17 i wpływania na wyniki referendum w sprawie ratyfikacji Umowy o stowarzyszeniu między Ukrainą a UE w kwietniu 2016 roku. W tym przypadku dla wpływu na lokalną debatę polityczną Rosja oprócz elektronicznych kanałów rozpowszechniania informacji, stosowała również oczne metody, na przykład przez fałszywych osób przedstawiających z siebie Ukraińców[24].

---

[20] Ibid., p. 8.

[21] How France successfully countered Russian interference during the presidential election, EURACTIV, [електронний ресурс], https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/

[22] Stelzenmuller Constantine, The impact of Russian Interference on Germany's 2017 Elections, Testimony before U.S. Senate Select Committee on Intelligence, Wednesday, June 28, 2017, [електронний ресурс], https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections

[23] Alandete David. Russian Network Used Venezuelan Accounts to Deepen Catalan crisis, El Pais, 11 November 2017, [електронний ресурс], https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html

[24] Brattberg Erik, Maurer, Tim. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks, Carnegie Endowment for International Peace, 2018,

Biorąc pod uwagę ostrzeżenia służb specjalnych o potencjalnym zagrożeniu związanym z ingerencją Rosji w systemy informacyjne i wyborcze, władze holenderskie podjęły szereg środków zapobiegawczych. W szczególności zrezygnowali z elektronicznego głosowania i automatycznego liczenia głosów, a także zakazały urzędnikom komisji wyborczych korzystania z poczty elektronicznej i urządzeń pamięci masowej USB. W wyniku wybory Holenderskie 2017 roku nie doświadczyły znaczącego wpływu ze strony Rosji[25].

Ogólnie obraz ingerencji Rosji w wybory miał dość typowy wzór. Najpierw partie polityczne lub instytucje państwowe zgłaszali o nieuprawnionej ingerencji w ich sieci, kompromitacji poczty elektronicznej i kradzieży danych osobowych. Następnie skradzione dane wyciekły i rozprzestrzeniły się za pośrednictwem sieci społecznościowych i botów, a później te wycieki zostali wykorzystywane przez tradycyjne media do publikowania najbardziej sensacyjnych danych.

W tym samym czasie „zbiorniki drenażowe" (media publikujące niezweryfikowane informacje), powiązane lub kontrolowane przez władze rosyjskie, publikowały pomyłkowe lub fałszywe historie, zachęcając do spolaryzowanych dyskusji i prowokując myślenie spiskowe.

Susan Davis podsumowuje, ponieważ rosyjskie kierownictwo wykorzystało wolność słowa i prasy do delegitymizacji instytucji demokratycznych w państwach członkowskich NATO, „nie ma wątpliwości, że udział Rosji w takich operacjach będzie kontynuowany w najbliższej przyszłości"[26]. Uważamy, że logikę tę należy ekstrapolować na ukraińskie realia, zwłaszcza że w poprzednich latach próby takiej ingerencji w Ukrainie już istniały. Ponadto w Ukrainie Rosja wykorzystuje praktycznie cały arsenał swoich działań wywrotowych[27] aby sprawdzić ich skuteczność i rozpowszechnić to narzędzie wpływu na późniejsze cele regionalne i globalne.

Potwierdzeniem tej tezy są informacje z otwartych źródeł o ujawnieniu i zablokowaniu sieci agitatorów internetowych zaangażowanych przez rosyjskie

---

[електронний ресурс], https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[25] Ibid.

[26] Russian Meddling in Elections and Referenda in the Alliance..., p.10.

[27] Rasmussen Anders Fogh and Chertoff Michael, West still isn't prepared to stop Russia meddling into elections, POLITICO, [електронний ресурс], https://www.politico.com/magazine/story/2018/06/05/russia-election-meddling-prepared-218594

służby specjalne w celu przygotowania się do ingerencji w wybory prezydenta Ukrainy w 2019 roku. W szczególności zaangażowanie mieszkańców miast Dnipro, Kryvy Rih i Nikopol, którzy są administratorami grup w sieciach społecznościowych, dla przygotowania trampoliny do manipulacji opinią publiczną. Klienci postawili zadanie znaleźć blogerów i aktywnych użytkowników sieci społecznościowych, które miały publikować wiadomości polityczne wysyłane z Rosji w celu uzyskania nagród pieniężnych. Kolejnym zadaniem było przyciągnięcie „fałszerzy" do rejestrowania stron internetowych w ukraińskim segmencie nazw domen oraz wyszukiwanie i zamawianie usług przez obywateli Ukrainy w celu promowania zasobów internetowych i treści w firmach informatycznych zlokalizowanych w południowo-wschodnich regionach Ukrainy. Zgodnie z planami rosyjskich służb specjalnych takie działania musiały ukrywać ich zaangażowanie do upowszechniania fałszywych wiadomości i popularyzacji niektórych prorosyjskich uczestników wyborów.

Rosyjscy kuratorzy zaplanowali zaostrzenie sytuacji społeczno-politycznej w przeddzień i podczas wyborów prezydenckich. W tym celu wykonawcy musieli „przekręcić" wiadomości, aby zdyskredytować władze państwowe i samorząd lokalny oraz stworzyć rzekomo patriotyczny kierunek w sieciach społecznościowych. Na tych stronach zaplanowano publikację materiałów niszczących, w tym wezwania do gwałtownych zmian w porządku konstytucyjnym Ukrainy i naruszenia jej integralności terytorialnej[28].

Na początku lutego 2019 roku Służba Bezpieczeństwa Ukrainy ujawniła mieszkańca obwodu czernihowskiego, który prowadził antyukraińską agitację w sieciach społecznościowych zgodnie z instrukcjami służb specjalnych Federacji Rosyjskiej i przeszukał współpracowników dla rozpowszechniania fałszywych informacji w celu manipulacji opinią publiczną i wpłynięcia na nastroje wyborcze podczas wyborów prezydenckich[29].

W połowie lutego 2019 roku przerwano działalności „Białej Kominiarki", obywatela Ukrainy współpracującego z agentami rosyjskimi i przygotowującego

[28] На Дніпропетровщині СБУ викрила підготовку РФ до втручання у майбутні вибори Президента України (відео), 30.08.2018, [електронний ресурс], https://ssu.gov.ua/ua/news/1/category/1/view/5159#.zrUem400.dpbs

[29] На Чернігівщині СБУ викрила організатора мережі антиукраїнських інтернет-агітаторів, 7.02.2019, [електронний ресурс], https://ssu.gov.ua/ua/news/1/category/21/view/5681#.avZZwvs6.dpbs

zakłócenia procesu wyborczego zaraz po zakończeniu pierwszej tury wyborów prezydenckich w obwodzie Czerniowieckim.

W pierwszym etapie, w celu podniesienia „stopnia" aktywności protestacyjnej w społeczeństwie, organizatorzy sfilmowali i opublikowali w sieci Internet wideo z wezwaniem do obalenia porządku konstytucyjnego w Ukrainie i siłowego przejęcia władzy. Zadaniem „Białej Kominiarki" było także zaangażowanie przywódców stowarzyszeń publicznych i oddzielnych działaczy z różnych regionów Ukrainy w proces nieuznawania wyborów przez „lud", zwołanie „Wiece", nałożenie wymogów na władzę której nie można spełnić. W wyniku zaplanowane zajęć budynki administracyjne władz państwowych, w tym Rady Najwyższej Ukrainy i przelać krew. Dla fizycznego zachwytu i pozbawienia uprawnień przywódców organów państwowych i ścigania zaplanowano wykorzystać „na ciemno" działaczy struktur patriotycznych. Plan przewidywał zorganizowanie pokojowego wiecu w celu sprowokowania starć z organami ścigania, którzy „z tyłu" powinni atakować „grupy bojowe".

Datą przejścia do aktywnych działań wybrany 31 marca 2019 roku – dzień wyborów prezydenckich w Ukrainie. Natychmiast po zamknięciu lokali wyborczych, zgodnie z hasłami „fałszowania" wyników wyrazu woli obywateli, planowano zwołać wiece w Kijowie i regionach, a także sprowokować ofiary ludzkie dla radykalizacji i mobilizacji społeczeństwa[30].

Innym udokumentowanym faktem były próby uzyskania przez rosyjskie służby wywiadowcze danych o sieciach komunikacyjnych zapewniających wybory Prezydenta Ukrainy. W tym celu mieszkaniec Dniepra stworzył i zarządzał grupą w rosyjskiej sieci społecznej zakazanej w Ukrainie rozpowszechniającej fałszywe wiadomości i inne destrukcyjne materiały, w tym publiczne apele o zmianę granic terytorium i granicy państwowej Ukrainy.

Internetowy prowokator, jako pracownik wykonawcy w branży telekomunikacyjnej, przeprowadzał korespondencję elektroniczną z mieszkańcem Rosji. Obywatel rosyjski interesował się gromadzeniem danych o sieciach strategicznie ważnych operatorów telekomunikacyjnych, lokalizacji węzłów telekomunikacyjnych i okresach czasu niezbędnych do ich przywrócenia po uszkodzeniu.

---

[30] "Біла балаклава". СБУ розкрила новий план Росії щодо зриву виборів в Україні, 19 лютого 2019, Тиждень.ua, [електронний ресурс], https://tyzhden.ua/News/226813

Według rosyjskich służb specjalnych, masowe uszkodzenia linii kablowych i urządzeń niektórych operatorów telekomunikacyjnych zakłócą stabilne funkcjonowanie jednostek Państwowego Rejestru Wyborców, jak również zablokują pracę poszczególnych jednostek Jednolitego Systemu Informacyjnego i Analitycznego „Wybory" [31].

Przedstawione przykłady pokazują znaczącą „nieobojętność" Rosji na przebieg ukraińskich wyborów i wysokie stawki dokonywane na nich z zewnątrz. Biorąc pod uwagę fakt iż przeciwko Ukrainie nadal trwa hybrydowa wojna i rosyjska agresja zbrojna, ingerencja Rosji w wybory ukraińskie w celu przynajmniej zniekształcenia ich wyników, a idealnie – doprowadzenia do władzy prorosyjskich polityków – jest w pełni zgodna z jej interesami strategicznymi.

Te same przykłady dają nadzieję, że państwo ukraińskie odpowiednio ocenia takie zagrożenia i podejmuje wysiłki, aby je zapobiegać i neutralizować. W szczególności Centralna Komisja Wyborcza utworzyła specjalną grupę roboczą z udziałem SBU i Specjalnej Służby Komunikacyjnej, w celu szczegółowej analizy technicznej i audytu systemów CKW, ich uruchamiania i całodobowego zapewnienia bezpieczeństwa Centralnego Systemu Wyborczego.[32]. W rezultacie udało się zneutralizować rosyjskie ataki DDoS na CKW, dokonane w dniach 24-25 lutego 2019 roku. W związku z tymi atakami cybernetycznymi Rada Bezpieczeństwa Narodowego i Obrony wraz z Służbą Bezpieczeństwa i policją opracowały mechanizmy cyberobrony CKW wraz z partnerami ze Stanów Zjednoczonych [33]. Jednocześnie dużą rolę w neutralizowaniu destrukcyjnych wpływów na społeczeństwo ukraińskie odgrywają politycy i społeczeństwo obywatelskie jako całość.

Badanie działań wywrotowych i ukierunkowanych ataków informacyjnych na społeczeństwo amerykańskie i szereg krajów w UE dowodzi, że nawet dojrzałe demokracje nie są jeszcze w stanie oprzeć się trwającej ingerencji w

---

[31] СБУ викрила наміри спецслужб РФ блокувати роботу систем, задіяних для забезпечення проведення виборів (відео), 26.02.2019, [електронний ресурс], https://ssu.gov.ua/ua/news/1/category/2/view/5775#.HqDw7Cn8.dpbs

[32] ЦВК та СБУ створять спеціальну групу - представник спецслужби, 12.02.2019, [електронний ресурс], https://dt.ua/UKRAINE/cvk-ta-sbu-stvorvat-specialnu-grupu-predstavnik-specsluzhbi-302478_.html

[33] Порошенко розповів про кібератаки на ЦВК з російської сторони, 26.02.2019, [електронний ресурс], https://dt.ua/POLITICS/poroshenko-rozpoviv-pro-kiberataki-na-cvk-z-rosiyskoyi-storoni-303983_.html

stabilność ich demokratycznego rozwoju. Ukraina, w obliczu przedłużających się operacji wojskowych i zagrożeń dla państwowości, pilnie potrzebuje zarówno wewnętrznej konsolidacji politycznej, jak i uwagi oraz pełnego poparcia sojuszników i partnerów, ponieważ chodzi o wspólne niebezpieczeństwa i istotną potrzebę wspólnych reakcji na rzeczywiste wyzwania i zagrożenia naszych czasów.

Bibliografia

1. "Біла балаклава". СБУ розкрила новий план Росії щодо зриву виборів в Україні, 19 лютого 2019, Тиждень.ua, [електронний ресурс], https://tyzhden.ua/News/226813
2. Выступление и дискуссия на Мюнхенской конференции по вопросам политики безопасности. 10 февраля 2007 года, [електронний ресурс], http://kremlin.ru/events/president/transcripts/24034
3. Мельничук Ігор, Інтеграційні проекти Російської Федерації на пострадянському просторі. – Чернівці: Рута, 2015. – 400 с.
4. На Дніпропетровщині СБУ викрила підготовку РФ до втручання у майбутні вибори Президента України (відео), 30.08.2018, [електронний ресурс], https://ssu.gov.ua/ua/news/1/category/1/view/5159#.zrUem400.dpbs
5. На Чернігівщині СБУ викрила організатора мережі антиукраїнських інтернет-агітаторів, 7.02.2019, [електронний ресурс], https://ssu.gov.ua/ua/news/1/category/21/view/5681#.avZZwvs6.dpbs
6. Порошенко розповів про кібератаки на ЦВК з російської сторони, 26.02.2019, [електронний ресурс], https://dt.ua/POLITICS/poroshenko-rozpoviv-pro-kiberataki-na-cvk-z-rosiyskoyi-storoni-303983_.html
7. СБУ викрила наміри спецслужб РФ блокувати роботу систем, задіяних для забезпечення проведення виборів (відео), 26.02.2019, [електронний ресурс], https://ssu.gov.ua/ua/news/1/category/2/view/5775#.HqDw7Cn8.dpbs
8. Alandete David. Russian Network Used Venezuelan Accounts to Deepen Catalan crisis, El Pais, 11 November 2017, [електронний ресурс], https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html
9. Brattberg Erik, Maurer, Tim. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks, Carnegie Endowment for International Peace, 2018, [електронний ресурс],

https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

10. Charlie Savage. Assange, Avowed Foe of Clinton, Timed Email Release for Democratic Convention. New York Times (JULY 26, 2016). [електронний ресурс] https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html

11. Chivvis Christopher S. Understanding Russian "Hybrid Warfare" and What Can be Done About it, Testimony of Chistopher S. Chivvis. The Rand Corporation. Before the Committee of Armed Services United States House of Representative, p. 1., [електронний ресурс], https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

12. Dave Aitel. Guest editorial: The DNC hack and dump is what cyberwar looks like. Ars Technica (Jun 17, 2016), [електронний ресурс], https://arstechnica.com/information-technology/2016/06/guest-editorial-the-dnc-hack-and-dump-is-what-cyberwar-looks-like/

13. Galante, Laura & Ee Shaun, Defining Russian Election Interference: an Analysis of Select 2-14 to 2018 Cyber Enabled Incidents. Atlantic Council, Scowcroft Center for Strategy and Security, September 2018, p. 7.

14. GRIZZLY STEPPE – Russian Malicious Cyber Activity. December 29, 2016. Reference Number: JAR-16-20296A, [електронний ресурс], https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

15. How France successfully countered Russian interference during the presidential election, EURACTIV, [електронний ресурс], https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/

16. Jensen, Michael. "RUSSIAN TROLLS AND FAKE NEWS: INFORMATION OR IDENTITY LOGICS?" Journal of International Affairs, vol. 71, no. 1.5, 2018, pp. 115–124, JSTOR, [електронний ресурс], www.jstor.org/stable/26508125

17. Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. Release Date: October 7, 2016, [електронний ресурс], https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

18. Obama expels 35 Russian diplomapts in retaliation for US election hacking, [електронний ресурс], https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack

19. Rasmussen Anders Fogh and Chertoff Michael, West still isn't prepared to stop Russia meddling into elections, POLITICO, [електронний ресурс], https://www.politico.com/magazine/story/2018/06/05/russia-election-meddling-prepared-218594

20. Russian Meddling in Elections and Referenda in the Alliance. General Report by Susan DAVIS (United States) General Rapporteur - 181 STC 18 E fin. 11 November 2018, [електронний ресурс], https://www.nato-pa.int/sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSIAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf

21. Stelzenmuller Constantine, The impact of Russian Interference on Germany's 2017 Elections, Testimony before U.S. Senate Select Committee on Intelligence, Wednesday, June 28, 2017, [електронний ресурс], https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections

22. Świątkowska, Joanna. Działania prowadzone w cyberprzestrzeni jako metoda ingerencji w demokratyczny proces wyborczy // Walka informacyjna : uwarunkowania, incydenty, wyzwania / pod redakcją naukową Hanny Batorowskiej. - Kraków : Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją, 2017. - S. 254-263., [електронний ресурс], http://hdl.handle.net/11716/2031

23. Tomz Michael & Weeks Jessika L.P. Public Opinion and Foreign Electoral Intervention, p. 24–26., [електронний ресурс], https://web.stanford.edu/~tomz/working/TomzWeeks-ElectoralIntervention-2018-08-24.pdf

24. Van De Velde. J. The Law of Cyber Interference in Elections. Available at SSRN 3043828 (2017), p.10., [електронний ресурс], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828