DOI:10.59800/bn/196691

Paweł Pelc[1]
Akademickie Centrum Polityki Cyberbezpieczeństwa, Akademia Sztuki Wojennej, Polska

CYBERPRZESTRZEŃ JAKO ELEMENT WALKI INFORMACYJNEJ – DOŚWIADCZENIA Z KONFLIKTU W UKRAINIE

CYBERSPACE AS AN ELEMENT OF INFORMATION WARFARE – EXPERIENCE FROM THE CONFLICT IN UKRAINE

Abstrakt: Rosyjska agresja na Ukrainę od 2014 r. przechodziła różne fazy. Istotnym elementem działań Federacji Rosyjskiej zarówno w fazach konfliktu hybrydowego, jak i konfliktu kinetycznego była wojna informacyjna prowadzona w stosunku do ludności ukraińskiej oraz mieszkańców państw trzecich, niezaangażowanych bezpośrednio w konflikt. W tych działaniach wykorzystywane są nowe technologie, takie jak sztuczna inteligencja i deepfake czy sieci społecznościowe, ale też bardziej tradycyjne ataki przy użyciu narzędzi hakerskich, służących uzyskaniu dostępu do sieci i poszczególnych komputerów.

Słowa kluczowe: wojna informacyjna, cyberprzestrzeń, dezinformacja, media społecznościowe, deepfake

Abstract: Russian aggression against Ukraine has gone through various phases since 2014. However, in both the hybrid conflict and kinetic conflict phases, an important element of the Russian Federation's actions has been information warfare conducted against both the Ukrainian population and residents of third party countries not directly involved in the conflict. These operations use both new technologies, such as artificial intelligence and deepfake or social networks, but also more traditional

[1] 0000-0002-5007-568X, pawel.pelc@gmail.com

attacks using various types of hacking tools designed to gain access to networks and individual computers.

Keywords: information warfare, cyberspace, disinformation, social media, deepfake

Wstęp

Konflikt w Ukrainie rozpoczął się w 2014 r. od rosyjskiej aneksji Krymu, poprzedzonej zajęciem go przez jednostki pozbawione oznaczeń państwowych, a następnie od ataku w Donbasie, przypisywanego pierwotnie przez stronę rosyjską lokalnym separatystom. W wyniku tzw. porozumień mińskich doszło w znacznym stopniu do zamrożenia konfliktu i lokalizacji, jeśli chodzi o działania kinetyczne. Cały czas, nawet po zamrożeniu, strona rosyjska prowadziła jednak działania o charakterze wojny hybrydowej[2]. Ukraina stała się poligonem rosyjskich działań w cyberprzestrzeni[3], wymierzonych m.in. w jej infrastrukturę energetyczną, kolejową czy medialną[4]. Wirus NotPetya, rozprzestrzeniający się w 2017 r. za pomocą oprogramowania do

[2] E. Jakubiak wskazuje, że pojęcie wojny hybrydowej odnosi się do zaprzeczalnych i tajnych działań wspieranych przez groźbę użycia lub użycie sił konwencjonalnych lub nuklearnych, aby wpływać na politykę wewnętrzną krajów będących jej celem. Według niej wojna hybrydowa jest zbiorem działań wojskowych i niewojskowych o niestandardowej skomplikowanej naturze, a jej sprawca jest trudny do precyzyjnego ustalenia i zmienny w swej naturze. Autorka zwraca także uwagę na to, że działania hybrydowe wykorzystują kombinacje konwencjonalnych i niekonwencjonalnych metod. Por.: E. Jakubiak, *Hybrid warfare as a new type of armed conflict in the modern world*, „Studia Bezpieczeństwa Narodowego" 2022, zeszyt 24, s. 72, 79–80.

[3] Legalna definicja cyberprzestrzeni jest zawarta w art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz. U. z 2022 r. poz. 2091) i do tej definicji odwołuje się art. 2 pkt 1 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. Dz. U. z 2024 r., poz. 248). Por. także: K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, nr 2, s. 8–12; C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023, s. 27–31.

[4] K. Geers (red.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallin 2015.

rozliczeń podatkowych, przeniósł się z Ukrainy na inne kraje i wyrządził szkody licznym przedsiębiorcom[5]. Związane z tym atakiem spory prawne, dotyczące w szczególności dochodzenia odszkodowań od zakładów ubezpieczeń, toczyły się przez wiele lat[6]. Wraz z działaniami kinetycznymi i w cyberprzestrzeni Federacja Rosyjska podejmowała w tym czasie także aktywne akcje propagandowe w ramach toczonej przez siebie walki informacyjnej. W pełni odzwierciedla to koncepcję prowadzenia działań wojennych przez Federację Rosyjską – zgodnie z nią wojnę ma charakteryzować stosowanie środków informacyjnych i psychologicznych w celu wsparcia działań kinetycznych[7]. Istotnym jej elementem były argumenty historyczne, dotyczące dziedzictwa Rusi Kijowskiej, a także kwestionujące odrębność narodu ukraińskiego i związki Krymu z Ukrainą[8].

Działania informacyjne oraz w cyberprzestrzeni nasiliły się jeszcze na początku 2022 r. – hakerzy Federacji Rosyjskiej zaatakowali nie tylko serwery rządowe, lecz także banki. Elementem wojny informacyjnej stały się setki fałszywych powiadomień o zagrożeniach bombowych, a także fałszywe SMS-y ostrzegające przed rzekomymi awariami bankomatów. Towarzyszyło to koncentracji wojsk rosyjskich wokół granic Ukrainy. Według strony ukraińskiej te działania miały na celu wywołać panikę wśród ludności, doprowadzić do ewentualnego niezadowolenia i potencjalnie prowokowania protestów, co w rezultacie osłabiło ukraińską hrywnę. Aby osłabić nacisk

[5] Merck, FedEx (za pośrednictwem TNT Experss), Saint-Gobain, Maersk, Mondelez, Reckitt, a w Polsce m.in. także Raben i InterCars.

[6] Zob.: P. Słowiński, *NotPetya – analiza z perspektywy kryminalistyki i polskiego prawa karnego*, „Problemy Współczesnej Kryminalistyki" 2021, t. 25, s. 117–142, https://journals.indexcopernicus.com/api/file/viewByFileId/1584929 (dostęp: 20 lutego 2024 r.); A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, "Wired", 22 sierpnia 2018 r., https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (dostęp: 20 lutego 2024 r.).

[7] P. Krawczyk, J. Wiśnicki, *Mity i stereotypy narzędziem walki psychologiczno-informacyjnej Rosji w wojnie z Ukrainą*, "Cybersecurity and Law" 2023, nr 2, s. 346–347.

[8] L. Fijałkowska, *Elementy historycznoprawne w antyukraińskiej propagandzie Federacji Rosyjskiej w latach 2013–2022*, „Studia Prawno-Ekonomiczne" 2022, t. CXXIV, s. 9–20, https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjzo4bQn7qEAxXxQvEDHdMsAI0QFnoECA4QAQ&url=https%3A%2F%2Fbibliotekanauki.pl%2Farticles%2F2140612.pdf&usg=AOvVaw0qz0ouSHiplnM8CCZGsnnf&opi=89978449 (dostęp: 20 lutego 2024 r.).

rosyjskiej propagandy, strona ukraińska zakazała działalności trzech kanałów telewizyjnych kojarzonych z Rosją, oskarżając je o szerzenie rosyjskiej propagandy. Wcześniej – w 2014 r. – wyłączono dostęp do rosyjskiej telewizji państwowej na terenie Ukrainy[9].

Celem niniejszego artykułu jest analiza rosyjskich działań w cyberprzestrzeni i w sferze informacyjnej w trakcie kinetycznej fazy konfliktu. Przedmiotem zainteresowań będą także przeciwdziałania podejmowane przez stronę ukraińską, co doprowadzi do wysnucia wniosków płynących dla Polski z tych doświadczeń.

Kinetyczna faza konfliktu

Do obecnej fazy kinetycznej konfliktu doszło 24 lutego 2022 r., kiedy wojska Federacji Rosyjskiej zaatakowały Ukrainę z terytorium Rosji, Białorusi i okupowanego Krymu. Atak miał swoje uzasadnienie także na polu wojny informacyjnej[10]: „prezydent Rosji Władimir Putin wystąpił z orędziem do narodu, podczas którego ogłosił początek wojskowej operacji specjalnej mającej na celu obronę ludności Donbasu przed «ludobójstwem» oraz «demilitaryzację i denazyfikację Ukrainy»[11]". Jako podstawę dla wszczęcia agresji wskazał prośbę republik separatystycznych o pomoc i wolę obrony ludności, która „od ośmiu

[9] Por.: J. Marson, *Russians Have Already Started Hybrid War With Bomb Threats, Cyberattacks, Ukraine Says*, 13 lutego 2022 r., https://www.wsj.com/articles/russians-have-already-started-hybrid-war-with-bomb-threats-cyberattacks-ukraine-says11644748413?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.); J.K. Melchior, *The Cyberspace Front in the Attacks on Ukraine*, "The Wall Street Journal", 19 lutego 2022 r., s. A15.

[10] M. Pietras określa walkę informacyjną jako charakterystyczny przypadek procesu sterowania społecznego, którego celem jest niszczenie oponenta za pomocą informacji w trzech głównych obszarach: cyberprzestrzeni, infosferze (obejmującej także systemy informacyjne niewchodzące w skład sieci) oraz noosferze – obszarze mentalności nie tylko pojedynczego człowieka, lecz także narodów i grup społecznych. Por.: M. Pietras, *Wojna informacyjna jako współczesne narzędzie działań nieregularnych*, "Cybersecurity and Law" 2022, nr 1, s. 24.

[11] *Przemówienie Prezydenta Federacji Rosyjskiej Władimira Putina do współobywateli*, Ambasada Rosji w Polsce, 3 marca 2022 r., https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/przem_wienie_prezydenta_federacji_rosyjskiej_w_adimira_putina_do_wsp_obywateli_moskwa_24_lutego_2022/ (dostęp: 14 sierpnia 2024 r.).

lat jest ofiarą ludobójstwa ze strony kijowskiego reżimu”[12]. Zapowiedział oddanie pod sąd tych, którzy popełnili „krwawe zbrodnie”, również przeciwko obywatelom Rosji[13]. Rosyjskie działania zbrojne przeciwko Ukrainie konsekwentnie nazywane są przez stronę rosyjską „specjalną operacją wojskową” albo nawet „misją pokojową”[14], która ma na celu rozbrojenie Ukrainy oraz zaprowadzenie porządku w kraju[15].

Uderzenie wojsk Federacji Rosyjskiej zostało poprzedzone atakiem hakerskim na sieć satelitarną VIASAT, z której korzystały też wojska ukraińskie[16]. W późniejszym okresie, już po rosyjskim ataku kinetycznym na terytorium Ukrainy, rosyjscy hakerzy wybierali także na cel innych dostawców Internetu[17] (w tym satelitarną sieć Starlink[18], przy czym do części ataków na infrastrukturę dostawców Internetu wykorzystano najprawdopodobniej udoskonaloną wersję narzędzia użytego wcześniej do ataku na modemy w sieci VIASAT[19]) oraz elementy infrastruktury energetycznej[20] i inne elementy infrastruktury

[12] *ibidem.*

[13] A. Wilk, M. Domańska, *Rosyjski atak na Ukrainę (24 lutego, godz. 9.00)*, Ośrodek Studiów Wschodnich, 24 lutego 2022 r., https://www.osw.waw.pl/pl/publikacje/analizy/2022-02-24/rosyjski-atak-na-ukraine-24-lutego-godz-900 (dostęp: 20 lutego 2024 r.).

[14] M. Zadorożna, *The impact of wartime information strategy on defence capabilities. The case of the Russo-Ukrainian war*, ”Cybersecurity and Law” 2023, nr 2, s. 290–291.

[15] P. Krawczyk, J. Wiśnicki, *Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022*, ”Cybersecurity and Law” 2023, nr 1, s. 199–200.

[16] Zob.: *Case Study. Viasat*, Cyber Peace Institute, czerwiec 2022 r., https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (dostęp: 20 lutego 2024 r.); Ch. Vasquez, E. Groll, *Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault*, CyberScoop, 10 sierpnia 2023 r., https://cyberscoop.com/viasat-ka-sat-hack-black-hat/ (dostęp: 4 marca 2024 r.).

[17] A. Vicens, *Ukraine's largest mobile communications provider down after apparent cyber attack*, CyberScoop, 12 grudnia 2023 r., https://cyberscoop.com/ukraines-largest-mobile-communications-provider-down-after-apparent-cyber-attack/ (dostęp: 4 marca 2024 r.).

[18] S. Fitzgerald, *Report: Moscow's Starlink Takedown Efforts Advancing*, Newsmax, 19 kwietnia 2023 r., https://www.newsmax.com/newsfront/russia-ukraine-starlink/2023/04/19/id/1116709/?ns_mail_uid=0fcc12bc-c2de-46ff-bed0-afe9362fd63d&ns_mail_job=DM462397_04192023&s=acs&dkt_nbr=0105024swcvf (dostęp: 4 marca 2024 r.).

[19] A. Vincens, *Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs*, CyberScoop, 21 marca 2024 r., https://cyberscoop.com/russian-military-intelligence-may-have-deployed-wiper-against-multiple-ukrainian-isps/ (dostęp: 21 marca 2024 r.).

[20] Por.: R. McMillan, D. Volz, *Internet Provider to Ukrainian Military Hit With Major Cyberattack*, “The Wall Street Journal”, 22 marca 2022 r., https://www.wsj.com/articles/

krytycznej[21]. Przynajmniej część z tych ataków była skorelowana z atakami kinetycznymi[22]. Operacje w cyberprzestrzeni – oprócz tych skierowanych przeciwko elementom infrastruktury krytycznej – służyły pozyskiwaniu informacji, w tym danych osobowych[23], a w szczególności dostępu do systemów wykorzystywanych przez armię ukraińską[24]. Kolejnym obszarem rosyjskich działań w cyberprzestrzeni było wprzęgnięcie ich w rosyjską kampanię dezinformacyjną[25], prowadzoną także przed rozpoczęciem w lutym 2022 r. kinetycznej fazy

internet-provider-to-ukrainian-military-hit-with-major-cyberattack-11648504218?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.); F. Bajak, *Ukraine says potent Russian hack against power grid thwarted*, Associated Press News, 13 kwietnia 2022 r., https://apnews.com/article/russia-ukraine-kyiv-technology-business-hacking-0147e33bc1846a3f8039f9c65a1b4b50?user_email=2f13c3ba3bc1824073117048cd530a2587844ce6575de478221117de2a1545ec (dostęp: 23 listopada 2023 r.).

[21] *The cyber war in Ukraine is as crucial as the battle in the trenches*, The Economist, 20 marca 2024 r., https://www.economist.com/europe/2024/03/20/the-cyber-war-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches?utm_content=article-link-4&etear=nl_today_4&utm_campaign=r.the-economist-today&utm_medium=email.internal-newsletter.np&utm_source=salesforce-marketing-cloud&utm_term=3%2F20%2F2024&utm_id=1862034&slug=europe&slug=2024&slug=03&slug=20&slug=the-cyberwar-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches (dostęp: 21 marca 2024 r.).

[22] *Russia seems to be co-ordinating cyber-attacks with its military campaign*, The Economist, https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign?etear=nl_today_7 (dostęp: 4 marca 2024 r.). Do odmiennych wniosków dochodzą autorzy raportu "Center for Strategic and International Studies": G.B. Mueller, B. Jensen, B. Valeriano, R.C. Maness, J.M. Macias, *Cyber Operations during the Risso-Ukrainian War*, lipiec 2023 r., s. 7–8.

[23] Więcej o działaniach podejmowanych przez Federację Rosyjską przed obecną fazą kinetyczną konfliktu: A.E. Levite, *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict*, kwiecień 2023 r., Washington, DC., s. 3–4.

[24] D. Catteler, D. Black, *The Myth of the Missing Cyberwar*, "Foreign Affairs", 6 kwietnia 2022 r., https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar (dostęp: 4 marca 2024 r.).

[25] Zob. więcej na temat traktowania dezinformacji jako aktu agresji oraz prób zdefiniowania pojęcia dezinformacji: K. Chałubińska-Jentkiewicz, *Dezinformacja jako akt agresji w cyberprzestrzeni*, "Cybersecurity and Law" 2021, nr 1, s. 14–19. Por. także: K. Chałubińska-Jentkiewicz, *Disinformation – and what else?*, "Cybersecurity and Law" 2021, nr 2, s. 9–19. Różnice między dezinformacją a propagandą objaśnia M.J. Wachowicz. Por.: M.J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, nr 1–2, s. 239–243. Według jego propozycji dezinformacja to:

• „świadome, umyślne i podstępne wprowadzanie w błąd przeciwnika przez ukrywający rzeczywiste zamierzenia dowolny podmiot państwowy lub pozapaństwowy w przestrzeni fizycznej lub informacyjnej za pomocą odpowiednio zniekształconych (dosłownie bądź kontekstowo) danych, informacji i dokumentów, w celu doprowadzenia dezinformowanego do podjęcia korzystnych dla dezinformatora decyzji (działań lub zaniechań), zmylenia dezinformowanego, odwrócenia jego uwagi, uzyskania efektu zaskoczenia,

konfliktu, w tym z wykorzystaniem mediów społecznościowych[26, 27]. Na terenach okupowanych przez siły rosyjskie podejmowano także działania, które miały na celu fizyczne odcięcie dostępu do ukraińskiej infrastruktury internetowej i zastąpienie go dostępem do infrastruktury kontrolowanej przez Federację Rosyjską. Ponadto w tych miejscach ukraińskie kanały telewizyjne zostały zastąpione prze rosyjskie, stanowiące element rosyjskiej antyukraińskiej propagandy. Połączone działania w środkach masowego przekazu i w cyberprzestrzeni – z wykorzystaniem mediów społecznościowych – przynosiły w wielu przypadkach skutek oczekiwany przez stronę rosyjską i skutecznie szerzyły jej dezinformację i propagandę[28].

Zgodnie z rosyjską doktryną funkcjonowanie w cyberprzestrzeni stanowi element wojny informacyjnej, w pełni wkomponowany

zniekształcenia realnego obrazu rzeczy i świata, jak również w celu ochrony godziwych i niegodziwych interesów dezinformatora;

• nieświadome i nieumyślne wprowadzanie w błąd przełożonych, sojuszników, podwładnych bądź otoczenia, współdziałających w dowolnej strukturze społecznej, przez mylne interpretowanie rozkazów, zarządzeń lub innej informacji taktyczno-operacyjnej, bądź pominięcie istotnych wskazówek (wytycznych) wykonawczych, niekiedy niepodanie we właściwym czasie potrzebnej informacji, używanie wieloznacznych bądź niezrozumiałych pojęć;

• świadome, umyślne i najczęściej podstępne wprowadzanie w błąd przełożonych, sojuszników, podwładnych bądź otoczenia, współdziałających w dowolnej strukturze społecznej oraz w przestrzeni fizycznej lub informacyjnej, przez ukrywający rzeczywiste zamierzenia dowolny podmiot, za pomocą odpowiednio zniekształconych (dosłownie bądź kontekstowo) danych, informacji i dokumentów, w celu doprowadzenia dezinformowanych do podjęcia korzystnych dla dezinformatora (ale niekiedy również dla dezinformowanego) decyzji – działań lub zaniechań: konstruktywnych bądź destruktywnych".

[26] P. Krawczyk, J. Wiśnicki, *Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine*, "Cybersecurity and Law" 2022, nr 2, s. 278–286. Por. także: P. Staniurski, *Trolling, fake news, infotainment. Rola mediów społecznościowych w prowadzeniu wojny informacyjnej na przykładzie działań podejmowanych w tym obszarze przez Federację Rosyjską,* w: D. Boćkowski, E. Dąbrowska-Prokopowska, P. Goryń, K. Gorynia (red.), *Dezinformacja – Inspiracja – Społeczeństwo, Social Cybersecurity*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2022, s. 51–62.

[27] T. Riley, *Russia's information war against Ukraine went stealth after Meta crackdown*, CyberScoop, 23 lutego 2022 r., https://cyberscoop.com/russias-information-war-ukraine-meta/ (dostęp: 4 marca 2024 r.).

[28] C. Gall, O. Chubko, D. Shapoval, *'Our Own Guys Are Shelling Us': How Russian Propaganda Plagues Ukraine*, 19 kwietnia 2023 r., https://www.nytimes.com/2023/04/19/world/europe/ukraine-russia-donbas-ropaganda.html?campaign_id=57&emc=edit_ne_20230419&instance_id=90593&nl=evening-briefing&regi_id=73957933&segment_id=130849&te=1&user_id=72f2a8e8dc7b7d6833244637427d007c (dostęp: 4 marca 2024 r.).

w inne działania propagandowe prowadzone przez Federację Rosyjską. W tym kontekście działaniom w cyberprzestrzeni przypisuje się rolę zakłócenia i przejęcia wrogich kanałów komunikacyjnych i zastąpienia ich własnym przekazem propagandowym[29]. Tego typu aktami były np. próby wykorzystania technologii deepfake[30] ze spreparowanym oświadczeniem ukraińskiego prezydenta Zełenskiego o kapitulacji sił ukraińskich i rozpowszechnienia go za pośrednictwem przejętych wcześniej kanałów komunikacji[31]. Te działania ograniczają się nie tylko do operacji na terenie Ukrainy, lecz także skierowane są do mieszkańców innych państw[32]. W swoich działaniach dezinformacyjnych skierowanych przeciwko Ukrainie i państwom jej sprzyjającym Rosja wykorzystuje także narzędzia oparte o sztuczną inteligencję, m.in. do tworzenia kolejnych deepfake'ów[33].

Z dostępnych danych i analiz wynika, że Federacja Rosyjska wykorzystuje cyberprzestrzeń w powiązaniu z innymi działaniami. Korzysta z niej w ramach ataków na infrastrukturę lub przeciwko

[29] A.E. Levite, *Integrating…*, *op. cit.*, s. 13–14.

[30] K. Basaj wskazuje, że „deepfake jest nową techniką manipulacji pozwalającą zamienić w jednym filmie dwie tożsamości. W szerszej definicji są to treści zsyntetyzowane przez sztuczną inteligencję. Próbki spreparowanych filmów z synchronizacją ust są modyfikowane tak, aby ruchy ust były zgodne z dźwiękiem". Zob.: K. Basaj, *Czym jest deepfake?*, „Biuletyn ACKS" 2021, wydanie specjalne nr 2, s. 3.

[31] Por.: M. Chwistek, *Do sieci trafił deepfake z prezydentem Zełeńskim. W fałszywym wideo „namawiał" do poddania Ukrainy*, Komputer Świat, 17 marca 2022 r., https://www.komputerswiat.pl/aktualnosci/wydarzenia/do-sieci-trafil-deepfake-z-prezydentem-zelenskim-w-falszywym-wideo-namawial-do/n40qel7 (dostęp: 4 marca 2024 r.); S. Gatlan, *Facebook removes deepfake of Ukrainian President Zelensky*, BleepingComputer, 16 marca 2022 r., https://www.bleepingcomputer.com/news/technology/facebook-removes-deepfake-of-ukrainian-president-zelenskyy/?mod=djemCybersecruityPro&tpl=cy (dostęp: 7 marca 2024 r.).

[32] R. McMillan, D. Volz, *Actors Recorded Videos for 'Vladimir.' It Turned Into Russian Propaganda*, "The Wall Street Journal", 1 grudnia 2023 r., https://www.wsj.com/tech/cybersecurity/actors-recorded-videos-for-vladimir-it-turned-into-russian-propaganda-7ff2ce8e (dostęp: 4 marca 2024 r.); M. Pomerleau, *Congress wants DOD to study information operations from Russia-Ukraine war*, DefenseScoop, 8 grudnia 2023 r., https://defensescoop.com/2023/12/08/congress-wants-dod-to-study-information-operations-from-russia-ukraine-war/ (dostęp: 4 marca 2024 r.).

[33] S.J. Freedberg Jr., *Brute force: Russia 'doubled down' on often-crude disinformation in 2023, says report*, Breaking Defense, 29 lutego 2024 r., https://breakingdefense.com/2024/02/brute-force-russia-doubled-down-on-often-crude-disinformation-in-2023-says-report/?utm_medium=email&_hsmi=296653794&_hsenc=p2ANqtz-8PNT86_y7kRH5VFfL_R3WIPbHnxphnUHLZ4WW8fGAuSwxWeW1n5l9btBC6KICBaxSq1HnpX4E1lcXf-L188poArC (dostęp: 6 marca 2024 r.).

operacjom militarnym prowadzonym przez stronę ukraińską, podczas akcji o charakterze szpiegowskim[34], ale także jako uzupełnienie działań dezinformacyjnych[35] zarówno w stosunku do społeczeństwa ukraińskiego, jak i mieszkańców państw trzecich – tych wspierających strony konfliktu oraz tych starających się zachować neutralność[36]. W tych działaniach wykorzystywane są zarówno nowe technologie, takie jak sztuczna inteligencja i deepfake czy sieci społecznościowe, jak i bardziej tradycyjne ataki z wykorzystaniem różnego rodzaju narzędzi hakerskich, służących uzyskaniu dostępu do sieci i poszczególnych komputerów. Jednocześnie propaganda rosyjska stara się wykorzystać dominację lewicowej poprawności politycznej w mediach społecznościowych tzw. głównego nurtu i rozprzestrzeniać swoje stanowisko w nieufnych wobec nich portalach przywiązanych do wolności słowa i tworzonych w opozycji do serwisów związanych z Big Tech[37]. Do szczególnie spektakularnych działań skierowanych m.in. do obiorcy nieufnego w stosunku do tzw. głównego nurtu można zaliczyć wywiad udzielony przez prezydenta Putina byłemu popularnemu prezenterowi prawicowej telewizji Fox News[38].

[34] D. Dziwisz, B. Sajduk, *Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej"*, w: A. Gruszczak (red.), *The War must go on. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*, 24 lutego 2023 r., s. 43–52.

[35] *The fight against pro-Kremlin disinformation*, The European Council, 20 stycznia 2023 r., https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro-kremlin-disinformation/ (dostęp: 6 marca 2024 r.).

[36] *Undermining Ukraine: How Russia widened its global information war in 2023*, Digital Forensic Research Lab, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/ (dostęp: 6 marca 2024 r.).

[37] Por.: K. Collier, *Blacklisted Russian propagandists thrive on right-wing apps Gab and Truth Social*, NBC News, 13 grudnia 2022 r., https://www.nbcnews.com/tech/internet/russias-ira-thriving-right-wing-apps-gab-truth-social-study-finds-rcna61449 (dostęp: 6 marca 2024 r.); S. Smalley, *Russian disinformation rampant on far-right social media platforms*, CyberScoop, 13 grudnia 2023 r., https://cyberscoop.com/russia-disinformation-gab-parler/ (dostęp: 6 marca 2024 r.).

[38] *Interview to Tucker Carlson*, Official Internet Resources of the President of Russia, 9 lutego 2024 r., http://en.kremlin.ru/events/president/news/73411 (dostęp: 6 marca 2024 r.). Por. także: T. Stanovaya, *Why Putin's Interview With Tucker Carlson Didn't Go to Plan*, 12 lutego 2024 r., https://carnegieendowment.org/politika/91614 (dostęp: 6 marca 2024 r.); D. Wroe, *Tucker Carlson, Vladimir Putin and the pernicious myth of the free market of ideas*, ASPI Strategist, 28 lutego 2024 r., https://www.aspistrategist.org.au/

Efekty synergii działań dezinformacyjnych z wykorzystaniem mediów społecznościowych i tradycyjnych były wykorzystywane przez Federację Rosyjską już przed wybuchem obecnej fazy kinetycznej agresji przeciwko Ukrainie[39]. Po jej wybuchu rządy państw zachodnich podjęły próbę ograniczenia wpływu rosyjskiej propagandy na swoje społeczeństwa, np. poprzez blokowanie dostępu do ich kanałów dezinformacyjnych. Sprowokowało to zarzuty o wprowadzanie cenzury i zamach na wolność słowa, jednak nie zahamowało działań rosyjskich z wykorzystaniem mediów społecznościowych lub w krajach trzecich, które nie ograniczyły dostępu do rosyjskich kanałów propagandowo-informacyjnych.

Gdy państwa zachodnie dążyły do osłabienia skuteczności rosyjskich działań propagandowych, podjęły jeszcze przed wybuchem obecnej kinetycznej fazy konfliktu bezprecedensowe decyzje o szybkim odtajnieniu informacji o rosyjskich cyberoperacjach przeciwko Ukrainie[40], a także wsparły działania ukraińskie w sferze cyberbezpieczeństwa.

Podsumowanie

Wojna w Ukrainie, która rozpoczęła się w 2014 r. od działań hybrydowych (w związku z zajęciem Krymu przez tzw. „zielone ludziki"), przeszła przez ograniczoną fazę kinetyczną (działania w Donbasie), ponowne działania o charakterze hybrydowym, by od 24 lutego 2022 r. wejść jeszcze raz w intensywną fazę kinetyczną. Elementem działań rosyjskich we wszystkich fazach tej wojny jest aktywnie prowadzona wojna informacyjna, w tym z wykorzystaniem

tucker-carlson-vladimir-putin-and-the-pernicious-myth-of-the-free-market-of-ideas/ (dostęp: 6 marca 2024 r.).

[39] *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*, United States Department of State Global Engagement Center, sierpień 2020 r., https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf (dostęp: 6 marca 2024 r.).

[40] Ch. Vasquez, *Ukraine information sharing a model for countering China, top cyber official says*, CyberScoop, 12 czerwca 2023 r., https://cyberscoop.com/information-sharing-china-threat/ (dostęp: 7 marca 2024 r.).

cyberprzestrzeni[41], trwająca zarówno w fazie działań hybrydowych, jak i działań kinetycznych (bez względu na ich skalę). Istotne elementy narracji rosyjskiej to w szczególności kwestionowanie odrębności narodu ukraińskiego, w tym także jego odrębności religijnej (stąd wspieranie działań patriarchatu moskiewskiego przez Federację Rosyjską i jej propagandę[42]), kwestionowanie samodzielności władz ukraińskich, oskarżanie ich o nazistowski charakter, a także o walkę z własnym społeczeństwem. Federacja Rosyjska wykorzystuje też mechanizmy „demokratyczne", takie jak referenda czy wybory, aby w ten sposób legitymizować aneksję części terytoriów ukraińskich.

Celem działań w sferze informacyjnej jest budowanie obrazu zgodnego z narracją promowaną przez Federację Rosyjską oraz dążenie do dezintegracji zarówno społeczeństwa ukraińskiego, jak i wsparcia innych społeczeństw i państw dla Ukrainy[43]. Elementem tych operacji dezinformacyjnych (m.in. z wykorzystaniem fake newsów[44]) jest kompromitacja wizerunku Ukraińców, dezawuacja, a także dyskredytacja i delegitymizacja Ukrainy oraz kwestionowanie jej samodzielności i podkreślanie zależności od państw Zachodu,

[41] G. Wilde, *Why Cyber Attacks on Ukrainians Aren't Working the Way Russia Expected*, Carnegie Endowment for International Peace, 11 marca 2024 r., https://carnegieendowment.org/2024/03/11/why-cyber-attacks-on-ukrainians-aren-t-working-way-russia-expected-pub-91931?utm_source=ctw&utm_medium=email&utm_campaign=buttonlink&mkt_tok=ODEzLVhZVS00MjIAAAGR3g8_OEaIEaMgnTOIVwcnOaymL8UiszkrN_U8H66y-4zHZauBTuMIraa7isTbjZ3jY_35LsDa1e76YwBRcjyaYvUSv5_3PaU2tuVGjqR6rAg (dostęp: 15 marca 2024 r.).

[42] Por.: N. Dubtsova, *From pulpit to propaganda machine: tracing the Russian Orthodox Church's role in Putin's war*, Reuters Institute, 6 lutego 2024 r., https://reutersinstitute.politics.ox.ac.uk/pulpit-propaganda-machine-tracing-russian-orthodox-churchs-role-putins-war (dostęp: 15 marca 2024 r.); J.K. Melchior, *Is Religious Liberty 'Under Attack' in Ukraine?*, "The Wall Street Journal", 2 marca 2024 r., https://www.wsj.com/articles/is-religious-liberty-under-attack-in-ukraine-russia-war-82b1f198 (dostęp: 23 marca 2024 r.).

[43] Por. *Ukraina 2022, Część I. 10 miesięcy rosyjskiej propagandy. Luty – Grudzień 2022*, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Ośrodek Studiów Przestrzeni Postsowieckiej; *Percepcja rosyjskiej agresji na Ukrainę w wybranych krajach*, kwiecień 2022 r., Ośrodek Studiów Przestrzeni Postsowieckiej; *Metody, narzędzia i kanały rosyjskiej walki informacyjnej w Europie, krajach postsowieckich i Turcji*, sierpień 2022 r., Ośrodek Studiów Przestrzeni Postsowieckiej; D. Gąsiewski, M. Bućka, *Wojna informacyjna Rosji z Ukrainą*, „Biuletyn" 2022, nr 2, Akademickie Centrum Komunikacji Strategicznej.

[44] K. Bąkowicz wskazuje, że fake news „oznacza wiadomość medialną, która jednocześnie nie jest ani prawdą, ani kłamstwem, opiera się na dezinformacji, często zawierając fragmenty prawdziwe". Zob.: K. Bąkowicz, *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, „Studia Medioznawcze" 2019, nr 3, s. 281.

w szczególności USA i innych krajów NATO[45]. Cyberprzestrzeń służy do pozyskiwania i udostępniania z wykorzystaniem narzędzi hakerskich wykradzionych prywatnych informacji, falsyfikowania pochodzenia danych informacji, m.in. dzięki fabrykowaniu portali informacyjnych, fałszowaniu źródeł (z wykorzystaniem technologii deepfake), a także do przejmowania witryn internetowych w celu wykorzystania ich jako źródeł działań dezinformacyjnych[46]. Tym samym cyberprzestrzeń staje się elementem tzw. wojny hybrydowej lub działań nieregularnych, wykracza bowiem poza sferę konfliktu kinetycznego i nie ogranicza się wyłącznie do terytorium Ukrainy i jej mieszkańców[47]. Strona ukraińska konsekwentnie próbuje temu przeciwdziałać m.in. przy wykorzystaniu stworzonych przez siebie odpowiednich struktur organizacyjnych[48].

Z przebiegu tego konfliktu można wyciągnąć szereg wniosków dotyczących zarówno operacji w cyberprzestrzeni, jak i działań w ramach wojny informacyjnej. Rosyjskie próby korzystania z technologii deepfake wskazują na istotną potrzebę budowania mechanizmów pozwalających na ich wykrywanie i odpowiednie oznaczanie oraz oddzielanie ich od informacji. Ukraińskie działania informacyjne z wykorzystaniem memów[49], które zapadają łatwo w pamięć, wskazują, jak prosty przekaz może być wykorzystany do podnoszenia morale własnego społeczeństwa oraz propagowania swojego stanowiska także w innych krajach. Działania informacyjno-propagandowe wykroczyły znacząco poza sferę środków masowej komunikacji i w dużym stopniu przeniosły się do mediów społecznościowych

[45] Ł. Małecki, *Fake news jako front wojny w Ukrainie*, „Studia Ukrainica Posnaniensia" 2023, nr 2, s. 57–70.

[46] S.L. Myers, *Spate of Mock News Sites With Russian Ties Pop Up in U.S.*, "The New York Times", 7 marca 2024 r., https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html?te=1&nl=the-evening&emc=edit_ne_20240307 (dostęp: 14 marca 2024 r.).

[47] Por.: K. Chałubińska-Jentkiewicz, *Dezinformacja …*, *op. cit.*, s. 9–24; M. Pietras, *Wojna informacyjna…*, *op. cit.*, s. 21–41.

[48] M. Zadorożna, *The impact…*, *op. cit.*, s. 290–292.

[49] Mem według definicji słownikowej to „chwytliwa porcja informacji rozpowszechniana w Internecie w formie krótkiego filmu, obrazka lub zdjęcia opatrzonego jakimś tekstem". Zob.: *mem*, w: S. Dubisz, *Wielki Słownik Języka Polskiego PWN*, Warszawa 2018, s. 840.

i cyberprzestrzeni. Często widać było także koordynację działań w środkach masowej komunikacji i cyberprzestrzeni w celu wprowadzania określonych treści do szerszego obiegu. Jednocześnie próby blokowania kanałów szerzących propagandę Federacji Rosyjskiej skutkowały zarzutami o cenzurę i propagowanie tych treści przez obrońców wolności słowa.

Istotnym elementem rosyjskiej propagandy jest oskarżanie strony ukraińskiej o nazizm oraz antysemityzm i to w kontekście żydowskich korzeni prezydenta Ukrainy. W przypadku ataku na Polskę Federacja Rosyjska najprawdopodobniej także chętnie skorzysta z podobnej narracji jako narzędzia do łamania woli oporu społeczeństwa i uzupełni ją zarzutami np. o rasizm (Polacy przyjmowali Ukraińców, a odmawiają przyjmowania osób z innych regionów świata dostarczanych na granicę przez służby białoruskie od 2021 r.), prześladowanie mniejszości narodowych lub religijnych, brak zdolności państwotwórczych, rusofobię, antyniemieckość, antyunijność i niepraworządność. Polska powinna być w pełni przygotowana do przeciwdziałania tego typu argumentom m.in. za pomocą efektywnych mechanizmów weryfikacji informacji, pojawiających się w sieciach społecznościowych i w przekazie medialnym, niekojarzących się jednak z lewicową cenzurą konserwatywnego przekazu.

Działania w cyberprzestrzeni i przestrzeni mediów społecznościowych oraz mass mediów będą traktowane przez Federację Rosyjską jako wsparcie i uzupełnienie działań kinetycznych. Podczas przygotowań do takiej ewentualnej agresji poza rozbudową obronnego potencjału kinetycznego niezbędne jest powiązane z nią budowanie zdolności do działań w cyberprzestrzeni (w tym do obrony elementów infrastruktury krytycznej przed potencjalnymi cyberatakami). Biorąc pod uwagę doświadczenia ukraińskie, ważnymi krokami są zapewnienie szerokiej koordynacji przygotowań militarnych i cywilnych oraz współpraca administracji publicznej i innych podmiotów z Wojskami Obrony Cyberprzestrzeni. Ich uprawnienia do prowadzenia aktywnych działań powinny być zapewnione również w momencie, w którym nie występują działania o charakterze kinetycznym, a zatem poza okresem klasycznego konfliktu zbrojnego.

Doświadczenie ukraińskie pokazuje także istotną wagę współpracy sojuszniczej w sferze cyberprzestrzeni, publikowania informacji wywiadowczych o planowanych działaniach rosyjskich w sferze cyberataków lub wojny informacyjnej czy szybkiej atrybucji rosyjskich cyberataków, tak by usunąć charakterystyczny dla działań hybrydowych element zaprzeczalności.

Jednocześnie należy być przygotowanym na rosyjskie operacje hybrydowe skierowane przeciw państwom i społeczeństwom niebędącym bezpośrednio przedmiotem działań kinetycznych i być w stanie im zapobiegać. Działania Federacji Rosyjskiej zarówno w fazie kinetycznej konfliktu, jak i ją poprzedzające powinny zatem interesować zagrożone państwa. Należy mieć świadomość, że już obecnie Polska jest przedmiotem działań hybrydowych skierowanych przeciwko niej (np. kryzys migracyjny na granicy z Białorusią, cyberataki na elementy infrastruktury krytycznej czy działania dezinformacyjne). Ułatwia to budowę mechanizmów zwiększających odporność na działania hybrydowe, dlatego obecny czas powinien zostać w tym celu jak najlepiej wykorzystany.

Konflikt w Ukrainie ma charakter przewlekły i obecnie nie widać scenariusza wróżącego jego szybkie zakończenie. Wszystko wskazuje na to, że w najbliższej przyszłości działania kinetyczne będą nadal uzupełniane działaniami o charakterze hybrydowym – także z wykorzystaniem cyberprzestrzeni, mediów społecznościowych i środków masowego przekazu w celu osłabienia pomocy Ukrainie przez państwa zachodnie, wsparcia Rosji ze strony państw spoza europejskiego kręgu kulturowego, a także dezintegracji społeczeństwa ukraińskiego i osłabiania jego woli oporu.

Bibliografia
References List

Bajak F., *Ukraine says potent Russian hack against power grid thwarted*, Associated Press News, 13 kwietnia 2022 r., https://apnews.com/article/russia-ukraine-kyiv-technology-business-hacking-0147e33bc1846a3f8039f9c65a1b4b50?user_email=2f13c3ba3bc1824073117048cd530a2587844ce6575de478221117de2a1545ec (dostęp: 23 listopada 2023 r.).

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023.

Basaj K., *Czym jest deepfake?*, „Biuletyn ACKS" 2021, wydanie specjalne nr 2.

Bąkowicz K., *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, „Studia Medioznawcze" 2019, nr 3.

Case Study. Viasat, Cyber Peace Institute, czerwiec 2022 r., https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (dostęp: 20 lutego 2024 r.).

Catteler D., Black D., *The Myth of the Missing Cyberwar,* "Foreign Affairs", 6 kwietnia 2022 r., https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberw (dostęp: 31 lipca 2024 r.).

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, nr 2.

Chałubińska-Jentkiewicz K., *Dezinformacja jako akt agresji w cyberprzestrzeni*, "Cybersecurity and Law" 2021, nr 1.

Chałubińska-Jentkiewicz K., *Disinformation – and what else?*, "Cybersecurity and Law" 2021, nr 2.

Chwistek M., *Do sieci trafił deepfake z prezydentem Zełeńskim. W fałszywym wideo „namawiał" do poddania Ukrainy*, Komputer Świat, 17 marca 2022 r., https://www.komputerswiat.pl/aktualnosci/wydarzenia/do-sieci-trafil-deepfake-z-prezydentem-zelenskim-w-falszywym-wideo-namawial-do/n40qel7 (dostęp: 4 marca 2024 r.).

Collier K., *Blacklisted Russian propagandists thrive on right-wing apps Gab and Truth Social*, NBC News, 13 grudnia 2022 r., https://www.nbcnews.com/tech/internet/russias-ira-thriving-right-wing-apps-gab-truth-social-study-finds-rcna61449 (dostęp: 6 marca 2024 r.).

Case Study. Viasat, Cyber Peace Institute, czerwiec 2022 r., https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (dostęp: 20 lutego 2024 r.).

Dubtsova N., *From pulpit to propaganda machine: tracing the Russian Orthodox Church's role in Putin's war*, Reuters Institute, 6 lutego 2024 r., https://reutersinstitute.politics.ox.ac.uk/pulpit-propaganda-machine-tracing-russian-orthodox-churchs-role-putins-war (dostęp: 15 marca 2024 r.).

Dziwisz D., Sajduk B., *Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej"*, w: A. Gruszczak (red.), *The War must go on. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*, 24 lutego 2023 r.

Fijałkowska L., *Elementy historycznoprawne w antyukraińskiej propagandzie Federacji Rosyjskiej w latach 2013–2022*, „Studia Prawno-Ekonomiczne" 2022, t. CXXIV, https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjzo4bQn7qEAxXxQvEDHdMsAI0QFnoECA4QAQ&url=https%3A%2F%2Fbibliotekanauki.pl%2Farticles%2F2140612.pdf&usg=AOvVaw0qz0ouSHiplnM8CCZGsnnf&opi=89978449 (dostęp: 20 lutego 2024 r.).

Fitzgerald S., *Report: Moscow's Starlink Takedown Efforts Advancing*, Newsmax, 19 kwietnia 2023 r., https://www.newsmax.com/newsfront/russia-ukraine-starlink/2023/04/19/id/1116709/?ns_mail_uid=0fcc12bc-c2de-46ff-bed0-afe9362fd63d&ns_mail_job=DM462397_04192023&s=acs&dkt_nbr=0105024swcvf (dostęp: 4 marca 2024 r.).

Freedberg Jr. S.J., *Brute force: Russia 'doubled down' on often-crude disinformation in 2023, says report*, Breaking Defense, 29 lutego 2024 r., https://breakingdefense.com/2024/02/brute-force-russia-doubled-down-on-often-crude-disinformation-in-2023-says-report/?utm_medium=email&_hsmi=296653794&_hsenc=p2ANqtz-8PNT86_y7kRH5VFfL_R3WIPbHnxphnUHLZ4WW8fGAuSwxWeW1n5l9btBC6KICBaxSq1HnpX4E1lcXf-L188poArC (dostęp: 6 marca 2024 r.).

Gall C., Chubko O., Shapoval D., *'Our Own Guys Are Shelling Us': How Russian Propaganda Plagues Ukraine*, "The New York Times", 19 kwietnia 2023 r., https://www.nytimes.com/2023/04/19/world/europe/ukrai

ne-russia-donbas-ropaganda.html?campaign_id=57&emc=edit_ne_20230419&instance_id=90593&nl=evening-briefing&regi_id=73957933&segment_id=130849&te=1&user_id=72f2a8e8dc7b7d6833244637427d007c (dostęp: 4 marca 2024 r.).

Gatlan S., *Facebook removes deepfake of Ukrainian President Zelensky*, BleepingComputer, 16 marca 2022 r., https://www.bleepingcomputer.com/news/technology/facebook-removes-deepfake-of-ukrainian-president-zelenskyy/?mod=djemCybersecruityPro&tpl=cy (dostęp: 7 marca 2024 r.).

Gąsiewski D., Bućka M., *Wojna informacyjna Rosji z Ukrainą*, „Biuletyn" 2022, nr 2, Akademickie Centrum Komunikacji Strategicznej.

GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem, United States Department of State Global Engagement Center, sierpień 2020 r., https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf (dostęp: 6 marca 2024 r.).

Geers K. (red.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallin 2015.

Greenberg T.A., *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, "Wired", 22 sierpnia 2018 r., https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (dostęp: 20 lutego 2024 r.)

Interview to Tucker Carlson, Official Internet Resources of the President of Russia, 9 lutego 2024 r., http://en.kremlin.ru/events/president/news/73411 (dostęp: 6 marca 2024 r.).

Jakubiak E., *Hybrid warfare as a new type of armed conflict in the modern world*, „Studia Bezpieczeństwa Narodowego" 2022, zeszyt 24.

Krawczyk P., Wiśnicki J., *Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine*, "Cybersecurity and Law" 2022, nr 2.

Krawczyk P., Wiśnicki J., *Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022*, "Cybersecurity and Law" 2023, nr 1.

Krawczyk P., Wiśnicki J., *Mity i stereotypy narzędziem walki psychologiczno-informacyjnej Rosji w wojnie z Ukrainą*, "Cybersecurity and Law" 2023, nr 2.

Levite A.E., *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict,* kwiecień 2023 r., Washington, DC.

Małecki Ł., *Fake news jako front wojny w Ukrainie*, „Studia Ukrainica Posnaniensia" 2023, nr 2.

Marson J., *Russians Have Already Started Hybrid War With Bomb Threats, Cyberattacks, Ukraine Says,* "The Wall Street Journal", 13 lutego 2022 r., https://www.wsj.com/articles/russians-have-already-started-hybrid-war-with-bomb-threats-cyberattacks-ukraine-says-11644748413?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.).

McMillan R., Volz D., *Internet Provider to Ukrainian Military Hit With Major Cyberattack*, "The Wall Street Journal", 22 marca 2022 r., https://www.wsj.com/articles/internet-provider-to-ukrainian-military-hit-with-major-cyberattack-11648504218?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.).

McMillan R., Volz D., *Actors Recorded Videos for 'Vladimir.' It Turned Into Russian Propaganda,* "The Wall Street Journal", 1 grudnia 2023 r., https://www.wsj.com/tech/cybersecurity/actors-recorded-videos-for-vladimir-it-turned-into-russian-propaganda-7ff2ce8e (dostęp: 4 marca 2024 r.).

Melchior J.K., *Is Religious Liberty 'Under Attack' in Ukraine?*, "The Wall Street Journal", 22 marca 2024 r., https://www.wsj.com/articles/is-religious-liberty-under-attack-in-ukraine-russia-war-82b1f198 (dostęp: 23 marca 2024 r.).

Melchior J.K., *The Cyberspace Front in the Attacks on Ukraine,* "The Wall Street Journal", 19 lutego 2022 r.

Mem, w: Dubisz S., *Wielki Słownik Języka Polskiego PWN*, Warszawa 2018.

Metody, narzędzia i kanały rosyjskiej walki informacyjnej w Europie, krajach postsowieckich i Turcji, Ośrodek Studiów Przestrzeni Postsowieckiej, sierpień 2022 r.

Mueller G.B., Jensen B., Valeriano B., Maness R.C., Macias J.M., *Cyber Operations during the Risso-Ukrainian War,* lipiec 2023 r.

Myers S.L., *Spate of Mock News Sites With Russian Ties Pop Up in U.S.*, "The New York Times", 7 marca 2024 r., https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html?te=1&nl=the-evening&emc=edit_ne_20240307 (dostęp: 14 marca 2024 r.).

Percepcja rosyjskiej agresji na Ukrainę w wybranych krajach, Ośrodek Studiów Przestrzeni Postsowieckiej, kwiecień 2022 r.

Pietras M., *Wojna informacyjna jako współczesne narzędzie działań nieregularnyc*h, "Cybersecurity and Law" 2022, nr 1.

Pomerleau M., *Congress wants DOD to study information operations from Russia-Ukraine war*, DefenseScoop, 8 grudnia 2023 r., https://defensescoop.com/2023/12/08/congress-wants-dod-to-study-information-operations-from-russia-ukraine-war/ (dostęp: 4 marca 2024 r.)

Przemówienie Prezydenta Federacji Rosyjskiej Władimira Putina do współobywateli, Ambasada Rosji w Polsce, 3 marca 2022 r., https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/przem_wienie_prezydenta_federacji_rosyjskiej_w_adimira_putina_do_wsp_obywateli_moskwa_24_lutego_2022/ (dostęp: 14 sierpnia 2024 r.).

Riley T., *Russia's information war against Ukraine went stealth after Meta crackdown*, CyberScoop, 23 lutego 2022 r., https://cyberscoop.com/russias-information-war-ukraine-meta/ (dostęp: 4 marca 2024 r.).

Russia seems to be co-ordinating cyber-attacks with its military campaign, https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign?etear=nl_today_7 (dostęp: 4 marca 2024 r.).

Słowiński P., *NotPetya – analiza z perspektywy kryminalistyki i polskiego prawa karnego*, „Problemy Współczesnej Kryminalistyki" 2021, t. 25, https://journals.indexcopernicus.com/api/file/viewByFileId/1584929 (dostęp: 20 lutego 2024 r.).

Smalley S., *Russian disinformation rampant on far-right social media platforms*, CyberScoop, 13 grudnia 2023 r., https://cyberscoop.com/russia-disinformation-gab-parler/ (dostęp: 6 marca 2024 r.).

Staniurski P., *Trolling, fake news, infotainment. Rola mediów społecznościowych w prowadzeniu wojny informacyjnej na przykładzie działań podejmowanych w tym obszarze przez Federację Rosyjską*, w: Boćkowski D., Dąbrowska-Prokopowska E., Goryń P., Gorynia K. (red.), *Dezinformacja – Inspiracja – Społeczeństwo, Social Cybersecurity*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2022.

Stanovaya T., *Why Putin's Interview With Tucker Carlson Didn't Go to Plan*, 12 lutego 2024 r., https://carnegieendowment.org/politika/91614 (dostęp: 6 marca 2024 r.).

The cyber war in Ukraine is as crucial as the battle in the trenches, The Economist, 20 marca 2024 r., https://www.economist.com/europe/2024/03/20/the-cyber-war-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches?utm_content=article-link-4&etear=nl_today_4&utm_campaign=r.the-economist-today&utm_medium=email.internal-newsletter.np&utm_source=salesforce-marketing-cloud&utm_term=3%2F20%2F2024&utm_id=1862034&slug=europe&slug=2024&slug=03&slug=20&slug=the-cyber war-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches (dostęp: 21 marca 2024 r.).

The fight against pro-Kremlin disinformation, The European Council, 20 stycznia 2023 r., https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro-kremlin-disinformation/ (dostęp: 6 marca 2024 r.).

Ukraina 2022, Część I. 10 miesięcy rosyjskiej propagandy. Luty – Grudzień 2022, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Ośrodek Studiów Przestrzeni Postsowieckiej.

Undermining Ukraine: How Russia widened its global information war in 2023, Digital Forensic Research Lab, 29 lutego 2024 r., https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/ (dostęp: 6 marca 2024 r.).

Vasquez Ch., *Ukraine information sharing a model for countering China, top cyber official says*, CyberScoop, 12 czerwca 2023 r., https://cyberscoop.com/information-sharing-china-threat/ (dostęp: 7 marca 2024 r.).

Vasquez Ch., Groll E., *Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault*, CyberScoop, 10 sierpnia 2023 r., https://cyberscoop.com/viasat-ka-sat-hack-black-hat/ (dostęp: 4 marca 2024 r.).

Vicens A., *Ukraine's largest mobile communications provider down after apparent cyber attack*, CyberScoop, 12 grudnia 2023 r., https://cyberscoop.com/ukraines-largest-mobile-communications-provider-down-after-apparent-cyber-attack/ (dostęp: 4 marca 2024 r.).

Vincens A., *Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs,* CyberScoop, 21 marca 2024 r., https://cyberscoop.com/russian-military-intelligence-may-have-deployed-wiper-against-multiple-ukrainian-isps/ (dostęp: 21 marca 2024 r.).

Wachowicz M.J., *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, nr 1–2.

Wilde G., *Why Cyber Attacks on Ukrainians Aren't Working the Way Russia Expected*, Carnegie Endowment for International Peace, 11 marca 2024 r., https://carnegieendowment.org/2024/03/11/why-cyber-attacks-on-ukrainians-aren-t-working-way-russia-expected-pub-91931?utm_source=ctw&utm_medium=email&utm_campaign=buttonlink&mkt_tok=ODEzLVhZVS00MjIAAAGR3g8_OEaIEaMgnTOIVwcnOaymL8UiszkrN_U8H66y4zHZauBTuMIraa7isTbjZ3jY_35LsDa1e76YwBRcjyaYvUSv5_3PaU2tuVGjqR6rAg (dostęp: 15 marca 2024 r.).

Wilk A., Domańska M., *Rosyjski atak na Ukrainę (24 lutego, godz. 9.00)*, Ośrodek Studiów Wschodnich, 24 lutego 2022 r., https://www.osw.waw.pl/pl/publikacje/analizy/2022-02-24/rosyjski-atak-na-ukraine-24-lutego-godz-900 (dostęp: 20 lutego 2024 r.).

Wroe D., *Tucker Carlson, Vladimir Putin and the pernicious myth of the free market of ideas,* ASPI Strategist, 28 lutego 2024 r., https://www.aspistrategist.org.au/tucker-carlson-vladimir-putin-and-the-pernicious-myth-of-the-free-market-of-ideas/ (dostęp: 6 marca 2024 r.).

Zadorożna M., *The impact of wartime information strategy on defence capabilities. The case of the Russo-Ukrainian war*, "Cybersecurity and Law" 2023, nr 2.